Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

BfDI

24. Tätigkeitsbericht

Tätigkeitsbericht zum Datenschutz für die Jahre 2011 und 2012

24. Tätigkeitsbericht

Tätigkeitsbericht 2011-2012

24. Tätigkeitsbericht

Dieser Bericht wurde am 24. April 2013 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 2011 und 2012 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – 24. Tätigkeitsbericht –

Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 24. April 2013 gemäß § 26 Absatz 1 des Bundesdatenschutzgesetzes.

Seite

Seite

Seite

Seite

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

Einführung

Die Berichtsperiode war geprägt von der längst überfälligen Diskussion über die Fortentwicklung des Datenschutzes. Die wichtigsten Impulse dafür setzte die Europäische Kommission mit ihren Gesetzesvorschlägen für einen europaweiten und modernen Datenschutz.

Leider wurde die überfällige Modernisierung des Datenschutzrechts in der deutschen Politik – entgegen wiederholter Ankündigungen der Bundesregierung – nicht angegangen. Bedauerlich ist es insbesondere, dass auch die Bemühungen um einen verbesserten Beschäftigtendatenschutz, über die ich schon vor zwei Jahren berichtet hatte, nicht vorangekommen sind. Zugleich sehen wir, dass die Bemühungen einzelner Datenschutzaufsichtsbehörden, global agierende Internetkonzerne zur Einhaltung der Datenschutzbestimmungen zu verpflichten, schnell an Grenzen stoßen. Dieses nationale Vakuum kann nur von europäischer Ebene befüllt werden.

Auch wenn die von der Europäischen Kommission vorgelegten Vorschläge verbesserungs- und diskussionsbedürftig sind, handelt es sich dabei um ein sehr ambitioniertes und wichtiges Vorhaben. Personenbezogene Daten können angesichts der Globalisierung von Datenströmen nur effektiv geschützt werden, wenn die Rechtsvorschriften mindestens europaweit harmonisiert, die grenzüberschreitende Koordinierung der Datenschutzaufsicht verbessert und wirksamere Sanktionsmöglichkeiten bei Verstößen gewährleistet werden.

Seit Inkrafttreten des Vertrags von Lissabon ist der Datenschutz ein europäisches Grundrecht. Deshalb ist es auch konsequent, dass das EU-Datenschutz-Paket nicht nur die Wirtschaft, sondern auch den öffentlichen Sektor umfasst. Neben einer Datenschutz-„Grundverordnung“ soll der Datenschutz bei Polizei- und Justizbehörden durch eine eigene Richtlinie garantiert werden. Bei deren Umsetzung in deutsches Recht müssen die vom Bundesverfassungsgericht formulierten Anforderungen weiterhin gewährleistet bleiben.

Das Datenschutz-Grundrecht kann aber nicht allein durch rechtliche Regelungen garantiert werden. In weitaus stärkerem Maße als bisher bedarf es technischer Gestaltungsanforderungen, also privacy by design und privacy by default, und verfahrensmäßiger Sicherungen, etwa Datenschutzfolgeabschätzungen und Gütesiegel. Hier ist die Wirtschaft in der Pflicht. Dies gilt umso mehr, als die Verknüpfung und Auswertung personenbezogener Daten, Stichwort Big Data, große wirtschaftliche Chancen eröffnen wird.

In die europäische Datenschutzdiskussion greifen auch mächtige wirtschaftliche Interessenvertretungen und Regierungsvertreter aus Drittstaaten ein. Vielfach werden dabei dramatische wirtschaftliche Nachteile beschworen, falls das europäische Datenschutzniveau wie geplant angehoben wird. Ich kann diese Argumente kaum nachvollziehen. Dies gilt insbesondere für die vor allem von Vertretern der Wirtschaft erhobene Forderung, das Datenschutzrecht dadurch zu „entschlacken“, dass man die angeblich unsensiblen Daten ganz ausklammert. Wie das Bundesverfassungsgericht schon vor vielen Jahren festgestellt hat, gibt es im Zeitalter der automatisierten Datenverarbeitung keine ihrer Natur nach unsensiblen personenbezogenen Daten. Diese Feststellung ist nach wie vor richtig. Ich habe mich deshalb darüber gefreut, dass der 69. Deutsche Juristentag 2012 Forderungen zur Verwässerung des Datenschutzes eine Absage erteilt hat.

Der Datenschutz war seit eh und je eine Reaktion auf Herausforderungen der Technik. Informationstechnik in Einklang mit gesellschaftlichen Werten zu gestalten, ist nach wie vor das Ziel des Datenschutzes. Ich sehe keinen Grund, warum unsere Gesellschaft im Internetzeitalter davon abrücken und sich vermeintlichen technischen oder wirtschaftlichen Sachzwängen bedingungslos ausliefern sollte.

Die Jahre 2011/2012 lassen sich auch mit beeindruckenden Zahlen beschreiben: 9 729 Bürgerinnen und Bürger haben sich in diesem Zeitraum an mich gewandt. Meine 85 Mitarbeiterinnen und Mitarbeiter haben 106 Kontrollen durchgeführt. Dabei musste ich insgesamt 15 Beanstandungen aussprechen.

Auch in dieser Berichtsperiode hat der Einsatz für den Datenschutz eine breite Unterstützung erfahren, für die ich mich bedanken möchte. Mein besonderer Dank gilt den Abgeordneten des Deutschen Bundestages aller Fraktionen und anderen Vertreterinnen und Vertretern öffentlicher und privater Stellen, die sich für den Datenschutz eingesetzt haben. Mein Dank richtet sich auch an die Bürgerinnen und Bürger, die auf Missstände hingewiesen und so zu einer schrittweisen Verbesserung der Datenschutzpraxis beigetragen haben. Ganz herzlich möchte ich schließlich meinen Mitarbeiterinnen und Mitarbeitern danken, die mit ihrer engagierten Arbeit einen wesentlichen Beitrag zur Stärkung des Datenschutzes geleistet haben.

Peter Schaar

1 Zusammenfassung aller Empfehlungen

Ich empfehle der Bundesregierung, bei der Europäischen Ermittlungsanordnung (EEA) ein hohes grundrechtliches Schutzniveau zu gewährleisten (vgl. Nr. 2.2.1).

Ich empfehle der Bundesregierung, sich im Rahmen der Beratungen zur EU-Verordnung über elektronische Identifizierung und Vertrauensdienste weiterhin für datenschutzrechtliche Verbesserungen einzusetzen (vgl. Nr. 2.3.4).

Die Vorgaben des EuGH in seinem Urteil zur Unabhängigkeit der österreichischen Datenschutzkommission müssen auch für den BfDI umgesetzt werden (vgl. Nr. 3.1).

Der Einsatz der Videoüberwachungstechnik in der Bundesverwaltung ist datenschutzkonform auszugestalten (vgl. Nr. 3.3.1).

Die Konzeption der Stiftung Datenschutz sollte so überarbeitet werden, dass sie ihre Aufgaben effektiv und wirklich unabhängig wahrnehmen kann (vgl. Nr. 3.6).

Ich empfehle der Bundesregierung, bei der Suche nach Optimierungsmöglichkeiten im sozialversicherungsrechtlichen Datenaustausch frühzeitig die datenschutzrechtlichen Aspekte der einzelnen Prozesse zu berücksichtigen (vgl. Nr. 4.2.1).

Aufgrund der Entscheidung des Bundesgerichtshofs (BGH) zu den Voraussetzungen des Auskunftsanspruchs nach § 101 Urheberrechtsgesetz (UrhG) werden künftig wohl mehr Kundendaten von Internetzugangsanbietern an Rechteinhaber übermittelt werden. Da der Auskunftsanspruch auf gravierende Rechtsverletzungen beschränkt werden sollte, empfehle ich dem Gesetzgeber, die geltende Rechtslage zu überprüfen und sie unter dem Gesichtspunkt der Verhältnismäßigkeit anzupassen (Nr. 5.2).

Bei der Inanspruchnahme von Cloud-Diensten sollten Auftraggeber den Cloud-Dienstleister sorgfältig auswählen, Einzelheiten zu Datenschutz und Datensicherheit genau regeln und die Staaten festlegen, in denen die Daten gespeichert und verarbeitet werden. Insbesondere (sensible) personenbezogene Daten sollten vor dem Einbringen in die Cloud unter alleiniger Kontrolle des Auftraggebers nach dem Stand der Technik verschlüsselt werden (vgl. Nr. 5.3).

Ich empfehle der Bundesregierung, Eingriffsbefugnisse der Sicherheitsbehörden in regelmäßigen Abständen auf ihre Effektivität, Notwendigkeit und Verhältnismäßigkeit zu überprüfen (vgl. Nr. 7.1).

Ich empfehle dem Gesetzgeber, den Sicherheitsbehörden nur auf der Grundlage einer umfassenden Evaluation neue Befugnisse einzuräumen und hierbei den „Leitfaden zur Durchführung von ex-post-Gesetzesevaluationen unter besonderer Berücksichtigung der datenschutzrechtlichen Folgen“ zu berücksichtigen (vgl. Nr. 7.1).

Ich empfehle dem Gesetzgeber, das Antiterrordateigesetz (ATDG) grundlegend zu evaluieren, die festgestellten Mängel und Defizite zu beheben (vgl. Nr. 7.2) und hieraus Schlussfolgerungen für das Rechtsextremismusdateigesetz (REDG) zu ziehen (vgl. Nr. 7.3).

Ich empfehle dem Gesetzgeber, im Gesetz zur Bekämpfung des Rechtsextremismus (REDG) Regelungen zum Schutz unbescholtener Personen hinreichend bestimmt und verhältnismäßig auszugestalten (vgl. Nr. 7.3).

Ich empfehle der Bundesregierung, bei standardisierten Leistungsbeschreibungen für die Entwicklung einer Software zur Durchführung von Quellen-Telekommunikationsüberwachungen und anderen eingriffsintensiven Maßnahmen festzulegen, dass die Funktionalität der Software klar zu regeln und sicherzustellen, dass insbesondere der Quellcode den Datenschutzbehörden für Kontrollzwecke bedingungsfrei zur Verfügung steht (vgl. Nr. 7.4.1).

Ich empfehle der Bundesregierung, bei der Entwicklung des Polizeilichen Informations- und Analysebundes (PIAV) zentrale datenschutzrechtliche Vorgaben zu beachten und im INPOL-Verbund die Speicherung sog. personenbezogener Hinweise (PHW) nur auf der Grundlage klarer Kriterien vorzunehmen (vgl. Nr. 7.4.5).

Ich empfehle den Polizeibehörden des Bundes, bei Fahndungsaufrufen im Internet und in sozialen Netzwerken den besonderen Bedingungen dieser Medien Rechnung zu tragen und insbesondere die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder entwickelten Eckpunkte zu beachten (vgl. Nr. 7.4.7).

Ich empfehle der Bundesregierung, die derzeitige AEO-Zertifizierungspraxis einer baldigen und umfassenden Evaluation zu unterziehen (Nr. 7.5.1).

Ich empfehle dem Gesetzgeber, eine im Lichte der NSU-Terrorakte notwendige Reform der Sicherheitsbehörden nur nach einer gründlichen und umfassenden Ermittlung der Ursachen und Fehlentwicklungen durchzuführen und dem Erfordernis einer effizienten Kontrolle der Nachrichtendienste umfassend Rechnung zu tragen (vgl. Nr. 7.7.6).

Ich empfehle dem Gesetzgeber, im Bundesbeamtengesetz eine ausreichende Rechtsgrundlage zu schaffen, damit Forschungsprojekte zur Aufarbeitung des Umgangs mit der NS-Vergangenheit von Mitarbeiterinnen und Mitarbeitern in Bundesministerien auf einer ausreichenden Rechtsgrundlage durchgeführt werden können (vgl. Nr. 8.6).

Ich empfehle dem Gesetzgeber, eine Neuvergabe der Steuer-ID in Fällen besonderer Schutzrisiken (z. B. Zeugenschutz, Adoption, Transsexuelle) zu regeln (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. 16.6; Wiederholung der Empfehlung aus dem 23. TB zu Nr. 9.3).

Die Bundesregierung sollte bei der Festlegung der Datenschutzstandards bei intelligenten Stromnetzen insbesondere in der Datenschutzverordnung nach dem Energiewirtschaftsgesetz einen hohen Datenschutzstandard gewährleisten und die Zweckbindung, Datensparsamkeit und Erforderlichkeit berücksichtigen (vgl. Nr. 10.1).

Der Gesetzgeber sollte der Empfehlung des Petitionsausschusses des Deutschen Bundestages folgen und in § 35 Absatz 2 Satz 2 Nummer 4 BDSG (Speicherung von bonitätsbezogenen Daten) die Frist bereits mit dem Tag der

erstmaligen Speicherung der betreffenden Daten beginnen lassen (vgl. Nr. 10.2).

Ich empfehle den gesetzlichen Krankenkassen, den verstärkten Wettbewerb im Gesundheitswesen nicht zu Lasten des Datenschutzes und der Persönlichkeitsrechte der Versicherten auszutragen (vgl. Nr. 11.1.1).

Ich empfehle den gesetzlichen Krankenkassen, die dem Medizinischen Dienst der Krankenversicherung (MDK) vorbehaltene Datenerhebung zu respektieren und dessen Kompetenzen nicht zu unterlaufen (vgl. Nr. 11.1.6 und 11.1.7).

Ich empfehle dem Gesetzgeber, in § 200 SGB VII den Begriff des Gutachtens in der gesetzlichen Unfallversicherung klarzustellen (vgl. Nr. 11.4.1).

Ich empfehle dem Gesetzgeber, sich in der nächsten Legislaturperiode des Themas Beschäftigtendatenschutz wieder anzunehmen und ein Beschäftigtendatenschutzgesetz zu schaffen, das die Registrierung und Überwachung am Arbeitsplatz wirksam beschränkt (vgl. Nr. 13.1).

Ich empfehle dem Gesetzgeber, ein datenschutzrechtliches Auskunftsrecht des Betroffenen in der Abgabenordnung zu verankern (Nr. 16.7).

2 Europa und Internationales

Auf die Herausforderungen, die sich aus der Globalisierung der Informationsverarbeitung ergeben, kann der Datenschutz immer weniger mit rein nationalen Instrumenten antworten. Dies gilt nicht nur für die Vorhaben zur Modernisierung der europäischen Datenschutzes. Im Folgenden soll auf wesentliche Entwicklungen auf europäischer und internationaler Ebene eingegangen werden.

2.1 Ein großer Wurf aus Brüssel: Die Reform des Europäischen Datenschutzrechts

Die Europäische Kommission hat am 25. Januar 2012 den Anstoß zu einer umfassenden Reform des Europäischen Datenschutzrechts gegeben. Damit hat die Debatte um eine Modernisierung des Datenschutzrechts eine neue – nunmehr gesamteuropäische – Dynamik bekommen.

Das von der Kommission vorgelegte Reformpaket besteht aus drei Teilen:

- Mitteilung der Kommission „Der Schutz der Privatsphäre in einer vernetzten Welt. Ein europäischer Datenschutzrahmen für das 21. Jahrhundert“, KOM(2012) 9 endgültig
- Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (JI-Richtlinie), KOM(2012) 10 endgültig
- Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig

Die Mitteilung der Europäischen Kommission erläutert den Reformbedarf des geltenden europäischen Datenschutzrechts und begründet die grundsätzlichen Schlussfolgerungen, die sie mit den Entwürfen zweier Rechtsakte daraus zieht. Die Datenschutz-Grundverordnung erfasst die Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen sowie durch öffentliche Stellen, soweit es sich nicht um Polizei und Justiz handelt (vgl. Nr. 2.1.1). Die vorgeschlagene JI-Richtlinie soll den Datenschutz im Bereich von Polizei und Justiz regeln (vgl. Nr. 2.1.2).

Das anspruchsvolle Reformvorhaben soll vor allem dazu dienen, das bestehende, im Wesentlichen aus dem Jahre 1995 stammende, europäische Datenschutzrecht fortzuentwickeln und an die Herausforderungen der Datenverarbeitung im 21. Jahrhundert anzupassen. Insgesamt sehe ich die Initiative der Europäischen Kommission sehr positiv, verbindet sie doch den Anspruch der Modernisierung des Datenschutzrechts mit dessen europaweiter Harmonisierung auf einem beachtlichen Niveau.

Seit der Präsentation der Vorschläge durch die Kommission wird darüber im Rahmen des Rechtsetzungsverfahrens im (aus den Regierungen der Mitgliedstaaten gebildeten) Rat der Europäischen Union sowie im Europäischen Parlament intensiv diskutiert. Die zuständige Ratsarbeitsgruppe DAPIX hat zunächst unter dänischer, anschließend unter zyprischer Präsidentschaft in zahlreichen Sitzungen über das Reformpaket beraten. Deutschland ist in der DAPIX federführend durch das Bundesministerium des Innern (BMI) vertreten. Ich hatte die Möglichkeit, auf Fachebene den Beratungen in der DAPIX beizuwohnen. Die Positionen der Bundesregierung werden innerstaatlich vor den Sitzungen der DAPIX zwischen den Ressorts abgestimmt. Auch hierbei wurde ich beteiligt.

In den vergangenen Monaten hat sich gezeigt, dass das BMI eine deutlich kritischere Position zu den Reformvorschlägen einnimmt als ich. So werden in der öffentlichen Debatte, aber auch in den Verhandlungen im Rat die bewährte Systematik und Regelungsstruktur des Datenschutzrechts wie etwa das Verbot mit Erlaubnisvorbehalt oder die Anknüpfung des Datenschutzrechts an den Begriff des personenbezogenen Datums insgesamt in Frage gestellt. Die Diskussion über solche grundsätzlichen Fragen ist notwendig und muss geführt werden. Es erstaunt allerdings, dass diese Themen erst dann in den Diskurs eingebracht wurden, als nach zehnjährigem Stillstand auf nationaler Ebene konkrete Reformvorschläge auf europäischer Ebene vorlagen.

Die Berichterstatter des zuständigen LIBE-Ausschusses im Europäischen Parlament haben ihre ersten Stellungnahmen mit entsprechenden Änderungsvorschlägen im Januar 2013 präsentiert.

Neben dem formellen Rechtssetzungsverfahren auf europäischer Ebene findet eine intensive und umfassende öffentliche Debatte über das Reformpaket statt. Datenschutzbehörden, Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft bringen ihre jeweiligen Vorstellungen und Bewertungen in den Diskurs ein. Offenbar wird allgemein anerkannt, dass das neue europäische Datenschutzrecht die rechtlichen Rahmenbedingungen für die nächsten Jahre festlegen wird. Dass die Datenschutzreform auch Auswirkungen über die Grenzen der EU hinaus haben wird,

belegen die nicht unbeträchtlichen Bemühungen von Unternehmen, Lobbygruppen und Regierungsvertretern insbesondere aus den Vereinigten Staaten von Amerika, den Rechtsetzungsprozess zu beeinflussen.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich intensiv mit dem Reformpaket auseinandergesetzt. Sie hat auf ihrer 83. Konferenz in Potsdam („Ein hohes Datenschutzniveau für ganz Europa!“) und ihrer 84. Konferenz in Frankfurt/Oder („Europäische Datenschutzreform konstruktiv und zügig voranbringen!“) jeweils Entschließungen verabschiedet (vgl. Kasten a und b zu Nr. 2.1). Im Juni 2012 haben die Datenschutzbeauftragten umfassende gemeinsame Stellungnahmen zum Reformpaket abgegeben (vgl. Anlage 5).

Es verwundert nicht, dass die Europäische Datenschutzreform in letzter Zeit das zentrale Thema der europäischen Datenschutzgremien war, insbesondere der Frühjahrskonferenz 2012 der Europäischen Datenschutzbeauftragten und der Artikel-29-Gruppe, in der die Datenschutzbehörden der EU-Mitgliedstaaten zusammenwirken. Letztere hat sich bislang in zwei ausführlichen Stellungnahmen dazu geäußert (WP 191 und 199, abzurufen unter http://ec.europa.eu/justice/data-protection/article-29/index_de.htm, vgl. auch Nr. 2.4.1).

Kasten a zu Nr. 2.1

Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22. März 2012 in Potsdam

Ein hohes Datenschutzniveau für ganz Europa!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union zu modernisieren und zu harmonisieren.

Der Entwurf einer Datenschutz-Grundverordnung enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

- das Prinzip Datenschutz durch Technik,
- der Gedanke datenschutzfreundlicher Voreinstellungen,
- der Grundsatz der Datenübertragbarkeit,
- das Recht auf Vergessen,
- die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen und
- die verschärften Sanktionen bei Datenschutzverstößen.

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst hohes Niveau für alle Mitgliedstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatliche Datenverarbeitungsvorgänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittelbar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutzniveaus den Mitgliedstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv. Die Konferenz bedauert deshalb, dass die Kommission grundsätzlich nur Unternehmen mit mindestens 250 Beschäftigten zur Bestellung von Datenschutzbeauftragten verpflichten will. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Über die bereits in dem Verordnungsentwurf vorgeschlagenen Modernisierungen hinaus hält die Konferenz weitere Schritte für erforderlich, die sie etwa in ihrem Eckpunktepapier für ein modernes Datenschutzrecht vom 18. März 2010 vorgeschlagen hat:

- eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,
- ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis eine Anhebung der Altersgrenze,

- die Förderung des Selbstdatenschutzes,
- pauschalierte Schadensersatzansprüche bei Datenschutzverstößen,
- einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,
- das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und
- die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.

Die Regelungen zur Risikoanalyse, Vorabkontrolle und zur Zertifizierung bedürfen der weiteren Präzisierung in der Verordnung selbst.

Für besonders problematisch hält die Konferenz die vorgesehenen zahlreichen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte, die dringend auf das unbedingt erforderliche Maß zu reduzieren sind. Alle für den Grundrechtsschutz wesentlichen Regelungen müssen in der Verordnung selbst bzw. durch Gesetze der Mitgliedstaaten getroffen werden.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf der Datenschutz-Grundverordnung vorgesehene Kohärenzverfahren, welches die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb vereinfacht und praktikabler gestaltet werden.

Die durch Artikel 8 der EU-Grundrechte-Charta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Europäischen Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter dem deutschen Datenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung). Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

Die Konferenz erklärt, dass sie den Gang des Gesetzgebungsverfahrens konstruktiv und kritisch begleiten wird.

Kasten b zu Nr. 2.1

Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. November 2012 in Frankfurt (Oder)

Europäische Datenschutzreform konstruktiv und zügig voranbringen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies bereits in ihrer Entschließung vom 21./22. März 2012 verdeutlicht. In zwei umfassenden Stellungnahmen vom 11. Juni 2012 haben die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl einzelner Aspekte der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtssetzungsprozess gegeben.

Angesichts der aktuellen Diskussionen in Deutschland und im Rat der Europäischen Union sowie entsprechender Äußerungen aus der Bundesregierung im Rahmen des Reformprozesses betont die Konferenz folgende Punkte:

- Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der Datenschutz-Grundverordnung an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall regeln und die so genannte alltägliche Datenverarbeitung weitgehend ungeregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden.

Jede Verarbeitung scheinbar „belangloser“ Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je. Deshalb lehnt es die Konferenz ab, angeblich „belanglose“ Daten von einer Regelung auszunehmen.

Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.

– Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich beizubehalten und insbesondere für die Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.
– Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.
– Mit Blick auf die Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich im Sinne dieser Positionen im Rat der Europäischen Union für die Belange eines harmonisierten Datenschutzrechts auf einem hohen Niveau einzusetzen.

Die Begleitung der Europäischen Datenschutzreform bedeutet für meine Mitarbeiterinnen und Mitarbeiter eine enorme zusätzliche Herausforderung, die aufgrund ihrer Breite fast alle Referate meines Hauses betrifft. Um eine möglichst effektive und koordinierte Arbeit zu leisten, habe ich eine interne Projektgruppe eingerichtet, der Mitarbeiter verschiedener Referate angehören.

2.1.1 Die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung bildet den Kern der europäischen Datenschutzreform. Sie enthält die zentralen Bausteine zur Modernisierung des Datenschutzrechts. Sie liegt daher bisher im Fokus der Beratungen im Rat der Europäischen Union und auch der öffentlichen Diskussion.

Den mit der Datenschutz-Grundverordnung verfolgten Ansatz der Kommission sehe ich grundsätzlich sehr positiv, denn sie bietet die Chance, die überfällige Modernisierung des im Kern aus den 1980er Jahren stammenden Datenschutzrechts endlich anzugehen. In diesem Zusammenhang sei daran erinnert, dass die im Jahre 2001 erfolgte Umsetzung der Europäischen Datenschutzrichtlinie 95/46/EG von der Bundesregierung nur als Zwischenschritt zu einer umfassenden Modernisierung des Datenschutzrechts verstanden worden ist. Das Bundesministerium des Innern hatte seinerzeit ein Gutachten in Auftrag gegeben, das den Reformbedarf und die notwendigen Schritte beleuchten sollte (vgl. 19. TB Nr. 1.2). Dieses Gutachten (von Roßnagel, Pfitzmann, Garstka – abrufbar unter http://www.datenschutz.bund.de) bot und bietet reichlich Stoff für eine fachliche und wissenschaftliche Diskussion. Datenschutzpolitische Folgen im Sinne gesetzgeberischer Aktivitäten hatte es jedoch kaum. In den vergangenen zehn Jahren wurde das Datenschutzrecht in Deutschland in einigen – zum Teil durchaus bedeutsamen – Details verändert, eine umfassende Modernisierung blieb jedoch aus (zur Modernisierung des Datenschutzrechts vgl. auch 23. TB Nr. 1).

Bei aller Zustimmung zur Initiative der Europäischen Kommission gibt es aber eine Reihe von Punkten, bei denen die Vorschläge noch deutlich nachgebessert werden müssen. Folgende Aspekte der Reform stehen derzeit im Mittelpunkt der Debatte.

Grundsätzliche Regelungsstruktur

Die Datenschutz-Grundverordnung hält an den bewährten Regelungsprinzipien und -strukturen des geltenden Datenschutzrechts fest. Danach dürfen personenbezogene Daten nur dann erhoben, verarbeitet und genutzt werden, wenn es hierfür eine Rechtsgrundlage gibt oder soweit der Betroffene eingewilligt hat. Forderungen aus Politik und Wirtschaft, dieses Prinzip für die „belanglose Datenverarbeitung“ aufzugeben, bin ich stets entgegengetreten. Darin sehe ich mich auch durch den 69. Deutschen Juristentag gestärkt, der entsprechende Forderungen jüngst zurückgewiesen hat (vgl. Beschlüsse des 69. Deutschen Juristentages München 2012, S. 32 ff., abrufbar unter http://www.djt.de/fileadmin/downloads/69/121206_djt_69_beschluesse_web_rz.pdf)

Wollte man in Zukunft nur noch eine besonders risikobehaftete Verarbeitung personenbezogener Daten im Einzelfall regeln und die so genannte alltägliche Datenverarbeitung weitgehend ungeregelt zulassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden. Jede Verarbeitung scheinbar „belangloser“ Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 klargestellt hat. Diese Aussage gilt im Zeitalter des Internets und der allgegenwärtigen Datenverarbeitung mehr denn je.

Auch ich halte es für richtig, die materiellen, organisatorischen und formalen Anforderungen zur Gewährleistung des Datenschutzes am Risiko der Datenverarbeitung für die Rechte der Betroffenen auszurichten. Dies ist im Entwurf der Datenschutz-Grundverordnung an einigen Stellen bereits der Fall, kann aber noch ausgebaut werden.

Beim Anwendungsbereich des Datenschutzrechts und hinsichtlich der grundsätzlichen Anforderungen an eine Verarbeitung personenbezogener Daten und bei den grundlegenden Rechten der Betroffenen sollte es jedoch keine Abstriche geben.

Die 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in ihrer Entschließung „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ deutlich dazu geäußert (vgl. Kasten b zu Nr. 2.1).

Gleiche Datenschutzregeln für Behörden und Unternehmen?

Die Datenschutz-Grundverordnung unterwirft Unternehmen, Vereine, Freiberufler, Gewerbetreibende grundsätzlich den gleichen Datenschutzregeln wie Behörden und andere öffentliche Stellen, soweit es sich nicht um Polizei- oder Strafverfolgungsbehörden handelt.

Dieser Ansatz ist schon in der geltenden Datenschutzrichtlinie 95/46/EG verankert, ebenso wie im Datenschutzrecht der meisten Mitgliedstaaten der EU. In Deutschland bestehen allerdings traditionell getrennte Regelungssysteme für den öffentlichen und den nicht-öffentlichen Bereich. Dies hat vor allem verfassungsrechtliche Gründe: Während sich bei der staatlichen Datenverarbeitung der Bürger als Träger von Grundrechten und der Staat als Grundrechtsverpflichteter gegenüber stehen, geht es beim Datenschutzrecht im Bereich der Wirtschaft um den Ausgleich der Interessen verschiedener Grundrechtsträger.

Diese verfassungsrechtlichen Unterschiede erfordern es allerdings nicht zwingend, unterschiedliche datenschutzrechtliche Regelungsregime zu haben. Die grundlegenden Prinzipien sind für beide Bereiche gleich, auch wenn sie sich verfassungsrechtlich unterschiedlich herleiten lassen. Eine klare Trennung beider Bereiche wird auch immer schwieriger, da sich der Staat in zunehmendem Maße privatrechtlich betätigt oder sich bei der Erfüllung seiner Aufgaben Privater bedient.

Gleichwohl sollten den Mitgliedstaaten Spielräume verbleiben, die Anforderungen der Datenschutz-Grundverordnung durch nationales Recht zu konkretisieren. Es ist u. a. zu gewährleisten, dass sie konkret festlegen können, welche Datenkategorien zur Erfüllung welcher Aufgaben zu welchen Zwecken verarbeitet und an welche andere Stellen sie übermittelt werden dürfen. Derartige Regelungen finden sich in großer Zahl im bereichspezifischen Datenschutzrecht. Wie der Entwurf der Datenschutz-Grundverordnung bereits vorsieht, muss sich die staatliche Datenverarbeitung auf Unions- oder mitgliedstaatliches Recht stützen. Dies ist in der Verordnung noch klarer herauszustellen, um hier Rechtssicherheit für die Mitgliedstaaten zu schaffen. Allerdings muss der neue EU-Rechtsrahmen zum Anlass genommen werden, die im deutschen Recht sehr zahlreichen und insgesamt nicht immer konsistenten bereichsspezifischen Datenschutzbestimmungen zu überprüfen.

Vorschläge, die Datenverarbeitung öffentlicher Stellen vollständig aus der Datenschutz-Grundverordnung herauszulösen und ihre Regelung einer Richtlinie zu überlassen, halte ich für unrealistisch. Aus meiner Sicht können die erforderlichen Spielräume auch innerhalb der Verordnung geschaffen werden, und es ist nicht notwendig, deshalb die gesamte Regelungsstruktur in Frage zu stellen und damit die Reform aufs Spiel zu setzen. Die mit der Verordnung angestrebte Harmonisierung des Datenschutzes auch im öffentlichen Bereich sehe ich insbesondere angesichts des immer intensiveren europaweiten Datenaustauschs zwischen staatlichen Stellen positiv. Dadurch würde das Datenschutzniveau in einigen Mitgliedstaaten deutlich erhöht und damit letztlich auch der Schutz personenbezogener Daten deutscher Bürgerinnen und Bürger verbessert.

Zu viele Befugnisse der Kommission oder wer konkretisiert die Datenschutz-Grundverordnung?

Der Entwurf der Datenschutz-Grundverordnung enthält eine große Zahl von Ermächtigungen für die Europäische Kommission, delegierte Rechtsakte oder Umsetzungsrechtsakte zu erlassen. Diese Möglichkeit ist durch den Vertrag von Lissabon eingeführt worden und soll die Kommission in die Lage versetzen, ähnlich einer Rechtsverordnung nach deutschem Recht konkretisierende Vorschriften zu erlassen. Dabei darf es sich allerdings nicht um wesentliche Fragen handeln. Diese müssen im förmlichen Rechtssetzungsverfahren in den Rechtsakten (Verordnung oder Richtlinie) unmittelbar festgelegt werden.

Mit den Datenschutzbeauftragten der Länder und der Artikel-29-Gruppe bin ich der Auffassung, dass die Kommission hier deutlich über das Ziel hinausgeschossen ist. So sind delegierte Rechtsakte in Fällen vorgesehen, in denen wesentliche Fragen geregelt werden sollen, die in der Verordnung selbst zu verankern wären. In anderen Fällen besteht kein Bedarf für eine europaweit einheitliche Harmonisierung, sodass es auch hier keine Notwendigkeit delegierter Rechtsakte gibt. Vielfach kann die Konkretisierung der Bestimmungen der Datenschutz-Grundverordnung auch den verantwortlichen Stellen selbst, der Praxis der Aufsichtsbehörden oder dem künftig vorgesehenen Europäischen Datenschutzausschuss überlassen werden.

Die Artikel-29-Gruppe hat hierzu eine Einzelbewertung der Delegationsermächtigungen in ihrem Arbeitspapier 199 vorgenommen (vgl. Nr. 2.1).

Das Marktortprinzip: Geltung des Datenschutzrechts auch für außereuropäische Unternehmen

Bisher knüpft die Geltung des europäischen Datenschutzrechts daran an, dass ein Unternehmen entweder seinen Sitz innerhalb der EU hat oder zumindest Mittel zur Datenverarbeitung nutzt, die sich in der EU befinden. Das Internet ermöglicht es aber auch Unternehmen, die in der

EU weder einen Sitz haben noch Mittel der Datenverarbeitung betreiben, Nutzer innerhalb der EU mit ihren Angeboten anzusprechen und deren personenbezogene Daten zu verarbeiten. Für solche Unternehmen, z. B. die Betreiber sozialer Netzwerke oder Suchmaschinen ohne verantwortliche Niederlassung in der EU, gilt bisher kein EU-Datenschutzrecht. Dies beeinträchtigt die Rechte der Betroffenen, erschwert deren Durchsetzung und stellt einen klaren Wettbewerbsnachteil für Unternehmen mit Sitz innerhalb der EU dar.

Deshalb haben nach der Grundverordnung auch Unternehmen mit Sitz außerhalb der EU auch dann das europäische Datenschutzrecht zu beachten, wenn sich ihre Dienstleistungsangebote bzw. Verkaufsaktivitäten an den europäischen Binnenmarkt richten und dabei personenbezogene Daten erhoben werden. Dieser „targeting approach“ wird von den Datenschutzbehörden in der EU begrüßt, da dann für jede an Einwohner innerhalb der EU gerichtete Datenverarbeitung nunmehr die gleichen Rahmenbedingungen gelten, unabhängig vom Sitz des Unternehmens.

Neue Instrumente des Datenschutzes: Recht auf Vergessenwerden und auf Datenübertragbarkeit

Die Risiken der elektronischen Datenverarbeitung erfordern innovative Ansätze. Das Recht auf Vergessen und das Recht auf Datenübertragbarkeit sollen die Datensouveränität der Betroffenen fördern, müssen in ihren Ausprägungen aber noch überdacht werden.

Das Recht auf Vergessenwerden soll den Betroffenen in die Lage versetzen, nicht nur gegen den Urheber öffentlich gemachter Daten vorzugehen. Sie sollen auch von Dritten die Löschung aller Verbindungen zu und Vervielfältigungen von den veröffentlichten Daten verlangen können. Der Urheber der Veröffentlichung ist daher verpflichtet, im Rahmen des Zumutbaren alle Dritten, die die veröffentlichten Daten verarbeiten, über das Löschungsersuchen des Betroffenen zu informieren.

Mit der Information der Dritten hat die Stelle, die die Daten ursprünglich veröffentlicht hat, allerdings ihre Schuldigkeit getan. Sie hat insbesondere nicht dafür Sorge zu tragen, dass Dritte, die die von ihr veröffentlichten Daten nutzen, dem Löschungsbegehren auch tatsächlich Folge leisten. Hier bleibt der Betroffene, wie schon bisher, auf sich alleine gestellt. In Zweifelsfällen wird er daher seine Löschungsrechte nicht rechtlich durchsetzen können. Auch wenn das „Recht auf Vergessenwerden“ in seiner derzeitigen Gestalt die hohen Erwartungen nicht wirklich erfüllt, die sein Name verspricht, weist es im Vergleich zur geltenden Rechtslage immerhin eine Verbesserung auf: Der Betroffene muss sich nicht mit einer Vielzahl ihm unbekannter Dritter auseinandersetzen, sondern kann sich mit seinem umfassenden Löschungsbegehren unmittelbar an den für die Veröffentlichung Verantwortlichen wenden, der dann Zweit- und Drittverwerter der von ihm veröffentlichten Daten informieren muss. Das Recht auf Vergessenwerden umfasst theoretisch auch Publikationen in Papierform, wobei völlig unklar ist, wie ein solches Recht in einer solchen Konstellation auch nur ansatzweise durchsetzbar sein soll. Hier wäre eine Nachjustierung des Vorschlags durchaus wünschenswert (vgl. Kasten a zu Nr. 2.1.1).

Das Recht auf Datenübertragbarkeit eröffnet dem Betroffenen die Möglichkeit, eine Kopie seiner Daten in elektronischer Form zu verlangen und persönliche Informationen von einem auf einen anderen Anbieter zu übertragen. Man denke hier an den Nutzer eines sozialen Netzwerks, der sein Profil auf ein anderes Netzwerk übertragen lassen möchte. Allerdings beschränkt sich dieses Recht nicht auf Web-2.0-Dienste, sondern gilt auch für andere Bereiche, etwa beim electronic banking oder bei Online-Versandhändlern. Da die elektronische Erfassung unseres Alltags zügig voranschreitet, etwa durch die Erfassung des Clickstreams im Internet und Bewegungs-, Surf- oder Kaufprofile, greift das Recht auf Datenübertragbarkeit ein Grundproblem der informationellen Selbstbestimmung auf. Während heute Unternehmen durch umfassende Datenspeicherung mehr über die Interessen und das Verhalten des Einzelnen wissen als die Betroffenen selbst, soll das Recht auf elektronische Herausgabe und Übertragbarkeit den Betroffenen ihre Datensouveränität ein Stück zurückgeben. Daher unterstütze ich diesen Ansatz. Allerdings ist auch hier zu untersuchen, inwieweit die Regelungen in jedem Einzelfall zu sinnvollen Ergebnissen führen. Dabei ist zu berücksichtigen, dass dem Betroffenen nicht nur die von ihm zur Verfügung gestellten Ausgangsdaten, sondern auch Auswertungen der verantwortlichen Stelle zur Verfügung zu stellen sind. Ob dies im Ergebnis immer sachgerecht ist, bedarf eingehender Erörterung (vgl. Kasten b zu Nr. 2.1.1).

Die Begrenzung der Profilbildung

Die Zusammenführung und Verknüpfung personenbezogener Daten zu Profilen gefährdet das Persönlichkeitsrecht in besonderem Maße. Durch Profile kann die Persönlichkeit eines Menschen, insbesondere sein Verhalten, seine Interessen und Gewohnheiten ermittelt, analysiert und prognostiziert werden. Oft erfolgt die Profilbildung ohne Kenntnis des Betroffenen. Dies trägt zu dem unterschwelligen Gefühl bei, permanent analysiert zu werden. Individuelle Datenprofile tragen wesentlich zum „gläsernen Bürger“ bzw. „gläsernen Kunden“ bei. Sie haben inzwischen in viele Lebensbereiche Einzug gehalten, etwa als Konsumentenprofil, Bewegungsprofil, Nutzerprofil oder Sozialprofil. Auch wenn Profile schon in der Offlinewelt gebildet wurden, werden sie erst in der Onlinewelt mit ihrer umfassenden Verfügbarkeit und Verknüpfbarkeit der Daten und der Durchdringung des Alltagslebens mit technischen Geräten zu einer der größten Gefahren für das Recht auf informationelle Selbstbestimmung.

Deshalb sehe ich es positiv, dass der Verordnungsentwurf in Artikel 20 eine eigene Vorschrift zur Profilbildung enthält. Allerdings geht dieser Ansatz nicht weit genug, denn er setzt erst bei der Verwendung bereits entstandener Daten an, für die dann bestimmte Verarbeitungsverbote definiert werden. Eine wirksame Regelung der Profilbildung

darf nicht erst bei der Nutzung, sondern muss bereits bei der Entstehung von Persönlichkeitsprofilen ansetzen. Auch lassen sich die Gefahren der Profilbildung nicht allein durch rechtliche Verbote bewältigen. Vielmehr bedarf es technologischer Ansätze, wie zum Beispiel wirksamen und rücknahmefesten Anonymisierungs- oder Verschlüsselungsmechanismen, die die Gefahren für die Persönlichkeitsrechte begrenzen. Umgekehrt könnte die Profilbildung unter Verwendung von Pseudonymen bei gleichzeitigem Verbot der Herstellung des unmittelbaren Personenbezugs privilegiert werden. Das deutsche Telemediengesetz enthält hier Ansätze, die auch auf eine europäische Regelung übertragen werden könnten.

Stärkung des technologischen Datenschutzes

Die Informationsverarbeitung und mit ihr auch der Datenschutz unterliegen einer ungeheuren technologisch bedingten Veränderungsdynamik. Ich hoffe deshalb, dass die Reform des europäischen Datenschutzrechts zu einer viel stärkeren Verankerung des technologischen Datenschutzes führt.

Der Entwurf der Datenschutz-Grundverordnung enthält in dieser Beziehung zahlreiche positive Ansätze, den technologischen Datenschutz auf europäischer Ebene zu stärken. Im Vergleich zur geltenden Richtlinie nimmt der technologische Datenschutz einen sehr viel breiteren Raum ein. Die Kommission hat offenbar die Notwendigkeit erkannt, in diesem Bereich auch auf der normativen Ebene deutlich mehr zu tun. An einigen Stellen sehe ich jedoch noch Verbesserungsbedarf:

Ein zeitgemäßer und zukunftsfähiger Datenschutz umfasst technisch-organisatorische Maßnahmen, die Datenschutz und Datensicherheit angemessen berücksichtigen. Dies ist eine der zentralen Forderungen aus dem Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus dem Jahre 2010 (vgl. 23. TB Nr. 1.2).

Im Verordnungsentwurf sind verschiedene Grundsätze und Vorgaben enthalten, die den technologischen Datenschutz auf breiter Ebene vorantreiben können. Insbesondere Kapitel IV befasst sich zu einem großen Teil mit diesen Fragen. Dazu gehören unter Anderem

– die Verpflichtung zu „Privacy by Design“, also zur Berücksichtigung von Datenschutzanforderungen bereits bei der Systemkonzeption,

– die Forderung nach „Privacy by Default“, d. h. nach datenschutzgerechten Grundeinstellungen etwa bei sozialen Netzwerken,

– die Verpflichtung zur Einhaltung technisch-organisatorischer Grundsätze der IT-Sicherheit zum Schutz personenbezogener Daten,

– die ebenfalls obligatorische Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung oder

– der wiederholte Hinweis auf die Notwendigkeit zur Durchführung technisch-organisatorischer Maßnahmen.

Leider sind die diversen Aspekte der Datensicherheit und technologischen Anforderungen über eine Vielzahl einzelner Regelungen verstreut, ohne dass die hohe Bedeutung des technologischen Datenschutzes an zentraler Stelle der Verordnung verdeutlicht wird. In einer solchen technischen „Zentralnorm“ sollten die elementaren Datenschutzschutzziele Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit als Zielvorgaben für technisch-organisatorische Maßnahmen in die in der Datenschutz-Grundverordnung verankerten Grundsätze des Datenschutzes aufgenommen werden. Diese Schutzziele sind bereits jetzt als Grundlage für die Durchführung technisch-organisatorischer Maßnahmen sowohl auf europäischer Ebene (vgl. WP 196 der Artikel-29-Gruppe zum Thema „Cloud Computing“, Nr. 5.3) als auch auf nationaler Ebene (vgl. Konferenz der Datenschutzbeauftragten des Bundes und der Länder [Hrsg.], Ein modernes Datenschutzrecht für das 21. Jahrhundert, 2010, Kapitel 3, www.datenschutz.bund.de, 23. TB Anlage 6) anerkannt.

Der Verordnungsentwurf enthält viele begrüßenswerte technikneutrale Gestaltungsansätze. Hierfür nur zwei Beispiele:

Die Grundsätze von „Privacy by Design“ und „Privacy by Default“ in Artikel 23 des Verordnungsentwurfs berücksichtigen bereits die im deutschen Datenschutzrecht bekannten Grundsätze der Datenvermeidung und Datensparsamkeit als Kerngedanken und gestalten diese weiter aus. Damit sollen etwaige Datenschutzprobleme bereits bei der Entwicklung neuer Technologien festgestellt werden, um den Datenschutz von vorneherein in die Gesamtkonzeption einzubeziehen – im Nachhinein können systemimmanente Datenschutzprobleme – wenn überhaupt – vielfach nur mühsam und mit viel Zeit- und Kostenaufwand behoben werden.

Das Instrument der Datenschutz-Folgenabschätzung (Privacy Impact Assessment – PIA) ist ein weiterer Baustein zur Implementierung datenschutzgerechter IT-Prozesse. Nicht erst durch den Artikel 33 des Entwurfs der Datenschutz-Grundverordnung, sondern auch durch die von der Europäischen Kommission vorangetriebene Entwicklung von PIAs für RFID-Systeme (vgl. 23. TB Nr. 5.9, WP 180 der Artikel-29-Gruppe) oder für Smart-Grid-/Smart-Metering-Systeme (vgl. Nr. 10.1) werden Datenschutz-Folgenabschätzungen eine zunehmend wichtigere Rolle einnehmen. Bislang handelt es sich dabei aber ganz überwiegend um freiwillige und unverbindliche Vorgaben. Ich begrüße es daher, dass die Durchführung solcher Folgenabschätzungen nunmehr in bestimmten Fällen verbindlich vorgeschrieben werden soll. Die Ergebnisse einer Datenschutz-Folgenabschätzung sollten nicht nur für Hersteller und Anwender, sondern auch für die Betroffenen transparent sein. Nur so kann nachvollzogen werden, welche Risiken bei welchen Datenverarbeitungsprozessen bestehen. Neben einer Dokumentationspflicht sollten

die Ergebnisse obligatorisch einem regelmäßigen Monitoring unterzogen werden.

Angesichts der zunehmenden Bedeutung der Anonymisierung und Pseudonymisierung als Mittel zur datenschutzfreundlichen Gestaltung von IT-Systemen und IT-Prozessen sowie zum Schutz der Privatsphäre bei der Nutzung von Internetdiensten sollten diese Mechanismen explizit an zentraler Stelle in den Rechtsakten verankert werden.

Europaweiter Mindeststandard im Datenschutz für Beschäftigte

Auch im Beschäftigtendatenschutz verfolgt die Europäische Kommission das Ziel eines hohen gemeinsamen Datenschutzniveaus in der EU. Das ist erfreulich. Ebenso wie in der nationalen Debatte (vgl. Nr. 13.1) findet der Beschäftigtendatenschutz aber auch in der Datenschutz-Grundverordnung nur wenig Platz, sodass weitreichender Verbesserungsbedarf besteht, um den großen Herausforderungen hinreichend Rechnung zu tragen.

So soll insbesondere zwar Artikel 82 der Datenschutz-Grundverordnung den Mitgliedstaaten die Befugnis eröffnen, eigene Regelungen im Bereich des Beschäftigtendatenschutzes zu treffen – daher auch die in diesem Bereich geringe Regelungstiefe des Verordnungsentwurfs – dies allerdings nur „in den Grenzen dieser Verordnung".

Diese Einschränkung wirft einige Fragen auf, denn jede spezifische Regelung des nationalen Rechts stellt für sich genommen eine Abweichung von den Vorgaben der Verordnung dar. Insofern kann die Bezugnahme auf die „Grenzen dieser Verordnung" sinnvoll nur so interpretiert werden, dass das nationale Recht der Terminologie und den Grundsätzen der Verordnung entsprechen muss und insgesamt nicht vom Schutzniveau der Verordnung abweichen darf.

Um tatsächlich einen qualifizierten Mindeststandard zu setzen und somit einen veritablen Mehrwert für den Datenschutz im Beschäftigungsverhältnis zu bringen, sollten die elementaren Anforderungen des Beschäftigtendatenschutzes eine Regelung in der Verordnung selbst erfahren. Hierbei ist angesichts der Bedeutung und Sensibilität der Beschäftigtendaten ein hohes Schutzniveau zu gewährleisten. Allerdings ist nicht zu übersehen, dass eine vollständige europaweite Harmonisierung der spezifischen Anforderungen an den Beschäftigtendatenschutz auf hohem Niveau nur schwer durchsetzbar sein wird. So hat die Europäische Kommission ein vor mehr als zehn Jahren begonnenes Vorhaben zu einem spezifischen Rechtsakt für den Beschäftigtendatenschutz bereits vor längerer Zeit mangels Erfolgsaussichten aufgegeben.

Erforderlich ist daher eine ausdrückliche Klarstellung im Verordnungstext, dass die Verordnung im Bereich Beschäftigtendatenschutz nur einen Mindeststandard setzt, es den Mitgliedstaaten aber unbenommen bleibt, im Interesse des Datenschutzes weitergehende Anforderungen zu normieren, damit es jedenfalls nicht zu einer Absenkung des in den Mitgliedstaaten bereits erreichten Schutzniveaus kommt. Diese Forderung findet sich auch in der Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 zur Datenschutz-Grundverordnung und wurde erneut bekräftigt in der Entschließung der 84. Konferenz am 7./8. November 2012 (vgl. Kasten b zu Nr. 2.1).

Erfreulich ist, dass die Datenschutz-Grundverordnung die Einwilligung als Rechtsgrundlage bei Vorliegen eines wesentlichen Ungleichgewichts zwischen dem Betroffenen und der verantwortlichen Stelle ausschließt. Damit konkretisiert der Verordnungsentwurf die bereits in der RL 95/46/EG und im BDSG enthaltene Anforderung der Freiwilligkeit als Voraussetzung für die Wirksamkeit datenschutzrechtlicher Einwilligungen.

Große praktische Auswirkungen würden sich daraus ergeben, dass eine mitgliedstaatliche Regelung der Verarbeitung personenbezogener Arbeitnehmerdaten nur durch Gesetz vorgesehen ist. Kollektivvereinbarungen (Betriebsvereinbarungen, Dienstvereinbarungen und Tarifverträge) werden dort nicht genannt. Ob man den Verordnungsentwurf dennoch so auslegen kann, dass die Mitgliedstaaten die Ermächtigung auf die Betriebs- und Tarifparteien delegieren dürfen, ist unsicher. Deshalb sollte in der Grundverordnung klargestellt werden, dass auch Kollektivvereinbarungen ausdrücklich als Ermächtigungsgrundlage für die Datenverarbeitung vorgesehen werden, um das mithilfe dieses Regelungsinstruments erreichte Datenschutzniveau für die Beschäftigten abzusichern.

Problematisch ist, dass die Europäische Kommission nach dem Verordnungsentwurf auch für den Beschäftigtendatenschutz ermächtigt werden soll, delegierte Rechtsakte zu erlassen. Der Kommission werden damit ähnliche Kompetenzen wie den Mitgliedstaaten zur Konkretisierung der Verordnung eingeräumt, so dass das Risiko einer unübersichtlichen Rechtslage besteht, wenn nationales Recht und delegierte Rechtsakte widersprüchliche Vorgaben enthalten sollten.

Betriebliche und behördliche Datenschutzbeauftragte – ein Erfolgsmodell des deutschen Datenschutzrechts wird europäisch

Zwiespältig ist die in der Grundverordnung vorgesehene Regelung zum behördlichen Datenschutzbeauftragten. Zu begrüßen ist zwar, dass Artikel 35 des Verordnungsentwurfs die obligatorische Benennung betrieblicher bzw. behördlicher Datenschutzbeauftragter vorsieht. Das ist aus europäischer Sicht ein Fortschritt, denn die geltende Datenschutzrichtlinie sieht die Benennung interner Datenschutzbeauftragter nur als Option für den nationalen Gesetzgeber (als Alternative zu umfassenden Meldepflichten gegenüber den Datenschutzaufsichtsbehörden) vor.

Mit der europaweiten Einführung betrieblicher und behördlicher Datenschutzbeauftragter sollen die bestehenden Meldepflichten für automatisierte Datenverarbeitungen an die Aufsichtsbehörden entfallen. Zu Recht – denn sie haben sich in der Praxis häufig als bürokratischer Aufwand ohne datenschutzrechtlichen Mehrwert erwiesen.

Mit deren Abschaffung macht die Kommission unverkennbar Anleihen bei der deutschen Regelung, nach der Meldepflichten nur in sehr eingeschränktem Umfang bestehen.

Da die neue Verpflichtung aber nur für Unternehmen mit mindestens 250 Mitarbeitern gelten soll, bleibt sie hinter der bewährten deutschen Regelung weit zurück. Danach sind öffentliche Stellen des Bundes generell zur Bestellung eines Datenschutzbeauftragten verpflichtet und für nicht-öffentliche Stellen gilt eine Benennungspflicht ab 20 mit der manuellen bzw. ab 10 mit der automatisierten Datenverarbeitung ständig beschäftigten Personen.

Während die Einführung betrieblicher und behördlicher Datenschutzbeauftragter aus europäischer Sicht also an sich als Fortschritt anzusehen ist, bleiben die vorgeschlagenen Regelungen hinter den Anforderungen zurück. Nur noch ca. 0,3 Prozent der deutschen Unternehmen müssten nach der neuen EU-Regelung einen Datenschutzbeauftragten benennen. Der sachfremde Schwellenwert von 250 Mitarbeitern verstellt zudem den Blick auf risikogeneigte Datenverarbeitungen, bietet Umgehungsmöglichkeiten und könnte in der Konsequenz zu einer weitgehenden Abschaffung des betrieblichen Datenschutzbeauftragten führen.

Der Schwellenwert von 250 Beschäftigten ist nicht nur viel zu hoch angesetzt. Die Mitarbeiterzahl ist auch als Anknüpfungspunkt ungeeignet, weil die Notwendigkeit einer internen Datenschutzkontrolle nicht von der Größe des Unternehmens, sondern vom Umfang der Datenverarbeitung und deren Risikopotential abhängt. Zu Recht haben Unternehmen, deren Datenverarbeitung einer Vorabkontrolle unterliegt oder die, wie etwa Adressmakler oder Wirtschaftsauskunfteien, personenbezogene Daten geschäftsmäßig übermitteln, nach deutschem Recht unabhängig von ihrer Größe einen Datenschutzbeauftragten zu bestellen.

Leider fehlen in der Datenschutz-Grundverordnung auch wichtige Instrumente, die die Unabhängigkeit des Datenschutzbeauftragten absichern. Dazu zählen die Verschwiegenheitspflicht und das Zeugnisverweigerungsrecht des Datenschutzbeauftragten, das Benachteiligungsverbot und vor allem der besondere Kündigungsschutz. Es ist zudem ein Unterschied, ob der Datenschutzbeauftragte der Unternehmensleitung organisatorisch unmittelbar unterstellt ist (so im BDSG) oder ob er, wie vorgeschlagen, lediglich ein unmittelbares Vorspracherecht hat.

Ich werde mich weiterhin dafür einsetzen, dass diese wichtigen Aspekte in die Reform des europäischen Rechtsrahmens einfließen und die Position des Datenschutzbeauftragten europaweit gestärkt wird.

Selbstregulierung als Instrument für besseren Datenschutz

Schon die Europäische Datenschutzrichtlinie von 1995 sieht die Einführung von Selbstregulierungsmechanismen zur Förderung des Datenschutzes vor. Diese Vorgabe wurde 2001 in deutsches Recht umgesetzt. Allerdings führt dieses wichtige Instrument jedenfalls in Deutschland seitdem ein Schattendasein (vgl. dazu Nr. 3.4).

Der Entwurf der Datenschutz-Grundverordnung schreibt die bestehende europarechtliche Vorgabe fort und sieht weiterhin die Möglichkeit der Schaffung von Verhaltensregeln auf nationaler und europäischer Ebene vor.

Die Vorschläge der Kommission sind allerdings recht allgemein gehalten und bedürfen der Präzisierung. Selbstregulierung kann nur dann erfolgreich sein, wenn folgende Voraussetzungen erfüllt sind:

- Verhaltensregeln dürfen die materiellen Vorschriften für bestimmte Sektoren konkretisieren und ergänzen, dürfen diese aber weder ersetzen noch neue Datenverarbeitungsbefugnisse schaffen.
- Es muss klare rechtliche Vorgaben geben, was Gegenstand von Verhaltensregeln sein kann (regulierte Selbstregulierung).
- Das Verfahren zur Anerkennung von Verhaltensregeln muss klar geregelt sein. Sie muss durch unabhängige vertrauenswürdige Instanzen vorgenommen werden.
- Verhaltensregeln müssen durchgesetzt werden können; Rechte der Aufsichtsbehörden dürfen nicht beschnitten werden.
- Verhaltensregeln müssen den Unternehmen Vorteile bieten, sonst werden sie nicht akzeptiert. Hauptvorteil ist eine höhere Rechtssicherheit und eine Bindung der Aufsichtsbehörden an die von ihnen selbst anerkannten Verhaltensregeln.

Einige der Voraussetzungen sind durch die Vorschläge der Kommission bereits erfüllt, bei anderen muss noch nachgebessert werden. Auf Ressortebene werden dazu vielversprechende Vorschläge diskutiert, die in die Verhandlungen im Rat eingebracht werden könnten.

Europäisches Datenschutzrecht muss europaweit einheitlich durchgesetzt werden

Die Globalisierung des Datenschutzes als Folge der zunehmend grenzüberschreitenden Verarbeitung personenbezogener Daten vor allem über das Internet durch Unternehmen aber auch Behörden erfordert ein gemeinsames Vorgehen der Datenschutzbehörden. Die geltende EU-Datenschutzrichtlinie 95/46/EG hat zwar zu einer Harmonisierung zentraler datenschutzrechtlicher Grundsätze innerhalb der EU geführt. Sie hat aber nicht in hinreichendem Maß zu einer einheitlichen Rechtsanwendung in der Praxis der weiterhin national organisierten Datenschutzaufsicht geführt.

Die Europäische Kommission hat diesen Umstand aufgegriffen und schlägt mit dem so genannten „One-Stop-Shop“ (Artikel 51 Absatz 2 des Verordnungsentwurfs) und dem Kohärenzverfahren (Artikel 58 ff. des Verordnungsentwurfs) Mechanismen vor, die zu einer einheitlichen Datenschutzpraxis in der EU in Fällen beitragen sollen, in denen ein Verantwortlicher in mehreren Mitgliedstaaten niedergelassen ist oder in denen Personen in mehreren Mitgliedstaaten von denselben Verarbeitungs-

vorgängen betroffen sind. Eine solche stärkere Harmonisierung der Datenschutzpraxis durch eine intensivere Zusammenarbeit der Aufsichtsbehörden halte ich für erforderlich. Ein Mehrwert könnte dabei von einem Kooperationsverfahren ausgehen, das – anders als es die Europäische Kommission mit dem „One-Stop-Shop“ beabsichtigt – nicht als EU-weite Zuständigkeit einer Datenschutzbehörde, sondern als „Federführung“ verstanden wird in Fällen, die mehrere Mitgliedstaaten betreffen. Zudem muss der mit dem Verordnungsvorschlag neu geschaffene EU-Datenschutzausschuss in strittigen Fällen und in Fällen von grundlegender Bedeutung für den EU-Datenschutz verbindlich zur einer einheitlichen Auslegung und Anwendung des EU-Rechts beitragen können.

Bei aller Notwendigkeit einer stärkeren Harmonisierung der Aufsichtspraxis darf die durch Artikel 8 der EU-Grundrechte-Charta und Artikel 16 des Vertrages über die Arbeitsweise der EU (AEUV) gewährleistete Unabhängigkeit der Datenschutzbehörden nicht aus dem Blick geraten. Mit dieser Unabhängigkeit unvereinbar ist vor allem die in dem Verordnungsentwurf vorgesehene Befugnis der Europäischen Kommission, einzelfallbehördliche Maßnahmen auszusetzen und Durchführungsrechtsakte zur „ordnungsgemäßen Anwendung“ der Verordnung im Hinblick auf Fälle zu erlassen, die im Kohärenzverfahren beraten werden. Die Rechtsanwendung muss schon den Aufsichtsbehörden selbst vorbehalten bleiben, soll der Unabhängigkeitsgrundsatz nicht ad absurdum geführt werden.

Kasten a zu Nr. 2.1.1

Stichwort: Recht auf Vergessenwerden

Jeder kennt die Situation: Man hat vor vielen Jahren personenbezogene Daten im Internet veröffentlicht, mit denen man inzwischen nicht mehr gern in Verbindung gebracht werden will. Oder schlimmer – ein Dritter hat nicht zutreffende Daten im Internet veröffentlicht. Mit Hilfe von Suchmaschinen sind solche Daten auf Dauer recherchierbar. Deshalb kam der verständliche Wunsch auf, es möge einen Rechtsanspruch und die technischen Mittel geben, diese Daten einfach zu beseitigen. Im Kern geht es bei dem Recht auf Vergessenwerden also darum, im Zeitalter des Internets Ansprüche auf Löschung personenbezogener Daten zu gewährleisten. Die radikale Lösung – einen „digitalen Radiergummi“, mit dem flächendeckend im Internet veröffentlichte Daten gelöscht werden könnten – wird es auf absehbare Zeit nicht geben: Daten können beliebig oft vervielfältigt und weltweit weiterverbreitet werden. Deshalb beschränkt sich der Entwurf der Datenschutz-Grundverordnung auch darauf, den schon nach geltendem Recht bestehenden Anspruch auf Löschung personenbezogener Daten maßvoll zu erweitern: Die für die Datenverarbeitung verantwortlichen Stellen sollen sich nach ihren Möglichkeiten auch um die Löschung der personenbezogenen Daten bei denjenigen kümmern, denen sie die Daten übermittelt haben.

Kasten b zu Nr. 2.1.1

Stichwort: Recht auf Datenübertragbarkeit

Fast jeder hat wohl schon einmal seinen Anbieter für soziale Netzwerke, Mobilfunkplattformen oder Internetdienste gewechselt und dabei seine Daten auf den neuen Anbieter oder die neue Plattform übertragen wollen. So einfach sich der Wechsel vollziehen lässt, so mühsam ist es oft genug, seine Daten „mitzunehmen“ und auf den neuen Anbieter, die neue Plattform zu übertragen. Entweder kann man die Daten schon nicht aus dem System des bisherigen Anbieters auf einfache Weise „herausziehen“ oder die verwendeten Datenformate sind so unterschiedlich, dass sie nicht in das System des neuen Anbieters übernommen werden können. Hier soll das Recht auf Datenübertragbarkeit Abhilfe schaffen. Der Einzelne soll einen Anspruch darauf erhalten, seine Daten in einem gängigen Format zu bekommen und dieses auch auf einen anderen Anbieter übertragen zu können. Was für das Mitnehmen der Telefonnummer seit vielen Jahren selbstverständlich ist, soll damit auch für Web-2.0-Dienste möglich sein.

2.1.2 Ein mühsamer Weg – Der Entwurf für eine neue Richtlinie im Bereich von Polizei und Justiz

Zusammen mit dem Entwurf für eine Datenschutz-Grundverordnung hat die Europäische Kommission auch einen Vorschlag für eine Richtlinie im Bereich von Polizei und Justiz vorgelegt. Dieser geht in die richtige Richtung, bedarf aber noch Verbesserungen. Entscheidend ist dabei die Klarstellung, dass die Richtlinie nur Mindeststandards für den nationalen Gesetzgeber setzt.

Der Entwurf einer Richtlinie für den Datenschutz im Bereich von Polizei und Justiz soll zusammen mit der parallel vorgelegten Datenschutz-Grundverordnung den Datenschutz nach Inkrafttreten des Vertrages von Lissabon in allen Bereichen rundum erneuern. Dieses Ziel habe ich von Anfang an unterstützt.

Der konkrete Richtlinienvorschlag hat bei mir allerdings gemischte Gefühle hervorgerufen. Mein Anliegen war und ist es, dass in der gesamten Europäischen Union ein möglichst hoher Datenschutzstandard sichergestellt ist. Dies gilt in besonderem Maße im Bereich von Polizei und Justiz, und zwar bei allen polizeilichen Datenverarbeitungen, unabhängig davon, ob diese grenzüberschreitend sind oder nicht. Der geltende Rahmenbeschluss 2008/977/JI (vgl. 22. TB Nr. 13.3.1) macht diese Unterscheidung und ist durch seine auf grenzüberschreitende Datenverarbeitungen begrenzte Anwendbarkeit gerade nicht geeignet, dieses wesentliche Ziel zu verwirklichen. Deswegen ist die Reform des geltenden europäischen Datenschutzrechts im Bereich von Polizei und Justiz weiterhin erforderlich und wird von mir unterstützt.

Gleichzeitig sehe ich in dem Entwurf der Kommission aber einige problematische Punkte. Wesentlich ist dabei die Unsicherheit, welches Maß an Harmonisierung mit der Richtlinie erreicht werden soll. Insbesondere die

Rechtsprechung des Bundesverfassungsgerichts hat in den letzten 30 Jahren dafür gesorgt, gerade im polizeilichen Bereich ein hohes Datenschutzniveau in Deutschland zu etablieren. Ich denke dabei an die Rechtsprechung zum Schutz des Kernbereichs privater Lebensgestaltung, zur Vorratsdatenspeicherung, zur Rasterfahndung oder zur Kennzeichnungspflicht von Daten, die bei der Telekommunikationsüberwachung erhoben worden sind. Entsprechende Bestimmungen fehlen im Entwurf der Kommission. Was würde mit diesen grundlegenden Regeln des deutschen Datenschutzrechts nach Inkrafttreten der Richtlinie geschehen? Ich bin mir darüber im Klaren: Wer sich entscheidet, Souveränität zugunsten der Europäischen Union abzugeben, der kann nicht erwarten, dass immer alles nach seinen Vorstellungen geschieht. Anders als bei der Datenverarbeitung zu wirtschaftlichen Zwecken sehe ich allerdings keine Notwendigkeit, nationales Recht zu „deckeln“ und die damit regelmäßig einhergehenden rechtlichen Auseinandersetzungen zu riskieren. Deshalb sollte die Richtlinie klarstellen, dass die Mitgliedstaaten in nationalen Regelungen ein höheres Datenschutzniveau vorsehen können, als die Richtlinie vorgibt. So würde ein robustes Datenschutzmindestniveau in der gesamten Europäischen Union festgelegt. Gleichzeitig wäre kein Mitgliedstaat in der Möglichkeit beschränkt, neues fortschrittlicheres Datenschutzrecht zu schaffen. Und dem Bundesverfassungsgericht käme weiterhin eine wichtige Rolle zu, gemeinsam mit dem Europäischen Gerichtshof die datenschutzrechtliche Rechtsprechung fortzuentwickeln.

Ich werde mich weiterhin dafür stark machen, den Richtlinienentwurf zu verbessern. Die Grundsätze für die Datenverarbeitung durch Polizei und Justiz sollten an die Grundverordnung angeglichen werden. Nationale Verarbeitungsbeschränkungen sollten weitergegeben, die unbescholtenen Bürger besser gegen eine polizeiliche Erfassung geschützt, die Möglichkeiten zur Übermittlung in unsichere Drittstaaten beschränkt, effiziente Datenschutzaufsicht sichergestellt werden. Diese Aufzählung umfasst nur einen Teil der Aufgaben, die alle Beteiligten des Gesetzesvorhabens noch vor sich haben.

Das Schicksal des Richtlinienentwurfs ist offen. Insbesondere der Rat hat eine sehr kritische Haltung eingenommen. Ich setze mich dafür ein, den Datenschutz in Europa insgesamt zu stärken, ohne bestehende Rechtsgarantien einzelner Mitgliedstaaten dabei zu schwächen. Die Einführung europaweiter Mindeststandards gerade in diesem besonders grundrechtsrelevanten Bereich kann hierfür den Weg ebnen.

2.2 Mehr Raum für Sicherheit?

Die grenzüberschreitende Zusammenarbeit der Sicherheitsbehörden wurde im Berichtszeitraum weiter verstärkt. Diesem Ziel dienen neue rechtliche Instrumente und die Modernisierung der technischen Mittel für den grenzüberschreitenden Datenaustausch. Kritisch sehe ich es, dass sensible personenbezogene Daten auch ohne ausreichende rechtliche und tatsächliche Garantien in Drittstaaten übermittelt werden.

2.2.1 Europäische Ermittlungsanordnung

Eine Richtlinie zur Europäischen Ermittlungsanordnung in Strafsachen soll die grenzüberschreitende Strafverfolgung erleichtern. Die Grundrechte der Betroffenen dürfen dabei nicht ausgehebelt werden.

Die Europäische Ermittlungsanordnung (EEA) führt zu einer umfangreichen Anerkennung von Ermittlungsentscheidungen zwischen den Mitgliedstaaten. Ein Mitgliedstaat muss die Entscheidung der Ermittlungsbehörden bzw. -gerichte eines anderen Staates vollstrecken. Der Entwurf spricht deshalb von Anordnungsstaat und Vollstreckungsstaat. Ich halte den Richtlinienentwurf für zu weitgehend. Es fehlen Regelungen zur Geltung hinreichender Mindeststandards, welche die Grundrechte der Betroffenen, also auch die Datenschutzrechte, hinreichend sichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert ebenfalls ein hohes grundrechtliches Schutzniveau (vgl. Kasten zu Nr. 2.2.1).

Mit dem Vertrag von Lissabon (vgl. 23. TB Nr. 13.1) wurden die Möglichkeiten ausgeweitet, auf europäischer Ebene das Strafrecht und das Strafverfahrensrecht zu beeinflussen. Der Vertrag ermöglicht es dem europäischen Gesetzgeber zum einen, hier Mindeststandards zu setzen. Zum anderen kann er die gegenseitige Anerkennung von Entscheidungen der Mitgliedstaaten regeln. Auf letztere Möglichkeit berufen sich die Verfasser des Entwurfs der Richtlinie zur EEA.

Dabei stehen die gegenseitige Anerkennung und die Mindeststandards in einem Abhängigkeitsverhältnis. Mit anderen Worten: Nur wenn umfassende Mindeststandards geregelt sind, kann die gegenseitige Anerkennung ausgebaut werden.

Mindeststandards im Strafverfahren fehlen jedoch noch in weiten Bereichen. Insbesondere mangelt es an expliziten Regelungen für die Übermittlung, Speicherung und Verwendung übermittelter Daten in den Mitgliedstaaten. Diese müssten geregelt haben, unter welchen Voraussetzungen die Behörden welche Daten erheben und verwenden und wie lange diese gespeichert werden dürfen. Die Verwendung müsste gegebenenfalls beschränkt werden, etwa bei Daten, die aus besonders eingriffsintensiven Ermittlungsmaßnahmen stammen (z. B. Telekommunikationsüberwachung, akustische Wohnraumüberwachung). Die Betroffenenrechte wären festzulegen (Anhörung, Auskunft, Benachrichtigung, Löschung, Berichtigung). Insbesondere im Hinblick auf die Verwendungsbeschränkungen enthält auch der Vorschlag für eine Datenschutzrichtlinie für den Bereich von Polizei und Justiz keine ausreichenden Regeln (vgl. unter Nr. 2.1.2).

Nach Mitteilung des Bundesministeriums der Justiz sieht der Richtlinienentwurf immerhin vor, dass der Vollstreckungsstaat die Maßnahme auch nach seinem eigenen Recht prüfen kann. Eine deutsche Behörde könnte also prüfen, ob die Maßnahme etwa gegen die Strafprozessordnung verstoßen würde. In diesem Fall hätte sie dann einen Grund, die Vollstreckung zu verweigern.

Verweigerungsgründe sind jedoch in einigen wesentlichen Bereichen unzureichend, etwa bei der Übermittlung personenbezogener Daten zwischen Mitgliedstaaten. Die Be-

hörde des Vollstreckungsstaates soll nach dem Entwurf sehr weitgehend verpflichtet sein, Daten aus ihren Datenbanken zu übermitteln sowie vorhandene Beweismittel zur Verfügung zu stellen. Wenn die Strafprozessordnung den Zugang beschränkt, etwa weil personenbezogene Daten aus einer Telekommunikationsüberwachung nur bei Straftaten von besonderem Gewicht verwendet werden dürfen, soll diese Einschränkung nach dem Entwurf wohl wegfallen. Dieser enthält jedenfalls – anders als die Strafprozessordnung – keine entsprechende Regelung. Nebulös ist die umfassende Verpflichtung, Ermittlungsanordnungen durchzuführen, „die keine Zwangsmaßnahmen sind".

Noch ist der Entwurf der EEA-RL nicht beschlossen. Zurzeit finden weiter Verhandlungen auf politischer Ebene statt. Ich erkenne an, dass sich die Bundesregierung bemüht, rechtsstaatliche Standards dadurch zu wahren, dass, soweit wie möglich, das innerstaatliche Recht als Schranke für zwischenstaatliche Übermittlungen gelten soll. Gleichwohl würde ich mir klarere Mindeststandards auf europäischer Ebene wünschen. Denn europäische Bürgerinnen und Bürger sollten europaweit darauf vertrauen dürfen, dass der Gesetzgeber ihre Grundrechte auch in den Richtlinien und Verordnungen berücksichtigt und diese entsprechend ausgestaltet. Eine Chance, einer zufrieden stellenden Lösung näher zu kommen, bietet der in der Diskussion befindliche Entwurf einer EU-Richtlinie zum Datenschutz bei Polizei und Justiz (vgl. Nr. 2.1.1).

Kasten zu Nr. 2.2.1

Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22. März 2012 in Potsdam

Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln

Zurzeit wird auf europäischer Ebene der Entwurf einer Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese hat massive Auswirkungen auf den Grundrechtsschutz der Bürgerinnen und Bürger in den EU-Mitgliedstaaten. Sie kann dazu führen, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.

Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Möglichkeiten der Mitgliedstaaten, eine entsprechende Anordnung eines anderen Mitgliedstaates zurückzuweisen, sind nicht immer ausreichend. Eingriffsschwellen, Zweckbindungs- und Verfahrensregelungen müssen gewährleisten, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden.

Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen. Die Anforderungen der EU-Grundrechte-Charta sind konsequent einzuhalten. Die Europäische Ermittlungsanordnung muss in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

2.2.2 Europol-Analysedateien

Die Verarbeitung personenbezogener Daten in Analysedateien beim Europäischen Polizeiamt wurde datenschutzrechtlich geprüft.

In früheren Tätigkeitsberichten habe ich mehrfach über die Aufgabe und Arbeitsweise des Europäischen Polizeiamtes (Europol) berichtet (vgl. zuletzt 23. TB Nr. 13.11).

2012 hat die die Gemeinsame Kontrollinstanz (GKI) von Europol schwerpunktmäßig Dateien kontrolliert, die Europol zu Analysezwecken errichtet hat. Ihr Kontrollbericht war bei Redaktionsschluss noch nicht öffentlich zugänglich. Kontrollberichte sind – wenn sie öffentlich zugänglich gemacht werden – auf der Internetseite der GKI einsehbar: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=de. Gleichwohl lässt sich über die Funktionsweise und die datenschutzrechtliche Problematik der Analysedateien einiges berichten.

Analysedateien werden zeitlich befristet für bestimmte Phänomen- bzw. Deliktsbereiche (z. B. zur Bekämpfung der organisierten Kriminalität oder des Terrorismus) eingerichtet. In ihnen verarbeitet Europol auch personenbezogene Daten, die aus den Europol-Mitgliedstaaten oder aus Drittstaaten stammen. Dadurch sollen – auch für die Behörden der Mitgliedstaaten – neue Erkenntnisse und Ermittlungsansätze gewonnen werden.

Welche Daten unter welchen Voraussetzungen in den Analysedateien verarbeitet werden dürfen, ist in dem Beschluss des Rates 2009/936/JI vom 30. November 2009 geregelt, der am 11. Dezember 2009 im Amtsblatt der Europäischen Union (L325 S. 14 ff.) veröffentlicht wurde. Verarbeitet werden danach nicht nur Daten von Verdächtigen, sondern auch von Kontakt- und Begleitpersonen, Zeugen, Opfern und Informanten bzw. Hinweisgebern. Die richtige Zuordnung eines Betroffenen zu diesen Personengruppen ist von maßgebender Bedeutung.

Nach dem o. g. Beschluss sind Kontakt- und Begleitpersonen solche Personen, bei denen ausreichende Gründe für die Annahme bestehen, dass über sie Informationen über (potentielle) Straftäter oder Verdächtige beschafft werden können, die für die Analyse relevant sind. Eine „Kontaktperson" ist daher, wer mit einer dieser Personen sporadisch in Kontakt steht – gleichgültig warum. Bei regelmäßigem Kontakt ist man nach der Definition des Beschlusses eine „Begleitperson".

Zu Kontakt- und Begleitpersonen in diesem Sinne dürfen auch sehr weitgehende – höchstpersönliche – Daten ge-

speichert werden, sofern Grund zu der Annahme besteht, dass diese Daten für die Analyse der Rolle des Betreffenden als Kontakt- oder Begleitperson erforderlich sind. Diese genügt, um zu einer Kontakt- oder Begleitperson Informationen verarbeiten zu dürfen, wie z. B.

- über deren wirtschaftliche und finanzielle Verhältnisse (Barvermögen, Aktien, Kontakte zu Banken und Kreditinstituten, sonstige Angaben zu ihrem Finanzgebaren etc.),
- zu ihrem Verhalten (Lebensweise, Gewohnheiten, regelmäßig aufgesuchte Orte etc.),
- aus anderen Datenbanken, in denen Informationen über die betreffende Person gespeichert sind (z. B. öffentliche und private Einrichtungen),
- über juristische Personen, die mit bestimmten Informationen in Zusammenhang stehen.

Dies habe ich bereits im Vorfeld des Ratsbeschlusses kritisiert. Nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) darf die deutsche Polizei Daten zu Kontakt- und Begleitpersonen nur unter deutlich engeren Voraussetzungen erheben und verarbeiten. „Vorausgesetzt sind konkrete Tatsachen für einen objektiven Tatbezug und damit für eine Einbeziehung in den Handlungskomplex der Straftatenbegehung, insbesondere eine Verwicklung in den Hintergrund oder das Umfeld der Straftaten“ (BVerfG, 1 BvR 1104/92 vom 25. April 2001). Bereits mit dem Merkmal „konkrete Tatsachen“ hat das Gericht im Vergleich zum Ratsbeschluss, in dem lediglich die Erforderlichkeit bzw. das Vorliegen ausreichender Gründe verlangt wird, eine deutlich höhere Eingriffsschwelle festgelegt.

Die Vorgaben des Bundesverfassungsgerichts sind in Deutschland bindend und von der deutschen Polizei zu beachten.

2.2.3 ZIS – Ein Informationssystem, das nicht gebraucht wird

Die Gemeinsame Kontrollinstanz Zoll stellte fest, dass die Zollbehörden der Mitgliedstaaten fast keine Daten in das Zollinformationssystem eingeben – und legt dessen Abschaffung nahe.

Das Zoll-Informationssystem (ZIS) steht im Schatten der bekannteren europäischen Informationssysteme, wie etwa dem Schengener Informationssystem (SIS) oder dem Europol-Informationssystem (EIS, vgl. Nr. 7.6.2). ZIS ist ein technisch und rechtlich kompliziertes Konstrukt, das unterschiedlichen Zwecken dient. Es soll die europäischen Zollbehörden dabei unterstützen, schwere, zollrechtlich relevante Verstöße gegen das Recht der einzelnen Mitgliedstaaten und das Recht der Europäischen Union zu verhindern und zu verfolgen.

ZIS wird von den Zollbehörden der Mitgliedstaaten der Europäischen Union kaum oder gar nicht genutzt – die Zollbehörden haben nur sehr wenige Daten eingespeichert. Dies ergab etwa eine Kontrolle, die die Gemeinsame Kontrollinstanz Zoll (GKI Zoll) unter Beteiligung meiner Behörde bei dem Europäischen Amt für Betrugsbekämpfung (OLAF) – wo die Datenbank technisch betrieben wird – durchgeführt hat. Diese Erkenntnis hatte ich schon im Berichtszeitraum 2005/2006 (vgl. 21. TB Nr. 32.5) gewonnen, als ich mich beim ZKA über das ZIS informierte. Offenbar hat sich an der fehlenden Akzeptanz der Zollfahndungsbehörden in den EU-Mitgliedstaaten nichts geändert.

Deshalb ist es konsequent, wenn die GKI Zoll als Ergebnis ihrer Kontrolle die Abschaffung von ZIS nahe legt, denn es wird offensichtlich nicht gebraucht.

Eine Reaktion der Mitgliedstaaten auf diese Empfehlung lässt leider auf sich warten. Offensichtlich fällt es den Verantwortlichen leichter, die Einrichtung neuer Dateien, Datenbanken und Informationssysteme zu beschließen, als diese bei erwiesener Nutzlosigkeit wieder abzuschaffen. Diese kostspielige Asymmetrie ließe sich vielleicht dadurch vermeiden, dass die Erforderlichkeit derartiger Systeme nicht bloß behauptet, sondern nachvollziehbar nachgewiesen werden muss, ehe man sie einrichtet.

2.2.4 Eurodac

Die Fingerabdruckdatenbank Eurodac soll zukünftig auch den Strafverfolgungsbehörden offen stehen. Datenschützer sehen das kritisch.

Der Vorschlag der Europäischen Kommission zur Änderung der Eurodac-Verordnung vom September 2012 will den Strafverfolgungsbehörden unter bestimmten Voraussetzungen Zugriff auf die Eurodac-Daten ermöglichen. In einem gemeinsamen Schreiben an die Europäische Kommission haben die Eurodac-Datenschutzaufsichtsgruppe und die Artikel-29-Gruppe der Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Union hervorgehoben, dass die Europäische Kommission keinen Nachweis dafür erbracht habe, warum die gegenwärtigen Instrumente der Strafverfolgungsbehörden nicht ausreichten und weshalb der Zugriff auf Asylbewerberdaten notwendig sei. Vor diesem Hintergrund erscheint beiden Datenschutzgruppen eine Zweckänderung der in Eurodac gespeicherten Daten nicht gerechtfertigt. Bei Redaktionsschluss waren die Verhandlungen im Europäischen Rat und im Europäischen Parlament über den Vorschlag der Europäischen Kommission noch nicht abgeschlossen.

Die gemeinsame Datenschutzaufsichtsgruppe (Eurodac Supervision Coordination Group) befasste sich mit zwei koordinierten Kontrollvorhaben. Zunächst wurde untersucht, welche Vorkehrungen Mitgliedstaaten getroffen haben, um die Pflicht zur vorzeitigen Löschung von Fingerabdruckdaten – z. B. wenn ein Asylbewerber innerhalb der Speicherdauer von bis zu zehn Jahren die Staatsangehörigkeit eines Mitgliedstaates erworben hat – umzusetzen. Bei meiner Prüfung zeigte sich, dass das Bundesamt für Migration und Flüchtlinge (BAMF) als die für den nationalen Teil des Eurodac-Systems zuständige Zentralbehörde einen entsprechenden Informationsaustausch mit den Einbürgerungsbehörden sichergestellt hat. In manchen Mitgliedstaaten wurden jedoch Defizite im Informationsfluss festgestellt. Den entsprechenden Kontrollbericht hat das beim Europäischen Datenschutzbeauftragten (EDPS) angesiedelte Sekretariat der gemein-

samen Datenschutzaufsichtsgruppe veröffentlicht (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/11-12-09_EURODAC_Report_EN.pdf). Das zweite Kontrollvorhaben, das die Verarbeitung unleserlicher Fingerabdrucke zum Gegenstand hat, stand bei Redaktionsschluss für diesen Tätigkeitsbericht zwar kurz vor dem Abschluss, ein Bericht lag jedoch noch nicht vor.

2.2.5 Visa-Informationssystem

Das europäische Visa-Informationssystem (VIS) hat seinen Betrieb aufgenommen.

Am 1. Oktober 2011 wurde nach mehrjähriger Planung und Vorbereitung mit dem europäischen Visa-Informationssystem der Betrieb für eine neue multinationale Datenbank aufgenommen (vgl. Nr. 8.9). Das VIS verfolgt zwar ähnliche Zwecke wie Eurodac (u. a. Vermeidung von Mehrfach-Anträgen, Identitätsverifizierung, vgl. Nr. 2.2.4), bezieht sich aber auf einen anderen Personenkreis. In der VIS-Datenbank werden nicht nur personenbezogene Daten von Visum-Antragstellern erfasst und bis zu fünf Jahre gespeichert, sondern auch von Personen, die Besuchseinladungen an visum-pflichtige Antragsteller richten. Neben den üblichen Angaben wie Name, Vorname und Geburtsdatum werden zu den Visum-Antragstellern auch biometrische Daten (Fotos und Fingerabdrücke) gesammelt.

Anders als bei Eurodac werden die Daten für das VIS zumeist aber nicht im Inland, sondern durch Konsulate und Botschaften der Mitgliedstaaten im Ausland erhoben und über nationale „Kopfstellen“ an die zentrale VIS-Datenbank in Straßburg weitergeleitet. Gegenwärtig wird das VIS bei den Auslandsvertretungen der Teilnehmerstaaten in Nordafrika, Naher Osten und im weiteren Bereich des Persischen Golfs genutzt (vgl. Kasten zu Nr. 2.2.5). Über weitere Regionen und Länder wird die Europäische Kommission entscheiden.

Die Datenschutzaufsicht über das VIS folgt einem ähnlichen Modell wie bei Eurodac: Der EDPS kontrolliert die zentrale VIS-Datenbank, während die Datenschutzbehörden der Mitgliedstaaten die jeweiligen nationalen Komponenten des VIS überprüfen. In Deutschland obliegt mir die datenschutzrechtliche Kontrolle, weil das Auswärtige Amt und das Bundesverwaltungsamt für den nationalen Teil des VIS verantwortlich sind. Um die Arbeit und die Kontrollschwerpunkte in den Mitgliedstaaten aufeinander abzustimmen, wurde auch beim VIS eine gemeinsame Kontrollaufsichtsgruppe unter Vorsitz des EDPS geschaffen, in der auch ich vertreten bin.

Kasten zu Nr. 2.2.5

Einsatzregionen des europäischen Visa-Informationssystems (Ende 2012)

Region 1: Nordafrika

- Algerien
- Ägypten
- Libyen
- Mauretanien
- Marokko
- Tunesien

Region 2: Naher Osten

- Israel
- Jordanien
- Libanon
- Syrien

Region 3: Persischer Golf und Umgebung

- Afghanistan
- Bahrain
- Iran
- Irak
- Kuwait
- Oman
- Katar
- Saudi-Arabien
- Vereinigte Arabische Emirate
- Jemen

2.3 IT goes Europe

Über die Verarbeitung personenbezogener Daten durch öffentliche Stellen wird zunehmend nicht mehr auf nationaler Ebene allein entschieden. Nicht nur die rechtlichen Rahmenbedingungen sondern auch technische Standards werden durch die Europäische Union vorgegeben. Außerdem ist die EU, bzw. von ihr eingerichtete Agenturen, zunehmend auch selbst Betreiberin von europaweiten Großsystemen. Leider klammern die Kommissionsvorschläge für einen neuen Rechtsrahmen für den Datenschutz in der EU (vgl. Nr. 2.1) die EU-Institutionen und die von ihnen betriebenen IT-Systeme aus. Dies gilt auch für deren Datenschutz-Kontrollstrukturen.

Für verschiedene durch europäische Agenturen betriebene Informationssysteme (Schengener Informationssystem, Europol, Eurojust, Zollinformationssystem) wurden eigenständige Kontrollgremien, so genannte Gemeinsame Kontrollinstitutionen (GKI) eingerichtet.

Dagegen arbeiten der Europäische Datenschutzbeauftragte und die nationalen Aufsichtsstellen sowohl bei der Kontrolle des europäischen Fingerabdrucksystems Eurodac (vgl. Nr. 2.2.4) als auch bei der Aufsicht über das neu eingerichtete europäische Visa-Informationssystem (VIS, vgl. Nr. 2.2.5) eng zusammen. Das Betriebsmanagement für die zentralen Datenbanken von Eurodac und VIS hat am 1. Dezember 2012 die im November 2011 neu ge-

gründete Europäische Agentur für IT-Großsysteme übernommen. Darüber hinaus soll diese Agentur voraussichtlich ab Frühjahr 2013 auch das Management für das Schengener Informationssystem der zweiten Generation (SIS II) übernehmen.

Ich trete dafür ein, die verschiedenen Modelle zur datenschutzrechtlichen Begleitung und Kontrolle europäischer IT-Systeme zu vereinheitlichen. Neben Synergieeffekten ließe sich so auch eine effektivere Datenschutzkontrolle im Sinne eines einheitlich hohen Schutzniveaus für die EU-Bürgerinnen und Bürger erreichen.

2.3.1 Binnenmarktinformationssystem

Im Dezember 2012 ist die IMI-Verordnung in Kraft getreten. Sie ermöglicht den Informationsaustausch und die Kommunikation zwischen den Mitgliedstaaten der Europäischen Union im Rahmen der EG-Dienstleistungsrichtlinie.

Das Anfang 2010 ans Netz gegangene Binnenmarktinformationssystem (Internal Market Information System – IMI) ermöglicht es einer Vielzahl von Behörden der 27 EU-Staaten, miteinander elektronisch zu kommunizieren, wenn beispielsweise Zweifel an der Echtheit der vom Dienstleistungserbringer vorgelegten Unterlagen bestehen und deshalb bei den zuständigen Behörden in dem ausstellenden Mitgliedstaat Nachfragen erforderlich werden (vgl. 22. TB Nr. 3.4.1).

Der bisher fehlende Rechtsrahmen hierfür ist nun durch die im Dezember 2012 in Kraft getretene europäische Verordnung (IMI-VO (EU) Nr. 1024/2012) geschaffen worden. Sie schafft Rechtssicherheit beim Umgang mit personenbezogenen Daten im IMI und ist eine wesentliche Voraussetzung für die verbindliche Anwendung datenschutzrechtlicher Grundsätze bei der Nutzung des IMI.

Ich wurde durch das Bundesministerium für Wirtschaft und Technologie (BMWi) über die Verhandlungen über den Entwurf der IMI-VO informiert und hatte Gelegenheit zur Stellungnahme. Auch wenn ich nicht alle meine Positionen durchsetzen konnte, ist es doch gelungen, in der zuständigen Ratsarbeitsgruppe tragfähige Kompromisse zu erzielen.

Ich werde die Anwendung der IMI-VO weiterhin begleiten und – gemeinsam mit den Datenschutzbeauftragten der Länder – auf die Einhaltung der Datenschutzvorschriften achten. Die IMI-VO sieht eine unabhängige Überwachung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die IMI-Akteure ihres Mitgliedstaates und die Gewährleistung des Schutzes der Rechte der betroffenen Personen durch die nationalen Datenschutzbehörden vor. Weiterhin kann auch der Europäische Datenschutzbeauftragte bei Bedarf die nationalen Kontrollstellen zu Zusammenkünften einladen, um die Überwachung des IMI und seiner Nutzung durch die IMI-Akteure zu gewährleisten.

2.3.2 epSOS: Wie sind Gesundheitsdaten bei der grenzüberschreitenden Übermittlung zu schützen?

Die Artikel-29-Gruppe hat datenschutzrechtliche Empfehlungen für die Umsetzung eines europäischen Pilotprojektes für die grenzüberschreitende Übermittlung von Gesundheitsdaten verabschiedet.

Gesundheitsdaten geben nicht nur Aufschluss über den individuellen Gesundheitszustand, Medikamentenbedarf sowie die notwendigen ärztlichen Behandlungen – sie ermöglichen auch weitreichende Prognosen über die zukünftige gesundheitliche Entwicklung und sind von großem wirtschaftlichem Wert. Deshalb stehen sie im Fokus des Interesses verschiedenster Akteure aus Wirtschaft, Gesundheitswesen und Verwaltung. Sie unterliegen der ärztlichen Schweigepflicht und – wenn sie von Sozialleistungsträgern für Aufgaben nach dem Sozialgesetzbuch verwendet werden – dem besonderen Schutz des Sozialgesetzbuchs. Auch das BDSG und das europäische Datenschutzrecht stufen sie als besonders schutzwürdig ein.

Gesundheitsdaten spielen auch im internationalen Kontext eine Rolle. epSOS (Smart Open Services for European Patients – Open eHealth Initiative for a European Large Scale Pilot of Patient Summary and Electronic Prescription) ist ein von der EU gefördertes Projekt, in dessen Rahmen europäischen Bürgerinnen und Bürgern grenzüberschreitende E-Health-Dienste angeboten werden sollen. Im Mittelpunkt steht die Entwicklung einer europaweiten Infrastruktur, die den Zugriff auf Gesundheitsdaten über Ländergrenzen hinweg ermöglicht, um die Versorgung von Patienten zu verbessern, die sich im europäischen Ausland aufhalten.

Wesentliche Anwendungsfälle der epSOS-Infrastruktur sind der grenzüberschreitende Zugriff auf eine elektronische medizinische Kurzakte (patient summary) und eine elektronische Verordnung (e-prescription). Die in einem Mitgliedstaat des Patienten geführte medizinische Kurzakte soll Angaben zu Erkrankungen, relevanten Eingriffen und Unverträglichkeiten enthalten, ähnlich einer elektronischen Patientenakte. Die elektronische Verordnung soll die Ausstellung von Rezepten am Ort der Behandlung im europäischen Ausland ermöglichen. Hierzu soll der Apotheker oder Arzt am Aufenthaltsort des Patienten auf die im anderen Mitgliedstaat geführte Medikationsakte, die Teil der medizinischen Kurzakte ist, zugreifen können. Die Übermittlung der Gesundheitsdaten soll nur mit Einwilligung der Betroffenen erfolgen.

Auch wenn sich Deutschland noch nicht an dem noch in der Testphase befindlichen Projekt beteiligt, habe ich im Rahmen der „Subgroup Health Data“ der Artikel-29-Gruppe an der Ausarbeitung von Datenschutzempfehlungen für epSOS mitgewirkt (abrufbar unter http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm). Danach sind ausdrückliche Einwilligungen der Betroffenen sowohl für die Teilnahme am Projekt als auch für die Bereitstellung der medizinischen Daten sowie für die konkrete Datenübermittlung erforderlich. Ebenso wichtig ist, dass für die Datenübertragung ein ho-

her technischer Sicherheitsstandard gilt, etwa eine Ende-zu-Ende-Verschlüsselung.

Der hohe Datenschutzstandard, der für die deutsche elektronische Gesundheitskarte gilt, muss weiterhin garantiert bleiben, auch bei der grenzüberschreitenden Datenverarbeitung. Dies ist mir besonders wichtig und darauf werde ich weiter hinwirken.

2.3.3 Sozialdaten kennen keine Grenzen mehr

Für den elektronischen Austausch von Sozialdaten auf europäischer Ebene (EESSI) gibt es jetzt eine gesetzliche Grundlage.

Die Arbeitnehmerfreizügigkeit gehört zu den Grundfreiheiten in der Europäischen Union. Haben Versicherte in mehreren Mitgliedstaaten gearbeitet, fallen über sie und ihre Familienangehörigen in den Sozialsystemen mehrerer Mitgliedstaaten Informationen an. Viele dieser Informationen müssen die Sozialversicherungsbehörden untereinander austauschen. Insbesondere die Sozialbehörden des Heimatstaates sind auf diese Informationen aus den Sozialbehörden der Staaten angewiesen, in denen die Arbeitsleistung erbracht wurde. Bislang erfolgt die Übermittlung in Papierform auf einer Vielzahl unterschiedlicher Formulare. Die Erstellung der Formulare in den jeweiligen Landessprachen ist aufwendig. Zum Teil werden die Anträge auch als unvollständig, falsch oder unleserlich ausgefüllt zurückgewiesen.

Künftig soll der Informationsfluss bei grenzüberschreitenden Sozialversicherungsfällen elektronisch abgewickelt werden. Die Übermittlung der jährlich über 15 Millionen Nachrichten nationaler Behörden soll über das EU-weite IT-System „EESSI – Electronic Exchange of Social Security Information“ erfolgen. EESSI soll in das Europäische Verwaltungsnetzwerk sTESTA eingebunden werden. Die inländische Infrastruktur wird von den Mitgliedstaaten jeweils in eigener Verantwortung aufgebaut. Ein Verzeichnis der nationalen Institutionen in den Sektoren Gesundheitsvorsorge, Renten, Arbeitslosigkeit und Familienleistungen, die in den elektronischen Datenaustausch einbezogen werden sollen, ist aus dem Internet abrufbar (http://ec.europa.eu).

Für die Einrichtung von EESSI hat die Europäische Union auf dem Verordnungswege Regelungen getroffen (VO 883/2004/EG; VO 987/2009/EG). Diese in den Mitgliedstaaten unmittelbar anwendbaren Regelungen klären weder die Fragen der innerstaatlichen Zuständigkeiten noch genügen sie datenschutzrechtlichen Anforderungen. Entsprechende ergänzende und konkretisierende Bestimmungen wurden daher in Deutschland im „Gesetz zur Koordinierung der Systeme der sozialen Sicherheit in Europa“ vom 22. Juni 2011 (BGBl. I 2011 S. 1202) getroffen.

Im Gesetzgebungsverfahren habe ich besonders darauf geachtet, dass die Stellen, die den Datenfluss zwischen den Mitgliedstaaten koordinieren, nur die Kompetenzen erhalten, die sie tatsächlich zur Aufgabenerfüllung benötigen. Wie die Träger der Sozialversicherungen (z. B. Kranken-, Renten-, Unfallversicherungen) des Heimatlandes von der Entsendung eines Versicherten in ein anderes Mitgliedsland benachrichtigt werden, wird ebenfalls durch das Gesetz klargestellt.

Ferner werden die deutschen Verbindungs- und Zugangsstellen bestimmt. Die Verbindungsstellen haben die Anfragen und Amtshilfeersuchen der Partnerstaaten zu beantworten. Die Zugangsstellen dienen als Inlandskontakt für den elektronischen Datenaustausch sowie die innerstaatliche Weiterleitung von Dokumenten und sonstigen Informationen. In Deutschland werden fünf solcher Zugangsstellen bei großen Sozialleistungsträgern eingerichtet.

Der Gesetzgeber hat meine Anregung aufgegriffen, die Nutzung sämtlicher Daten, also auch von berufsständischen Versorgungseinrichtungen, von Familienleistungen (Kindergeld, Elterngeld etc.) sowie der Beamtenversorgung, den strengen datenschutzrechtlichen Regelungen des Sozialgesetzbuches zu unterwerfen.

Noch fehlt die Informationstechnik, die eine sichere und den Bestimmungen entsprechende Übermittlung der Daten gewährleistet. Dies bereitet angesichts der Vielzahl der teilnehmenden Staaten und der unterschiedlichen rechtlichen und technischen Voraussetzungen noch einige Schwierigkeiten. Ich werde die technische Umsetzung zu gegebener Zeit auf ihre datenschutzrechtliche Konformität prüfen. EESSI soll ab Mai 2014 uneingeschränkt nutzbar sein – viel Zeit steht also für eine datenschutzgerechte Standardisierung und Implementierung der erforderlichen Schutzvorkehrungen nicht zur Verfügung.

2.3.4 Europaweite elektronische Identifizierung nur ohne Abstriche beim Datenschutz!

Die geplante EU-Verordnung zur gegenseitigen Anerkennung von elektronischen Identifizierungsmitteln innerhalb der Europäischen Union weist noch erheblichen datenschutzrechtlichen Nachbesserungsbedarf auf.

Am 7. Juni 2012 hat die Europäische Kommission einen Vorschlag für eine Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vorgelegt. Ziel ist die europaweite gegenseitige Anerkennung von elektronischen Identifizierungssystemen und die Harmonisierung von Regelungen über elektronische Vertrauensdienste, wie zum Beispiel elektronische Signaturen oder Zustelldienste.

Die elektronische Identifizierung kann derzeit in Deutschland mit der sog. eID-Funktion des neuen Personalausweises erfolgen. Damit kann sich ein Bürger etwa gegenüber einer Kommune ausweisen. Die Kommune erhält dann elektronisch die Daten des Ausweises, die sie zur eindeutigen Identifizierung der Person benötigt. Die eID-Funktion kann auch beim Onlinekauf eingesetzt werden. Dabei ist darauf zu achten, den Zugriff auf diejenigen personenbezogenen Daten des Ausweises zu beschränken, die für den jeweiligen Anwendungsfall unbedingt notwendig sind. So ist es etwa für den kostenpflichtigen Download von altersbeschränkten Videos für

den Verkäufer erforderlich aber auch ausreichend, wenn er das Alter des Kunden kennt. Der Name muss hingegen nicht zwingend genannt werden.

Diese datenschutzfreundliche Funktion, die eine pseudonyme Nutzung möglich macht, wird vom Entwurf der EU-Verordnung in Frage gestellt, denn sie fordert, dass die Identifizierungsdaten der natürlichen oder juristischen Person eindeutig zugeordnet sein müssen. Zudem ist die gegenseitige Anerkennung nur dem Grundsatz nach geregelt. So fehlen eindeutige und konkrete Regelungen zum Datenschutz und zur Datensicherheit. Es darf nicht dazu kommen, dass das bei der deutschen eID-Funktion erreichte hohe Datenschutzniveau durch die Verpflichtung abgesenkt wird, elektronische Identifizierungssysteme aus anderen Mitgliedstaaten anzuerkennen, die nicht einmal entfernt dem hier erreichten Datenschutzstandard entsprechen. Deshalb begrüße ich es, dass sich die Bundesregierung auf europäischer Ebene für datenschutzgerechte Regelungen zur elektronischen Identifizierung einsetzt.

2.4 Europäische und internationale Datenschutz-Zusammenarbeit

Zu einem gelebten Datenschutz gehört die grenzüberschreitende Zusammenarbeit der Datenschutzbehörden. Auch im Berichtszeitraum hat sich in Sachen Kooperation einiges getan.

2.4.1 Artikel-29-Gruppe

2.4.1.1 Die Future-of-Privacy-Subgroup

Die Unterarbeitsgruppe (Subgroup) „Future of Privacy" ist zuständig für Grundsatzfragen des Datenschutzes auf EU-Ebene. Sie hat sich im Berichtszeitraum insbesondere mit dem Vorschlag der Europäischen Kommission für eine EU-Datenschutz-Grundverordnung befasst (vgl. Nr. 2.1.1) und hierzu zwei Stellungnahmen der Artikel-29-Gruppe vorbereitet.

In der Stellungnahme 1/2012 (WP 191) vom 23. März 2012 begrüßt die Artikel-29-Gruppe den Kommissionsvorschlag im Hinblick auf die Stärkung der Position der betroffenen Person, die Ausweitung der Verpflichtungen des für die Datenverarbeitung Verantwortlichen sowie die Verbesserung der Stellung der Aufsichtsbehörden auf nationaler und internationaler Ebene. Trotz ihrer grundsätzlich positiven Haltung gegenüber der Verordnung ist die Datenschutzgruppe der Ansicht, dass der Vorschlag in Teilen präzisierungs- und verbesserungsbedürftig ist. In der Stellungnahme 8/2012 (WP 199) vom 5. Oktober 2012 ergänzt die Artikel-29-Gruppe ihre grundlegende Position zum Kommissionsvorschlag der Datenschutz-Grundverordnung. Die Stellungnahme enthält unter anderem eine Prüfung sämtlicher in dem Verordnungsvorschlag enthaltener Delegationsermächtigungen der Europäischen Kommission.

Zudem hat sich die Unterarbeitsgruppe mit den Themen „Schutz besonderer Kategorien personenbezogener Daten", „Meldepflichten" sowie „praktische Zusammenarbeit der Datenschutzbehörden" befasst. Die Beratungsergebnisse wurden in so genannten „Empfehlungsschreiben" (Advice Papers) zusammengefasst, die als Beitrag der Artikel-29-Gruppe zur Reformdiskussion an die Europäische Kommission übersandt wurden.

Eine Liste der im Berichtszeitraum von der Artikel-29-Gruppe angenommenen Stellungnahmen und sonstigen Dokumenten findet sich unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

2.4.1.2 Subgroup International Transfers

Die Subgroup International Transfers (Internationaler Datentransfer) befasste sich schwerpunktmäßig mit verbindlichen Unternehmensregelungen (Binding Corporate Rules, BCR) zur Übermittlung personenbezogener Daten in Drittstaaten, insb. für Auftragsdatenverarbeiter.

Die Subgroup International Transfers beschäftigte sich mit einer Vielzahl von Fragestellungen zur Übermittlung von personenbezogenen Daten in Drittstaaten. Diese ist nach Artikel 25 Absatz 1 der europäischen Datenschutzrichtlinie 95/46/EG grundsätzlich nur bei Gewährleistung eines angemessenen Datenschutzniveaus beim Empfänger zulässig, eine vielfach nicht erfüllte Anforderung.

Um dennoch den Datentransfer innerhalb global tätiger Unternehmensgruppen zu ermöglichen, werden hierfür verbindliche Unternehmensregelungen erarbeitet, die sich auf Artikel 26 Absatz 2 der Datenschutzrichtlinie stützen. Sie spielen angesichts der zunehmend grenzüberschreitenden Datenströme eine immer größere Rolle. Das europäische Verfahren der gegenseitigen Anerkennung von verbindlichen Unternehmensregelungen (vgl. 23. TB Nr. 10.1) wird inzwischen erfolgreich in der Praxis angewandt. Europaweit konnten bereits rund 40 solcher Unternehmensregelungen abgestimmt werden, rund 20 befinden sich im Abstimmungsverfahren.

Die Gruppe hat im Berichtszeitraum zudem verbindliche Unternehmensregelungen für Auftragsdatenverarbeiter („BCR for processors") entwickelt, für die aufgrund der technischen Entwicklung – insbesondere im Bereich des Cloud Computing – ein großer Bedarf gesehen wird. Working Paper (WP) 195 der Artikel-29-Gruppe vom 6. Juni 2012 listet die notwendigen Bestandteile solcher BCR for processors in Tabellenform auf. Ein entsprechendes Antragsformular wurde ebenfalls verabschiedet. Die Unterlagen sind unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm abrufbar. Das EU-weite Verfahren zur Abstimmung und Anerkennung von verbindlichen Unternehmensregelungen für Auftragsdatenverarbeiter steht den Unternehmen ab dem 1. Januar 2013 offen.

Die Teilnehmerstaaten der APEC („Asia-Pacific-Economic Cooperation") verwenden für internationale Datentransfers ein dem europäischen BCR-System ähnliches Verfahren, die sog. Cross-Border Privacy Rules (CBPR). Eine Arbeitsgruppe bestehend aus Vertretern der APEC und Mitgliedern der Subgroup International Transfers, an der auch ich mich beteilige, versucht, die beiden Systeme

zu harmonisieren und, wenn möglich, eine gewisse Interoperabilität zwischen BCR und CBPR herzustellen. Ziel ist es, global operierenden Unternehmen den grenzüberschreitenden Transfer von personenbezogenen Daten innerhalb der Unternehmensgruppe zu erleichtern, zugleich aber den Schutz der Daten auf einem weltweit möglichst einheitlichen, hohen Niveau zu gewährleisten.

2.4.1.3 Technologischer Datenschutz auch in Brüssel – Leitung der Technology Subgroup

Seit Oktober 2010 tagt die Technology Subgroup unter Leitung eines Vertreters des BfDI. Sie beschäftigt sich mit Fragen des technologischen Datenschutzes und ist mit mehr als 30 Teilnehmern die größte Untergruppe der Artikel-29-Gruppe.

Im Oktober 2010 hat ein Mitarbeiter meiner Dienststelle den Vorsitz der Technology Subgroup in Brüssel übernommen. Nach dem Arbeitsprogramm der Artikel-29-Gruppe beschäftigt sich diese Untergruppe schwerpunktmäßig mit technologischen Herausforderungen für den Datenschutz.

In den vergangenen zwei Jahren hat die Technology Subgroup im Auftrag der Artikel-29-Gruppe verschiedene Stellungnahmen erarbeitet. Dazu gehören Arbeitspapiere zu den Themen Gesichtserkennung, Meldung von Datenschutzverstößen, RFID PIA (vgl. 23. TB Nr. 5.9), verhaltenbasierte Onlinewerbung und Smart Metering (vgl. Nr. 10.1).

Eine der umfangreichsten und wichtigsten Stellungnahmen – bei der Vertreter der Landesdatenschutzbeauftragten und meiner Dienststelle als Berichterstatter fungiert haben – ist das Papier zu Cloud Computing (vgl. Nr. 5.3). Es beschreibt die Gefahren und Risiken der Datenspeicherung und Datenverarbeitung in der „Wolke“, analysiert das anwendbare Recht und die Verpflichtungen von Datenverarbeitern und enthält Empfehlungen für Cloud-Nutzer und Cloud-Anwender – auch im Zusammenhang mit der Datenübermittlung in Drittstaaten.

Darüber hinaus erarbeitete die Gruppe Positionen zu aktuellen Themen mit datenschutztechnischer Relevanz. Ein Schwerpunktthema in den letzten beiden Jahren war die Bewertung der neuen Google-Datenschutzerklärung (vgl. Nr. 5.9). Ein weiteres wichtiges Thema bildeten die Datenschutzbestimmungen und die Praxis des sozialen Netzwerks Facebook (vgl. Nr. 5.8.1).

2.4.1.4 Der neue „B(ee)TLE“

Als Konsequenz der Veränderungen durch den Vertrag von Lissabon hat die Artikel-29-Gruppe die neue Unterarbeitsgruppe „BTLE“ (Borders, Travel & Law Enforcement) eingerichtet.

Die neue Unterarbeitsgruppe beschäftigt sich mit datenschutzrechtlichen Themen aus den Bereichen der Grenz- und Migrationskontrolle und der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Prominenteste Themen waren bisher die Übermittlung von Fluggast- und Zahlungsverkehrsdaten in die USA.

Durch den Vertrag von Lissabon ist die Sonderrolle, die der Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen bisher eingenommen hatte (vgl. 23. TB Nr. 13.5), weitgehend weggefallen. Auf diese grundlegende Entwicklung hat die Artikel-29-Gruppe mit einer neuen Unterarbeitsgruppe reagiert und im Sommer 2011 die Borders, Travel & Law Enforcement (BTLE)-Unterarbeitsgruppe ins Leben gerufen. Diese neue Gruppe knüpft an die früheren Arbeiten der Artikel-29-Gruppe an, die sich schon vor dem Vertrag von Lissabon intensiv mit der Übermittlung von Fluggastdaten für polizeiliche Zwecke beschäftigt hatte.

Die europäischen Datenschutzbehörden bündeln in der BTLE-Unterarbeitsgruppe zugleich ihre Beratungskompetenz bei den zentralen Datenschutzthemen aus dem Bereich von Polizei und Justiz. Entsprechend hat die Frühjahrskonferenz der europäischen Datenschutzbeauftragten im Jahr 2012 entschieden, ihre früher hierfür eingesetzte Working Party on Police and Justice aufzulösen.

Seit ihrer Gründung hat die BTLE-Unterarbeitsgruppe eine Vielzahl von Beiträgen und Stellungnahmen zu datenschutzsensiblen Themen erarbeitet. Viel Raum hat die Ausarbeitung einer Stellungnahme zum Entwurf einer neuen Richtlinie für den Bereich von Polizei und Justiz eingenommen (vgl. Nr. 2.1.2). Darüber hinaus hat die Unterarbeitsgruppe mehrfach Äußerungen der Artikel-29-Gruppe zu den verschiedenen Initiativen und Abkommen vorbereitet, die der vermehrten Nutzung von Fluggastdaten zu polizeilichen Zwecken innerhalb und außerhalb von Europa dienen (vgl. Nr. 2.5.2). Von großer datenschutzpolitischer Bedeutung waren zudem das Abkommen mit den USA zur Übermittlung von Zahlungsverkehrsdaten sowie die Überlegungen der Europäischen Kommission zur Schaffung eines vergleichbaren europäischen Programms (vgl. Nr. 2.5.1). In einem von der BTLE-Subgroub vorbereiteten Schreiben an die Europäische Kommission hat sich die Artikel-29-Gruppe zu der Mitteilung der Kommission über „intelligente Grenzen“ (vgl. Nr. 2.5.3.3) geäußert.

Wie schon jetzt absehbar ist, bleibt in all diesen Bereichen viel zu tun. Dies gilt auch für ein neues großes Projekt der Luftfahrtindustrie, das noch für einigen Wirbel sorgen dürfte: den „Checkpoint of the Future“ (vgl. unter Nr. 2.5.3). Sowohl bei diesem als auch bei anderen Vorhaben sucht die BTLE-Unterarbeitsgruppe den kritischen Austausch auf Fachebene mit Vertretern der Europäischen Kommission sowie der beteiligten Industrien.

Die Unterarbeitsgruppe wird durch einen Mitarbeiter meiner Dienststelle gemeinsam mit einem niederländischen Kollegen koordiniert.

2.4.2 Europäische Datenschutzkonferenz

Die jährliche Frühjahrskonferenz („Spring Conference“) der europäischen Datenschutzbeauftragten befasste sich im Berichtszeitraum schwerpunktmäßig mit der EU-Datenschutzreform (vgl. Nr. 2.1).

Die Frühjahrskonferenz des Jahres 2011 wurde am 5. April in Brüssel gemeinsam vom Europäischen Datenschutzbeauftragten und dem Vorsitzenden der Artikel-29-Gruppe ausgerichtet. Sie verabschiedete eine Entschließung, welche die Notwendigkeit eines umfassenden EU-Datenschutz-Rechtsrahmens betont, der auch den Polizei- und Justizbereich umfasst.

Der Entschließungstext ist aus dem Internet abrufbar unter http://www.datenschutz.bund.de.

Zentrales Thema der am 4. Mai 2012 von der Nationalen Kommission für den Datenschutz (CNPD) in Luxemburg organisierten Konferenz war ebenfalls die Reform des EU-Datenschutzrechts. In ihrer Entschließung begrüßt die Konferenz die mit dem Reformvorhaben verfolgten Kernziele, nämlich die Stärkung der Rechte Betroffener, die Einführung des Verantwortlichkeitsprinzip („Accountability") für datenverarbeitende Stellen sowie die Stärkung der Rolle der unabhängigen Datenschutzbehörden.

Daneben behandelte die Konferenz Möglichkeiten zur Stärkung der Rechte von Internetnutzern, insbesondere bei Cloud Computing und Sozialen Netzwerken, den Schutz personenbezogener Daten in den Bereichen Polizei und Justiz sowie die Modernisierung anderer internationaler Datenschutzrechtsnormen, insbesondere der Datenschutz-Konvention 108 des Europarates sowie der OECD-Richtlinien (vgl. Nr. 2.4.5).

Der Entschließungstext ist auf der Internetseite der Nationalen Kommission für den Datenschutz abrufbar (http://www.cnpd.public.lu/fr/actualites/national/2012/04/spring-conference-2012/Resolution_on_the_European_data_protection_reform.pdf).

Auch in den Jahren 2011 und 2012 fanden daneben *„Case Handling Workshops"* unter der Verantwortung der Europäischen Datenschutzkonferenz statt, an denen Angehörige meiner Dienststelle teilgenommen haben. Diese Treffen haben sich gut bewährt, um auf europäischer Ebene Erfahrungen und Kenntnisse auszutauschen und auf diese Weise bei der Bearbeitung von Bürgereingaben und bei der Behandlung von ähnlich gelagerten Sachfragen zu einer vergleichbaren Verfahrensweise zu gelangen. Die letzten beiden Workshops wurden in Warschau (Oktober 2011) und in Budapest (September 2012) durchgeführt. Schwerpunktthemen waren hierbei u. a. Datenschutz in Sozialen Netzwerken, Datenschutz am Arbeitsplatz oder auch Wege und Methoden zur Bearbeitung von Fällen und Beschwerden, die grenzüberschreitende Übermittlungen personenbezogener Daten zum Gegenstand haben. Zielgruppe der Case Handling Workshops sind in erster Linie diejenigen Mitarbeiter der Datenschutzbehörden, die mit konkreten Problemen und Fragestellungen befasst sind (Arbeitsebene). Die einzelnen Workshops stehen Angehörigen von Datenschutzkontrollstellen aus ganz Europa offen. Daher können auch die Datenschutzbehörden von Staaten, die (noch) nicht der EU angehören, vom gemeinsamen Erfahrungsaustausch profitieren.

2.4.3 Internationale Datenschutzkonferenz

Die Internationalen Konferenzen der Datenschutzbehörden aus aller Welt gaben auch im Berichtszeitraum vielfältige Anstöße zur weiteren Intensivierung der Zusammenarbeit in einer globalisierten Datenwelt.

Gastgeber der 33. Internationalen Datenschutzkonferenz 2011 in Mexiko Stadt war das mexikanische Bundesinstitut für Zugang zu Informationen und Datenschutz (IFAI). Unter dem Titel „Privacy: The global age" befasste sich die Konferenz mit Fragen der Internationalität von Datenschutz und Datensicherheit. Angesichts zunehmend globaler Datenströme, deren Umfang täglich neue Superlative überschreitet, lässt sich das Recht auf Schutz personenbezogener Daten wirksam nur durch ein international abgestimmtes Vorgehen gewährleisten. Es wurden mehrere Resolutionen gefasst, die eine intensivere Zusammenarbeit zwischen den aus aller Welt zusammengekommenen Datenschutzbeauftragten herbeiführen sollen. So soll der Zugang von Datenschutzbehörden zur internationalen Konferenz durch ein klar geregeltes Akkreditierungsverfahren ermöglicht, ein Konzept zur Vertiefung der internationalen Zusammenarbeit der Aufsichtsbehörden entwickelt und die Zusammenarbeit zwischen den Datenschutzbehörden im Bereich der Durchsetzung des Datenschutzes verbessert werden.

Auf meine Initiative hin beschloss die Konferenz einstimmig eine Resolution zum Internetprotokoll Version 6 (IPv6) im Hinblick auf die einheitliche Nutzung von Identifikatoren bei der Implementierung dieses Protokolls (vgl. hierzu auch Nr. 5.6). Eine weitere Entschließung betraf den einheitlichen Datenschutz im Katastrophenfall einschließlich der Vereinfachung des datenschutzgerechten Datenaustauschs.

Die 34. Internationalen Datenschutzkonferenz 2012 in Uruguay wurde von der Regulierungs- und Kontrollabteilung für personenbezogene Daten in Uruguay (URCDP) unter dem Motto „Persönlichkeitsschutz und Technologie im Gleichgewicht" ausgerichtet. Im Fokus stand die Intensivierung der Zusammenarbeit und des Informationsaustauschs zwischen den Datenschutzbehörden in aller Welt, ein Thema, das auch in einer Resolution vertiefend behandelt wurde. Die von mir vorbereitete und von der Konferenz einstimmig angenommene Entschließung zum Cloud Computing enthält sechs grundlegende Empfehlungen für die Datenverarbeitung in der Cloud (vgl. hierzu auch unter Nr. 5.3).

Einen weiteren technologischen Schwerpunkt bildete das Thema Profiling. Die Konferenzteilnehmer erörterten die Entwicklung des Profilings auf verschiedenen Kontinenten sowohl im öffentlichen als auch im nicht-öffentlichen Bereich. Sie stellten fest, dass die Zusammenführung und Verknüpfung personenbezogener Daten zu Profilen eine zunehmende Gefahr für das Persönlichkeitsrecht darstellt. Die Gastgeber griffen die Problematik in ihrer sog. Uruguay-Erklärung auf, in der sie für eine rechtliche einwandfrei gestaltete und transparente Profilbildung eintraten.

Die Resolutionen und Erklärungen sind abrufbar unter http://www.datenschutz.bund.de.

Die 33. Internationale Konferenz hatte im Herbst 2011 eine Arbeitsgruppe eingesetzt, die Konzepte zur Vertiefung der internationalen Zusammenarbeit der Aufsichtsbehörden erarbeiten soll. Ich beteilige mich für Deutschland an den Beratungen. Der Vorsitz der Gruppe liegt bei Kanada (Privacy Commissioner of Canada – PCC) und Großbritannien (The Information Commissioner's Office – ICO). In einem nächsten Schritt wird Kanada in der Arbeitsgruppe ein Konzept für die Intensivierung der Zusammenarbeit zum Datenaustausch und zu Durchsetzung des Datenschutzes gegenüber Behörden vorlegen. Hintergrund der kanadischen Initiative dürfte sein, dass es bisher entsprechende Abkommen und abgestimmte Vorgehensweisen im Wesentlichen nur bilateral zwischen EWR/Artikel-29-Gruppe und USA/FTC gegeben hat. Jedoch bereits in der Madrid-Erklärung der 31. Internationalen Datenschutzkonferenz im Jahr 2009 wurde eine stärkere internationale Kooperation auch im öffentlichen Bereich gefordert (vgl. 23. TB Nr. 13.14).

Außerhalb der Internationalen Datenschutzkonferenz war im Frühjahr 2010 das Global Privacy Enforcement Network (GPEN) als informeller Zusammenschluss nationaler Datenschutzbehörden errichtet worden mit dem Ziel, die internationale Zusammenarbeit im Bereich der Durchsetzung des Datenschutzes im nichtöffentlichen Bereich zu verbessern. Das Netzwerk, das Anfang 2010 auf Initiative der FTC errichtet wurde, ist inzwischen auf 31 Mitglieder angewachsen. Im Mittelpunkt seiner Arbeiten stehen ein verbesserter gegenseitiger Erfahrungsaustausch, die Durchführung von Fortbildungsmaßnahmen gemeinsam mit Vertretern von Wirtschaft, Wissenschaft oder internationalen Organisationen sowie die Zusammenarbeit mit vergleichbaren Einrichtungen vor. Auch können ggf. Maßnahmen bilateraler Unterstützung und Kooperation vereinbart werden.

2.4.4 Verbesserte Zusammenarbeit der europäischen Datenschutzbehörden

Die Datenverarbeitung macht heute nicht mehr Halt an nationalen Grenzen. Datenschutzrechtliche Sachverhalte betreffen immer häufiger Personen in mehreren Mitgliedstaaten oder der gesamten EU. Für die Datenschutzbehörden ergibt sich hieraus die Notwendigkeit einer verstärkten grenzüberschreitenden Zusammenarbeit.

Bereits nach der EG-Datenschutzrichtlinie 95/46/EG bestehen die Möglichkeit und Notwendigkeit der Kooperation der nationalen Datenschutzbehörden in Sachverhalten mit grenzüberschreitender Dimension. So sieht Artikel 28 Absatz 6 vor, dass die Aufsichtsbehörden „für die zur Erfüllung ihrer Kontrollaufgaben notwendige gegenseitige Zusammenarbeit, insbesondere durch den Austausch sachdienlicher Informationen“ sorgen. Die praktische Zusammenarbeit erfolgt gegenwärtig vor allem im Rahmen der Artikel-29-Datenschutzgruppe und ihrer Unterarbeitsgruppen, insbesondere der „Technology Subgroup“ (vgl. Nr. 2.4.1.3).

Als Beispiel für die fruchtbare Kooperation der Datenschutzbehörden im Rahmen dieser Unterarbeitsgruppe möchte ich die im Verlauf des Jahres 2012 erfolgte Bewertung der neuen Datenschutzrichtlinie des Unternehmens Google hervorheben (vgl. Nr. 5.9). Die Bewertung wurde federführend durch die CNIL, die französische Datenschutzbehörde, vorgenommen. Die Unterarbeitsgruppe wurde dabei zu jedem Zeitpunkt in die technische Analyse einbezogen. Auch die Kommunikation zwischen Google und der CNIL, welche im gesamten Prozess stellvertretend für die Artikel-29-Datenschutzgruppe agierte, wurde innerhalb der Technology Subgroup abgestimmt und koordiniert. Als Ergebnis dieser Kooperation wurde am 16. Oktober 2012 seitens der Artikel-29-Gruppe ein Schreiben an Google versandt, das von den Datenschutzbeauftragten aller 27 Mitgliedstaaten unterzeichnet wurde.

Als weiteres Beispiel für gelungene Kooperation möchte ich die Zusammenarbeit der Datenschutzbehörden mit der ENISA, der Europäischen Agentur für Netz- und Informationssicherheit, zum Thema „Meldung von Datenschutzverstößen“ erwähnen. In enger Kooperation erarbeiten die Technology Subgroup und die ENISA hier eine Methodik zur Analyse des Schweregrades von Datenschutzverstößen.

Schließlich möchte ich auf die datenschutzrechtliche Bewertung des sozialen Netzwerkes Facebook hinweisen (vgl. Nr. 5.8.1). Unter Federführung der irischen Datenschutzbehörde wurde innerhalb der Technology Subgroup eine ausführliche Bewertung vorgenommen, die zur Erstellung zweier Audit Reports führte.

Die Beispiele „Google“ und „Facebook“ zeigen, wie wichtig ein einheitliches Vorgehen der Datenschutzbehörden der EU-Mitgliedstaaten in Fällen ist, in denen Personen in mehreren Mitgliedstaaten oder der gesamten EU betroffen sind.

Die Europäische Kommission hat die Globalisierung des Datenschutzes aufgriffen und schlägt in dem Entwurf der EU-Datenschutz-Grundverordnung die Einführung eines Verfahrens der verstärkten Zusammenarbeit, der Amtshilfe und der Kohärenz in Fällen vor, in denen mehrere Mitgliedstaaten von Verarbeitungsvorgängen eines Verantwortlichen betroffen sind (vgl. Nr. 2.1.1). Durch einen Abstimmungsmechanismus innerhalb des Europäischen Datenschutz-Ausschusses, des Nachfolgegremiums der Artikel-29-Gruppe, soll in diesen Fällen eine einheitliche Rechtsauslegung und Anwendungspraxis innerhalb der EU erreicht werden. Ich unterstütze dieses Ziel nachdrücklich. Hierbei muss allerdings sichergestellt sein, dass die Unabhängigkeit der Datenschutzaufsicht unangetastet bleibt und die Datenschutzbehörden „Herrinnen des Verfahrens“ bleiben. Zudem setzt eine effektive Kooperation voraus, dass die Aufsichtsbehörden mit den erforderlichen sächlichen und personellen Ressourcen ausgestattet werden.

2.4.5 OECD und Europarat

Sowohl der Europarat als auch die OECD arbeiten an der Novellierung ihrer jeweiligen Datenschutzinstrumente. Die strengeren Datenschutzregelungen in der Europäischen Union sind zwar davon nicht direkt betroffen, inspirieren aber auch die Diskussion in diesen Gremien.

Nicht nur aufgrund der großen geographischen Reichweite – 47 Staaten sind Mitglied des Europarats; die OECD hat 34 Mitgliedstaaten – tragen deren Datenschutz-Instrumente zur Verbreitung und Stärkung des Datenschutzes bei. So war das 1981 in Kraft getretene Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten („Übereinkommen 108“) das erste verbindliche internationale Instrument im Bereich des Datenschutzes. Es hat eine Vielzahl nationaler und internationaler Entwicklungen im Datenschutz initiiert und vorangebracht. Ich begrüße es, dass der Europarat beabsichtigt, das Übereinkommen 108 zu modernisieren. Grundlegende Ziele sind zum einen die Anpassung an neue Herausforderungen an den Datenschutz, die mit der technologischen Entwicklung sowie dem Internet einhergehen, wie z. B. dem Cloud Computing oder der Nutzung sozialer Netzwerke. Zum anderen soll Kohärenz mit den Datenschutzbestimmungen in der EU, die momentan einer umfassenden Reform unterzogen werden (vgl. Nr. 2.1), sichergestellt werden.

Positiv bewerte ich, dass nach den Vorschlägen für eine überarbeitete Fassung des Übereinkommens der Anwendungsbereich der Konvention weiterhin umfassend bleiben und die Koordination der Datenschutzaufsichtsbehörden verbessert werden sollen. Die Anregungen, die ich im Rahmen der Verhandlungen auf Fachebene eingebracht habe, wurden im Wesentlichen aufgegriffen. Insbesondere differenzieren die Vorschriften zum grenzüberschreitenden Datentransfer nun nach Übermittlungen zwischen Vertragsstaaten und solchen mit Nicht-Vertragsstaaten. Die Vorschriften lassen dabei Raum für strengere EU-Regelungen. Dies begrüße ich ausdrücklich, denn gerade bei der grenzüberschreitenden Datenübermittlung ist die Kompatibilität mit dem Entwurf der Datenschutz-Grundverordnung der EU von besonderer Bedeutung.

Die Revision der aus dem Jahr 1980 stammenden OECD Privacy Guidelines wurde durch eine Expertengruppe vorbereitet, bestehend aus Regierungsvertretern, Mitarbeitern von Datenschutzaufsichtsbehörden – darunter auch Mitarbeiter meiner Dienststelle –, Wissenschaftlern, Wirtschaftsvertretern und Vertretern der Zivil- und der Internetgesellschaft. Nach ihrem Vorschlag sollen die grundlegenden Begriffsbestimmungen der Guidelines, etwa die Definition personenbezogener Daten, und die Grundprinzipien der Datenverarbeitung, wie etwa die Zweckbindung und die Datensicherheit, unangetastet bleiben. Ausgeweitet und konkretisiert werden soll hingegen das Konzept der Verantwortlichkeit („Accountability“) der Daten verarbeitenden Stellen. Diese sollen dazu verpflichtet werden, den in den Guidelines niedergelegten Datenschutzgrundsätzen mit Hilfe eines Datenschutzprogramms Geltung zu verschaffen. Wichtiger Bestandteil eines solchen Datenschutzprogramms soll eine Meldepflicht für schwerwiegende Datenschutzverstöße sein, wie sie auch der Vorschlag für eine EU-Datenschutz-Grundverordnung vorsieht. Weiterhin werden die OECD-Mitgliedstaaten zu erweiterten Maßnahmen im Bereich des Datenschutzes auf nationaler Ebene aufgefordert. Hierzu gehören u. a. nationale Datenschutzstrategien und die Einrichtung von unabhängigen Datenschutzaufsichtsbehörden. Schließlich fordern die Guidelines eine stärkere internationale Zusammenarbeit im Bereich Datenschutz, inklusive Maßnahmen zur Förderung von Interoperabilität zwischen verschiedenen Datenschutzsystemen, etwa mit der APEC (vgl. Nr. 2.4.1.2). Die OECD Guidelines stellen nur Mindeststandards dar (vgl. Artikel 5 der Guidelines). Der OECD-Rat soll voraussichtlich im Frühjahr 2013 mit den Revisionsvorschlägen befasst werden.

2.5 Internationaler Datenschutz – Einzelfragen

2.5.1 SWIFT-Daten in die USA – ein Blindflug?

Die Auseinandersetzung um die Übermittlungen von „SWIFT“-Zahlungsverkehrsdaten in die USA geht weiter. Die Berichte der Gemeinsamen Kontrollinstanz Europol nähren Zweifel, ob die in dem Abkommen eingebauten Beschränkungen wirken. Für skandalös halte ich es, dass die als geheim einzustufenden Kontrollberichte nicht den Parlamenten vorgelegt werden.

Die Nutzung von Zahlungsverkehrsdaten des Dienstleisters SWIFT (Society for Worldwide Interbank Financial Telecommunication) durch US-Sicherheitsbehörden ist durch US-Medien im Jahr 2006 aufgedeckt worden. Seither ist sie ein Dauerbrenner der transatlantischen Auseinandersetzung über die Voraussetzungen, unter denen sensible Daten unverdächtiger Bürger zum Zwecke der Terrorismusbekämpfung verarbeitet werden dürfen (vgl. zuletzt 23. TB Nr. 13.6).

In den vergangenen zwei Jahren hat sich die Diskussion über das am 1. August 2010 in Kraft getretene Abkommen zwischen der Europäischen Union und den USA auf die Frage zugespitzt, in welchem Maße auf der Grundlage des Abkommens welche Daten über den Atlantik geschickt werden. Entscheidende Bedeutung kommt dabei Europol zu. Denn das Abkommen weist dem europäischen Polizeiamt eine Art Wächterrolle zu. Ohne eine positive Entscheidung, mit der Europol im Einzelfall bestätigt, das konkrete US-amerikanische Ersuchen um Übermittlung der Zahlungsverkehrsdaten halte die Grenzen des Abkommens ein, darf SWIFT keine Daten aus der EU in die USA übermitteln. Auf den Interessenskonflikt, in den Europol damit gebracht wurde, hatte ich schon in meinem letzten Tätigkeitsbericht hingewiesen (23. TB Nr. 13.6). Die datenschutzrechtlichen Kontrollen bei Europol haben meine Zweifel an dem Abkommen bestätigt. Die Gemeinsame Kontrollinstanz Europol (GKI Europol), in der auch Mitarbeiter meiner Behörde vertreten sind, hat in ihren bis zum Redaktionsschluss vorliegenden zwei öffentlichen Berichten die Probleme

angesprochen. Im ersten, 2011 vorgelegten Kontrollbericht von der GKI Europol, wurde festgestellt, dass die Ersuchen der US-Seite zu abstrakt und zu allgemein seien. Daher könne nicht wirklich überprüft werden, ob die Vorgaben des Abkommens eingehalten wurden, die Ersuchen auf das notwendige Minimum zu begrenzen. Zudem würden wesentliche Informationen zur Begründung der US-Ersuchen nur mündlich mitgeteilt und seien daher mangels einer Dokumentation einer Prüfung entzogen. Auch der zweite, 2012 veröffentlichte Bericht verdeutlicht die Schwierigkeiten bei der Anwendung des Abkommens. Zwar stellt die GKI Europol einige Fortschritte fest. Es bleibt jedoch ein großes Fragezeichen, ob die Forderung des Europäischen Parlaments erfüllt ist, den Umfang der übermittelten Daten auf das notwendige Minimum zu begrenzen. Denn die GKI Europol darf die konkreten Fakten und Zahlen zur Anwendung des Abkommens nicht veröffentlichen. Die Ersuchen, die Europol aus den USA erreichen, sind vor der ersten Prüfung durch die GKI Europol von den USA in toto als „geheim“ eingestuft worden und haben seither diese Einstufung behalten. Die GKI Europol war deshalb verpflichtet, die vollständigen Berichte über die Kontrollen ebenso als „geheim“ einzustufen. Diese sehr weit gehende Klassifizierung erschwert die Berichterstattung, Diskussion und Bewertung des Abkommens in einem Maße, das ich im Sinne des Demokratieprinzips für nicht hinnehmbar halte. Selbst die Abgeordneten der nationalen Parlamente und des Europäischen Parlaments sollen deswegen diese wichtigen Informationen zur Bewertung des Abkommens nicht erhalten. Die politische Bewertung des Abkommens liegt letztendlich in der Hand der europäischen Parlamente. Diese dürfen die Kontrollberichte allerdings nicht einsehen, auch nicht in ihren eigens für solche Fälle vorgesehenen Geheimschutzstellen. Und dies, obwohl Abgeordnete so genannte geborene Geheimnisträger sind. Diese Auffassung vertreten zumindest Europol, die Europäische Kommission und die US-Regierung. Als Konsequenz führt eine Einstufung durch die US-Seite dazu, dass die europäischen Parlamentarier nicht Kenntnis von der praktischen Umsetzung des Abkommens erlangen können, obwohl sie die politische Verantwortung tragen und darüber zu entscheiden haben, in welchem Umfang die Finanzdaten aus Europa in die USA übermittelt werden. Derartige Blindflüge darf es in der Demokratie nicht geben. Die GKI Europol hat daher entschieden, den Abgeordneten des Europäischen Parlaments in einer die Geheimschutzvorschriften von Europol achtenden Art und Weise Zugang zu den vollständigen Kontrollberichten zu gewähren. Das letzte Wort in dieser Auseinandersetzung ist noch nicht gesprochen, soviel scheint sicher.

2.5.2 Immer wieder Fluggastdaten

Flugzeuge ziehen nicht bloß Kondensstreifen am Himmel hinter sich her. Immer umfangreicher werden auch die – allerdings nicht flüchtigen – Datenspuren, die Flugpassagiere hinterlassen. Kein Wunder, dass diese Daten vielfältigen Begehrlichkeiten ausgesetzt sind.

Ob und wie von den Fluggesellschaften für geschäftliche Zwecke erhobene Passagierdaten (sog. Passenger Name Records, PNR) ohne Vorliegen von Verdachtsmomenten für Zwecke der Gefahrenabwehr und Strafverfolgung genutzt werden dürfen, gehört nunmehr schon zu den Klassikern der datenschutzrechtlichen Auseinandersetzungen. Dies gilt national, europäisch und vor allem transkontinental im Verhältnis zu den USA. Im Berichtszeitraum standen zwei Entwicklungen im Mittelpunkt: Die Abkommen mit den USA und Australien einerseits (vgl. Nr. 2.5.2.1) und der Entwurf für eine Richtlinie der Europäischen Union anderseits, mit der die europäischen Polizeibehörden selbst berechtigt würden, PNR-Daten zu polizeilichen Zwecken ohne konkreten Anlass zu erheben und zu verarbeiten (vgl. Nr. 2.5.2.2).

2.5.2.1 Übermittlung von Fluggastdaten nach Übersee

Die sehr umfangreiche Übermittlung europäischer Fluggastdaten in die USA wird auf Basis eines neuen Abkommens fortgesetzt. Immer mehr Staaten orientieren sich an diesem Vorbild. Meine kritische Bewertung daran hat sich nicht geändert.

Seit mehr als 10 Jahren verlangen US-Sicherheitsbehörden vor jedem Flug in die USA zu verschiedenen Zeitpunkten von unterschiedlichen Akteuren eine Vielzahl personenbezogener Passagierdaten und verwenden sie für Zwecke der Terrorismusbekämpfung und weitere Zwecke (vgl. zuletzt 23 TB Nr. 13.9). Selbst Spezialisten fällt es mittlerweile schwer, den vollständigen Überblick über die Vielzahl von Übermittlungsverpflichtungen zu behalten. Die vermutlich sensibelste betrifft die PNR (Passenger Name Record)-Daten, die von den Fluggesellschaften für die Durchführung einer Reise erhoben werden. Zu den PNR-Daten gehören auch Angaben zu Kreditkarten- und Telefonnummern, E-Mail- und Kontakt-Adressen und speziellen Essenswünschen.

Seit dem Sommer 2012 erfolgt die Übermittlung von PNR-Daten auf der Grundlage eines neuen zwischen der EU und den USA geschlossenen Abkommens. Ein neues Abkommen zur Übermittlung von PNR-Daten hat die EU auch mit Australien abgeschlossen. Insbesondere zu dem Abkommen mit den USA habe ich nicht nur im Grundsatz, sondern auch in verschiedenen Details Kritik geübt. Zentraler Kritikpunkt der Stellungnahme der Artikel-29-Gruppe, vom 6. Januar 2012, an der ich wesentlich mitgewirkt habe, bleibt die unverändert lange Speicherung sämtlicher Daten für 15 Jahre.

Zwar sehe ich es positiv, wenn nunmehr auf die Daten im Regelfall nach einiger Zeit nur noch „maskiert“ (ohne Nennung des Namens des jeweiligen Passagiers) zugegriffen werden soll. Dies ändert aber nichts daran, dass sämtliche Daten für den gesamten Zeitraum vollständig gespeichert bleiben. Das Abkommen lässt auch hinsichtlich der Zwecke, zu denen die Daten verwendet werden dürfen, vieles offen. Nicht zufrieden bin ich ferner mit den Rechtsschutzmöglichkeiten für europäische Bürgerinnen und Bürger nach US-amerikanischem Recht. Im Vergleich zu früheren oder vergleichbaren Regelungen enthält das neue Abkommen zwar mehr Bezugnahmen auf verschiedene US-amerikanische Gesetze. Doch bleiben erhebliche Zweifel, ob diese wirklich den Rechtsschutz für Europäer an denjenigen von US-Bürgern an-

gleichen. Eine gerichtliche Überprüfung der Speicher- und Verarbeitungspraxis der US-Behörden nach dem PNR-Abkommen bleibt Betroffenen ohne US-Wohnsitz jedenfalls weiterhin verwehrt.

Für zweifelhaft halte ich es, ob nach dem PNR-Abkommen auch Passagierdaten bloßer Überflüge ohne Landung in den USA übermittelt werden dürfen, Die US-Behörden verlangen von den Fluggesellschaften auch Passagier-Daten, wenn US-amerikanischer Luftraum nur berührt wird, etwa bei Direktflügen aus Europa in die Karibik.

Schließlich beobachte ich mit Sorge, dass immer mehr Staaten nach dem US-Modell die Vorab-Übermittlung von umfangreichen Passagierdaten fordern, darunter solche, die man auch bei bestem Willen kaum als demokratisch bezeichnen kann. Ich bin gespannt auf die Antworten aus Berlin und Brüssel.

2.5.2.2 PNR für Europa?

Die Europäische Kommission hat einen Vorstoß zur anlasslosen Speicherung von Fluggastdaten unternommen.

Werden PNR-Daten zukünftig auch von europäischen Sicherheitsbehörden ohne Vorliegen eines konkreten Verdachts genutzt und gespeichert? Die Europäische Kommission hat jedenfalls im Februar 2011 einen neuen Entwurf vorgelegt, der dies vorsieht. Schon seit vielen Jahren wurde im Rat kontrovers über das Vorhaben diskutiert. Ein erster Entwurf mit vergleichbarer Zielrichtung stammt von November 2007 (vgl. 22. TB Nr. 13.5.3), wurde aber nach heftiger Kritik zunächst nicht weiterverfolgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 16./17. März 2011 die kritischen Punkte deutlich gemacht (vgl. Kasten zu Nr. 2.5.2.2). Auch der neue Entwurf bleibe konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten durch Polizei und Strafverfolgungsbehörden geeignet und erforderlich sei, um Terrorismus und schwere Kriminalität zu bekämpfen.

Darüber hinaus fordert der Entwurf die Rechtsprechung des Bundesverfassungsgerichts gleich an zwei Stellen heraus. Zum einen würde eine verdachtslose Speicherung aller PNR-Daten eine weitere anlasslose Vorratsdatenspeicherung schaffen – dieses Mal nicht bei den Anbietern von Telekommunikationsdiensten, sondern unmittelbar bei Grenz- oder Polizeibehörden. Das Gericht hatte in seinem Urteil zur anlasslosen Vorratsdatenspeicherung (Urteil vom 2. März 2010, 1 BvR 256/08) klargestellt, dass die Wahrnehmung der Handlungsfreiheit der Bürgerinnen und Bürger nicht total erfasst und registriert werden dürfe. Dies gehöre zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland (vgl. 23. TB Nr. 6.1). Die Luft für Vorratsdatenspeicherung ist also nicht nur datenschutzpolitisch, sondern schon verfassungsrechtlich sehr, sehr dünn.

Die andere verfassungsrechtliche Frage betrifft die geplanten Datenabgleiche. Vorgesehen ist unter anderem, die Daten aller Passagiere mit vordefinierten Risikoprofilen abzugleichen. Die Nähe zur Rasterfahndung liegt auf der Hand. Eine präventive Rasterfahndung ist allerdings nach der Rechtsprechung des Bundesverfassungsgerichts unzulässig, solange keine hinreichend konkrete Gefahr für hochrangige Rechtsgüter vorliegt (Beschluss vom 4. April 2006, 1 BvR 518/02 – vgl. 21. TB Nr. 5.2.3).

Ein weiterer großer Streitpunkt betrifft eine Regelung, die in dem Entwurf der Kommission gar nicht vorkommt. Verschiedene Mitgliedstaaten und Parlamentarier wollen auch die Flüge innerhalb der Europäischen Union einbeziehen. Erfasst wären also nicht mehr nur Fernflüge, sondern auch Flüge zwischen Berlin und Paris oder Köln und Rom. Dann aber wäre es nur logisch, Bahn-, Schiffs- und Busreisende gleich mit zu erfassen. So breitet sich die „Kultur der Überwachung“ – gleich einem Ölfleck auf dem Wasser – immer weiter aus. Es ist zu hoffen, dass die verfassungsrechtlichen „Ölsperren“ dieser Entwicklung Einhalt gebieten.

Kasten zu Nr. 2.5.2.2

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011

Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!

Die EU-Kommission hat am 2. Februar 2011 einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt.

Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlass- und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen ausfindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten.

Auch der neue Entwurf bleibt konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten geeignet und erforderlich ist, um dieses Ziel zu fördern. Ein solches Zusammenspiel von Vorratsspeicherung und Rasterung von Passagierdaten ist weder mit der EU-Grundrechtecharta noch mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung vereinbar. Dies gilt insbesondere im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts, das in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten gemahnt hat:

Zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört es, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Hierfür hat sich die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen.

Ein solches System würde noch weiter reichende Eingriffe in die Bürgerrechte ermöglichen, wenn sogar Vorschläge zur Speicherung der Fluggastdaten bei Flügen innerhalb der Europäischen Union und von Daten der Bahn- und Schiffsreisenden Eingang in diese Richtlinie finden würden.

Dieser Entwurf verdeutlicht erneut, dass ein schlüssiges Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit fehlt, welches die Grundrechte der Betroffenen hinreichend gewährleistet.

Die Konferenz fordert daher die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.

2.5.3 Zur Zukunft der Grenz- und Luftsicherheitskontrollen

Grenz- und Sicherheitskontrollen machen niemandem Spaß, sind lästig und kosten Zeit. Nachdem sie über Jahrzehnte weltweit reduziert und innerhalb des Schengenraums völlig abgeschafft worden waren, erleben sie seit einiger Zeit eine Renaissance, insbesondere seit den Terroranschlägen von 2001. Kein Wunder, dass dabei zunehmend Technik eingesetzt wird.

Sowohl die Luftfahrtindustrie als auch die Politik erweisen sich als eifrige Ideengeber. Ein Konzept des Luftfahrtverbandes IATA macht schon im Titel eines großen Projekts seine Zielsetzung deutlich: die Schaffung des „Checkpoint of the Future“ (vgl. 23. TB Nr. 7.3.2). Auch im Bundesministerium des Innern wird an neuen Konzepten zur Flugsicherheit gearbeitet. Das erneute Ausrollen der Körperscanner ist nur eine Maßnahme. Daneben stehen Pläne zur Fortentwicklung der biometrischen Grenzkontrollen und von Programmen für sog. registrierte Vielreisende. Überlegungen zu „intelligenten Kontrollen“ hat schließlich auch die Europäische Kommission angestellt.

2.5.3.1 „Checkpoint of the Future“ – eine Diskriminierungsfalle?

Die Sicherheitsschleusen am Flughafen der Zukunft sollen den „gefährlichen Passagier“ aufspüren. Ungerechtfertigte Intensiv-Kontrollen und diskriminierende Praktiken sind dabei vorprogrammiert. Und ob damit wirklich mehr Sicherheit erreicht wird, erscheint fraglich.

Schon in meinem letzten Tätigkeitsbericht hatte ich über die ersten noch recht vagen Überlegungen des Luftfahrtverbandes IATA berichtet, ein Modell für einen „Checkpoint of the Future“ zu schaffen (23. TB Nr. 7.3.2). Nach den weiterentwickelten Plänen zu einer „risikobasierten Sicherheitskontrolle“ sollen mehr Passagiere in kürzerer Zeit abgefertigt werden können. Zudem sollen mehr und mehr Reisende nach einer Sicherheitsüberprüfung als „registrierte Vielreisende“ (registered travellers) in entsprechenden Programmen erfasst werden.

Das neue Gedankengebäude der IATA wirft viele Fragen auf, vor allem: Wie will man herausfinden, wer ein „gefährlicher Passagier“ ist? Denn Ziel der Sicherheitskontrolle soll es ja nicht mehr in erster Linie sein, gefährliche Gegenstände zu identifizieren.

Es ist nahe liegend, dass ein umfassendes Profiling des Passagiers erfolgt, unter Einbeziehung seines Verhaltens am Flughafen. Wesentlich wären nach den Vorstellungen der IATA auch die Daten von Fluggesellschaften und der Sicherheitsbehörden.

Viele Punkte bleiben in dem Konzept der IATA allerdings offen: Welche Annahmen sollen der Entscheidung zugrunde gelegt werden? Wer soll die Bewertungen, Vermutungen und Fakten für diese neue Art der Risikobewertung bzw. des „Scoring“ liefern, auswerten und speichern? Und wer soll letztendlich die Entscheidung treffen? Die Artikel-29-Gruppe hat sich dieses wichtigen Themas angenommen und ist dabei, genau diese Fragen mit der IATA zu diskutieren.

Ich begegne dieser neuen Grundausrichtung des IATA-Modells mit großer Skepsis. Rechtfertigt es das Motiv der Kosteneffizienz, jeden Passagier mit allen möglichen polizeilichen Datenbanken und zusätzlich noch gegen abstrakte Gefährdungsprofile abzugleichen? Ist es überhaupt möglich, jedem Passagier objektiv nachvollziehbar ein Risiko zwischen 1 und 5 oder 1 und 10 zuzuschreiben, ohne zu diskriminieren und ohne gegen Persönlichkeitsrechte zu verstoßen? Wie die IATA angibt, soll die weltweite Umsetzung des Projekts je nach anwendbarem Recht unterschiedlich sein. Der Maßstab für das rechtlich Zulässige bei der Nutzung von personenbezogenen Daten sei schließlich national. Es wird also nicht einen „Checkpoint of the Future“ geben, sondern viele.

Sollten sich die Vorstellungen von der „Sicherheitsschleuse der Zukunft“ durchsetzen, wäre die gegenwärtige Gleichbehandlung der Reisenden („one-size-fits-all“) passé. Risikoreisende, aber auch nicht registrierte Wenigflieger, Angehörige bestimmter Ethnien und Altersgruppen, Bürgerinnen und Bürger bestimmter Staaten, würden einer noch intensiveren Kontrolle als heute unterzogen, während die kommerziell besonders interessanten Geschäftskunden und andere Vielreisenden mehr oder minder durchgewunken würden. Ob sich ein solches Szenario mit unseren Vorstellungen von Persönlichkeits-, Grund- und Menschenrechten vereinbaren ließe, halte ich für zweifelhaft. Für fraglich halte ich auch, ob ein solches System wirklich zu mehr Sicherheit führen würde, lädt es doch mutmaßliche Terroristen geradezu ein, in die wenig kontrollierte Gruppe der registrierten Vielflieger eingereiht zu werden.

Ich werde mich jedenfalls dafür einsetzen, dass die Persönlichkeitsrechte der Passagiere auch bei der Weiterentwicklung der Sicherheit am Flughafen nicht abstürzen.

2.5.3.2 Vom Nackt- zum Körperscanner

Begleitet von einer intensiven öffentlichen Auseinandersetzung hatte das Bundesministerium des Innern (BMI) Körperscanner für zehn Monate erprobt. Die Geräte wur-

den danach als zu fehleranfällig wieder in die Forschungsstelle verbracht. Nun werden Geräte mit aktualisierter Software eingesetzt.

Die Erprobung des Körperscanners war ein Schwerpunktthema in meinem letzten Tätigkeitsbericht (23. TB Nr. 7.3.1). Das Bundesministerium des Innern hatte erstmals probeweise einen Körperscanner an einem deutschen Flughafen eingesetzt – und nach einer zehnmonatigen Testphase am Hamburger Flughafen festgestellt, die Geräte seien noch zu fehleranfällig. Sie wurden wieder zurück in die Forschungsstelle der Bundespolizei gebracht.

Für die Passagiere war die Teilnahme an der Erprobung freiwillig. Darauf hatte ich Wert gelegt. Die Geräte erfüllten im Wesentlichen die Voraussetzungen, auf die sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung geeinigt hatte (abgedruckt im 23. TB S. 89). Wichtig ist insbesondere, dass die eingesetzten Geräte im Vergleich zu früheren Modellen, die in der Presse auch als „Nacktscanner" bezeichnet worden waren, keine Bilder von wirklichen Körpern generierten. Das Bundesministerium des Innern hatte mir mitgeteilt, dass es diese Anforderungen teilt. Die modernen Körperscanner verwenden stattdessen Piktogramme („typisierte Strichmännchen"), auf die ein auffälliger Gegenstand projiziert wird.

Seit Dezember 2012 werden bei der Sicherheitskontrolle wieder Körperscanner eingesetzt, dieses Mal am Frankfurter Flughafen. Weiterhin ist dort niemand gezwungen, sich vom Körperscanner durchleuchten zu lassen. Zu der Sicherheitskontrolle mittels Körperscanners gibt es für jeden Passagier weiterhin eine Alternative. Konkrete Ergebnisse oder eigene Kontrollerkenntnisse zu diesen Geräten habe ich noch nicht. Die Entscheidung, sie wieder einzusetzen, wurde kurz vor Redaktionsschluss getroffen. Mir ist von der Bundespolizei mitgeteilt worden, es handele sich der Art nach um denselben Gerätetyp, der auch in Hamburg verwendet wurde. Ich werde den Einsatz der Geräte weiterhin kritisch begleiten und die Einhaltung der datenschutzrechtlichen Voraussetzungen konzeptionell und vor Ort überprüfen.

2.5.3.3 Die Zukunft der biometrischen Grenzkontrolle

Das Bundesministerium des Innern (BMI) will die bestehenden Projekte zur biometrischen Grenzkontrolle zusammenfassen.

Das BMI hat Pläne zur Fortentwicklung der biometrischen Grenzkontrollen auf deutschen Flughäfen. Eine Zusammenführung der bisherigen Projekte scheint auch mir geboten. Gegenwärtig werden am Flughafen Frankfurt zwei parallele biometrische Erkennungsverfahren betrieben.

Im Rahmen der „automatisierten biometriegestützten Gesichtserkennung (ABG)" identifizieren sich freiwillig registrierte Reisende („registered travellers") bei der Einreise durch einen Abgleich der Iris. Dafür werden die Iris gescannt und die Übereinstimmung mit einem lokal und mit Einverständnis des Betroffenen gespeicherten Bild der Iris festgestellt (vgl. 22. TB Nr. 4.5.2 und 23. TB Nr. 3.5). EU-Bürger mit biometrischen Reisedokumenten können sich im Rahmen des Projektes „EasyPass" an bestimmten Kontrollschleusen auch für eine automatisierte Kontrolle entscheiden, bei der ein Abgleich der Gesichtsfelder erfolgt. Der Abgleich erfolgt über die im Pass gespeicherten biometrischen Daten, so dass eine zusätzliche lokale Speicherung nicht erforderlich ist (vgl. 22. TB Nr. 6.4 und 23. TB Nr. 3.5).

Die technischen Anforderungen zur Datensicherheit waren in beiden Projekten im Wesentlichen erfüllt.

Bedenken hatte ich allerdings in rechtlicher Hinsicht. Der Irisabgleich ist durch Entscheidungen des Gesetzgebers überholt, bei amtlichen Ausweisdokumenten den Fingerabdruck und das Gesichtsbild als die zulässigen Formen der biometrischen Identifikation zu verwenden. Zudem legt der Schengener Grenzkodex (SGK) europaweit fest, wie die Mitgliedstaaten Grenzkontrollen an den Außengrenzen des Schengenraumes durchzuführen haben. Bei Flügen in den Schengenraum findet diese Grenzkontrolle am Frankfurter Flughafen statt. Wie der SGK in Artikel 7 Absatz 2 vorschreibt, dürfen die Bürgerinnen und Bürger der EU bei der Einreise in den Schengenraum keiner systematischen Datenbankabfrage unterworfen werden. Die Kontrollschleusen sind aber in beiden Systemen technisch so eingestellt, dass sie jeden die Schleuse passierenden Reisenden einer Vollabfrage unterziehen. Diese Praxis hielt ich für unvereinbar mit der Vorgabe der nichtsystematischen Abfrage gemäß SGK.

Meine Anmerkungen hat das BMI bei Fortentwicklung der biometrischen Grenzkontrollen aufgenommen. Es hat angekündigt, beide Projekte mit ihren unterschiedlichen Zwecksetzungen unter dem EasyPass-RTP (Registered Traveller Programme) zusammenzuführen und dabei auf den Irisabgleich zu verzichten. Vorgesehen ist, die EasyPass-Kontrollschleusen zum Ende des Jahres 2013 auf den fünf passagierstärksten Flughäfen auszurollen. Ein weiteres Jahr später soll die Funktionalität der Schleusen so ergänzt werden, dass auch Drittstaatler mithilfe einer automatisierten Grenzkontrolle einreisen können, sofern sie sich zuvor einer Sicherheitsüberprüfung unterzogen und sich haben registrieren lassen. Dann können durch ein und dieselbe automatisierte Schleuse sowohl die EU-Bürger als auch die registrierten Drittstaatsangehörigen gehen. Um der Regelung des Artikels 7 Absatz 2 SGK zukünftig Rechnung zu tragen, werden die EasyPass-Kontrollschleusen mit einem Zufallsgenerator ausgestattet.

Die Ankündigungen aus dem BMI begrüße ich. Den Fortgang des Projekts werde ich weiterhin kritisch begleiten.

2.5.3.4 Nicht besonders intelligent: „smart borders"

Die Europäische Kommission plant unter dem Schlagwort der „intelligenten Grenzen" die Errichtung eines Einreise-/Ausreiseregisters und will die Programme für „registrierte Reisende" stärken. Besonders kritisch sehe

ich das geplante Register, mit dem alle Grenzübertritte von Drittstaatsangehörigen erfasst werden sollen.

Die Europäische Kommission sagt, die Außengrenzen der Europäischen Union sollten „intelligenter“ werden. Die groben Linien dafür hat sie in einer Mitteilung aus dem Oktober 2011 skizziert. Intelligente Grenzen bedeuten danach, die Ein- und Ausreise aller Nicht-EU-Bürger elektronisch zu erfassen und die Einreise für Drittstaatsangehörige zu erleichtern, wenn sie sich zuvor überprüfen und registrieren lassen. Allerdings sollen Drittstaatsangehörige nicht verpflichtet werden, sich vor der Einreise anzumelden, so wie man es aus den USA kennt (Electronic System for Travel Authorization – ESTA).

Besonders kritisch betrachte ich das Kernstück der Überlegungen: die Errichtung eines sog. Einreise-/Ausreise-Registers (entry/exit). Dahinter verbirgt sich eine riesige Datei, in der jeder Grenzübertritt von allen Drittstaatsangehörigen unabhängig davon gespeichert werden soll, ob sie zur Einreise ein Visum brauchen. Begründet wird dies damit, die Grenzübertritte so effektiver kontrollieren zu können. Auch gäbe es gegenwärtig keine verlässlichen Daten über die Anzahl von sog. overstayers, also solcher Einreisenden, die länger als erlaubt in der EU bleiben. Dies sei erheblich, weil „overstayer“ das Hauptproblem der irregulären Zuwanderung in der EU seien.

Ich habe schon Zweifel, ob es überhaupt mit verhältnismäßigem Aufwand machbar ist, angesichts der vielen Land- und Seegrenzen in Europa ein solches System aufzubauen und zu verwalten. Die USA mit ihren geografisch bedingt weitaus einfacher zu kontrollierenden Außengrenzen haben bereits vor Jahren mit dem Aufbau eines solchen Systems begonnen – bisher ohne durchschlagenden Erfolg. Unabhängig von der Machbarkeit eines solchen Systems ist mir auch nicht ersichtlich, wie die Erforderlichkeit und Verhältnismäßigkeit einer Datenbank diesen Ausmaßes begründet werden kann. Denn gerade im Hinblick auf die sog. overstayer ist schon nicht klar, welchen konkreten Beitrag das System erbringen könnte. Die bloße Erlangung genauerer Zahlen zur irregulären Einwanderung könnte die Maßnahme jedenfalls nicht begründen.

Der zweite Baustein neben dem Einreise-/Ausreiseregister stellt das Registrierungsprogramm für Vielreisende dar („Registered Traveller Programme“ – RTP). Aus Sicht der Kommission wäre es nicht sinnvoll, sämtliche Drittstaatsangehörige, die in den Schengen-Raum einreisen, ein und derselben Kontrolle zu unterwerfen. Diesen vielreisenden Drittstaatsangehörigen würde der Grenzübertritt erleichtert, wenn sie sich zuvor einer Sicherheitsüberprüfung unterzogen haben und sich registrieren lassen. An dieser Stelle ergibt sich der konkrete Berührungspunkt mit dem „Checkpoint of the Future“ (vgl. Nr. 2.5.3.1) und den Plänen aus dem Bundesinnenministerium zum Easy-Pass-RTP (vgl. Nr. 2.5.3.3).

Nach den bisherigen Überlegungen sollen beide Systeme biometrische Identifizierungen vorsehen. Es bleibt auch insofern abzuwarten, was die Gesetzentwürfe hierzu konkret sagen werden und wie dabei den datenschutzrechtlichen Anforderungen – insbesondere im Hinblick auf die Vermeidung exzessiver Vorratsdatenspeicherungen – Rechnung getragen werden kann.

Abschließend erlaube ich mir die ketzerische Frage, ob es denn wirklich intelligent ist, auf alle möglichen Sicherheitsgefährdungen nur eine Antwort zu finden: Zusätzliche Datenspeicherung, umfassende Registrierung und Rasterung auf Vorrat.

2.5.4 Datenschutzentwicklungen in den USA

Ein von der US-Regierung vorgelegtes Grundlagenpapier enthält eine „Consumer Privacy Bill of Rights“. Die Federal Trade Commission (FTC) veröffentlichte einen Bericht mit Empfehlungen zum Daten- und Verbraucherschutz in einer vernetzten Welt. Verbindliche Datenschutzregeln für den nicht-öffentlichen Bereich fehlen in den USA aber leider immer noch weitgehend.

Im Februar 2012 – fast zeitgleich mit den Vorschlägen der EU-Kommission zur EU-Datenschutzreform (vgl. Nr. 1) – legte die US-Regierung ein Weißbuch mit dem Titel „Consumer Data Privacy in a Networked World: A Framework of Protecting Privacy and Promoting Innovation in the Global Digital Economy” vor. Das Papier enthält eine Zusammenfassung von Verbraucherrechten in der digitalen Welt („Consumer Privacy Bill of Rights“) mit sieben grundlegenden Anforderungen an die Verarbeitung personenbezogener Daten: Transparenz, Information, Zweckbindung, Erforderlichkeitsgrundsatz/Datensparsamkeit, Betroffenenrechte, Verantwortlichkeit und Datensicherheit. Die Consumer Privacy Bill of Rights soll – so die Ankündigung der Obama-Administration – vom Kongress möglichst mit einer gesetzlichen Regelung umgesetzt werden. Allerdings sind seit der Vorlage keine entsprechenden Aktivitäten bekannt geworden, weder aus dem US-Senat noch aus dem Repräsentantenhaus. Auch die an den Kongress gerichtete Forderung im Weißbuch, die Befugnisse der FTC zur Durchsetzung der Verhaltensregeln zu erweitern, ist bisher nicht umgesetzt.

Der Entwurf setzt ganz wesentlich auf Selbstregulierung und verzichtet auf verbindliche Datenschutzregeln, wie sie etwa im EU-Datenschutzrecht vorgesehen sind und nach den Kommissionsvorschlägen auch erhalten bleiben sollen (vgl. Nr. 1.1). In diesem Sinne schlägt die US-Regierung vor, dass im Rahmen von „Multi-Stakeholder“-Verfahren in den verschiedenen Sektoren Verhaltensregeln erarbeitet werden, die die in der Consumer Privacy Bill of Rights gewährten Rechte konkretisieren. Bei der Erarbeitung der rechtsverbindlicher Verhaltensregeln sollen auch internationale Partner wie u. a. die Europäische Union eingebunden werden. Der Safe-Harbor-Rechtsrahmen könnte so möglicherweise künftig durch konkretere Verhaltensregeln ergänzt werden.

Die FTC hat 2012 den Bericht „Protecting Consumer Privacy in an era of rapid change“ veröffentlicht. Darin empfiehlt sie den Unternehmen best practice-Lösungen zu erarbeiten und einzusetzen. Solche Lösungen sind u. a. privacy by default und privacy by design. Weiterhin gehört dazu, Verbrauchern verstärkte Kontrolle über ihre

Daten einzuräumen, beispielsweise durch vereinfachte Wahlmöglichkeiten und größere Transparenz.

Besonderen Handlungsbedarf sieht die FTC in folgenden Bereichen:

– do not track (Integration im Web-Browser)

– mobile services (bessere Information der Verbraucher)

– data brokers (höhere Transparenz bezüglich deren Datenverarbeitung)

– large platform providers (Gefahr der umfassenden Beobachtung)

– sector specific enforceable self regulatory codes, die vom Departement of Commerce mit Industrievertretern entwickelt werden sollen. Dies dient der Umsetzung des Weißbuchs der US-Regierung (s. o.).

Auch hier wurde der Kongress aufgefordert, durch klare gesetzliche Regeln für Unternehmen sicherzustellen, dass die Anwendung von datenschutzrelevanten Lösungen nicht zu wirtschaftlichen Nachteilen führt. Gefordert wurden auch Regelungen zur Datensicherheit und Datenverlusten sowie angemessene Auskunftsrechte für die Betroffenen. Ich gehe davon aus, dass die FTC ihre Ziele weiterverfolgen wird, auch wenn eine entsprechende Kongressbefassung noch aussteht.

Meine durch mehrere Besuche und Gegenbesuche in den Jahren 2011 und 2012 erlangten guten Kontakte zur FTC werde ich auch künftig vertiefen. Allerdings wäre es wünschenswert, wenn auf US-Seite über durchaus bedenkenswerte Vorschläge und Ankündigungen hinaus auch verbindliche Datenschutzregeln beschlossen würden, die dem in Europa bereits seit langem gewährleisteten Schutzniveau entsprechen. Dies wäre nicht nur im Sinne der Bürgerinnen und Bürger beiderseits des Atlantiks, sondern würde auch den transatlantischen Informations- und Datenaustausch, etwa im Rahmen von Cloud-Diensten (vgl. Nr. 5.3), fördern.

2.5.5 Foreign Account Tax Compliance Act – FATCA

Zur Umsetzung von FATCA haben EU-Mitgliedstaaten, darunter Deutschland, ein Musterabkommen mit den USA erarbeitet. Dabei geht es auch um Datenschutz.

Die Umsetzung von FATCA (vgl. Kasten zu Nr. 2.5.5) hat erhebliche datenschutzrechtliche Probleme aufgeworfen. So stellte sich die Frage, ob die Datenübermittlung an die US-Steuerbehörde auf der Grundlage von §§ 4b und 4c BDSG oder auf Basis einer Einwilligung zulässig ist. Klärung sollen bilaterale Abkommen bieten, auf deren Inhalt sich fünf EU-Mitgliedstaaten (Frankreich, Italien, Spanien, Vereinigtes Königreich und Deutschland) mit den USA verständigt haben. Ein entsprechendes Musterabkommen wurde am 26. Juli 2012 vorgestellt. Dabei verpflichten sich die fünf Staaten, von den in ihrem Gebiet ansässigen Finanzinstituten die Informationen über für US-Kunden geführte Konten zu erheben und der US-Behörde zur Verfügung zu stellen. Im Gegenzug verpflichten sich die USA, alle Finanzinstitute des jeweiligen Vertragspartners von der Pflicht auszunehmen, mit der US-Steuerbehörde Vereinbarungen abzuschließen, um in den USA Quellensteuereinbehalte unter FATCA zu vermeiden.

Dieses Musterabkommen schafft einen Rahmen für die Meldung bestimmter Kontodaten durch die Finanzinstitute an ihre jeweiligen Steuerbehörden mit anschließendem Austausch der betreffenden Daten im Rahmen der bestehenden bilateralen Doppelbesteuerungsabkommen. Derzeit bereitet das Bundesministerium der Finanzen (BMF) das bilaterale Abkommen zwischen Deutschland und den USA vor. Weiterhin wird eine nationale Rechtsgrundlage für den Transfer der Daten von den Finanzinstituten an die nationalen Finanzbehörden erarbeitet. Ich war von Beginn an durch das BMF in das Verfahren eingebunden und habe mich für die Einhaltung eines angemessenen Datenschutzniveaus eingesetzt.

Auch die Artikel-29-Gruppe der Europäischen Datenschutzbeauftragten hat sich mit dem Thema befasst. Ihr Vorsitzender hat in einem Schreiben vom 21. Juni 2012 die Generaldirektion Steuern und Zollunion (TAXUD) der Europäischen Kommission auf die datenschutzrechtlichen Problemstellungen von FATCA hingewiesen.

Nach derzeitigem Verhandlungsstand soll im Abkommen selbst eine Zweckbindungsregelung verankert werden. Entgegen meinen Vorstellungen sollen aber die verfahrensrechtlichen Sicherungen sowie die technischen und organisatorischen Maßnahmen zur Datensicherheit in einer bloßen Durchführungsvereinbarung zum Abkommen geregelt und damit nicht unmittelbar Vertragsinhalt werden.

Kasten zu Nr. 2.5.5

Foreign Account Tax Compliance Act – FATCA

Der Foreign Account Tax Compliance Act „FATCA“ ist ein im März 2010 in Kraft getretenes US-Gesetz zur Erfassung von Vermögenswerten von in den USA steuerpflichtigen Personen und Gesellschaften auf Konten im (US-)Ausland.

Kern von FATCA sind erweiterte Melde- und Berichtspflichten von Banken und sonstigen Finanzinstituten im Ausland (Foreign Financial Institutions – FFIs) gegenüber der amerikanischen Steuerbehörde (Internal Revenue Service – IRS). Zur Aufklärung von Steuerdelikten müssen steuerlich relevante Informationen über US-Personen weitergegeben werden. Neben Einlagenkonten, Depots und Beteiligungen bei Banken, die bereits durch die sogenannten QI-Abkommen erfasst werden, sind u. a. auch Fondsgesellschaften und bestimmte Versicherungsverträge wie Renten- und Kapitallebensversicherungen betroffen.

Durch FATCA müssen alle FFIs auf Basis einer vertraglichen Regelung mit der amerikanischen Steuerbehörde die Konten ihrer Geschäftspartner auf eine potentielle Steuerpflicht in den USA hin überprüfen und mit Einverständnis des US-Kunden regelmäßig detaillierte Meldungen bzgl. der steuerpflichtig kategorisierten Konten und Zahlungen an die IRS übermitteln. Zu den betreffenden Daten gehören unter anderem Namen, Adressen und US-Steuernummern der betreffenden Kunden sowie Transaktionsdaten und Salden ihrer Konten. Die US-Kunden müssen diesem Eingriff in das Bankgeheimnis ausdrücklich zustimmen und zugunsten der US-Behörden umfassend auf das Bankgeheimnis verzichten. Tun sie dies nicht, müssen die betreffenden Finanzintermediäre ihre Geschäftsbeziehungen zu diesen Kunden beenden. Zu den Betroffenen zählen nicht nur in Deutschland lebende US-Bürger, sondern auch europäische Bürger, wenn sie in den USA steuerpflichtig sind.

Die Nichtteilnahme eines FFIs ahndet das IRS mit einem Einbehalt (Quellenbesteuerung) in Höhe von 30 Prozent auf alle Zahlungen an das FFI, die auf einen US-Vermögenswert zurückzuführen sind. FATCA stellt die FFIs somit weltweit vor die Wahl, entweder personenbezogene Daten von US-Kunden den US-Behörden zugänglich zu machen oder aber einen Quellensteuerabzug auf die US-Wertpapiererträge in Kauf zu nehmen.

3 Grundsatzangelegenheiten

3.1 Unabhängigkeit der Datenschutzbehörden

Das Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Oktober 2012 zur mangelnden Unabhängigkeit der österreichischen Datenschutzkommission ist weitgehend auf meine Rechtsstellung übertragbar.

Bereits im Jahr 2010 hatte der EuGH in einem Vertragsverletzungsverfahren entschieden, dass die Organisation der deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich auf Landesebene nicht den in der EG-Datenschutzrichtlinie 95/46 festgelegten Anforderungen an eine „völlige Unabhängigkeit“ genügt (Urteil vom 9. März 2010, C-518/07 – vgl. 23. TB Nr. 2.1). Die unabhängige Stellung der Datenschutzbehörden solle gewährleisten, dass diese ihre Aufgaben frei von äußerer Einflussnahme wahrnehmen könnten. Jegliche Form politischer oder institutioneller Einflussnahme, etwa in Form einer staatlichen Aufsicht, oder auch nur der Anschein staatlicher Beeinflussung sei hiermit unvereinbar. Inzwischen haben die Länder die Rechtsstellung ihrer Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich an die Vorgaben des EuGH angepasst.

Im öffentlichen Bereich kommt es sogar in noch viel stärkerem Maße als bei der Datenschutzkontrolle über die Wirtschaft darauf an, dass die Exekutive keinerlei Einfluss auf die Aufgabenwahrnehmung der Kontrollbehörde nehmen kann, da sie ihrerseits durch diese überwacht wird. Das BMI hat bislang allerdings keine Konsequenzen aus diesem Urteil gezogen.

Mit Urteil vom 16. Oktober 2012 (C-614/10) hat der EuGH seine Rechtsprechung zu den Anforderungen an die „völlige Unabhängigkeit“ der Datenschutzbehörden bestätigt und erstmals auf den öffentlichen Bereich ausgedehnt. Gegenstand des von der Europäischen Kommission eingeleiteten Vertragsverletzungsverfahrens war die Rechtsstellung der österreichischen Datenschutzkommission (DSK), die in Österreich sowohl die Datenschutzkontrolle im öffentlichen als auch im nicht-öffentlichen Bereich wahrnimmt. Die Bundesrepublik Deutschland ist dem Verfahren als Streithelferin zur Unterstützung Österreichs beigetreten.

Es überrascht nicht, dass der EuGH in dem Verfahren gegen die Republik Österreich erneut betont, die europarechtlich geforderte völlige Unabhängigkeit der Datenschutzbehörden sei umfassend zu verstehen. Völlige Unabhängigkeit bedeute nicht nur den Ausschluss unmittelbarer Einflussnahme in Form von Weisungen, sondern auch jeder Form mittelbarer Einflussnahme staatlicher Stellen, die zur Steuerung der Entscheidungen der Datenschutzbehörde geeignet sei. Hiermit nicht zu vereinbaren sei u. a., dass das geschäftsführende Mitglied der österreichischen DSK ein der Dienstaufsicht unterliegender Bundesbeamter sei. Es könne nicht ausgeschlossen werden, dass das geschäftsführende Mitglied der DSK sich bei seinen Entscheidungen durch die die Dienstaufsicht führende Bundesbehörde beeinflussen lasse. Weiterhin monierte der EuGH die organisatorische Eingliederung der DSK in das Bundeskanzleramt, welches nach österreichischem Recht die Sach- und Personalausstattung der DSK bereitstellt. Dass die Geschäftsstelle der DSK aus Beamten besteht, die dienst- und besoldungsrechtlich dem Bundeskanzleramt zugeordnet sind und daher auch dessen Dienstaufsicht unterliegen, berge die Gefahr der Beeinflussung der DSK-Entscheidungen. Das Bundeskanzleramt werde schließlich selbst durch die DSK kontrolliert.

Auch wenn aus dem Beitritt der Bundesrepublik Deutschland als Streithelferin zur Unterstützung Österreichs keine unmittelbare Rechtswirkung für Deutschland ausgeht, entfaltet das Urteil eine deutliche Signalwirkung. Die durch das BDSG vorgegebene Rechtsstellung des BfDI ist der vom EuGH beanstandeten Rechtslage in Österreich in vielfacher Hinsicht vergleichbar: Der BfDI untersteht der Rechtsaufsicht der Bundesregierung und der Dienstaufsicht des BMI. Organisatorisch ist er zudem beim BMI eingerichtet. Die Mitarbeiter des BfDI sind Bedienstete des BMI, das über Stellenbesetzungen und Beförderungen mitentscheidet und die Dienstaufsicht über die Mitarbeiter des BfDI ausübt.

Die Bundesrepublik Deutschland sollte sich eine dritte Lektion aus Luxemburg ersparen und die Rechtsstellung des BfDI dem Erfordernis völliger Unabhängigkeit anpassen. Solange dies noch nicht geschehen ist, müssen die bestehenden Rechtsvorschriften im Sinne der europa-

rechtlich geforderten völligen Unabhängigkeit ausgelegt werden. Ich bin mit dem Bundesministerium des Innern über diese Frage im Gespräch.

3.2 Die Verwaltung wird elektronisch

Die Digitalisierung macht um die öffentliche Verwaltung keinen Bogen. Der hierfür vorgesehene Rechtsrahmen muss den Datenschutz garantieren und zugleich die Transparenz von Verwaltungshandeln verbessern.

3.2.1 Die E-Akte – Das Ende der Übersichtlichkeit

Die elektronische Aktenführung wirft einige datenschutzrechtliche Fragen auf, die sich nicht einfach beantworten lassen.

Der Übergang zur elektronischen Aktenführung ist im vollen Gange. Einige Behörden haben ihre Aktenführung bereits auf eine elektronische Form umgestellt, in vielen Bereichen wird an entsprechenden Vorhaben gearbeitet. Allein in diesem Bericht beschäftige ich mich mit verschiedenen Fragestellungen im Zusammenhang mit der elektronischen Aktenführung:

– Elektronische Kriminalakte bei der Bundespolizei (vgl. Nr. 7.6.1)

– E-Akten beim Bundesamt für Verfassungsschutz und beim BND (vgl. Nr. 7.7.3)

– E-Akten und elektronischer Postverkehr bei der Bundesagentur für Arbeit (vgl. Nr. 12.2.1)

– Automatisierte Personalakte (vgl. Nr. 13.3)

Nicht nur im E-Government-Gesetz (vgl. Nr. 3.2.3), sondern auch in einzelnen Verwaltungsbereichen sollen spezialgesetzliche Rahmenbedingungen für die Einführung elektronischer Akten geschaffen werden, z. B. im Sicherheitsüberprüfungsgesetz (vgl. Nr. 7.8.1), durch den Entwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten (vgl. Nr. 8.13) oder den Entwurf eines Gesetzes zur Einführung der elektronischen Akte in Strafsachen.

Sofern in den Akten personenbezogene Daten gespeichert werden, führt die elektronische Aktenhaltung im Vergleich zur klassischen Papierakte zu erheblich höheren Risiken für den Datenschutz. Denn Daten in elektronischen Akten können leichter ausgewertet, mit anderen Daten zusammengeführt oder verändert werden als dies in Papierakten möglich ist. Deshalb bedarf es bei der Einführung von elektronischen Akten deutlich höherer Anforderungen an die technischen und organisatorischen Maßnahmen zum Datenschutz, die jedoch grundsätzlich mit den in § 9 BDSG und der dazugehörenden Anlage genannten Instrumenten abgedeckt werden können.

Darüber hinaus verschwimmt mit der elektronischen Aktenführung die hergebrachte Aufteilung behördlicher Datenverarbeitung in (Papier-)Akten und elektronisch erschließbare Dateien: Während die Akte in klassischer Weise dazu dient, das behördliche Vorgehen zu dokumentieren und die jeweiligen Einzelfälle zu bearbeiten, ist es der Sinn (in der Regel automatisierter) Dateisysteme, Daten strukturiert und aktenübergreifend vorzuhalten, um sie besser auswerten und mit anderen Daten verknüpfen zu können. Vor allem das bereichsspezifische Datenschutzrecht knüpft an die Verarbeitung personenbezogener Daten in Akten einerseits und die dateimäßige Verarbeitung andererseits auch unterschiedliche materiellrechtliche Anforderungen (vgl. Nr. 7.7.3 für den Bereich der Nachrichtendienste).

Die elektronische Aktenführung wird in der Regel durch Dokumentenmanagementsysteme (DMS) unterstützt, die das Auffinden und Bearbeiten einzelner Vorgänge oder Dokumente im Vergleich zur klassischen Papierakte deutlich erleichtern. Je nach Ausgestaltung enthalten bereits die im DMS gespeicherten Metadaten personenbezogene Daten, nach denen im System recherchiert werden kann. In diesem Falle handelt es sich bei dem DMS um eine automatisierte Verarbeitung im Sinne von § 3 Absatz 2 BDSG, was entsprechende Konsequenzen etwa für die zu treffenden technischen und organisatorischen Maßnahmen nach der Anlage zu § 9 BDSG hat. Das gleiche gilt grundsätzlich auch dann, wenn die in den Dokumenten der elektronischen Akte enthaltenen personenbezogenen Daten recherchierbar und auswertbar gespeichert sind, sei es, weil es sich um originär elektronische Dokumente handelt oder um eingescannte Dokumente, die mit einer OCR-Software ausgewertet werden können.

Weil das Führen elektronischer Akten in der Regel als automatisierte Verarbeitung anzusehen ist, bedarf es entsprechender Schutzmaßnahmen. Auch bei der elektronischen Aktenführung muss gewährleistet sein, dass die gespeicherten personenbezogenen Daten nicht schrankenlos ausgewertet oder aktenübergreifend miteinander verknüpft werden können. Hierzu bedarf es technischer Lösungen, indem etwa Datenformate gewählt werden, die eine Auswertbarkeit verhindern oder erschweren. Bei der Konzeption von DMS ist darauf zu achten, dass im Hinblick auf die Metadaten das Prinzip der Datenvermeidung und Datensparsamkeit beachtet wird und durch entsprechende Zugriffs- und Abschottungsmechanismen keine unzulässigen Zugriffe oder Verknüpfungen stattfinden. Die technischen und organisatorischen Vorgaben sind durch rechtliche Rahmenbedingungen etwa zur Gewährleistung der Zweckbindung zu flankieren.

3.2.2 Die gescannte Akte – Projekt RESISCAN

Für das rechtssichere Einscannen von Papierdokumenten liegt inzwischen der Entwurf der Technischen Richtlinie vor.

Das Führen elektronischer Akten erfordert regelmäßig die Digitalisierung von Papierdokumenten, die die Behörden von Bürgerinnen und Bürgern, Unternehmen und sonstigen Dritten erhalten. Nachhaltige Effektivitätsgewinne

lassen sich nur erzielen, wenn diese Papierdokumente eingescannt und die Originale vernichtet werden können („ersetzendes Scannen“).

Das E-Government-Gesetz (EGovG, vgl. Nr. 3.2.3) soll die rechtlichen Voraussetzungen für die Verwendung eingescannter Dokumente im Rechtsverkehr schaffen. Die entsprechende Vorschrift (§ 7 EGovG-E) fordert die bildliche und inhaltliche Übereinstimmung von Papieroriginal und elektronischer Kopie, wobei die verwendeten Verfahren dem Stand der Technik entsprechen müssen.

Die für die praktische Umsetzung festzulegenden technischen Einzelheiten sollen Bestandteil einer Technischen Richtlinie (TR RESISCAN) sein, an deren Entwicklung das Bundesamt für die Sicherheit in der Informationstechnik (BSI) – unter meiner Mitwirkung – zurzeit arbeitet. Die TR RESISCAN soll nicht die Prüfung der Zulässigkeit des Scannens an sich ersetzen, die sich aus anderen Rechtsvorschriften, etwa dem EGovG, ergeben muss. Bei der Festlegung des Schutzbedarfs und der darauf basierenden technischen Anforderungen orientiert sich die TR RESISCAN an der Systematik des IT-Grundschutzes. Die Beratungen standen bei Redaktionsschluss kurz vor dem Abschluss. Ich rechne mit der baldigen Veröffentlichung im Bundesanzeiger.

Bei der Ausarbeitung eines zusätzlichen erläuternden Dokuments, des „rechtlichen Anhangs“, wurde diskutiert, inwieweit das Scannen aus datenschutzrechtlicher Sicht einen eigenständigen Vorgang des Verarbeitens oder Nutzens personenbezogener Daten darstellt, der einer Rechtsgrundlage bedarf. Diese Frage verliert allerdings dann an Relevanz, wenn das EGovG verabschiedet wird, da dann eine Rechtsvorschrift existiert. Für spezielle Bereiche, beispielsweise für Personalakten (vgl. Nr. 13.2), bestehen ohnehin spezifische Vorschriften.

3.2.3 Ein Gesetz für das E-Government

Mit dem E-Government-Gesetz soll die Verwaltung internettauglich werden. Zugleich sollen die Voraussetzungen zur elektronischen Aktenführung geschaffen werden – das wirft einige datenschutzrechtliche Fragen auf, die sich nicht einfach beantworten lassen.

Die Bundesregierung hat am 19. September 2012 den Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung und zur Änderung weiterer Vorschriften beschlossen und dem Bundesrat zugeleitet. Bei Redaktionsschluss befand sich der Gesetzentwurf in den parlamentarischen Beratungen des Deutschen Bundestages. An der vorausgegangenen Ressortabstimmung habe ich mich intensiv beteiligt.

Der Entwurf besteht aus zwei Teilen: Artikel 1 enthält das eigentliche E-Government-Gesetz (EGovG), in den weiteren Artikeln wird eine Vielzahl von Bundesgesetzen geändert und an die elektronische Verwaltung angepasst.

Die Mehrzahl der Regelungen betrifft Fragen der Verwaltungsorganisation sowie der Rechtsverbindlichkeit elektronischen Handelns von Verwaltung und Bürgern. Gleichwohl wirken sich die Vorschriften auf Belange von Datenschutz und Datensicherheit aus. Nicht zuletzt ergibt sich durch – allerdings nur zaghafte – Ansätze zu Open Government und Open Data auch eine Verzahnung mit dem freien Zugang zu Informationen der öffentlichen Verwaltung (vgl. meinen 3. TB zur Informationsfreiheit Nr. 2.4).

Nach der zentralen Vorgabe des Gesetzentwurfs sollen die Behörden ihre Aktenführung in den kommenden Jahren grundsätzlich auf eine (ausschließlich) elektronische Form umstellen (vgl. Nr. 3.2.1)

Gemeinsame Verfahren

Auf meine Anregung wurde in § 11 EGovG-E eine datenschutzrechtliche Vorschrift zu gemeinsamen Verfahren aufgenommen. Der Text dieser Vorschrift geht auf eine Musterregelung zu gemeinsamen Verfahren zurück, die der Arbeitskreis Verwaltungsmodernisierung der Datenschutzbeauftragten des Bundes und der Länder entwickelt hat.

Ziel ist es, die gemeinsame Verarbeitung und Nutzung personenbezogener Daten durch verschiedene Behörden in einem einheitlichen Datenbestand zu erleichtern, ohne das Datenschutzniveau abzusenken.

Die Vorschrift soll vor allem Konstellationen erfassen, bei denen

– die beteiligten Stellen nicht bereits von vornherein feststehen und deshalb nicht gemeinsam bestimmen können, wem die Federführung obliegen soll (z. B. bei dem internetbasierten Online-Genehmigungsverfahren für Großraum- und Schwertransporte – Verfahrensmanagement Großraum- und Schwertransporte – VEMAGS) oder

– öffentliche und nicht-öffentliche Stellen beteiligt sind (z. B. VEMAGS, medizinische Fallakten), für die beteiligten Stellen unterschiedliches Datenschutzrecht gilt und eine Mitentscheidung über das Verfahren und Weiterentwicklungen faktisch nicht möglich ist (z. B. medizinische Fallakten).

Georeferenzierung von Registern

Weiterhin gibt das EGovG vor, dass standortbezogene Register mit einer einheitlichen standardisierten Georeferenzierung zu versehen sind. Betrachtet man jeweils die einzelnen Register, ist es datenschutzrechtlich von eher geringer Relevanz, wenn eine Variante der Georeferenzierung durch eine andere ersetzt wird. Durch die mit der Verwendung einheitlicher Geokoordinaten einhergehende Standardisierung können Daten aus unterschiedlichen Registern jedoch wesentlich leichter verknüpft werden. Somit führt die einheitliche Georeferenzierung auch zu einem deutlich höheren Risiko für das Recht auf informationelle Selbstbestimmung. Deshalb ist für jedes Register zu prüfen, ob eine einheitliche Georeferenzierung tat-

sächlich erforderlich ist. Ich lehne daher Vorschläge ab, diese auch auf Melde-, Pass-, Personalausweis- und Personenstandsregister zu erstrecken.

Ersetzung der Schriftform oder wie sicher ist De-Mail

Der Gesetzentwurf sieht durch Änderungen verwaltungsverfahrensrechtlicher Bestimmungen (VwVfG, SGB X, Abgabenordnung) vor, dass künftig die Schriftform u. a. auch durch eine absenderbestätigte De-Mail ersetzt werden kann. Heute ist das nur bei Verwendung einer qualifizierten elektronischen Signatur möglich, die sich bislang aber kaum durchgesetzt hat.

Diese Gleichsetzung der De-Mail mit der Schriftform ist isoliert betrachtet zunächst kein Datenschutzproblem. Durch die damit von der Bundesregierung erwartete sehr viel häufigere Verwendung der De-Mail ist allerdings die Frage der Datensicherheit dieses Verfahrens wieder in den Mittelpunkt der Beratungen gerückt (vgl. 22. TB Nr. 6.6 und 23. TB Nr. 3.3). Denn De-Mail bietet standardmäßig keine durchgehende Ende-zu-Ende-Verschlüsselung. Die Nachrichten werden bei den De-Mail-Anbietern entschlüsselt und wieder verschlüsselt. Dies wird vor allem beim Versand besonders schutzbedürftiger Daten per De-Mail als problematisch betrachtet, z. B. bei Gesundheitsdaten.

Aus meiner Sicht ist bei der Nutzung von De-Mail eine Ende-zu-Ende-Verschlüsselung nur dann verzichtbar, wenn der Schutzbedarf der Daten als „normal“ eingestuft wird, etwa bei der Aktualisierung von Adressdaten durch einen Sozialversicherungsträger. In diesen Fällen reicht das im Vergleich zur einfachen E-Mail schon deutlich höhere Niveau an Datensicherheit der De-Mail aus (vgl. auch Nr. 3.2.4). Auch bei hohem Schutzbedarf (z. B. beim Versand von Bankdaten) kann dann auf die Ende-zu-Ende-Verschlüsselung verzichtet werden, wenn eine Risikoanalyse ein geringes Restrisiko ergibt. Personenbezogene Daten mit einem sehr hohen Schutzbedarf (etwa medizinische Gesundheitsdaten) erfordern hingegen stets die Verwendung einer Ende-zu-Ende-Verschlüsselung. Diese Position habe ich im Gesetzgebungsverfahren zum E-Government-Gesetz deutlich gemacht.

3.2.4 De-Mail-Zertifizierung

Erste Datenschutzzertifikate konnten an De-Mail-Dienste-anbieter erteilt werden. Trotzdem sind noch nicht alle Fragen gelöst.

Am 3. Mai 2011 trat das De-Mail-Gesetz in Kraft. Über das Gesetzgebungsverfahren hatte ich bereits in meinem letzten Tätigkeitsbericht (vgl. 23. TB Nr. 3.3) informiert. De-Mail ist eine einfache Möglichkeit, elektronische Nachrichten und Dokumente vertraulich, sicher und nachweisbar zu versenden. Ein Unternehmen, das De-Mail-Dienste anbieten will, muss sich vorab beim Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditieren lassen. Im Rahmen der Akkreditierung wird die Einhaltung des Datenschutzes durch ein Gutachten einer sachverständigen und unabhängigen Stelle für Datenschutz festgestellt. Das Gutachten wird von mir geprüft und bei Unbedenklichkeit ein Datenschutzzertifikat erteilt. Die Datenschutzprüfung basiert auf einem Kriterienkatalog, der in meiner Verantwortung liegt. Er ist derzeit in der Fassung 1.2. auf meiner Internetseite (www.datenschutz.bund.de) und über den Elektronischen Bundesanzeiger abrufbar.

Die Erteilung von Zertifikaten als Voraussetzung für die Aufnahme einer gewerblichen Tätigkeit ist ein Novum für mein Haus. Seit Inkrafttreten des Gesetzes habe ich der Mentana Claimsoft GmbH, der T-Systems International GmbH und der T-Deutschland GmbH ein Datenschutzzertifikat nach dem De-Mail-Gesetz erteilt. Alle drei Unternehmen haben zudem die für die Aufnahme ihres De-Mail-Dienstes notwendige Akkreditierung durch das BSI erhalten.

Einige datenschutzrechtliche Forderungen, die ich bereits im letzten Berichtszeitraum eingebracht hatte, wurden im Gesetzgebungsverfahren leider nicht oder nur teilweise berücksichtigt, insbesondere die Forderung nach kürzeren Fristen für die Aufbewahrung von personenbezogenen Daten. Die akkreditierten De-Mail-Diensteanbieter (DMDA) müssen, um ihre Dokumentationspflicht zu erfüllen, Daten wie die Protokollierung der Kontoeröffnung oder der Kündigung noch zehn Jahre nach dem Ende des Vertragsverhältnisses speichern. Die ursprünglich vorgesehene Frist betrug 30 Jahre. Weiter sollte der Dokumentenablagedienst nach einer ausschließlich vom Nutzer zu steuernden Verschlüsselung erfolgen und nicht, wie nun vorgesehen, durch den DMDA. Allerdings haben die DMDA die Dokumentenablage, die nach dem Gesetz optional angeboten werden kann, bislang nicht umgesetzt.

Gesetzlich nicht geklärt ist die Frage, ob auch besonders schutzbedürftige Daten wie Sozial- oder Gesundheitsdaten mittels De-Mail versendet werden dürfen. Entgegen meiner Forderung nach einer zwingenden Ende-zu-Ende-Verschlüsselung hat sich der Gesetzgeber dafür entschieden, diese müsse von den Anbietern lediglich optional angeboten werden. Die De-Mail ist vor einem unberechtigten Zugriff deutlich besser geschützt als die herkömmliche E-Mail, denn die Nachricht wird in einer sicheren Umgebung erzeugt, versendet und zugestellt (Transport- und Inhaltsverschlüsselung). Die Inhaltsverschlüsselung wird aber vor dem Versand und vor der Zustellung kurzzeitig aufgehoben, um die vom Gesetz vorgesehene Überprüfung des De-Mail-Inhaltes auf Schadsoftware zu ermöglichen. Aufgrund meiner Erkenntnisse aus den Zertifizierungsverfahren weiß ich, dass die Sicherheitsanforderungen an die IT-Sicherheit des DMDA sehr hoch sind, damit ein unberechtigter Zugriff sowohl durch Außen- wie durch Innentäter möglichst unterbunden wird. Die Entschlüsselung und Schadsoftwareprüfung erfolgen in einem Sicherheitsrechenzentrum, das den Anforderungen des BSI entsprechen muss. Gegen unberechtigte Zugriffe von innen muss der DMDA sicherstellen, dass die Entschlüsselung zur Prüfung auf Schadsoftware automatisch erfolgt und sehr restriktive Zugriffsrechte bestehen.

Sämtliche personenbezogenen Daten sind verschlüsselt abzulegen.

Unbeschadet dieser Sicherheitsvorgaben halte ich bei besonders schutzbedürftigen Daten eine Ende-zu-Ende-Verschlüsselung für erforderlich. So sollten Stellen, die besonders schützenswerte personenbezogene Daten untereinander austauschen, z. B. Krankenkassen oder andere Sozialleistungsträger, diese De-Mail-Nachrichten stets Ende-zu-Ende-verschlüsseln. Dies ist auch geboten, weil solche Einrichtungen durch die große Menge der versendeten Daten einem erhöhtem Angriffsrisiko und damit einem entsprechenden Schadenspotential unterliegen (Kumulationseffekt). Versenden sie besonders schutzbedürftige personenbezogene Daten an den Bürger/Kunden, richtet sich die Verpflichtung zur Ende-zu-Ende-Verschlüsselung nach dem Schutzbedarf des jeweiligen Datums. Dieser ist anhand der Grundschutzmethodik des BSI von der datenverarbeitenden Stelle festzustellen. Darüber hinaus ist es erforderlich, zumindest vor dem erstmaligen Versand eine Einwilligung des Betroffenen einzuholen, oder festzustellen, ob dieser den Zugang über diesen Kommunikationsweg ausdrücklich eröffnet hat.

Um allen Nutzern von De-Mail Hinweise zum datenschutzkonformen Umgang damit zu geben, habe ich eine entsprechende Handreichung erarbeitet (vgl. auch Anlage 6).

3.3 Videoüberwachung

Videoüberwachung ist seit vielen Jahren ein wichtiges Datenschutzthema – die Kamera ist wohl das meist verwendete Symbol für Überwachung. Auch wenn andere Überwachungstechniken heute mindestens die gleiche Bedeutung erlangt haben, hat mich die Videoüberwachung auch in dieser Berichtsperiode gleich mehrfach beschäftigt. Neben den in diesem Kapitel zusammengeführten Themen sei dabei insbesondere auf die Videoüberwachung am Arbeitsplatz hingewiesen, auf die wegen des engen Sachzusammenhangs in Kapitel 13 zum Beschäftigtendatenschutz näher eingegangen wird.

3.3.1 Versteckte Kamera – auch in der Bundesverwaltung?

Meine Umfrage zum Einsatz von Videoüberwachungstechnik schafft erstmals einen Überblick über den Umfang der Videoüberwachung in der Bundesverwaltung – und deckt datenschutzrechtlichen Nachholbedarf auf. Eine Orientierungshilfe zum datenschutzgerechten Einsatz von Videoüberwachung in der Bundesverwaltung soll Abhilfe schaffen.

Ob in Wohnanlagen, Bahnhöfen, Tankstellen, Einkaufspassagen, Kaufhäusern, Taxen, Kinos oder sogar in Schwimmbädern – Videoüberwachung gehört heute zum Alltag. Auch in der Bundesverwaltung kommen tausende von Videokameras zum Einsatz. Bislang fehlte es allerdings an verlässlichen Zahlen.

Um mir einen Überblick über Art und Umfang der eingesetzten Videoüberwachungstechnik in der Bundesverwaltung zu verschaffen, habe ich in der Berichtsperiode eine Erhebung bei den Bundesbehörden und Bundesgerichten durchgeführt. Von allen Bundesbehörden wollte ich wissen, wie viele Videokameras eingesetzt werden. Ich habe zudem nach der jeweiligen Rechtsgrundlage, der Aufnahme in das Verfahrensverzeichnis, der Durchführung einer Vorabkontrolle, der Kennzeichnung der Videoüberwachung, der Festlegung von Zugriffsrechten und den bestehenden Löschfristen gefragt. Darüber hinaus habe ich Angaben zu der Art der Videoüberwachung (reine Übertragung oder Aufzeichnung) erbeten.

Allein die Anzahl der in der Bundesverwaltung im Innen- und Außenbereich zur Eigensicherung eingesetzten Videokameras lässt aufhorchen: Die 615 öffentlichen Stellen des Bundes, die Videoüberwachung nutzen, setzen über 17 500 Videokameras ein, hauptsächlich zur Sicherung der Liegenschaften und der sich darin aufhaltenden Personen und zur Zugangskontrolle. Nicht mitgezählt sind dabei die Kameras von anderen Stellen, die die Behörden des Bundes mitnutzen, wie z. B. die Bundespolizei die von der Deutschen Bahn betriebenen Videokameras auf Bahnhöfen (vgl. Nr. 3.3.2). 392 Stellen stützen ihre Videoüberwachung dabei auf § 6b BDSG als Rechtsgrundlage, 121 Stellen beriefen sich auf spezialgesetzliche Ermächtigungen, insbesondere aus dem Bundespolizeigesetz.

Während die überwiegende Anzahl der Stellen wenige Kameras bei wenigen Liegenschaften nutzen, setzen 190 Stellen mehr als 9 Kameras im Außen- und Innenbereich ein, 22 Stellen sogar jeweils 100 Kameras oder mehr. Hier stellt sich in besonderem Maße die Frage nach der Erforderlichkeit, zumal eine flächendeckende Überwachung des Außen- und Innenbereichs die Gefahr detaillierter Bewegungs- und Verhaltensprofile birgt.

Überrascht hat mich vor allem die Verbreitung datenschutzrechtlicher Mängel, zumal die datenschutzrechtlichen Vorgaben für die „offene“, d. h. sichtbare Videoüberwachung in öffentlich zugänglichen Räumen seit 2001 in § 6b BDSG geregelt sind (vgl. Kasten a zu Nr. 3.3.1).

Die Umfrage hat immer wiederkehrende, geradezu typische Problemfelder aufgezeigt (vgl. dazu auch die Auswertung im Kasten b zu Nr. 3.3.1):

Unzureichende Kenntnis der Rechtsgrundlagen

Fast jede sechste Stelle (97) konnte keine oder nur unzureichende Angaben zur rechtlichen Grundlage ihrer Videoüberwachung machen. Es lässt sich zwar nicht ausschließen, dass im Einzelfall auch Kameras angegeben wurden, die nicht der Beobachtung des öffentlich oder nicht-öffentlich zugänglichen Raums, sondern etwa der Dokumentation wissenschaftlicher Tests ohne jeglichen Personenbezug dienen. Der Befund lässt aber befürchten, dass sich eine beachtliche Zahl verantwortlicher Stellen

nicht über die datenschutzrechtlichen Grundlagen der Videoüberwachung im Klaren ist.

Fehlender Hinweis auf Videoüberwachung

Jede dritte Stelle (209) hat keinen gesonderten Hinweis auf die Videoüberwachung angebracht, obwohl diese mehrheitlich (119) auf § 6b BDSG gestützt wurde, der diese Hinweispflicht ausnahmslos vorsieht. Die „versteckte Kamera“ scheint daher leider auch in der Bundesverwaltung weit verbreitet zu sein.

Unterbliebene Vorabkontrolle

Die fehlende Durchführung einer Vorabkontrolle und die unterbliebene Aufnahme in das Verfahrensverzeichnis erwiesen sich ebenfalls als auffällig. Im Rahmen einer Vorabkontrolle gem. § 4d Absatz 5 BDSG hat der behördliche Datenschutzbeauftragte die rechtliche Zulässigkeit der beabsichtigten Verarbeitung zu prüfen, sowie sich zu vergewissern, ob die vorgesehenen technischen und organisatorischen Maßnahmen ausreichend und angemessen sind. Hierzu hat er eine Risikoanalyse durchzuführen und ein Sicherheitskonzept zu erstellen. Für ihre automatisierten Verarbeitungen haben die öffentlichen Stellen zudem die Angaben gem. § 4e BDSG sowie die Rechtsgrundlage der Verarbeitung in einem Verzeichnis festzulegen.

Jeweils über die Hälfte der Behörden gab an, die Videoüberwachung nicht in ihr Verfahrensverzeichnis aufgenommen (315 Stellen) und keine Vorabkontrolle durchgeführt zu haben (352 Stellen). 58 bzw. 77 Stellen konnten auf diese Fragen keine Antwort geben. Die Aufnahme in das Verfahrensverzeichnis und die Durchführung einer Vorabkontrolle sind bei dem Einsatz von Videokameras zwar nur erforderlich, wenn die Datenverarbeitung automatisiert stattfindet. Angesichts der verbreiteten digitalen Kameratechnik ist dies allerdings in aller Regel der Fall.

Zu lange Speicherungsdauer

Zu bemängeln war schließlich auch die überlange Speicherdauer der Bilddaten. Etwa die Hälfte der erfassten Stellen gab an, Videoüberwachung mit Aufzeichnungsfunktion vorzunehmen. Hiervon löschen nur wenige Stellen (58) die Aufzeichnungen innerhalb von 72 Stunden oder zumindest innerhalb einer Woche (69 Stellen). In den überwiegenden Fällen beträgt die Speicherdauer bis zu einem Monat (72 Stellen), bei einigen Stellen (30) sogar noch länger – viel zu lang für einen datenschutzkonformen Einsatz von Videoüberwachung!

Auch wenn die Informationsbeschaffung durch Fragebogen nicht die eingehende Vor-Ort-Kontrolle ersetzen kann, hat die Umfrage doch mit aller Deutlichkeit einen nahezu flächendeckenden Beratungsbedarf bei dem Thema „Videoüberwachung“ gezeigt. Die Erkenntnisse aus der Umfrage habe ich zum Anlass genommen, eine ausführliche Orientierungshilfe für einen datenschutzkonformen Einsatz von Videoüberwachungstechnik zu erstellen, die es den verantwortlichen Stellen erleichtert, für einen datenschutzgerechten Einsatz der Videoüberwachung zu sorgen (vgl. Anlage 7). Ferner werde ich bei denjenigen Stellen, bei denen die Erhebung gravierende Mängel ergeben hat, auf deren Abstellung hinwirken. Die datenschutzkonforme Videoüberwachung wird auch zukünftig Gegenstand meiner Kontrollen sein.

Kasten a zu Nr. 3.3.1

§ 6b 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.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Kasten b zu Nr. 3.3.1

Auswertung der Umfrage zum Einsatz von Videoüberwachungstechnik in der Bundesverwaltung, beruhend auf den Angaben der 615 erfassten Stellen.

Überwachungsbereich[1]	Stellen	Prozentangaben (gerundet)
Überwachung Außenbereich	472	
Überwachung Innenbereich	357	
Innen- und Außenbereich	217	
Anzahl Kameras		
mehr als 9 Kameras	190	
mehr als 49 Kameras	60	
mehr als 99 Kameras	22	
Rechtsgrundlage[1]		
§ 6b BDSG	392	
§§ 12ff. BDSG	26	
Spezialgesetze, u. a. BPolG	121	
keine Angaben, ungenaue Angaben	97	
Verfahrensübersicht		
aufgenommen	242	*39 %*
nicht aufgenommen	315	*51 %*
keine Angabe	58	*10 %*
	= 615	
Vorabkontrolle		
durchgeführt	186	*30 %*
nicht durchgeführt	352	*57 %*
keine Angabe	77	*13 %*
	= 615	
Hinweis auf Videoüberwachung		
Text/Piktogramm	355	*58 %*
kein Hinweis	209[2]	*34 %*
keine Angabe	51[3]	*8 %*
	= 615	
Speicherdauer		
bis zu 3 Tagen	58	*9 %*
bis zu 1 Woche	69	*11 %*
bis zu 1 Monat	72	*12 %*
über 1 Monat	30	*5 %*
keine Speicherung (reine Übertragung)	327	*53 %*
keine Angabe (trotz Aufzeichnung)	14	*2 %*
keine Angabe von Fristen	43	*7 %*
	= 615	

1 Mehrfachnennungen möglich.
2 davon gaben 119 Stellen § 6b als Rechtsgrundlage an, der eine Hinweispflicht ausdrücklich vorsieht.
3 davon gaben 15 Stellen § 6b als Rechtsgrundlage an, der eine Hinweispflicht ausdrücklich vorsieht.

3.3.2 Was der versuchte Bombenanschlag am Bonner Bahnhof lehrt

Die fehlenden Videoaufzeichnungen am Bonner Bahnhof haben die Diskussion um die Videoüberwachung in öffentlichen Räumen neu entfacht. Für neue Gesetze besteht kein Anlass, denn die Aufzeichnung scheiterten nicht am Recht, sondern an den technischen Mitteln.

Das öffentliche Erstaunen war groß, als bekannt wurde, die installierten Videokameras auf dem Bonner Hauptbahnhof hätten keine Bilder von dem versuchten Bombenanschlag aufgenommen und könnten daher zur Aufklärung des Vorfalls nichts beitragen. Wie üblich ließ der Ruf nach schärferen Sicherheitsgesetzen nicht lange auf sich warten. Um es vorweg zu nehmen: Die Bahnsteige auf dem Bonner Hauptbahnhof durften videoüberwacht werden, und Aufzeichnungen wären auch erlaubt gewesen. Dies ist geltendes Recht und ergibt sich aus § 27 Bundespolizeigesetz. Danach ist der Bahnhof ein gefährdeter Ort, an dem das Mittel der Videoüberwachung eingesetzt werden darf. Ich habe dies nie in Zweifel gezogen.

Wenn in Bonn nichts aufgezeichnet wurde, mag dies technische oder auch finanzielle Gründe haben. Bei der Videoüberwachung auf Bahnhöfen gibt es ein unübersichtliches Nebeneinander von Bundespolizei und Deutscher Bahn. Faktisch gehören die Videokameras meistens der Deutschen Bahn, die Bundespolizei kann sich bei Bedarf auf diese Kameras aufschalten und speichert dann die Aufnahmen in aller Regel auf eigenen Geräten. Die Funktionsfähigkeit der Videoüberwachung hängt deshalb wesentlich davon ab, wer welche Ressourcen für die Technik zur Verfügung stellt.

Nach Pressemeldungen wird derzeit nur etwa jeder zehnte Bahnhof videoüberwacht, bei weniger als drei v. H. erfolgen Aufzeichnungen. Selbst wenn die Überwachungsmöglichkeiten ausgeweitet würden, erscheint eine flächendeckende Videoaufzeichnung an allen Bahnhöfen illusorisch, von rechtlichen Aspekten – wie z. B. dem Grundsatz der Verhältnismäßigkeit – einmal ganz abgesehen.

Meine Mitarbeiter sind gegenwärtig im Gespräch mit der Bundespolizei, um vernünftige und praktikable Lösungen zu erarbeiten, wie nachvollziehbare Sicherheitsinteressen mit der gebotenen Erforderlichkeit und Verhältnismäßigkeit datenschutzkonform in Einklang gebracht werden können.

Abgesehen von diesen Fragen der rechtlichen Grenzen der Videoüberwachung bleibe ich dabei, dass die flächendeckende Videoüberwachung weder das Kriminalitätsproblem lösen noch dem Terrorismus wirksam begegnen kann. Nicht zuletzt dies macht der Bonner Vorfall deutlich. Den oder die Täter haben die Videokameras nicht abgeschreckt. Auch dies sollte man zur Kenntnis nehmen.

Videoüberwachung kann sinnvoll sein, wenn sie in ein polizeiliches Gesamtkonzept eingepasst ist. Sie mag den Blick im Einzelfall auf einen Täter richten. Sie ist aber kein Allheilmittel, kann auch im Sicherheitsbereich den Menschen nur unterstützen, nicht aber ersetzen, und darf den Blick auf die eigentlichen Ursachen der Kriminalität nicht verstellen.

3.3.3 Beobachtungsdrohnen

Die Videobeobachtung geht in die dritte Dimension. Unbemannte Luftsysteme (Unmanned Aerial Systems, UAS) – umgangssprachlich „Drohnen" – sind Trägersysteme für immer leistungsfähigere Überwachungstechnik. Gefahren für die Privatsphäre sind dabei vorprogrammiert.

Schon bei isolierter Betrachtung gehen von bestimmten Techniken besondere Gefahren aus. Dies ist etwa bei der Videoüberwachung der Fall, was den Gesetzgeber veranlasst hat, deren Einsatzbedingungen und die dabei zu beachtenden Datenschutzvorgaben im BDSG und in anderen Rechtsvorschriften festzuschreiben. Ein zusätzliches Überwachungspotential ergibt sich, wenn verschiedene Techniken miteinander kombiniert werden. Ein Paradebeispiel dafür sind die Video- oder Beobachtungsdrohnen, komplexe Systeme, in denen Flug- und Steuerungstechnik, WLAN- und andere Funktechniken mit der Videoelektronik verbunden werden (vgl. Kasten zu Nr. 3.3.3).

Ich habe Zweifel, ob die geltenden gesetzlichen Regelungen zur Videoüberwachung den besonderen Gefährdungen des Persönlichkeitsrechts, die vom Einsatz von Beobachtungsdrohnen ausgehen, ausreichend Rechnung tragen. Der Gesetzgeber ist aufgerufen, zu prüfen, inwieweit die vorhandenen Gesetze den technischen Entwicklungen angepasst werden müssen.

Flugdrohnen werden von der Bundeswehr (vgl. Nr. 3.3.3.3) und der Bundespolizei (vgl. Nr. 3.3.3.2) eingesetzt. Aber auch im privaten Bereich erfreuen sie sich vor allem als flugtechnische Geschicklichkeitsspiele großer Beliebtheit (vgl. Nr. 3.3.3.4).

Kasten zu Nr. 3.3.3

Beobachtungsdrohnen

Die Bundespolizei verwendet zwei Arten von Beobachtungsdrohnen. Zum einen ein wenige Kilogramm schweres Leichtflugzeug „Aladin", welches mehrere 1000 Meter hoch fliegen kann. Zum anderen einen ca. ein Kilogramm schweren „Fancopter", der in der Regel 10 bis 20 Meter hoch fliegt. Beide Drohnenformen sind mit austauschbaren Foto- und Videokameras versehen.

Die Foto- und Videoaufnahmen des „Aladin“ werden an die tragbare Bodenstation (mit Monitor) live übertragen. Gespeichert werden die Bilder in der Beobachtungsdrohne. Personenbezogene Daten können bedingt durch die Auflösung der Video- und Kamerasysteme und die Flughöhe in der Regel nicht erhoben werden.

Die Foto- und Videoaufnahmen des „Fancopter“ werden an die ebenfalls tragbare Bodenstation (mit Monitor) übertragen. Gespeichert werden die Bilder in der Drohne. Personenbezogene Daten können bedingt durch die Auflösung der Video- und Kamerasysteme und die Flughöhe erhoben werden.

Die Einsätze erfolgten zur (Bundestagsdrucksache 17/8693; Nr. 13):

– Überwachung/Aufklärung im Rahmen von Schleusungen im Grenzbereich,
– Aufklärung von Geländeabschnitten im Rahmen einer Erpresserlage,
– Überwachung von Gleisanlagen aufgrund von gefährlichen Eingriffen in den Bahnverkehr,
– Luftbildaufnahmen von Objekten,
– Objektüberwachung/Zugriffsunterstützung an einer Bahnanlage und
– Objektaufklärung/Erkennen von BTM-Anbau an einer Lagerhalle.

Das sind die Beobachtungsdrohnen der Bundespolizei:

„Aladin“

„Fancopter“

3.3.3.1 Regelungen im Luftverkehrsgesetz

Ich konnte erreichen, dass bei der verkehrsrechtlichen Zulassung von unbemannten Luftfahrtsystemen datenschutzrechtliche Anforderungen beachtet werden müssen.

Nach einer Änderung luftverkehrsrechtlicher Vorschriften können seit Mitte 2012 künftig auch unbemannte Luftfahrtsysteme (Unmanned Aerial Systems – UAS) den Luftraum nutzen. UAS werden dabei in Abgrenzung zu ferngesteuerten Flugmodellen luftverkehrsrechtlich bemannten Flugzeugen gleichgestellt. Der Aufstieg von UAS bedarf einer Erlaubnis nach § 16 Absatz 1 Nummer 7 der Luftverkehrs-Ordnung (LuftVO).

Da mit kamerabestückten UAS Menschen gefilmt und in ihrer Bewegung beobachtet werden können, sind bei deren Einsatz datenschutzrechtliche Aspekte berührt.

Daher habe ich mich im parlamentarischen Verfahren dafür eingesetzt, dass eine Erlaubnis nur erteilt werden darf, wenn beim Aufstieg von UAS das Recht auf informationelle Selbstbestimmung nicht verletzt wird.

Der Deutsche Bundestag ist dem gefolgt und hat eine entsprechende Ergänzung des § 16 Absatz 4 Satz 1 LuftVO beschlossen. Eine Erlaubnis zum Aufstieg eines UAS wird jetzt nur erteilt, wenn die beabsichtigten Nutzungen nicht zu einer Gefahr für die Sicherheit des Luftverkehrs oder die öffentliche Sicherheit oder Ordnung führen können, insbesondere im Fall von § 16 Absatz 1 Nummer 7 LuftVO die Vorschriften über den Datenschutz nicht verletzt werden.

Daher haben die zuständigen Erlaubnisstellen (in aller Regel die Landesluftfahrtbehörden) im Rahmen der Prüfung entsprechender Erlaubnisanträge zum Einsatz von UAS künftig in jedem Einzelfall im Rahmen pflichtgemäßen Ermessens auch zu prüfen, ob der Erlaubnis eine Verletzung des Datenschutzes als Versagungsgrund entgegensteht. Dies begrüße ich ausdrücklich.

Damit einheitliche Kriterien bei der Umsetzung dieser Neuregelung angewandt werden, hat das Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS) im Sommer 2012 „Gemeinsame Grundsätze des Bundes und der Länder für die Erteilung der Erlaubnis zum Auf-

stieg von unbemannten Luftfahrtsystemen gemäß § 16 Absatz 1 Nummer 7 Luftverkehrsordnung (LuftVO)“ veröffentlicht. Ich habe das BMVBS bei deren Abfassung beraten und danke für die Übernahme meiner Empfehlungen.

Positiv möchte ich auch hervorheben, dass die Bundesregierung in einem Bericht an den Ausschuss für Verkehr, Bau und Stadtentwicklung des Deutschen Bundestages erklärt hat, der Zugang zur UAS-Technologie solle so gestaltet werden, dass einem Missbrauch, z. B. durch Ausspionieren der Privatsphäre Dritter, vorgebaut wird.

3.3.3.2 Fliegende Videokameras bei der Bundespolizei

Bisher verwendet bei der Bundespolizei nur die Spezialkräfteeinheit „GSG 9“ Flugdrohnen. Hierbei kommen zwei Drohnensysteme mit unterschiedlichen Kamera- und Videosystemen zum Einsatz. Ich konnte mir ein System bei einem „Testflug“ ansehen.

Mit Kameras bestückte ferngesteuerte Flugdrohnen eröffnen Sicherheitsbehörden neue Möglichkeiten der Überwachung. Bei der Bundespolizei setzt bislang nur die „GSG 9“ solche Geräte ein. Je nach technischer Ausstattung werden die von der Kamera aufgenommenen Einzelaufnahmen und Videos an eine „Bodenstation“ gesendet.

Ich betrachte die Videoüberwachung mittels Drohnen stets als heimliche Datenerhebungsmaßnahme. Heimlich bedeutet, dass die betroffene Person nicht erkennt, dass sie gerade einer Überwachungsmaßnahme unterzogen wird, sei es, dass sie das Fluggerät selbst nicht bemerkt, sei es, dass sie nicht einschätzen kann, inwieweit sie vom Vorgang der Bildaufnahme oder -aufzeichnung selbst konkret betroffen ist. Sofern dabei personenbezogene Daten erhoben und verarbeitet werden, darf die Bundespolizei Drohnen daher nur zur Vorbeugung von Straftaten gem. § 28 Absatz 1 Bundespolizeigesetz (BPolG) oder zur Strafverfolgung gem. § 100h Strafprozessordnung (StPO) einsetzen. Danach sind unter Beachtung von verfassungsrechtlichen Grenzen auch heimliche Foto-, Video- und Tonaufzeichnungen zulässig.

Die verwendeten Flugmodelle sind mit austauschbaren Foto- und Videokameras versehen. Bislang setzt die „GSG 9“ nach eigener Aussage ihre Drohnensysteme vornehmlich zur vorbeugenden Bekämpfung von Straftaten ein, ohne dabei personenbezogene Daten zu erheben, z. B. bei Übersichtsaufnahmen von Bahnanlagen und Lagerhallen. Gegen diese Form der Überwachung habe ich grundsätzlich keine Bedenken.

Ich werde die Verwendung von Videodrohnen bei der Bundespolizei weiterhin genau beobachten, bietet doch die immer ausgefeiltere Technik zunehmend die Möglichkeit, personenbezogene Daten in einer für den Betroffenen nicht erkennbaren Weise zu erheben und zu verarbeiten.

3.3.3.3 Beobachtungsdrohnen bei der Bundeswehr – nur eine Übung?

Die Bundeswehr setzt mit Videotechnik bestückte Flugdrohnen zu Übungszwecken ein. Manche Bürgerinnen und Bürger befürchten dadurch die Verletzung ihrer Privatsphäre.

Wenn man derzeit über Drohnen bei der Bundeswehr spricht, steht deren militärischer Einsatzzweck im Mittelpunkt. Allerdings sind diese Geräte durchgängig mit Videotechnik ausgerüstet, so dass sich auch Fragen des Datenschutzes stellen. Die Bundeswehr trainiert auch in Deutschland den Umgang mit unbemannten Luftfahrzeugen (Flugdrohnen) für den militärischen Einsatz. Die hierfür notwendigen Übungsflüge finden bei Tag und Nacht in exakt definierten Korridoren, so genannten Flugbeschränkungsgebieten, statt. Da die Flugdrohnen der Bundeswehr u. a. zur Aufklärung dienen, sind diese in der Regel mit aufwendiger, hochauflösender Kamera- und Aufnahmetechnik ausgestattet. Mit Hilfe der entsprechenden technischen Vorrichtung können die Flugdrohnen Foto-, Video- und sonstige Datensignale an die Bodenstationen senden.

Den Eingaben von Bürgern entnehme ich die Sorge, dass im Rahmen dieser Übungs- und Aufklärungsflüge beim Überfliegen von Wohngebieten unrechtmäßige Aufnahmen von Personen oder Privateigentum gefertigt und die Betroffen dadurch in ihren Persönlichkeitsrechten verletzt werden. Da für die Betroffenen nicht erkennbar ist, welche Aufnahmen erfolgen und was mit diesen anschließend geschieht, befürchten sie insbesondere eine mögliche Auswertung der Aufnahmen und deren weitere Verwendung oder Nutzung. Diese Sorgen nehme ich sehr ernst.

Das Bundesministerium der Verteidigung (BMVg) hat mir versichert, die für die Übungsflüge eingesetzten Flugdrohnen könnten Personen, die sich außerhalb von Ortschaften im Sensorbereich aufhielten, zwar als solche entdecken, nicht aber identifizieren. Personenbezogene oder personenbeziehbare Daten im Sinne des § 3 BDSG könnten nicht erhoben werden. Ich teile die Auffassung, dass bei perspektivischen Aufnahmen von oben die Erkennbarkeit von Personen erheblich eingeschränkt ist, weil nur wenige Identifizierungsmerkmale erfasst werden. Gleichwohl kann im Einzelfall eine Identifizierung möglich sein, wenn etwa besondere persönliche Merkmale der Person hinzukommen oder wenn eine Verknüpfung mit weiteren Erkenntnissen hergestellt werden kann, wie etwa mit Häusern oder Grundstücken, die der Person zugeordnet werden können.

Laut BMVg erfolgt auch keine Auswertung der Sensorbilder. Eine Nutzung der Daten im Rahmen der Ausbildung sei ebenfalls nicht vorgesehen. Vielmehr würden die Daten bei der nächsten Flugkampagne überschrieben. Im Übrigen weist das BMVg darauf hin, dass nach den anzuwendenden Dienstvorschriften der Flugkurs bei Ausbildungsflügen zu planen sei und die unbemannten Luftfahrzeuge dabei größere Abstände zu Ortschaften und Häuseransammlungen einzuhalten hätten.

Mir liegen bislang keine Erkenntnisse über andere als die planmäßig dargestellten Einsätze der Flugdrohnen vor. Ebenso habe ich keine Hinweise auf eine Verwendung der Aufnahmen oder Daten oder gar auf einen Datenmissbrauch. Ich werde gleichwohl den Einsatz von Flugdrohnen weiterhin kritisch begleiten.

3.3.3.4 Was macht mein Nachbar gerade?

Die zurzeit im Hobbybereich beworbenen Flugdrohnen sind vom Anwendungsbereich des Bundesdatenschutzgesetzes als privat-persönliche Tätigkeit nach § 1 Absatz 2 Nummer 3 BDSG ausgenommen, soweit sie ausschließlich als flugtechnisches Geschicklichkeitsspielgerät genutzt werden.

Wird Deutschland zu einem Land von Voyeuren? Für den Einstieg in die Drohnen-Fliegerei braucht‘s nicht viel Geld: Zwar geben die Hersteller in den Bedienungsanleitungen meist deutliche Hinweise auf datenschutzrechtliche Regeln. Dennoch tauchen immer öfter private Spionage-Videos aus Nachbars Garten bei YouTube auf.

Die Luftverkehrsordnung regelt zum Thema Privatsphärenschutz, dass die Fluggenehmigungen von den jeweils zuständigen Landesluftfahrtbehörden nur erteilt werden sollen, „wenn die beabsichtigten Nutzungen (…) die Vorschriften über den Datenschutz nicht verletzen“ (vgl. Nr. 3.3.3.1).

Bereits im meinem letzten Tätigkeitsbericht hatte ich auf diese Problematik hingewiesen (vgl. 23. TB Nr. 5.13). Im Berichtszeitraum haben mich erneut mehrere Eingaben zu den im Handel frei erhältlichen, als Spielzeuge beworbenen und über eine spezielle Software per Smartphone oder Tablet PC steuerbaren Fluggeräten erreicht. Hierbei übertragen die Bordkameras der Drohne Live-Bilder auf die Bildschirme des Nutzers. Diese Flugdrohnen mit geringer Reichweite und Flughöhe bedürfen keiner Zulassung oder Aufstiegserlaubnis, so dass Verkauf und Einsatz keinen Beschränkungen unterliegen. Die Anfragen und Beschwerden bezogen sich in der Hauptsache auf die private Nutzung und deren Zulässigkeit.

Ich halte gleichwohl den Einsatz solcher Flugdrohnen im Hinblick auf die hiervon ausgehenden Gefahren für die Privatsphäre – die Flughöhe der Drohne beträgt nach meinen Recherchen bis zu 6 Metern mit einer Reichweite von etwa 50 Metern – für eine potenzielle Bedrohung der Privatsphäre. Es ist dem Zweck dieses Gerätes naheliegend, dass es auch dazu eingesetzt wird, das Verhalten anderer Menschen (heimlich) zu beobachten. Dass dies regelmäßig unter Missachtung fremden Eigentums durch Überwindung von Grundstücksgrenzen erfolgen wird – man denke an den Flug in Nachbars Garten über den Zaun hinweg – erhöht die Missbrauchsgefahr.

Da der Einsatz der Drohnen im rein privaten Bereich erfolgt, halte ich das BDSG bei einer ausschließlich Verwendung als flugtechnisches Geschicklichkeitsspiel allerdings nicht für anwendbar. Die Regelungen des Bundesdatenschutzgesetzes gelten nicht für Privatpersonen im rein privaten Bereich, zum Beispiel beim Einsatz von Videotechnik zwischen Nachbarn.

Wenn jemand das Gerät auf der Straße fliegen lässt und seinen Nachbarn ohne dessen Wissen fotografiert, muss dies nicht gegen das Datenschutzrecht verstoßen. Anders sieht es aus, wenn Behörden (vgl. o. Nr. 3.3.3.2) oder Unternehmen mit der Kamera etwas ausspionieren, wenn unerlaubte Fotografien gemacht oder Drohnen kommerziell genutzt werden. Dann würde das Datenschutzrecht greifen. Die Abgrenzung ist in der Praxis sicherlich schwierig.

Zivilrechtliche Unterlassungsansprüche mögen bestehen, setzen aber voraus, dass die Drohne bemerkt und dann auch noch einem konkreten Nutzer zugeordnet werden kann. Daher sehe ich bei der Durchsetzung der Abwehransprüche erhebliche praktische Schwierigkeiten. Schließlich könnte der Einsatz der Flugdrohnen sogar strafrechtlich relevant sein, jedenfalls dann, wenn Aufnahmen einen gegen Einblick besonders geschützten Raum betreffen. Dies könnte bereits bei der Überwindung eines Sichtschutzes mittels Drohne der Fall sein und als Verstoß gegen § 201a StGB gewertet werden, der mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft wird.

Da es sich bei dem Einsatz von Flugdrohnen im privaten Bereich um ein aktuelles, bundesweit bestehendes Problem handelt, erörtere ich die Thematik auch mit meinen Kollegen in den Ländern. Insbesondere gilt es, die Weiterentwicklung dieser und technisch ähnlicher Geräte im Auge zu behalten.

3.4 Besserer Datenschutz durch Selbstregulierung?

Das vor mehr als zehn Jahren ins Bundesdatenschutzgesetz eingefügte Instrument der Selbstregulierung hat die damit verbundenen Erwartungen nicht erfüllt. Abgesehen von einem Sonderfall im Bereich der Presse ist es erst im Jahre 2012 zum ersten Mal gelungen, eine Selbstregulierung erfolgreich auf den Weg zu bringen.

Mit Umsetzung der EG-Datenschutzrichtlinie 95/46/EG wurde es den Wirtschaftsverbänden durch § 38a BDSG ermöglicht, der zuständigen Aufsichtsbehörde Verhaltensregeln (Codes of Conduct) vorzulegen. Damit verbunden war die Vorstellung, die Wirtschaft könnte die notwendigerweise allgemein gehaltenen Vorschriften des Bundesdatenschutzgesetzes konkretisieren, um damit den Datenschutz besser handhabbar zu machen. Dies sollte sowohl den verantwortlichen Stellen die Anwendung des Datenschutzrechts erleichtern, als auch den Betroffenen mehr Klarheit bei der Wahrnehmung ihrer Rechte verschaffen und die Tätigkeit der Aufsichtsbehörden vereinfachen. Dieser an sich zu begrüßende Ansatz hat sich in der Praxis bisher aber nicht durchgesetzt. Dies hat verschiedene Ursachen.

In Politik und Wirtschaft ist die Vorstellung weit verbreitet, die Selbstregulierung sei dazu gedacht, Defizite bei der Gesetzgebung auszugleichen und neue Regelungen

zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu schaffen. Solche Überlegungen orientieren sich offensichtlich an Selbstverpflichtungen der Wirtschaft in anderen Bereichen, in denen es noch keine gesetzlichen Regelungen gibt und aufgrund der Selbstregulierung auch nicht geben soll. Dies ist beim Datenschutzrecht aber anders: § 38a BDSG soll kein neues Datenschutzrecht oder neue Befugnisse schaffen. Dies bleibt Aufgabe des Gesetzgebers. Selbstregulierung im Sinne von § 38a BDSG ist auf die Konkretisierung des bestehenden Datenschutzrechts beschränkt.

Gerade in den letzten Jahren wurden datenschutzpolitische Debatten über die Notwendigkeit der Anpassung datenschutzrechtlicher Rahmenbedingungen dadurch abgebrochen, dass die Politik – vor allem das Bundesministerium des Innern (BMI) – eine Selbstregulierung zur Lösung unübersehbarer Probleme in Aussicht gestellt hat. In der jüngeren Vergangenheit gibt es gleich zwei Beispiele, in denen dieses Vorgehen ganz oder teilweise gescheitert ist: Beim so genannten Geodatenkodex des Branchenverbandes BITKOM (vgl. 23. TB Nr. 4.1.3) und bei der geplanten Selbstregulierung für soziale Netzwerke.

Der Geodatenkodex sollte als Selbstverpflichtung der entsprechenden Unternehmen einen datenschutzgerechten Umgang mit so genannten Panoramadiensten (z. B. Google Street View oder Bing Street Side) sicherstellen. Das BMI wollte gesetzgeberisch die rote Linie festlegen, die beim Umgang mit personenbezogenen Daten im Internet nicht überschritten werden dürfe. Am Ende hatte sich die öffentliche Aufregung um die Angebote gelegt und es kam weder eine anerkannte Selbstregulierung noch das angekündigte „Rote-Linie-Gesetz“. Der Versuch des zuständigen Verbandes, Verhaltensregeln vorzulegen, die den gesetzlich vorgesehenen Standard sogar unterschreiten, konnte nicht gut gehen. Der von der Wirtschaft schließlich in Kraft gesetzte Geodatenkodex wurde – anders als in § 38a BDSG vorgesehen – den Aufsichtsbehörden überhaupt nicht vorgelegt. Er genügt nicht einmal den gesetzlichen Anforderungen, wie die Datenschutzaufsichtsbehörden festgestellt haben, und bleibt sogar hinter den Zusagen zurück, die die Firma Google für ihren Dienst „Streetview“ dem Hamburgischen Beauftragten für den Datenschutz und die Informationsfreiheit gegeben hatte. Anschließend hat sich der eigens zu diesem Zweck von der Wirtschaft gegründete Verein lange Zeit noch nicht einmal an seine eigenen Regeln gehalten, denn erst eineinhalb Jahre nach Unterzeichnung des Kodexes nahm die zentrale Anlaufstelle im September 2012 ihre Arbeit auf. Inzwischen steht das Portal www.geodatendienstekodex.de zur Verfügung, fristet jedoch ein Schattendasein.

Als im Jahre 2011 die öffentliche Debatte um den Datenschutz in sozialen Netzwerken einen vorläufigen Höhepunkt erreichte, ging das BMI wieder nach demselben Muster vor. Es ergriff die Initiative zur Schaffung einer Selbstregulierung. Seitdem beraten verschiedene Branchenvertreter über einen Kodex für den Datenschutz in sozialen Netzwerken. Die Arbeiten an diesen Verhaltensregeln kommen indes kaum voran.

Es gibt aber auch erfolgreichere Beispiele der Selbstregulierung:

Eher unbemerkt von der Öffentlichkeit berät eine Arbeitsgruppe der Kommission für Geoinformationswirtschaft (GIW-Kommission) und der Konferenz der Datenschutzbeauftragten des Bundes und der Länder über einen GeoBusiness Code of Conduct. Zweck dieser Selbstregulierungsinitiative ist es, für Unternehmen, die Geoinformationen von der öffentlichen Hand bekommen, einheitliche und standardisierte Regeln zum Umgang mit diesen Informationen zu schaffen und damit die allgemeinen gesetzlichen Bestimmungen zu konkretisieren. Gleichzeitig soll den bereitstellenden Verwaltungen eine Orientierungshilfe gegeben werden, um ihnen die Auslegung der einschlägigen datenschutzrechtlichen Bestimmungen zu erleichtern. Der Code of Conduct konnte allerdings bisher nicht der zuständigen Aufsichtsbehörde vorgelegt werden, weil es von einzelnen Datenschutzbehörden noch Vorbehalte gibt. Dies zeigt ein weiteres Dilemma von Selbstregulierung auf: Die föderale Struktur der Datenschutzaufsicht macht die Einführung bundesweit anerkannter Verhaltensregeln zuweilen zu einem mühsamen und langwierigen Prozess.

Als bisher einziges erfolgreiches Beispiel einer Selbstregulierung kann der Code of Conduct der Versicherungswirtschaft angesehen werden (vgl. Nr. 10.4).

Als Fazit bleibt festzuhalten: Selbstregulierung im Sinne von § 38a BDSG kann nur dann erfolgreich sein, wenn sich die Wirtschaft im Dialog mit den Aufsichtsbehörden konstruktiv und ernsthaft im Sinne der Förderung des Datenschutzes in bestimmten Sektoren einsetzt. Dies ist ein zeitlich und inhaltlich anspruchsvolles und sorgfältig zu planendes Unterfangen. Wer Selbstregulierung als „Blitzableiter“ zur Befriedung datenschutzpolitischer Debatten oder als Ersatz für notwendige gesetzgeberische Aktivitäten einsetzt, verhindert nicht bloß sinnvolle datenschutzrechtliche Lösungen, sondern diskreditiert das Instrument selbst.

3.5 Transparenz – auch bei Datenschutzpannen!

Auch wenn beim Datenschutz gilt, Vorbeugen ist besser als heilen, lassen sich doch Datenpannen nicht völlig ausschließen. Ob aus Nachlässigkeit oder vorsätzlich: Wenn personenbezogene Daten abhanden kommen, kann dies erhebliche Nachteile für die Betroffenen und wirtschaftliche Schäden für die verantwortliche Stelle mit sich bringen. Öffentliche Stellen und Unternehmen tun sich trotzdem schwer, angemessen mit derartigen Vorfällen umzugehen. Seit mehreren Jahren wird deshalb auf nationaler, europäischer und internationaler Ebene daran gearbeitet, hier für mehr Transparenz zu sorgen. Dabei verspricht man sich von den Meldepflichten zweierlei: Zum einen sollen die verantwortlichen Stellen dazu angehalten werden, sich intensiver um IT-Sicherheit und Datenschutz zu kümmern. Zum anderen sollen die Betroffenen in die Lage versetzt werden, Gegenmaßnahmen zu treffen, Schäden zu erkennen und zu begrenzen.

3.5.1 Datendiebstahl – verhindern, erschweren, entdecken

Daten – ob personenbezogen oder nicht – sind begehrt und stellen ein Handelsgut dar. Betroffene Stellen ergreifen oft erst dann Maßnahmen zur „Data Leakage Prevention", wenn sich ein Datendiebstahl ereignet hat.

Ende 2012 wurde im Bundesministerium der Gesundheit ein schwerer Datendiebstahl bekannt, bei dem mutmaßlich ein Administrator seine Befugnisse missbraucht hat. Die Ermittlungen laufen noch. Bereits im 15. TB (Nr. 30.7) hatte ich auf die „Allmacht" des Systemverwalters hingewiesen und verschiedene Maßnahmen empfohlen, um dessen Arbeiten kontrollierbar und transparent zu machen, damit entsprechende Missbrauchsfälle überhaupt entdeckt und nachgewiesen werden können. Aus gegebenem Anlass möchte ich nochmals eine Reihe von Punkten auflisten, die helfen können, eine Datendiebstahl zu erschweren oder zumindest frühzeitig zu entdecken. Bei allen hier genannten Maßnahmen und besonders beim Einsatz von speziellen Data Leakage Prevention-Systemen sind immer auch Fragen des Beschäftigtendatenschutzes (vgl. Nr. 13f.) zu berücksichtigen.

Privilegierte oder administrative Berechtigungen umfassen weitergehende Zugriffsberechtigungen auf IT-Systeme, Softwarekomponenten oder Daten, als arbeitstäglich erforderlich sind. Grundsätzlich sollten umfassende (privilegierte) Berechtigungen nur solchen Rollen, Gruppen oder Personen zugewiesen werden, die überwiegend mit der Administration von IT betraut sind. Die Zugehörigkeit der Mitglieder einer Gruppe muss nachweisbar und revisionssicher dokumentiert sein; bei Änderung der Tätigkeiten müssen die Berechtigungskonzepte aktualisiert werden. Berechtigungskonzepte sollten bei Aktualisierung der Sicherheitskonzepte (mindestens jährlich) auf Plausibilität und Notwendigkeit überprüft werden. Zudem wird empfohlen, die Systemprotokolle, die die Arbeit der Administratoren dokumentieren, regelmäßig zu überprüfen. Weiter rege ich an, die einschlägigen IT-Sicherheitsempfehlungen aus den Grundschutzkatalogen des BSI zu beachten und umzusetzen (vgl. Kasten zu Nr. 3.5.1)

Sicherheitsvorfälle, die auf krimineller Energie beruhen, lassen sich trotz aller erdenklichen Sicherheitsmaßnahmen nicht verhindern. Das Risiko einer Entdeckung kann einzelne Täter abschrecken. Um Manipulationen früh zu entdecken und den unerwünschten Abfluss von Daten zu begrenzen, sollten im IT-Betrieb Kontrollmaßnahmen (spontan und periodisch) durchgeführt werden.

Kasten zu Nr. 3.5.1

Folgende Sicherheitsempfehlungen des IT-Grundschutzes beschäftigen sich mit dieser Thematik:

- Funktionstrennung: Die Aufgabenverteilung und die hierfür erforderlichen Funktionen (vgl. M 2.5 Aufgabenverteilung und Funktionstrennung) sind so zu strukturieren, dass operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden, um Interessenskonflikte bei den handelnden Personen zu minimieren oder ganz zu verhindern.
- Rollen: Die Zuordnung von Personen oder Personengruppen zu Rollen erleichtert die Verwaltung von Berechtigungen (vgl. M 2.8 Vergabe von Zugriffsrechten).
- Restriktive Rechtevergabe: Werden an Mitarbeiter besonders weitgehende Rechte vergeben (z. B. an Administratoren), so sollte dies möglichst restriktiv erfolgen (vgl. M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle). Hierbei ist zum einen der Kreis der privilegierten Benutzer möglichst einzuschränken und zum anderen sind nur die für die Durchführung der Arbeit benötigten Rechte zu vergeben. Für alle Aufgaben, die ohne erweiterte Rechte durchgeführt werden können, sollten auch diese privilegierten Benutzer unter einer Kennung mit Standardrechten arbeiten. Insbesondere bei Aushilfskräften und externen Dienstleistern ist darauf zu achten, dass diese nur die Dienste verwenden und nur auf die Daten zugreifen dürfen, die sie tatsächlich benötigen.
- Erforderlichkeitsprinzip („Need to know"): Durch Anwendung des Need to Know Prinzips und des Vier Augen Prinzips ist sicherzustellen, dass Berechtigungen auf den verschiedenen Ebenen (z. B. Zutritt zu Räumen, Zugang zu Informationssystemen) zielgerichtet vergeben werden und auch praktikabel sind (vgl. M 2.6 Vergabe von Zutrittsberechtigungen und M 2.7 Vergabe von Zugangsberechtigungen).
- Vertrauenswürdigkeit des Personals: Bei sicherheitskritischen Betriebsumgebungen empfiehlt es sich, die Mitarbeiter auf die besonderen Datenschutz- und Sicherheitsvorgaben zu verpflichten und die Vertrauenswürdigkeit bestätigen zu lassen (vgl. M 3.33 Sicherheitsüberprüfung von Mitarbeitern). Besonderes Gewicht ist hierbei auf die Vertrauenswürdigkeit von Personen mit besonderen Funktionen und Berechtigungen zu legen (vgl. M 3.10 Auswahl eines vertrauenswürdigen Administrators und Vertreters). Um Mitarbeiter entsprechend ihrer Qualifikationen und Kompetenzen einsetzen zu können, sollte es ein Personalkonzept geben (vgl. M 3.51 Geeignetes Konzept für Personaleinsatz und -qualifizierung). Dazu gehört die Analyse sicherheitsrelevanter personeller Faktoren (vgl. M 3.83).

- Arbeit von und mit Externen: Wenn Externe für die Institution Aufgaben übernehmen, bei denen sie Zugriff auf vertrauliche Daten erhalten können, müssen hierfür geeignete Regelungen getroffen werden (vgl. M 2.226 Regelungen für den Einsatz von Fremdpersonal). Dies beginnt mit dem Abschluss von Vertraulichkeitsvereinbarungen (vgl. M 3.55 Vertraulichkeitsvereinbarungen). Aktionen Betriebsfremder sollten kontrolliert und protokolliert werden (vgl. M 2.16 Beaufsichtigung oder Begleitung von Fremdpersonen). Auch bei der Auswahl geeigneter externer Dienstleister müssen diverse Sicherheits- und Datenschutzaspekte beachtet werden (vgl. M 2.252 Wahl eines geeigneten Outsourcingdienstleisters), aber auch bei der Beendigung von Verträgen mit Externen (vgl. M 2.307 Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses). Externe Administratoren sollten nicht dauerhaft unbeaufsichtigt an sicherheitsrelevanten IT-Systemen arbeiten, durch qualifizierte interne Mitarbeiter sollten zumindest sporadisch deren Tätigkeiten gesichtet werden.
- Privilegierte Rollen: Personen mit so genannten privilegierten Rollen wie Administratoren haben weitgehende Zugriffsrechte und gleichzeitig ein umfassendes Fachwissen. Auch um Administratoren vor Verdächtigungen zu schützen, sollten die Rechte so restriktiv wie möglich vergeben werden und Arbeiten unter privilegierten Berechtigungen protokolliert werden. Es sollte keine Person geben, die Zugriffsberechtigungen auf alle Systeme hat (vgl. M 2.38 Aufteilung der Administrationstätigkeiten).
- Berechtigungen dokumentieren und kontrollieren: Berechtigungen sind zu dokumentieren.
- Kein Zugriff ohne Authentisierung: Der Zugriff auf alle IT-Systeme und Dienste muss durch sichere Verfahren zur Identifikation und Authentisierung des zugreifenden Benutzers abgesichert werden.
- Sicherheitsvorfälle: Trotz aller Sicherheitsvorkehrungen können Sicherheitsvorfälle nie ganz ausgeschlossen werden. Daher muss eine Vorgehensweise aufgebaut werden, um mit Sicherheitsvorfällen im Akutfall vernünftig umgehen zu können (vgl. M 6.58 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen). Neben der Festlegung der Rollen, Verantwortlichkeiten und Verhaltensregeln müssen für die effektive Behandlung von Sicherheitsvorfällen die Betroffenen richtig mit deren Auswirkungen umgehen und Vorfälle unverzüglich melden (vgl. M 6.60 Festlegung von Meldewegen für Sicherheitsvorfälle).

3.5.2 Meldepflicht bei Datenschutzpannen

Die Informationspflicht bei Datenpannen hat sich grundsätzlich bewährt. Eine von mir durchgeführte bundesweite Erhebung über die gemeldeten Fälle zeigt, dass die Meldepflicht von den verantwortlichen Stellen ernst genommen wird. Angesichts zahlreicher Datenpannen bei öffentlichen Stellen sollte auch der öffentliche Bereich meldepflichtig werden.

Seit dem 1. September 2009 müssen nicht-öffentliche Stellen und ihnen gleich gestellte öffentlich-rechtliche Wettbewerbsunternehmen gravierende Datenschutzpannen der zuständigen Aufsichtsbehörde anzeigen sowie die Betroffenen informieren und ihnen Handlungsempfehlungen unterbreiten. § 42a BDSG sieht eine solche Informationspflicht vor, wenn sensible Daten unrechtmäßig in die Hände Dritter gelangt sind und schwerwiegende Beeinträchtigungen für die Betroffenen drohen. Bei einem Verstoß droht ein Bußgeld von bis zu dreihunderttausend Euro oder mehr.

Die Regelung hat sich – trotz einer wahrscheinlich hohen Dunkelziffer nicht gemeldeter Vorfälle – bewährt. Die Publizitätspflicht motiviert die verantwortlichen Stellen, mehr für die Datensicherheit und den Datenschutz zu tun; zugleich versetzt sie die Betroffenen in die Lage, negative Konsequenzen frühzeitig zu erkennen und Sicherheitsmaßnahmen zu ergreifen.

Nach einer bundesweiten Erhebung unter den Aufsichtsbehörden, die ich nach Ablauf der ersten 18 Monate seit Inkrafttreten der Informationspflicht durchgeführt habe, wurden fast 90 Fälle gemeldet, davon vier in meinem Zuständigkeitsbereich. Ganz überwiegend handelte es sich um Bankverbindungs- und Kreditkartendaten, die den verantwortlichen Stellen durch Diebstahl oder Verlust von Datenträgern, durch Fehlversendungen von E-Mails und Briefen, durch fehlerhafte Zugriffsmöglichkeiten auf Online-Mitgliederseiten oder durch Hacking abhanden gekommen sind. Zum Teil waren auch besonders sensible Informationen wie Gesundheitsdaten betroffen.

Das Risiko des Abhandenkommens sensibler Daten besteht bei Unternehmen und Behörden gleichermaßen. Dies belegen zahlreiche Vorfälle aus der jüngeren Vergangenheit, etwa der Hackerangriff auf die Server des Zolls im Sommer 2011 oder die Datenspionage durch einen externen IT-Mitarbeiter im Bundesministerium der Gesundheit im Herbst 2012 (vgl. Nr. 3.5.1). Es ist für mich nicht nachvollziehbar, warum öffentliche Stellen bislang von der Informationspflicht ausgeschlossen sind. Dass es auch anders geht, zeigt beispielsweise das Berliner Datenschutzgesetz, das seit dem Jahr 2011 die Informationspflicht bei Datenpannen auf die Berliner Landesverwaltung erstreckt. Der Bund sollte diesem guten Beispiel folgen, zumal er auch hier einmal mehr von den Modernisierungsbestrebungen auf europäischer Ebene eingeholt zu werden droht: Auch der Entwurf der Europäischen Kommission für eine europaweit einheitliche Datenschutz-Grundverordnung (vgl. Nr. 2.1) sieht eine Informationspflicht bei Datenpannen für den öffentlichen und den nicht-öffentlichen Bereich gleichermaßen vor.

3.5.3 Meldepflicht mit einigen Tücken – der neue § 109a TKG

Anbieter öffentlich zugänglicher Telekommunikationsdienste sind seit Mai 2012 verpflichtet, Vorfälle, die zu einer Verletzung von personenbezogenen Daten führen, gegenüber den Aufsichtsbehörden und – unter gewissen Umständen – den Betroffenen anzuzeigen. Die praktische Umsetzung der gesetzlichen Vorgaben ist allerdings nicht immer unproblematisch.

Im Rahmen der Novellierung des Telekommunikationsgesetzes (vgl. Nr. 6.4) wurde auch eine neue europäische Vorschrift (Artikel 4 Absatz 3 bis 5 E-Privacy-Richtlinie) zur Meldung von Datenschutzvorfällen bei Telekommunikationsanbietern in deutsches Recht umgesetzt. Die bis dahin über den Verweis des § 93 Absatz 3 TKG a. F. geltende Informationspflicht des § 42a BDSG (vgl. Nr. 3.5.2) wurde durch § 109a TKG ersetzt. Auch wenn die beiden Vorschriften im Hinblick auf die grundsätzliche Ausrichtung ähnlich sind, liegen im Detail doch gravierende Unterschiede.

§ 109a TKG regelt das Verfahren, das ein Anbieter öffentlich zugänglicher Telekommunikationsdienste befolgen muss, sobald er eine Datenschutzverletzung festgestellt hat. Zunächst hat eine Meldung sowohl gegenüber der Bundesnetzagentur als auch beim BfDI zu erfolgen. Die Meldung muss immer – unabhängig von den konkreten Umständen des zu meldenden Vorfalls – erfolgen und ist im Gegensatz zu § 42a BDSG unbeschränkt, so dass auch kleinere Vorfälle mit potentiell weniger schweren Auswirkungen mitgeteilt werden müssen.

Um dieses Verfahren für die meldepflichtigen Unternehmen zu vereinfachen, hat die Bundesnetzagentur in Absprache mit mir Leitlinien erstellt, die das Verfahren erläutern.

Nach der obligatorischen Meldung des Vorfalls muss der Telekommunikationsanbieter in einem weiteren Schritt prüfen, ob zusätzlich noch die von der Datenschutzverletzung Betroffenen zu informieren sind. Dies hat immer dann zu geschehen, wenn Betroffene durch den Vorfall schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt sein können. Eine Ausnahme kommt lediglich dann in Betracht, wenn die betroffenen Daten durch geeignete technische Vorkehrungen, wie z. B. ein als sicher anerkanntes Verschlüsselungsverfahren, vor einer unberechtigten Kenntnisnahme geschützt sind. Schließlich legt § 109a TKG den Unternehmen noch die Verpflichtung auf, ein Verzeichnis zu führen, in dem sämtliche meldepflichtigen Vorfälle der letzten fünf Jahre aufzuführen und Angaben zu den Umständen und Auswirkungen der Verletzungen sowie zu den ergriffenen Abhilfemaßnahmen festzuhalten sind.

Im Grundsatz befürworte ich die Meldepflicht von Datenschutzvorfällen. Zum einen muss sich das Unternehmen mit einem Vorfall auseinandersetzen, zum anderen werden die Risiken für die Betroffenen durch entsprechende Vorschriften transparent und sie können so mit der Situation oft einfacher umgehen. Nicht zuletzt erhalten die Datenschutzaufsichtsbehörden einen besseren Überblick und können bei einer Häufung von Vorfällen bei einem bestimmten Unternehmen ihre Aufsichtstätigkeit zielgerichteter und somit effizienter ausüben.

Allerdings haben sich bei der praktischen Anwendung der Vorschrift bereits nach kurzer Zeit verschiedene Probleme aufgetan.

Die schwellenlose Meldepflicht soll theoretisch dazu führen, dass sämtliche Datenschutzvorfälle bekannt werden und aufgearbeitet werden können. Wie sich in der Praxis allerdings zeigt, ist die Zahl der die Aufsichtsbehörden erreichenden Mitteilungen bereits nach kürzester Zeit massiv angestiegen. Zumindest mittelfristig kann möglicherweise eine sinnvolle Bearbeitung der Meldungen ohne eine massive Aufstockung des zur Verfügung stehenden Personals nicht mehr gewährleistet werden. Weitere Probleme liegen in der teils nicht schlüssigen Formulierung der gesetzlichen Vorgaben. Bereits die Frage, wann eine Verletzung des Schutzes personenbezogener Daten vorliegt, birgt Streitpotential. So ist es nach der Legaldefinition einer Datenschutzverletzung in § 3 Nummer 30a TKG zumindest fraglich, ob eine solche überhaupt vorliegen kann, wenn die Daten entsprechend § 109a Absatz 1 Satz 3 TKG durch geeignete technische Vorkehrungen gesichert sind und somit eine unrechtmäßige Verwendung grundsätzlich ausgeschlossen ist. Würde eine Datenschutzverletzung in diesen Fällen aber verneint, entfiele zwangsläufig die Meldepflicht an die Aufsichtsbehörden, was im Widerspruch zu der Gesetzessystematik stünde. Danach soll ja gerade die Aufsichtsbehörde entscheiden, ob die implementierten technischen Vorkehrungen den Anforderungen genügen und somit eine Benachrichtigung der Betroffenen entbehrlich machen.

Ich gehe davon aus, dass die praktischen Erfahrungen zur Optimierung des Verfahrens beitragen können. In enger Zusammenarbeit mit der Bundesnetzagentur werde ich auf nationaler und auf europäischer Ebene an Lösungsvorschlägen arbeiten, die zu einer besseren Umsetzbarkeit der gesetzlichen Vorgaben beitragen. Einzelne Projekte sind bereits angelaufen. So habe ich mit der Bundesnetzagentur einen Meldebogen entworfen, der den meldepflichtigen Unternehmen über die Websites der Behörden zur Verfügung gestellt wird und somit das Meldeverfahren vereinfacht. Ebenso beteilige ich mich an einem Projekt, bei dem die Artikel-29-Gruppe zusammen mit der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) ein Verfahren zur Bestimmung der Schwere von Datenschutzverstößen entwickelt (vgl. Nr. 2.4.4). Bereits im Zusammenhang mit der Meldung soll ersichtlich werden, wie gravierend ein Datenschutzvorfall tatsächlich ist und somit – gerade aufgrund der zu erwartenden großen Anzahl von eingehenden Meldungen – den Aufsichtsbehörden ein Mittel zur Priorisierung der Bearbeitung an die Hand geben.

3.6 Was lange währt, wird nicht immer gut – Stiftung Datenschutz

Lange hat die Bundesregierung um die Konzeption der Stiftung Datenschutz gerungen – das Ergebnis ist enttäu-

schend. Ich habe daher, wie auch die Datenschutzbehörden der Länder, auf eine Mitwirkung im Stiftungsbeirat vorerst verzichtet.

Die im Koalitionsvertrag von 2009 vorgesehene Stiftung Datenschutz, die Produkte und Dienstleistungen auf ihre Datenschutzfreundlichkeit hin prüfen, Bildung im Bereich des Datenschutzes stärken, den Selbstdatenschutz durch Aufklärung verbessern und ein Datenschutzaudit entwickeln sollte, hat noch immer nicht ihre Arbeit aufgenommen. Die Satzung der Stiftung Datenschutz, auf die sich die Bundesregierung erst nach langwierigen Verhandlungen geeinigt hat, lässt zweifeln, ob sie nach derzeitiger Konzeption ihren Aufgaben sachgerecht nachkommen kann.

Immer wieder (vgl. 23. TB Nr. 2.5) habe ich ausgeführt, dass ich die Idee der Stiftung Datenschutz begrüße, die personelle und finanzielle Unabhängigkeit der Stiftung von der Daten verarbeitenden Wirtschaft aber für unverzichtbar halte. Diese unerlässlichen strukturellen Rahmenbedingungen der Stiftungsarbeit habe ich in einem im Februar 2011 veröffentlichten Diskussionspapier erneut betont und vertieft dargelegt. Diese Überlegungen sind auf meiner Internetseite www.datenschutz.bund.de unter dem Suchbegriff „Diskussionspapier“ abrufbar.

Leider haben meine Vorschläge, wie auch die zahlreichen Gesprächsangebote der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, kein Gehör gefunden. Anders ist es nicht erklärbar, dass die Stiftung Datenschutz nach der jetzigen Konzeption maßgeblich auf Zustiftungen aus der Wirtschaft angewiesen ist und den Wirtschafts- und wirtschaftsnahen Vertretern im Stiftungsbeirat ein deutliches Übergewicht einräumt. Verbrauchervertrauen in die Datenschutzkonformität von Produkten und Dienstleistungen lässt sich so nicht herstellen. Es steht vielmehr zu befürchten, dass die Daten verarbeitende Wirtschaft ihren Einfluss auf die Stiftung nutzt, um unter dem Deckmantel einer Bundesstiftung werbewirksame, aber wenig aussagekräftige Gütesiegel zu entwickeln.

Bislang lässt sich auch nicht absehen, ob und unter welchen Bedingungen die Stiftung die Ergebnisse von Datenschutzauditierungen, die von dritter Seite durchgeführt werden sollen, im Nachhinein auf Stichhaltigkeit prüfen und notfalls korrigieren kann. Dies ist besonders problematisch, weil es die Datenschutzbehörden sind, die in der täglichen Aufsichtspraxis mit möglicherweise allzu großzügig vergebenen Datenschutz-Gütesiegeln konfrontiert werden.

Ich habe daher im Einvernehmen mit den Datenschutzbeauftragten der Länder, denen die Stiftungssatzung ebenfalls zwei Entsendungsrechte in den Stiftungsbeirat einräumt, auf eine Mitwirkung im Beirat der Stiftung vorerst – bis zu einer befriedigenden Neukonzeption – verzichtet.

4 Technologischer Datenschutz

Datenschutz ist ganz wesentlich eine Reaktion auf technologische Herausforderungen. Deshalb gibt es in diesem Tätigkeitsbericht wohl kein Thema, bei dem die Informationstechnik keine Rolle spielt. In diesem Kapitel werden Projekte und Themen behandelt, bei denen technologische Fragen im Vordergrund stehen. Das sind zum einen Großprojekte wie die elektronische Gesundheitskarte oder das unlängst unsanft entschlafene ELENA-Projekt, das die Verarbeitung elektronischer Gehaltsnachweise zum Gegenstand hatte. Zum anderen werden technische Querschnittsthemen behandelt, die nahezu überall eine Rolle spielen, etwa die Anforderungen an ein sicheres Löschen von Daten.

4.1 Elektronische Gesundheitskarte endlich in Sicht?

Nach Jahren der Stagnation hat die Einführung der elektronischen Gesundheitskarte endlich an Fahrt aufgenommen. Zur Förderung der Organspendebereitschaft der deutschen Bevölkerung kann die Karte einen wesentlichen Beitrag leisten.

Nicht nur Flughafen- und Bahnhofsprojekte ziehen sich länger hin als angekündigt. Gleiches gilt auch für anspruchsvolle Informatikvorhaben wie die elektronische Gesundheitskarte (eGK).

Obwohl die jetzige Krankenversichertenkarte nach § 291a SGB V bis spätestens zum 1. Januar 2006 zu einer elektronischen Gesundheitskarte (eGK) erweitert werden sollte, gibt es diese heute nicht, zumindest nicht mit den versprochenen Leistungsmerkmalen. Nachdem die für die Entwicklung der eGK zuständige gematik 2010 entschieden hatte, dass die Leistungserbringer für die medizinischen Anwendungen und die Kostenträger für die administrativen Anwendungen jeweils die alleinige Verantwortung übernehmen sollten (vgl. 23. TB Nr. 3.4), einigte man sich auch darauf, zunächst nur folgende Anwendungen einzuführen:

– ein online gestütztes Versichertenstammdatenmanagement (VSDM)

– die Einführung eines Notfalldatensatzes (NFDM)

– die adressierte Kommunikation der Leistungserbringer (KOM-LE)

Nach dieser Neuorientierung wurden die Projektstrukturen bei der gematik neu verteilt und die Lasten- und Pflichtenhefte erarbeitet. Unabhängig davon startete der Basis-Rollout der eGK. Bis zum Ende des Berichtszeitraumes waren ca. 70 Prozent der Versicherten, d. h. ca. 50 Millionen Versicherte in Deutschland, in Besitz der neuen eGK, die sich aber von der alten Krankenversichertenkarte nur durch die Aufnahme eines Lichtbildes und eines Speicherchips unterscheidet.

Der Anwendungsbereich der eGK wurde zum 1. November 2012 durch das Gesetz zur Regelung der Entscheidungslösung im Transplantationsgesetz (s. o. Nr. 11.5.5) erweitert: die eGK soll bei der Förderung der Organspendebereitschaft der deutschen Bevölkerung eingesetzt werden. Nach dem geänderten § 291a Absatz 3 SGB V soll die eGK zum einen die Erklärungen der Versicherten zur Organ- und Gewebespende und zum anderen die Hinweise der Versicherten auf das Vorhandensein und den

Aufbewahrungsort von solchen Erklärungen aufnehmen können; Letzteres gilt auch für Vorsorgevollmachten oder Patientenverfügungen. Da die Aufnahme der vollen Erklärung mit den derzeit ausgegebenen Karten technisch nicht möglich ist, dürfte dies frühestens im Jahre 2016 in Betracht kommen. Mit entsprechenden Testen könnte bereits im Jahre 2014 begonnen werden; vorher dürfte schon der Test zur Aufnahme von Hinweisen starten. Im Rahmen der parlamentarischen Beratungen ist auch diskutiert worden, ob den Krankenkassen ein einmaliges Schreibrecht auf der eGK eingeräumt werden soll, um dadurch die Hinweise der Versicherten auf der eGK zu dokumentieren. Dies könnte deshalb sinnvoll sein, da alle Krankenkassen ihre Versicherten anschreiben und über die Organspende informieren müssen. Ein solches einmaliges Schreibrecht könnte ich aus datenschutzpolitischer Sicht akzeptieren, um eine Beschleunigung und Erhöhung der Bereitschaft der Bevölkerung zur Abgabe der Organspendeerklärung zu erreichen. Dabei muss aber sichergestellt sein, dass die Datenschutz- und Datensicherheitsstandards der eGK gewahrt bleiben und insbesondere technisch abgesichert wird, dass die Krankenkassen keine anderen Zugriffsrechte auf medizinische Daten erhalten.

Die ebenfalls zeitweise diskutierte Einrichtung eines zentralen Registers aller entsprechenden Erklärungen lehne ich ab. Der Gesetzgeber hat die gematik mit der Erstellung eines Berichtes beauftragt, der die Verfahren zur Unterstützung der Versicherten bei der Verwaltung ihrer Daten zur Organ- und Gewebespende beschreiben soll. Dieser Bericht muss dem Deutschen Bundestag bis zum 30. Juni 2013 vorgelegt werden. Mit Interesse sehe ich den dort vorgeschlagenen Verfahren entgegen. Auch in Zukunft werde ich ein kritischer, aber auch konstruktiver Akteur bei der Einführung der eGK bleiben.

4.2 Elektronische Einkommensnachweise – Neue Lösungen für alte Probleme?

Auch in den vergangenen zwei Jahren hatte ich mich intensiv mit Projekten zu beschäftigen, die den Umgang mit Einkommensnachweisen erleichtern sollen. Das über mehr als zehn Jahre entwickelte Projekt ELENA, das immer wieder Gegenstand erbitterter öffentlicher Debatten war, wurde 2011 endgültig beerdigt. Das „Erbe“ sollen zwei neue Projekte (Bea und OMS) antreten. Es ist zu hoffen, dass die Projektverantwortlichen für diese Nachfolgeverfahren nicht wie bei ELENA dabei stehen bleiben, das immer schwieriger zu handhabende System elektronischer Einkommensnachweise mit mehr als hundert unterschiedlichen Einkommensbegriffen und vielfältigen, teilweise zweifelhaften Übermittlungspraktiken elektronisch abzubilden. Vielmehr muss untersucht werden, wie sich dieses komplexe System vereinfachen lässt. Ein positiver Nebeneffekt könnten dabei Lösungen sein, die mit weniger Daten und reduzierten Datenübermittlungen auskommen.

4.2.1 Das Ende des ELENA-Verfahrens – unsanft entschlafen

Das ELENA-Verfahren, wurde im Jahr 2011 beendet. Allerdings gilt auch hier vielleicht das Sprichwort: „Wo sich eine Tür schließt, geht eine andere Tür (hier: zwei Türen) wieder auf“.

Über das Verfahren „Elektronischer Entgeltnachweis (ELENA-Verfahren)“, das ursprünglich einmal „JobCard-Verfahren“ hieß, habe ich seit meinem 20. TB regelmäßig berichtet (20. TB Nr. 4.1.1.1, zuletzt 23. TB Nr. 11.1.3.). Seit dem 1. Januar 2010 wurde eine große Anzahl von Entgeltbescheinigungsdaten aller Beschäftigten in Deutschland in einer riesigen Datenbank gespeichert. Im Jahr 2011 wurde das Verfahren – für manchen unerwartet – schließlich von den zuständigen Ministerien beendet und das entsprechende Gesetz durch den Bundestag aufgehoben.

Das Verfahren stand stets – auch aus datenschutzrechtlichen Gründen – in der Kritik. Das Bundesverfassungsgericht nahm 2010 mehrere Verfassungsbeschwerden von Arbeitgebern an, zu denen ich eine gutachterliche Stellungnahme abgegeben habe. Bevor es aber eine Entscheidung über die Verfassungsmäßigkeit des ELENA-Verfahrens treffen konnte, beschloss die Bundesregierung 2011, das ELENA-Verfahren möglichst schnell zu beenden. Begründet wurde dies damit, dass sich die aus Datenschutzgründen erforderlichen Signaturkarten nicht schnell genug verbreiten würden. Die Verfassungsbeschwerdeverfahren wurden mittlerweile eingestellt. Ich bedauere es, dass damit die Frage der Verfassungsmäßigkeit des ELENA-Verfahrens, die ein Jahrzehnt lang die Diskussion begleitet hat, nicht höchstrichterlich beantwortet wurde.

Der Gesetzgeber hob die ELENA betreffenden gesetzlichen Regelungen durch Gesetz vom 23. November 2011 (BGBl. I S. 2298) auf, das am 3. Dezember 2011 in Kraft trat. Bereits drei Tage später habe ich den Datenbankhauptschlüssel vernichtet. Nur mit diesem digitalen Schlüssel war der Zugriff auf die in der ersten Phase des Projekts bereits seit 2010 verschlüsselt gespeicherten Entgeltdaten von mehr als 35 Millionen Arbeitnehmern möglich. Sowohl die Datenstelle der Träger der Rentenversicherung (DSRV) als Betreiberin der ELENA-Datenbank als auch die Fa. ITSG als ehemalige „Registratur Fachverfahren“ haben aufgrund der hohen technischen Sicherheitsstandards beim ELENA-Verfahren sowie wegen der Sensibilität der Daten und nicht zuletzt, weil das Verfahren im kritischen Blick der Öffentlichkeit stand, Löschverfahren entwickelt, die den Sicherheitsstandards für die Löschung staatlicher Geheimnisse entsprechen. Die Löschung der Daten ist sowohl bei der DSRV als auch bei der Fa. ITSG unter meiner sowie unter Kontrolle des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) erfolgreich durchgeführt worden. Die Daten sind nun auch physikalisch nicht mehr vorhanden.

Bereits mit der Verkündung der Entscheidung, das ELENA-Verfahren einstellen zu wollen, haben das BMWi und das BMAS in einer gemeinsamen Erklärung die Erarbeitung eines Konzeptes zu einem elektronischen Meldeverfahren angekündigt, bei dem die von der Wirtschaft für das ELENA-Verfahren gemachten Investitionen berücksichtigt würden. Mittlerweile hat die Bundesregierung entsprechende Nachfolgeverfahren aufgesetzt.

An den Projekten „Bescheinigungen elektronisch annehmen – Bea“ der Bundesagentur für Arbeit und „Optimierte Meldeverfahren in der Sozialen Sicherung – OMS“ des BMAS bin ich beteiligt.

4.2.2 Bea lebt! Das Projekt Bescheinigungen elektronisch annehmen

Mit dem Verfahren „Bea“ will die Bundesagentur für Arbeit die Lücke schließen, die das eingestellte Projekt ELENA hinterlassen hat.

Das Verfahren „Bescheinigungen elektronisch annehmen – Bea“ der Bundesagentur für Arbeit (BA) ist aufgesetzt worden, nachdem ELENA (vgl. Nr. 4.2.1) aufgegeben wurde. Gegenstand von Bea ist es, vor allem die Arbeitsbescheinigung, die ein Arbeitgeber bei Beendigung des Arbeitsverhältnisses für den Arbeitnehmer erstellen muss und die zur Berechnung des Arbeitslosengeldes benötigt wird, elektronisch an die BA zu übermitteln. Der Arbeitnehmer erhält umgehend nach Eingang der Bescheinigung bei der BA von dieser einen Ausdruck des gespeicherten Datensatzes, so dass er eventuelle falsche Einträge umgehend berichtigen lassen kann. Gleichzeitig soll die Bescheinigung grundsätzlich nur noch auf Verlangen des Arbeitnehmers erstellt werden. Die Anzahl ausgestellter Bescheinigungen wird sich dadurch vermutlich deutlich reduzieren. Nach der bisherigen Rechtslage muss der Arbeitgeber ein Papierformular ausfüllen und dieses dem Arbeitnehmer aushändigen, unabhängig davon, ob der Arbeitnehmer einen Antrag auf Leistungen bei der BA stellt oder einen Anspruch auf derartige Leistungen hat.

Der vorgesehene Umfang des Datensatzes ging zunächst über den der Papierbescheinigung hinaus. Insbesondere sollte der Arbeitgeber ein vertragswidriges Verhalten des Arbeitnehmers, das zur Kündigung geführt hat, näher konkretisieren, z. B. Diebstahl, Mobbing o. Ä. Dies ist für die Prüfung einer Sperrzeit gemäß § 159 SGB III relevant. Ich konnte erreichen, dass der Umfang des Datensatzes in diesem Punkt deutlich reduziert wurde. Der Arbeitgeber ist, wie in der bisherigen Papierbescheinigung, nur noch verpflichtet anzugeben, ob überhaupt ein vertragswidriges Verhalten Anlass für die Kündigung war. Konkrete Angaben zum Fehlverhalten des Arbeitnehmers dürfen nicht in die Bescheinigung eingetragen werden. Im Hinblick auf § 159 SGB III wird die BA das Vorliegen eines solchen Verhaltens zum Anlass nehmen, Arbeitnehmer und Arbeitgeber gesondert über die Hintergründe zu befragen.

Darüber hinaus habe ich mich für ein Widerspruchsrecht des Arbeitnehmers gegen die elektronische Übermittlung vom Arbeitgeber direkt an die BA eingesetzt. Denn diese stellt eine Abkehr von dem Grundsatz dar, dass personenbezogene Daten in erster Linie beim Betroffenen zu erheben sind. Widerspricht der Arbeitnehmer der elektronischen Übermittlung, bleibt es bei der bisherigen Papierbescheinigung, die der Arbeitgeber dem Arbeitnehmer aushändigen muss. Dieser muss die Bescheinigung dann selbst bei der BA vorlegen oder kann sie, wenn er keinen Leistungsantrag stellt, für eigene Zwecke verwahren. Über das Widerspruchsrecht muss der Arbeitnehmer spätestens anlässlich der Beendigung seines Arbeitsverhältnisses vom Arbeitgeber informiert werden.

Die vorgesehenen Änderungen für die Übersendung der Arbeitsbescheinigung müssen noch gesetzlich nachgebildet werden. Zum Redaktionsschluss befand sich der entsprechende Gesetzentwurf des BMAS in der Ressortabstimmung. Ich werde das Gesetzgebungsverfahren und die Umsetzung des Projektes weiter begleiten.

4.2.3 OMS – Optimierte Meldeverfahren in der Sozialen Sicherung

ELENA ging, OMS kommt – oder: Auf der Suche nach machbaren Optimierungsmöglichkeiten im sozialversicherungsrechtlichen Datenaustausch.

Um die Erkenntnisse aus ELENA (vgl. Nr. 4.2.1) weiter nutzen zu können, hat die Bundesregierung Ende 2011 beschlossen, eine Machbarkeitsstudie zu Optimierungsmöglichkeiten beim Datenaustausch in den verschiedenen sozialversicherungsrechtlichen Verfahren zu erarbeiten. Federführend ist das Bundesministerium für Arbeit und Soziales (BMAS). Das Projekt „Optimierte Meldeverfahren in der Sozialen Sicherung – OMS“ hat Anfang 2012 seine Arbeit aufgenommen und soll bis Ende 2013 einen Abschlussbericht erstellen. Dieser soll die Bundesregierung in die Lage versetzen, Verbesserungen beim Datenaustausch im Sozialversicherungsrecht jenseits von ELENA zu initiieren.

Vorbedingungen der Studie sind der Verzicht auf die Nutzung der qualifizierten elektronischen Signatur sowie auf eine Vorratsdatenspeicherung. Das Projekt besteht aus verschiedenen Arbeitsgruppen, die den status quo verschiedener Melde-, Beitrags- und Bescheinigungsverfahren feststellen und dann dafür Optimierungsvorschläge erarbeiten und bewerten sollen. Ich beteilige mich an diesen Arbeitsgruppen. Da mit den entsprechenden Bewertungen vor kurzem begonnen worden ist, ist es für mögliche Ergebnisse dieses Projektes noch zu früh. Die zu untersuchenden Optimierungsvorschläge reichen von minimalen Ergänzungen einzelner Datensätze über die Einführung eines multifunktionalen Datensatzes und einer zentralen Annahmestelle (ähnlich wie bei ELENA) bis hin zur durchgängigen Nutzung des sog. Prozessdatenbeschleunigers (P23R) für alle untersuchten Verfahren (vgl. Kasten zu Nr. 4.2.3).

Die grundlegenden Fragen des sozialversicherungsrechtlichen Meldewesens bleiben bei diesem Projekt allerdings teilweise auf der Strecke. Anstatt kleine Verbesserungen an Datensätzen einzelner Verfahren zu erreichen oder die papierbasierte Meldung in die elektronische Form zu bringen, wäre es zum Beispiel aus meiner Sicht sinnvoll gewesen, über eine grundlegende inhaltliche Reform nachzudenken. Seit Jahren trete ich dafür ein, die verschiedenen Einkommens- bzw. Entgeltbegriffe zu reduzieren. Mit der Vereinheitlichung dieses Datenkranzes würden die Bürokratiekosten erheblich abgebaut. Leider wurde dieser Vorschlag zum wiederholten Male nicht berücksichtigt. Ich befürchte, dass – auch aufgrund der zur

Verfügung stehenden Zeit – im Ergebnis nur kleinteilige Änderungen diskutiert und wirklich grundsätzliche Fragen nicht angegangen werden. Immerhin wird die am Ende abzuliefernde Machbarkeitsstudie alle eingegangenen Vorschläge beinhalten, und nicht nur die, die tatsächlich betrachtet worden sind. Es besteht also noch Hoffnung, dass sich die Bundesregierung als Empfänger der Studie entschließt, grundsätzliche Probleme anzugehen, die im Projekt OMS noch keine Berücksichtigung gefunden haben.

Kasten zu Nr. 4.2.3

P23R ist ein vom BMI initiiertes E-Government-Forschungsprojekt. Das P23R-Prinzip umfasst Grundlagen und Methoden, die den Datenaustausch zwischen Wirtschaft und Verwaltung einfacher, sicherer und transparenter gestalten sollen. Es spezifiziert ein Infrastrukturkonzept, auf dessen Grundlage Unternehmen ihre gesetzlichen Informations- und Meldepflichten in einer abgesicherten Umgebung effizient erfüllen können.

4.3 IT-Konsolidierung

Der IT-Betrieb fast aller Geschäftsbereichsbehörden des BMI soll unter der fachlichen Gesamtverantwortung der Bundesstelle für Informationstechnik (BIT) beim Bundesverwaltungsamt zusammengefasst werden.

Die BIT soll – neben der IT im Bundesverwaltungsamt – ab Ende 2012 an den beiden Standorten Köln und Wiesbaden schrittweise IT-Dienstleister werden für

- das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
- das Statistisches Bundesamt,
- das Bundesinstitut für Sportwissenschaft,
- das Bundesinstitut für Bevölkerungsforschung,
- das Bundesamt für Migration und Flüchtlinge,
- das Beschaffungsamt des Bundesministeriums des Innern,
- die Fachhochschule des Bundes für öffentliche Verwaltung,
- die Bundesakademie für öffentliche Verwaltung,
- die Bundeszentrale für politische Bildung,
- die Bundesanstalt Technisches Hilfswerk,
- das Bundesamt für Kartographie und Geodäsie und
- das Bundesamt für Sicherheit in der Informationstechnik.

Die IT der Sicherheitsbehörden des BMI sollen erst danach konsolidiert werden.

Planungen zur Bündelung der Informationstechnik im Geschäftsbereich des BMI existieren bereits seit einigen Jahren. Auch in den Geschäftsbereichen des BMF oder des BMVBS bestehen Dienstleistungszentren mit ähnlichen Zielen.

Die jetzt geplante Zusammenfassung der IT des BMI-Geschäftsbereichs im Bundesverwaltungsamt habe ich von Anfang an beratend begleitet. Als erster Schritt ist die Übernahme der IT des Statistischen Bundesamts (StBA) Anfang 2013 vorgesehen.

Bei der Übernahme der IT durch die BIT handelt es sich um Auftragsdatenverarbeitung nach § 11 BDSG. Daher müssen zuvor nicht nur die technisch-organisatorischen Maßnahmen nach § 9 BDSG, sondern auch die Vorgaben des § 11 BDSG vollständig umgesetzt sein (vgl. Kasten zu Nr. 4.3). Folglich genügt beispielsweise die alleinige Vorgabe der Fachanforderungen mit Schutzbedarfsklassifizierung durch den Auftraggeber bei weitem nicht.

Da das StBA Mitglied im Statistischen-Verbund (Artikel 91c GG, § 3a BStatG) ist, muss der Umgang mit den entsprechenden Anwendungen noch geklärt werden. Weiter sind die sich aus dem Statistikgeheimnis (§ 16 BStatG) ergebenden Besonderheiten zu beachten. Dies gilt insbesondere für das Abschottungsgebot durch organisatorische, personelle und räumliche Trennung sowie eine umfassende Belehrung und Verpflichtung aller Personen, die mit statistischen Daten in Berührung kommen könnten.

Nach einer Rahmenvereinbarung zwischen dem Hauptpersonalrat und dem BMI vom 19. April 2012 sollen alle Personen, die überwiegend in der IT beschäftigt sind, in die BIT wechseln. Dies darf aber nicht dazu führen, dass die abgebenden Stellen nicht mehr über ausreichendes eigenes IT-Fachwissen verfügen. Nur mit eigenem Sachverstand über die Funktionsweise von IT-Systemen können sie „gleichberechtigt“ beispielsweise Service Level Agreements verhandeln oder Neuplanungen von IT bedarfsgerecht durchführen. Auch im Hinblick auf die Verpflichtungen der fachlich zuständigen Stellen als Auftraggeber gemäß § 11 BDSG müssen diese in der Lage sein, die Verfahrensabläufe und die Maßnahmen zur IT-Sicherheit beim BVA zu beurteilen und ggf. entsprechende Weisungen zu erteilen.

Im Rahmen meiner Beratung habe ich ausdrücklich und mehrfach darauf hingewiesen, dass

- das Gebot der Abschottung nur durch ein hohes Schutzniveau für die besonders schützenwerten personenbezogenen Daten gewährleistet werden kann,
- für datenschutzrechtliche Kontrollen durch den bDSB des StBA und durch meine Dienststelle eine umfassende und revisionssichere Protokollierung zu implementieren ist
- und die Empfehlung zur „Mandantenfähigkeit“ („Orientierungshilfe Mandantenfähigkeit – Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur“ des Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder) zu beachten ist.

Insbesondere sehe ich die behördlichen Datenschutzbeauftragten neben dem Datenschutzbeauftragten der BIT in der Pflicht, nach der IT-Konsolidierung den Datenschutz der einzelnen Fachanwendungen zu gewährleisten.

Da weiterhin noch ungeklärte Fragen zum Datenschutz bestehen bzw. einige wichtige Aspekte nicht ausreichend berücksichtigt und mit meinem Einvernehmen umgesetzt wurden, werde ich die Konsolidierung im Geschäftsbereich des BMI weiterhin sehr kritisch beobachten.

Kasten zu Nr. 4.3

Bei der IT-Konsolidierung besonders wichtige schriftlich festzulegende Vorgaben (vgl. § 11 Absatz 2 BDSG):

- Den Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen.
- Die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen.
- Die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers.
- Die mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen.
- Den Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält.
- Die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

4.4 Technische Standardisierung immer wichtiger

Neben Rechtsvorschriften werden technische Standards für den Datenschutz immer wichtiger. Ich beteilige mich an deren Ausarbeitung.

Der Standardisierung von technischen Architekturen und Prozessen als Grundlage für technische Anforderungen an den Datenschutz kommt eine immer höhere Bedeutung zu. Auch im Entwurf der Datenschutz-Grundverordnung (vgl. Nr. 2.1.1) finden sich zahlreiche Verweise auf die Festlegung technischer Standards. Neben der Mitwirkung auf nationaler Ebene beteilige ich mich daher vermehrt an Standardisierungsvorhaben im internationalen und nationalen Bereich.

In vielen Bereichen der IT-Sicherheit haben sich technische Standards etabliert. Durch die unmittelbare Verknüpfung mit dem technologischen Datenschutz tangieren diese zwangsläufig datenschutzrechtliche und -technische Aspekte. Daher ist es umso wichtiger, sich bereits frühzeitig an der Entwicklung von Standards zu beteiligen, um größtmöglichen Einfluss auf das Ergebnis zu nehmen.

Auf nationaler Ebene wirke ich derzeit im Rahmen der Aktivitäten des DIN (Deutsches Institut für Normung) unter anderem bei der Erarbeitung und Überarbeitung der Normen

- Vernichtung von Datenträgern (DIN 66399) (vgl. Nr. 4.6)
- Karten und persönliche Identifikation (NA 043-01-17 AA) und
- Biometrie (NA 043-01-37 AA)

mit (vgl. 23. TB Nr. 5.3).

Neben der Unterstützung der Interoperabilität und des Datenaustausches zwischen Anwendungen und Systemen geht es bei „Karten und persönliche Identifikation“ und „Biometrie“ vor allem auch um das Einbringen von nationalen Interessen in die internationale Normung. Durch meine Mitwirkung in diesen Gremien des DIN strebe ich an, die datenschutzrechtlichen Aspekte – z. B. zum Schutz der Privatsphäre in der Biometrie – besser in diesen Technologie zu verankern. Dabei arbeite ich eng mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen. Auch neue Vorhaben, die erst in die Normung eingebracht werden sollen, werden von mir mit beraten. Hierzu zählt beispielsweise die Erarbeitung von Standards zur Datenlöschung (vgl. Nr. 4.5).

Im Zuge der Reform des europäischen Datenschutzrechtes (vgl. Nr. 2.1) und der zunehmenden Akzeptanz von datenschutzfreundlichen Konzepten wie Privacy by Design oder der Datenschutzfolgen-Abschätzung (Privacy Impact Assessment, PIA) gewinnt die internationale Standardisierung immer mehr an Gewicht. Auf internationaler Ebene wurde innerhalb der ISO (International Organization for Standardization) eine Arbeitsgruppe gegründet, welche sich ausschließlich mit den Themen „Identitätsmanagement“ und „technologischen Datenschutz“ beschäftigt und unter anderem Standards zu den Themen PIA oder Cloud Computing erarbeitet. Die Normung des Datenschutzes auf globaler Ebene gestaltet sich dabei sehr schwierig. Das liegt zum Teil daran, dass die Normung nicht nur die regionalen deutschen (bzw. europäischen) datenschutzrechtlichen Anforderungen berücksichtigen muss, sondern darüber hinaus eine Vielzahl von Wünschen anderer Staaten und Regionen. Meine grundsätzliche Haltung sieht deshalb vor, dass ISO-Normen nur solche Fragen und Inhalte ansprechen und normieren sollten, die übergeordnete Datenschutzfragen betreffen. Erste Ansätze werden im Rahmen des Projektes der ISO 29100 („Privacy Framework“) erarbeitet.

Hier sehe ich Möglichkeiten, grundsätzliche Prinzipien und eine Rahmenarchitektur für den technologischen Datenschutz zu standardisieren.

Allerdings plädiere ich dafür, diese so allgemein wie möglich zu halten und Aspekte des europäischen Datenschutzes innerhalb der Europäischen Normungsorganisationen zu bearbeiten. Hier wäre eine Norm unter dem

Dach von CENELEC (europäische Normung im Bereich Elektrotechnik) vorstellbar. Zusammen mit ETSI (Normung im Bereich Telekommunikation) und CEN (Normung in allen anderen technischen Bereichen) bildet CENELEC das europäische System für technische Normen und wäre der geeignete Ort, um die spezifisch europäischen Datenschutzaspekte zu normieren.

In Hinblick auf die unglaubliche Geschwindigkeit, in der neue Technologien entstehen und veralten, müssen die Standardisierungsvorhaben entbürokratisiert und der Prozess der Entwicklung von Standards verschlankt werden. Andernfalls droht die Standardisierung dem ständigen technologischen Fortschritt hinterher zulaufen.

Auch künftig wird der Stellenwert technischer Standards weiter zunehmen. Ich werde mich weiterhin an Standardisierungsvorhaben beteiligen und meine Mitarbeit und die enge Kooperation auf nationaler und internationaler Ebene – auch im Zuge der künftigen Entwicklungen bei der Datenschutz-Grundverordnung – weiter intensivieren.

4.5 Datenlöschung – eine Leitlinie

Die Löschung digitaler Daten ist nicht immer einfach. Bisweilen mangelt es aber auch an der Kenntnis und Bereitschaft der Verantwortlichen, sich mit gesetzlichen Vorgaben zur Datenlöschung auseinanderzusetzen.

Der Löschung von Daten kommt in einer digitalen Welt immer mehr Bedeutung zu. Während Vernichten von Papier recht einfach zu bewerkstelligen ist, bereitet das Löschen von digitalen Medien häufig Schwierigkeiten. Dies hängt zum einen damit zusammen, dass in der digitalen Welt Daten mit unterschiedlichen Löschfristen hoch integriert in Datenbanken gespeichert werden und der Löschprozess unterschiedliche Verknüpfungen berücksichtigen muss. Hier können IT-Lösungen greifen, welche die gesetzlich gebotenen Datenlöschungen von vornherein berücksichtigen.

Bisweilen sehen die für IT-Verfahren Verantwortlichen aber auch gar nicht ein, warum sie einmal gespeicherte Daten überhaupt löschen sollen – schließlich gehört die Knappheit digitaler Speichermöglichkeiten ein für alle Mal der Vergangenheit an. Bisweilen mangelt es auch ganz einfach an Sensibilität.

Die Bemühungen der Wirtschaft den Prozess des Löschens von Daten zu standardisieren, unterstütze ich; bei der Ausarbeitung einer Leitlinie dazu war ich beratend tätig.

Auch die Bundesverwaltung stellt vermehrt ihre papiergebundene Vorgangsbearbeitung auf die digitale Welt um (siehe auch digitale Personalakte, Nr. 13.3). Mit der Umstellung von Papier auf elektronische Bearbeitung entsteht in der Regel ein neues Problem: die Datenlöschung. In sehr vielen Geschäftsprozessen und IT-Anwendungen werden nämlich personenbezogene Daten verarbeitet und genutzt, die den Vorschriften des Datenschutzes unterliegen.

Die Datenschutzgrundsätze zur Erforderlichkeit, Datenvermeidung und Datensparsamkeit verpflichten dazu, nicht mehr benötigte Daten zu löschen. So enthält Artikel 6 der EU-Datenschutzrichtlinie von 1995 eine Lösch- und Anonymisierungsvorgabe. Das deutsche Bundesdatenschutzgesetz (BDSG) schreibt in den §§ 20 Absatz 2 und 35 Absatz 2 die Löschung für diejenigen Daten vor, die für die rechtlich zulässigen Zwecke nicht mehr erforderlich sind. Die Prinzipien wurden in ISO 29100 (siehe Nr. 4.4) als „*Data minimization*“ und „*Use, retention and disclosure limitation*“ aufgegriffen.

In der Praxis wird die Rechtsvorgabe zur Datenlöschung oft nur unzureichend umgesetzt. Sie stößt auf vielfältige Probleme, insbesondere

- werden Löschungsgebote von für die Verarbeitung Verantwortlichen bisweilen als unnötig oder kostenträchtig angesehen,
- würde die Löschung den Weg verbauen, die Daten zu einem späteren Zeitpunkt für einen (noch) unbekannten Zweck zu verwenden,
- sehen technische Systeme vielfach keine vollständige und nicht reversible Löschung von Daten vor,
- fällt es verantwortlichen Stellen schwer, für Datenbestände das Ende von Prozessen und damit konkrete Löschfristen festzulegen,
- weil viele Beteiligte differenzierte Löschregeln verstehen müssen, um die Löschmechanismen in den beteiligten IT-Systemen zu implementieren und
- weil es an klaren Vorstellungen fehlt, wie die korrekte Umsetzung der Löschregeln überprüft und nachgewiesen werden kann.

Um eine rechtskonforme, geordnete Löschung von personenbezogenen Daten sicherzustellen, müssen verantwortliche Stellen daher ein Regelwerk entwickeln und Verantwortung zuweisen. Die Etablierung eines solchen Löschkonzepts ist eine komplexe und umfangreiche Aufgabe. Die Erfolgsaussichten für die Entwicklung eines konkreten Löschkonzepts können verbessert werden, wenn die verantwortliche Stelle auf einen bewährten Vorschlag zur Vorgehensweise und zur Gestaltung zurückgreifen kann. In der vorliegenden Leitlinie wird eine Vorgehensweisen für die Etablierung eines betrieblichen Löschkonzepts vorgeschlagen.

Die Möglichkeit einer internationalen Standardisierung der Leitlinie wird durch das DIN geprüft. Die Leitlinie unterstützt verantwortliche Stellen dabei, ihre rechtlichen Pflichten zur Löschung personenbezogener Daten zu erfüllen. Sie gibt Empfehlungen für die Inhalte, den Aufbau und die Zuordnung von Verantwortung in einem datenschutzkonformen Löschkonzept. Die Vorgehensweise und Strukturierungsvorschläge sind auf alle verantwortlichen Stellen übertragbar. Die Leitlinie richtet sich primär an Verantwortliche für den Datenschutz und an Personen, die an der Entwicklung eines Löschkonzepts mitarbeiten. Die Leitlinie ist auf meiner Internetseite unter www.datenschutz.bund.de veröffentlicht.

Ein Löschkonzept kann nur dann mit akzeptablem Aufwand etabliert werden, wenn alle Beteiligten die Löschre-

geln nachvollziehen können und die Komplexität der Anforderungen überschaubar bleibt. Einfache Regeln sind daher der Schlüssel zum Erfolg. Die Leitlinie empfiehlt aus diesem Grund die Verwendung standardisierter Löschfristen und sogenannter Löschklassen, die gegebenenfalls organisationsspezifisch angepasst werden. Diese Löschklassen reduzieren die Komplexität der unterschiedlichen Löschanforderungen und bilden den Kern des Löschkonzepts. Sie werden für die Zuordnung von personenbezogenen Datenbeständen zu Löschregeln verwendet. Ein Löschkonzept der hier vorgeschlagenen Art hat für eine verantwortliche Stelle vielfältigen Nutzen:

- Es dient dem Schutz der Betroffenen im Sinne des Rechts auf informationelle Selbstbestimmung.
- Die verantwortliche Stelle erfüllt ihre Rechtspflichten und kann hinsichtlich der Einhaltung von Löschpflichten ihre Datenschutzkonformität belegen.
- Prozesse werden klarer festgelegt, weil durch die Pflicht zur Löschung ihr Ende definiert werden muss.
- Die Datenhaltung wird systematisiert und konsolidiert, weil auch Altbestände in die Löschung einbezogen werden müssen und diese dadurch bereinigt werden. Dadurch können auch der Aufwand und die Kosten für Datenmigrationen bei Systemwechseln erheblich reduziert werden.
- Durch die Bereinigung von Datenbeständen und das Auflösen unnötiger Redundanz können Kosten im IT-Betrieb gesenkt werden.
- Da das Löschkonzept Soll-Vorgaben für die Löschung von Datenbeständen macht, können daraus mit geringem Aufwand Prüfbedingungen für Audits abgeleitet werden.
- Durch die systematische Erfassung der personenbezogenen Daten erhält der Verantwortliche für Datenschutz einen Überblick über diese Bestände und die relevanten Systeme.
- Nicht zuletzt verbessert die Diskussion um Löschregeln und die konstruktive Gestaltung von Geschäfts- und IT-Prozessen die Verankerung des Datenschutzes innerhalb der verantwortlichen Stelle.

In der Leitlinie werden auch zentrale Begriffe definiert, die in den Diskussionen um Löschregeln benötigt werden. Sie erleichtern die Verständigung zwischen fachlichen Anwendern, IT-Verantwortlichen, Systementwicklern, Management, Verantwortlichen für den Datenschutz und anderen Beteiligten. Die Umsetzungsvorgaben für eine regelgerechte Löschung von personenbezogenen Daten in IT-Systemen können bereits bei der Konzeption von Geschäftsprozessen hilfreich sein. Für Systementwicklungs- und Systembeschaffungsprozesse können aus ihnen Löschanforderungen definiert werden. Die Leitlinie gibt zudem Software-Herstellern Hinweise darauf, wie IT-Systeme die Aufgaben der Löschung personenbezogener Daten durch verantwortliche Stellen unterstützen können.

Ich hoffe, dass Beteiligten die hier gegebene Möglichkeit nutzen, sich besser mit der Frage der Löschung in digitalen Systemen oder bei der Verarbeitung von digitalen Akten auseinanderzusetzen und daraus die notwendigen Konsequenzen ziehen.

4.6 Vernichtung von Datenträgern – neue DIN-Norm 66399 verabschiedet

Die im September 2012 veröffentlichte neue DIN-Norm zur Datenträgervernichtung (DIN 66399) ermöglicht der verantwortlichen Stelle als „Herr der Daten", die Schutzklassen und Sicherheitsstufen flexibel zu bestimmen und die für Ihren Bedarf angemessene Vernichtung von Datenträgern zu wählen.

Die neue DIN 66399 ersetzt die bisherige DIN 32757. Ich habe bereits im 23. Tätigkeitsbericht (Nr. 5.3) über die Probleme berichtet, die sich bei der Datenträgervernichtung durch moderne Technologien, neuere Materialen, Recycling– und Umweltaspekte ergeben. Das Resultat ausgedehnter Sitzungen mit Vertretern der Abfallwirtschaft und der Gerätehersteller besteht im Wesentlichen aus folgenden Änderungen:

- Klassifizierung der Daten in drei Schutzklassen
  Die Ermittlung des Schutzbedarfs und die Zuordnung der Schutzklasse sowie der Sicherheitsstufen dient der Klassifizierung der anfallenden Daten.
- Sechs Materialklassifizierungen
  Erstmals definiert die Norm unterschiedliche Materialklassifizierungen und berücksichtigt dabei die Größe der Informationsdarstellung auf den Datenträgern. Es wird unterschieden zwischen Papierdokumenten, optischen, magnetischen oder elektronischen Datenträgern und Festplatten.
- Sieben Sicherheitsstufen
  Statt bisher fünf Sicherheitsstufen definiert die neue DIN 66399 jetzt sieben Sicherheitsstufen. Ein wesentlicher Unterschied ist die neue Stufe P-4 mit einer Teilchenfläche von max. 160 mm².
- Die Aufnahme neuer Datenträger
  Die neue Norm bietet derzeit weltweit als einziger Standard eine umfassende Orientierung für die Vernichtung von „neuen Medien" (z. B. CD, DVD, Festplatten, USB-Stick, Speicherkarten). Mit der Einführung von zwei zusätzlichen Sicherheitsstufen, die der technischen Entwicklung Rechnung tragen sollen, werden zudem zukünftige Entwicklungen bereits im heutigen Standard berücksichtigt.

Die neue Norm definiert neben den reinen Anforderungen an Maschinen zur Vernichtung von Datenträgern auch die Prozesse rund um die Datenträgervernichtung. DIN 66399 ist somit die umfassendste, kompletteste Norm rund um das Thema Datenträgervernichtung. Gemeinsam mit dem nationalen Normungsgremium hoffe ich, die Norm auf internationaler Ebene verankern zu können.

4.7 Schadprogramm-Erkennungssystem des BSI: Nur bedingt datenschutzgerecht

Auch bei der Bekämpfung von Schadsoftware muss der Datenschutz gewährleistet sein. Ich habe das hierfür vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) eingesetzte Verfahren geprüft und dabei erhebliche Mängel festgestellt.

Die Umsetzung und Überführung eines Datenerhebungs- und Datenverwendungskonzepts des BSI sieht die automatisierte Untersuchung von Angriffen auf das Regierungsnetz vor. Ich habe mich im Rahmen einer Kontrolle über den Betrieb des Verfahrens informiert.

Nach § 3 Absatz 1 BSIG ist das BSI für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik des Bundes zuständig. Es soll Stellen des Bundes vor möglichen Sicherheitsproblemen warnen und insbesondere Schadprogramme und Gefahren für die Kommunikationstechnik erkennen (§ 5 BSIG). Hierzu hat das BSI das Verfahren „Schadprogramm-Erkennungssystem (SES)“ eingerichtet, das Angriffe auf die Kommunikationsinfrastruktur des Bundes erkennen und zu geeigneten Abwehrmaßnahmen führen soll. Das SES analysiert den ein- und ausgehenden Kommunikationsverkehr von Datendiensten automatisch mittels Sensoren – bei konkretem Verdacht auch manuell. Anwendung findet es in folgenden (Bundes-)Netzen: Informationsverbund Berlin-Bonn (IVBB), Netz der Bundeswehr, Übergang zum DOI-Netz (vormals TESTA, über das die Länder und EU-Einrichtungen angebunden sind) und Informationsverbund der Bundesverwaltung (IVBV).

Weitere Anbindungen sind in Planung: Bundesfinanznetz und Netz der Wasser- und Schiffsfahrtsverwaltung (BVBS-WAN). Für den Bundesbereich regelt § 2 Absatz 3 BSIG, welche Behörden nicht durch das SES überwacht werden dürfen. Meine Kontrolle ergab, dass das BSI die Regelung in allen Punkten umgesetzt hat.

Pro Netz werden Sensoren an definierten Übergabepunkten eingerichtet, die den ein- und ausgehenden Datenverkehr analysieren und verdächtige Datenströme selektieren und ausleiten. Dadurch können Angriffe auf die Kommunikationsinfrastruktur des Bundes detektiert werden. An den Sensoren wird auf der Basis voreingestellter Signaturen eine automatische Vorprüfung des Datenstroms vorgenommen. Nur Daten mit Indikation auf Schadprogramme oder Gefahren für die Kommunikationstechnik des Bundes werden ausgeleitet (erste Stufe). Grundlage für die Prüfung bilden Signaturlisten, die aus verschiedenen Quellen zusammengestellt und ständig angepasst werden, beispielsweise Meldungen aus den CERTs (Computer Emergency Response Teams).

Ausschließlich Daten mit Verdachtsmomenten werden anschließend über eine gesicherte Verbindung komplett zum BSI übertragen. Dort werden diese in einer zweiten Stufe einer intensiven automatisierten Analyse in einer speziellen Umgebung unterzogen. Stellt sich hierbei heraus, dass es sich nicht um einen Angriffsversuch oder eine Gefahrenquelle handelt, werden die Daten umgehend gelöscht. Die danach verbliebenen Fälle werden von speziell ausgebildeten Mitarbeitern auf Testsystemen manuell untersucht. Liegt ein Schadprogramm oder Angriff vor, wird der komplette Datensatz in einer (SES-)Datenbank gespeichert, in der nach Abschluss des Falls ausschließlich die nachgewiesenermaßen zu elektronischen Angriffen gehörigen Daten enthalten sind. Die Vorgaben des BSI-Gesetzes werden bei Analyse und Auswertung strikt beachtet.

Auch die Informationspflichten an den Betroffenen werden – wie ich feststellen konnte – umgesetzt.

Leider ging das BSI bei der Übermittlung entsprechender Informationen an Sicherheitsbehörden zu weit. So wurden regelmäßig Daten an eine Sicherheitsbehörde, die nicht explizit im Gesetz genannt ist, im Rahmen der Spionageabwehr übermittelt. Ich habe dies beanstandet. Das BSI hat das entsprechende Verfahren danach unverzüglich eingestellt.

Weitere Probleme gab es bei der Löschung von personenbezogenen Daten nach Ende der Fallbearbeitung in der SES-Datenbank. Auch in diesem Punkt konnte ich eine Einigung mit dem BSI erreichen.

Nach § 5 Absatz 7 BSIG dürfen personenbezogene Daten, die den Kernbereich privater Lebensgestaltung betreffen, sowie Daten, die unter § 3 Absatz 9 BDSG fallen, nicht verwendet werden, sie sind unverzüglich zu löschen. Wie die Kontrolle mit Hilfe der gesetzlich vorgeschriebenen Dokumentation ergeben hat, haben solche Fälle vorgelegen. Die entsprechenden Daten waren zwar irreversibel gelöscht, die Dokumentation ergab aber, Schwierigkeiten den Begriff „Kernbereich privater Lebensführung“ inhaltlich zu bewerten. Das BSI hat nach eigenen Angaben Schwierigkeiten, diese Vorgabe zu interpretieren und bei der manuellen Analyse eine richtige Zuordnung zu finden. Ich habe angeregt, die Beurteilungskriterien präziser zu fassen und die mit der manuellen Analyse befassten Mitarbeiter entsprechend zu schulen, was das BSI aufgegriffen hat. Außerdem habe ich hierzu meine Beratung angeboten.

Wie ich ferner festgestellt habe, fehlt für die Nutzer des SES ein formales Benutzerverwaltungsverfahren. Auch dies wurde in zwischen vom BSI behoben.

Die von mir nach § 25 Absatz 1 BDSG beanstandeten erheblichen Mängel hat das BSI umgehend aufgegriffen und entsprechende Maßnahmen eingeleitet. Den Ausbau der „Netze des Bundes“ und die damit verknüpften Sicherheitsfragen und Überwachungstechniken werde ich weiterhin aufmerksam beobachten.

4.8 Aufräumen am Arbeitsplatzrechner

Auch auf Arbeitsplatzrechnern müssen personenbezogenen Daten zeitgerecht gelöscht werden.

In fast allen von mir kontrollierten Behörden entdecken meine Mitarbeiterinnen und Mitarbeiter „Dateileichen“ an den Arbeitsplätzen. So ist es weit verbreitet, Originaldokumente als Musterschreiben zu nutzen. Diese Dokumente enthielten – teilweise sehr sensible – perso-

nenbezogene Informationen, z. B. interne Beurteilungen, disziplinarrechtliche Maßnahmen gegenüber Mitarbeitern, Informationen über Krankheiten der Mitarbeiter oder sehr persönliche Daten und Bescheide zu „Kunden“ der Behörde die in jedem Fall hätten gelöscht sein müssen. Auch werden ungeschützt Dokumente, z. B. in gängigen Office-Formaten, per E-Mail weitergeleitet.

Jeder einzelne Punkt ist ein klarer Datenschutzverstoß.

Diese Maßnahmen können das Aufräumen des Arbeitsplatzrechners erleichtern:

- Werden statt „Musterschreiben“ Dokumentenvorlagen (z. B. bei Word) verwendet, können diese ohne Personenbezug erstellt und wiederverwendet werden.
- Eine einheitliche transparente Struktur der Ablage hilft die Übersicht über vorhandene Dokumente zu erhalten. Dokumente können z. B. in Verzeichnissen nach Sachlagen oder nach zeitlichen Angaben strukturiert werden. Viele Betriebssysteme unterstützen das Auffinden von Dokumenten durch Suchkriterien wie Erstellungsdatum oder Dokumententyp.
- Die Verwendung von Verschlüsselungsprogrammen ist durch Schulungen zu üben, so dass schützenswerte Daten nur verschlüsselt mittels E-Mail versandt werden.

Ich werde mich dafür einsetzen, dass in allen Behörden in etwa jährlichem Abstand entsprechende Datenschutzschulungen angeboten werden und die behördlichen Datenschutzbeauftragten regelmäßig Arbeitsplatzkontrollen durchführen.

4.9 Dokumentationspflichten bei der Entwicklung von Software und deren Nutzung

Bei Kontrollen musste ich wiederholt feststellen, dass die von verantwortlichen Stellen vorgelegten Unterlagen die datenschutzrechtlichen Dokumentationspflichten verletzten.

Die Revisionsfähigkeit von Systemen ist eine wichtige Voraussetzung bei datenschutzrechtlichen Kontrollen und Beratungen. Da die Systeme immer komplexer werden, ist die Prüfung des Systems nur möglich, wenn entsprechende Unterlagen vorliegen, die deren Funktionsweise und den dabei vorgesehenen Umgang mit personenbezogenen Daten dokumentieren. Auch meine Kontrollaufgaben kann ich nur dann wahrnehmen, wenn das zu kontrollierende System in ausreichendem Maß „revisionsfähig“ ist.

Die Revisionsfähigkeit von Hard- und Software ergibt aus dem Einleitungssatz zur Anlage von § 9 BDSG. Dort werden technische und organisatorische Maßnahmen gefordert, um die Ausführungen des Gesetzes zu gewährleisten. Datensicherheit setzt auch immer voraus, dass der verantwortlichen Stelle bewusst ist, welche Systeme wo eingesetzt werden und welchen Funktionsumfang sie haben. Außerdem muss die verantwortliche Stelle wissen, wie die personenbezogenen Daten im System verarbeitet werden. Insofern dient die Verfahrensdokumentation in erster Linie den Verfahrensverantwortlichen und darf nicht als lästige Verpflichtung gegenüber möglichen Kontrolleuren missverstanden werden.

Immer wieder werden Fragen an mich herangetragen, was unter dem Begriff Dokumentation zu verstehen ist und welchen Umfang sie haben soll. Unter „Dokumentation“ werden im Allgemeinen alle Unterlagen verstanden, die die Funktionsweise, die unterschiedlichen Rollen, die Bedingungen für den Betrieb sowie Wartungs- und Pflegeanweisungen erklären. Es gibt nicht eine Dokumentation, sondern verschiedene Dokumente, die an unterschiedliche Zielgruppen gerichtet sind (vgl. Kasten zu Nr. 4.9).

Nur wenn diese Dokumente vollständig vorliegen, ist die Revisionsfähigkeit des Verfahrens gewährleistet und damit eine wichtige Grundlage zur Datensicherheit gegeben.

Immer wieder musste ich im Berichtszeitraum feststellen, dass die Pflicht einer ausreichenden Dokumentation von der verantwortlichen Stelle verletzt wurde (vgl. z. B. Nr. 3.5.1, 9.6). Grundsätzlich müssen zwar nicht bei jedem Einsatz von Software alle im Kasten zu Nr. 4.9 genannten Dokumente vorliegen. So verlange ich etwa bei Einsatz von Standardprogrammen nicht die Vorlage des Quellcodes. Beim Einsatz von speziell entwickelter Software mit spezifischen Funktionalitäten und bei Verarbeitung sehr schützenswerter Daten liegt das anders. Dann ist für die datenschutzrechtliche Bewertung des Systems die Vorlage des Quellcodes und weiterer Unterlagen eine notwendige Voraussetzung.

Wie umfangreich eine Dokumentation sein muss, kann ebenfalls unterschiedlich bewertet werden. Die entsprechenden DIN-Normen 66230 Programmdokumentation, 66231 Programmentwicklungsdokumentation und 66232 Datendokumentation wurden leider 2004 zurückgezogen und können nicht mehr herangezogen werden. Gleichwohl gibt es internationale (ISO-, EN-)Standards, die sich mit den Dokumentationspflichten befassen, beispielsweise EN 15380 für die Dokumentation des Datenaustauschs. Ich empfehle deshalb allen verantwortlichen Stellen, entsprechende Dokumente nach den gültigen Normen einzufordern. Auch die Zertifizierung von Systemen und Programmen beispielsweise nach den Common Criteria verlangt die Vorlage entsprechender Dokumente. Sie bilden somit die Richtschnur, welche Dokumente vorhanden sein müssen.

Im Übrigen weise ich darauf hin, dass im Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik entsprechende Anforderungen fixiert sind, beispielsweise in Maßnahme „M 2.62 Software-Abnahme- und Freigabe-Verfahren“. Auch verschiedene Gerichte haben sich bereits mit dieser Frage befasst und die Programmdokumentation explizit gefordert, beispielsweise das OLG Karlsruhe, das in der vertraglichen Pflicht zur Überlassung einer Dokumentation implizit auch eine Pflicht zur Quellcodeübergabe sah (OLG Karlsruhe, Computer und Recht 1999, 11). Das LG Frankfurt hat für

jeden Programmerstellungsvertrag eine Auslieferung des Quellcodes verlangt, und das schon vor der Abnahme (LG Frankfurt, BB Beilage 1993, Nr. 3, 4 und 5 [ODER Computer und Recht 1993, 693]). Besonders bei „Datenschutz-kritischen“ Anwendungen werde ich die Einhaltung der Dokumentationspflichten weiterhin genau beobachten.

Kasten zu Nr. 4.9

Ich empfehle allen verantwortlichen Stellen grundsätzlich folgende Teile vor dem Wirkbetrieb bereitzuhalten:

- Installationsdokumentation,
- Benutzerdokumentation,
- Bedienungsanleitungen (Fehlerbeschreibungen etc.),
- Datenflussdokumentation,
- Programmdokumentation (Quellcode, Beschreibung zur Übersetzung des Quellcodes etc.),
- Methodendokumentation (Beschreibung verwendeter Algorithmen, mathematischer Modelle etc.),
- Datendokumentation (welche Daten wie bearbeitet werden, Wertebereiche, Löschkonzept, Datenflussdiagramm, Import-/Exportschnittstellen etc.),
- Testdokumentation (Nachweis über den erfolgreichen Testlauf vor Beginn des Wirkbetriebs, Testdatenbestand) und
- Entwicklungsdokumentation.

5 Internet

5.1 Auskunftsanspruch nach § 101 UrhG – Zeig mir Deine IP und ich sage Dir, wer Du bist

Aufgrund der Entscheidung des Bundesgerichtshofs (BGH) zu den Voraussetzungen des Auskunftsanspruchs nach § 101 Urheberrechtsgesetz (UrhG) werden künftig wohl mehr Kundendaten von Internetzugangsanbietern an Rechteinhaber übermittelt werden. Der Gesetzgeber ist zur Überprüfung der gesetzlichen Regelungen aufgerufen.

Nach wie vor erreichen mich Eingaben von Bürgerinnen und Bürgern, die kostenpflichtig abgemahnt wurden, weil sie widerrechtlich Dateien über das Internet heruntergeladen hätten. Die Abmahngebühren können sich dabei im Einzelfall auf mehrere tausend Euro summieren. In den Abmahnschreiben wurde den Anschlussinhabern mitgeteilt, die Rechteinhaber hätten ihre Adresse über die Internetzugangsanbieter erhalten. Diese haben bei Verdacht von Urheberrechtsverletzungen die Möglichkeit, auf Grund gerichtlicher Anordnung die Kundendaten eines Anschlussinhabers zu erfahren. Wenn der Internetzugangsanbieter aufgrund einer solchen Anordnung die Kundendaten (Name und Anschrift) an den Rechteinhaber weitergibt, ist dies datenschutzrechtlich nicht zu beanstanden (vgl. 23. TB Nr. 4.8).

Gleichwohl sehe ich die Entwicklungen in diesem Bereich weiterhin kritisch. Von den Rechteinhabern beauftragte Unternehmen setzen spezielle Software ein, um Internettauschbörsen systematisch nach Urheberrechtsverletzungen zu durchsuchen. Spezielle gesetzliche Regelungen hierzu existieren nicht. Die Gerichte sehen die automatisierte Ermittlung der IP-Adressen möglicher Rechteverletzer jedoch als zulässig an.

Darüber hinaus wurden die Voraussetzungen, unter denen die Internetzugangsanbieter zur Auskunft verpflichtet werden können, auf Grund der am 10. August 2012 veröffentlichten BGH-Entscheidung zu den Voraussetzungen des § 101 UrhG (I ZB 80/11), weiter abgesenkt. Im Rahmen des Gesetzgebungsverfahrens zur Einführung des Auskunftsanspruchs hatte ich zum Ausdruck gebracht, dass dieser auf gravierende Fälle zu begrenzen sei (vgl. 21. TB Nr. 6.5). Mit dem neuen § 101 UrhG wurde dann eine komplizierte Regelung des Auskunftsanspruches geschaffen, zu dessen Voraussetzungen auch in der Rechtsprechung unterschiedliche Meinungen vertreten wurden. Einige Gerichte gingen von dem Verdacht einer „Rechtsverletzung in gewerblichem Ausmaß“ als Voraussetzung für die gerichtliche Anordnung aus und lehnten Anträge von Rechteinhabern zum Beispiel dann ab, wenn es sich um ältere Musiktitel handelte. Seit der BGH-Entscheidung ist die Schwere des Rechtsverstoßes nicht zu prüfen, sondern es genügt der Verdacht einer einfachen Rechtsverletzung.

Da die Instanzgerichte sich an der Entscheidung des BGH orientieren werden, dürfte die Zahl der Auskunftsersuchen zunehmen. Deshalb stellt sich die Frage, ob diese Rechtslage nicht einen unverhältnismäßigen Eingriff in das Fernmeldegeheimnis der Anschlussinhaber darstellt. Da nach meiner Ansicht der Auskunftsanspruch auf gravierende Rechtsverletzungen beschränkt werden sollte, empfehle ich dem Gesetzgeber, die geltende Rechtslage zu überprüfen und sie unter dem Gesichtspunkt der Verhältnismäßigkeit anzupassen.

5.2 „ACTA“ – ad acta!?

Nach europaweiten Protesten hat das Europäische Parlament am 4. Juli 2012 das Handelsübereinkommen zur Bekämpfung von Produkt- und Markenpiraterie (Anti-Counterfeiting Trade Agreement – ACTA) mit großer Mehrheit abgelehnt. Das Übereinkommen wird bis auf weiteres nicht in Kraft treten.

In meinem 23. TB (Nr. 4.7) hatte ich über die Verhandlungen zu ACTA berichtet, dessen endgültige Version seit Dezember 2010 vorlag. Als bekannt wurde, dass die Europäische Union und 22 ihrer Mitgliedstaaten ACTA am 26. Januar 2012 gezeichnet hatten, wurde die Kritik gegen das Übereinkommen lauter. Die Kritiker von ACTA sorgten sich, das Urheberrecht würde zu Lasten

der Internetnutzer verschärft werden. Sie befürchteten insbesondere Internetzensur und Netzsperren nach dem „Three-Strikes-Modell“ und eine Überwachung des Internetverkehrs.

Die Kritik der Gegner war durchaus begründet, da der endgültige Vertragstext viele unbestimmte Regelungen enthält. Aus den Bestimmungen lassen sich zwar keine konkreten Verpflichtungen zur Änderung des bestehenden Rechts entnehmen, sie lassen aber einen großen Interpretationsspielraum offen, bis hin zu einer Verpflichtung der Zugangsprovider zur Überwachung und Filterung des Internetverkehrs. Die Regelungen hätten somit als Vorwand verwendet werden können, um sich für Verschärfungen der Vorschriften zur Durchsetzung von Urheberrechten zu Lasten von Informationsfreiheit und Datenschutz einzusetzen.

Nach der massiven Kritik der Öffentlichkeit teilte das Bundesministerium der Justiz (BMJ) im Februar 2012 mit, Deutschland werde das Übereinkommen zunächst nicht zeichnen. Und die Europäische Kommission erklärte, das Übereinkommen vom Europäischen Gerichtshof (EuGH) auf seine Vereinbarkeit mit den europäischen Grundrechten prüfen zu lassen. Auf diese Prüfung kam es dann letztlich aber nicht mehr an. Das Europäische Parlament entschied sich dagegen, seine Abstimmung über ACTA bis nach der Entscheidung des EuGH zu vertagen. Es stimmte am 4. Juli 2012 gegen ACTA. Damit können auch die Mitgliedstaaten der EU dem Übereinkommen nicht mehr wirksam beitreten.

Das Ende von ACTA ist sicherlich nicht der Schlusspunkt hinter Bestrebungen, zu internationalen Übereinkünften zur Durchsetzung der Rechte des geistigen Eigentums zu kommen. Anders als bei dem gescheiterten Vorhaben dürfen die Regelungen aber nicht zu Lasten des Schutzes der personenbezogenen Daten und der Informationsfreiheit der Bürgerinnen und Bürger gehen. Die verschiedenen Rechtspositionen müssen in einen angemessenen Ausgleich gebracht werden.

5.3 Cloud Computing – heiter bis wolkig

Cloud Computing hat sich zu einem gängigen Geschäftsmodell entwickelt. Grund genug, mich auf nationaler und internationaler Ebene intensiv dieses Themas anzunehmen.

Cloud Computing hat sich innerhalb weniger Jahre von einem Technologietrend mit überschaubaren Angeboten hin zu einem festen Geschäftsmodell entwickelt und auf dem weltweiten Markt etabliert. Die Cloud ist für uns allgegenwärtig geworden; egal ob sie vom Smartphone zum Abrufen von gespeicherten E-Mails, Fotos oder Musik oder für komplexe IT-Prozesse genutzt wird. Oft wissen oder merken wir nicht einmal, dass wir Cloud-Dienste in Anspruch nehmen und wo die Daten liegen oder wo „gerechnet“ wird. Dabei kann die Verwendung von Cloud nicht nur die Datenverarbeitung erleichtern und z. B. zu Kosteneinsparungen führen; unter bestimmten Voraussetzungen können auch weitere Synergieeffekte und zum Beispiel ein Plus an IT-Sicherheit erreicht werden.

Über die Risiken des oft praktizierten Modells der Auftragsdatenverarbeitung nach der europäischen Datenschutzrichtlinie und § 11 BDSG für das Speichern und Verarbeiten von Daten in weltweit vernetzte Rechenzentren habe ich bereits ausführlich im 23. TB (Nr. 5.6) berichtet. Hier hat es mit der Verabschiedung verbindlicher Unternehmensregelungen für Auftragsdatenverarbeiter („BCR for processors“) durch die Artikel-29-Gruppe allerdings im Berichtszeitraum eine wichtige Entwicklung gegeben (vgl. Nr. 2.4.1.2).

Problematisch ist in diesem Zusammenhang aber weiterhin die Zugriffsmöglichkeit staatlicher Stellen, insbesondere aus Drittstaaten auf Daten, die in der Cloud gespeichert sind. Dieses Problem betrifft z. B. Anbieter von Cloud-Diensten, die Regelungen wie dem US-Patriot Act unterliegen und damit zur Herausgabe von Daten an fremde Sicherheitsbehörden verpflichtet werden könnten. Selbst Anbieter, die Subunternehmen von US-amerikanischen Firmen mit Sitz innerhalb Europas sind, aber die Daten außerhalb der USA speichern, können davon betroffen sein. Diese Einschätzung wurde jüngst durch das Institute for Information Law der Universität Amsterdam in einer Studie bestätigt (http://www.ivir.nl/index-english.html).

Nicht zuletzt deshalb halte ich es für nötig, die in die Cloud auszulagernden (insbes. sensiblen) personenbezogenen Daten vor dem Hochladen sicher und unter alleiniger Kontrolle des Auftraggebers nach dem Stand der Technik zu verschlüsseln.

Die Rechtsunsicherheit bei der Verarbeitung außerhalb der EU/des EWR und das hohe Datenschutzniveau innerhalb der EU könnten allerdings auch ein Gewinn und Standortvorteil für Cloud „Made in Germany“ oder Europa mit sich bringen.

Die IT-Sicherheitsbranche und Datenschutzbeauftragte setzen sich intensiv mit dem Thema auseinander (vgl. auch Kasten zu Nr. 5.3). Es gibt allerdings weiterhin viele offene Fragen.

Es wäre z. B. denkbar, eine allgemeine Rechtsgrundlage für Datenschutzzertifizierungen und Gütesiegel ähnlich wie bei der De-Mail in Deutschland (vgl. Nr. 3.2.4) zu schaffen. Internationale Normen und Standards könnten für weltweite Vergleichbarkeit von sicheren und datenschutzgerechten Cloud-Lösungen sorgen. Weitere Entwicklungen, wie etwa die erwartete neue EU-Datenschutzverordnung (vgl. Nr. 2.1.1), werden vermutlich auch Veränderungen beim Rechnen in der Wolke mit sich bringen.

Es bleibt also spannend.

Kasten zu Nr. 5.3

Arbeitsgruppen und Veröffentlichungen zum Cloud Computing

Mit einer Entschließung der 82. Konferenz der Beauftragten für den Datenschutz des Bundes und der Länder wurde die Orientierungshilfe – Cloud Computing angenommen. Sie richtet sich an Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche und soll den datenschutzgerechten Einsatz dieser Technologie fördern. http://www.datenschutz.bund.de

Die Artikel-29-Datenschutzgruppe hat im Juli 2012 das Working Paper WP 196 der europäischen Datenschutzbeauftragten veröffentlicht, welches auf rechtliche Probleme und Risiken beim Cloud Computing aufmerksam macht und entsprechende Hinweise gibt. Kerninhalte des Papiers sind Ausführungen zum anwendbaren Recht für die Pflichten und Verantwortlichkeiten von Cloud-Anbietern und Cloud-Anwendern, technisch-organisatorische Maßnahmen zum Schutz der Daten in der Cloud sowie rechtliche und technische Vorgaben für Datentransfers in Drittstaaten. Es wird insbesondere darauf hingewiesen, dass alle Subunternehmer benannt und alle relevanten Details offen gelegt und vertraglich geregelt werden sollten. Aufgenommen in die Opinion wurden auch technische und organisatorische Maßnahmen des Datenschutzes und der Datensicherheit, wie Sie in der Veröffentlichung „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder veröffentlicht wurden. Demnach sind neben der Vertraulichkeit, Integrität und Verfügbarkeit ebenso die Schutzziele Isolierung (entspricht dem in Deutschland gebräuchlichen Begriff der Unverkettbarkeit), Intervenierbarkeit, Rechenschaft und Portabilität aufgeführt.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf#h2-1

Weitere Diskussionen auf internationaler Ebene fanden in der Arbeitsgruppe der IWGDPT (International Working Group on Data Protection in Telecommunications) im Frühjahr 2012 und auf der 34. Internationalen Datenschutzkonferenz in Uruguay im letzten Herbst statt (vgl. Nr. 2.4.3). In ihrem Sopot Memorandum weist die IWGDPT auf ein hohes Transparenzgebot hin, während auf der internationalen Datenschutzkonferenz in einer Entschließung unter anderem die Überprüfung und Einhaltung eines ausreichenden Datenschutzniveaus sowie die frühzeitige Berücksichtigung und Implementierung des sogenannten „Privacy by Design“ (PbD) in den Vordergrund gestellt wurden.
http://datenschutz-berlin.de/content/nachrichten/datenschutznachrichten/%2027-april-2012,
http://www.datenschutz.bund.de

Der BfDI engagierte sich zudem in der AG-Rechtsrahmen der Trusted-Cloud-Initiative des BMWi (http://www.trusted-cloud.de) und in mehreren Arbeitsgruppen der AG4 des IT-Gipfels der Bundesregierung. Dabei wurden in beiden Bereichen Papiere mit Datenschutzbezug erarbeitet. Die Veröffentlichung „Datenschutzrechtliche Lösungen für Cloud Computing – Ein rechtspolitisches Thesenpapier“ der AG-Rechtsrahmen geht in ihren zehn Thesen auf die Problematiken beim Cloud Computing im Zusammenhang mit der Auftragsdatenverarbeitung, der Erteilung von Testaten und mögliche Akkreditierungen ein. Ein innerhalb der UAG Cloud des IT-Gipfels erarbeitetes Dokument „Rechtliche Anforderungen an Cloud Computing – Sichere Cloud-Dienste“ steht leider immer noch aus. Bei einer Veranstaltung der AG4 in Bonn im September 2012 hat sich gezeigt, dass Cloud innerhalb der IT-Branche ein kontrovers diskutiertes Thema ist und dass weiterhin offene Fragen der IT-Sicherheit und des Datenschutzes bestehen, auch wenn sich bei vertraglicher Beauftragung zur Nutzung von Cloud-Diensten im Vergleich zum klassischen IT-Outsourcing rein datenschutzrechtlich gesehen bis auf die Unbekanntheit des Ortes der Speicherung und Verarbeitung nicht „all zu viel“ geändert hat.

Allgemein werden derzeit immer wieder Forderungen nach Standards und Zertifizierungen beim Cloud Computing gestellt. In einem ersten Schritt hat das Bundesamt für die Sicherheit in der Informationstechnik (BSI) ein Eckpunktepapier unter meiner Mitwirkung erstellt und veröffentlicht, welches Basisanforderungen, Anforderungen an hohe Vertraulichkeit und hohe Verfügbarkeit auf Grundlage des IT-Grundschutzes beim Einsatz von Cloud Computing sowie Hinweise zum Datenschutz enthält. Das Eckpunktepapier ist unter (http://www.bsi.de) abrufbar. In einem nächsten Schritt ist man gerade dabei eine IT-Sicherheitszertifizierung von Cloud-Technologien vorzubereiten. Schon in naher Zukunft wird es beim Cloud Computing geprüfte IT-Sicherheit in Deutschland geben.

5.4 Stillstand: der Cookie-Paragraph

Es ist unklar, ob und auf welcher Grundlage die als Cookie-Paragraph bekannte Regelung der E-Privacy-Richtlinie in Deutschland angewendet werden soll.

Die Sache ist festgefahren: Das zuständige Bundesministerium für Wirtschaft und Technologie bleibt bei seiner Meinung, das Einwilligungserfordernis für das Setzen von Cookies sei eigentlich schon immer im Telemediengesetz (TMG) festgeschrieben gewesen (vgl. 23. TB Nr. 4.4), die Datenschutzaufsichtsbehörden wenden bisher weiterhin überwiegend die Widerspruchsregelung des § 15 Absatz 3 TMG an, die EU-Kommission schweigt. Sie prüft.

Verunsichert sind die Anbieter von Internetdiensten, die ihr Angebot rechtskonform gestalten wollen, und die Nutzer, die sich nicht heimlich beobachten lassen wollen. Nach einer Lösung gefragt sind immer wieder die Datenschutzbehörden, die für Anbieter und Nutzer gleichermaßen Ansprechpartner sind.

Wie soll eine Lösung aussehen? Der Vorstoß der SPD-Bundestagsfraktion vom Januar 2012 (Bundestagsdrucksache 17/8454), die Einwilligungslösung durch eine Änderung des TMG festzuschreiben, war erfolglos. Ebenso meine Bemühungen im Rahmen der Novellierung des Telekommunikationsgesetzes (vgl. Nr. 6.4). Einschwenken auf die Position des Ministeriums? Direktes Anwenden der Richtlinie wegen nicht erfolgter Umsetzung? Warten auf ein Zeichen der Kommission? Einen Königsweg gibt es hier wohl nicht. Vielleicht bleibt nur der (Um-)Weg über ein Gericht, das zumindest die Richtung weisen kann.

Erste technische Realisierungen für eine Einwilligung werden schon eingesetzt oder entwickelt. Da aber auch hier Unklarheiten bestehen, hat die Artikel-29-Gruppe begonnen, verschiedene Lösungen zu sammeln und zu bewerten, um europaweit zu einer einheitlichen Umsetzung des Cookie-Paragraphen zu gelangen. Sie orientiert sich dabei auch an ihrer „Stellungnahme zur Ausnahme von Cookies von der Einwilligungspflicht“ (WP 194). Die Ergebnisse werden zu gegebener Zeit veröffentlicht.

Auf internationaler Ebene gibt es Bestrebungen, einen „Do-not-track-Standard“ (DNT) zu entwickeln, der es den Nutzern ermöglichen soll, eine verbindliche Willenserklärung zur Erfassung ihres Surfverhaltens beim Besuch einer Website abzugeben. Dies umfasst dann auch das Setzen von Cookies. Der DNT-Standard, an dem vom W3C (World Wide Web Consortium) gearbeitet wird, sollte ursprünglich Anfang 2013 veröffentlicht werden. Allerdings ziehen sich die Arbeiten – auch aufgrund von unterschiedlichen Interessen und deutlichen Zielkonflikten innerhalb der W3C-Arbeitsgruppe – noch hin.

Die Artikel-29-Gruppe hat daher erhebliche Zweifel, ob der Standard – jedenfalls in seiner „weichen“ Form, wie ihn die meisten wirtschaftsnahen Vertreter in der W3C befürworten – tatsächlich die Anforderungen des Artikels 5 Absatz 3 der E-Privacy-Richtlinie erfüllen wird. Europarechtskonform wäre nur eine Lösung, bei der das „do not track“ im Header eines Browser-Befehls verbindlich ist und nicht erst das Einblenden von Werbung, sondern auch schon das Setzen von Cookies und das Erheben von Daten für Werbezwecke verhindert. Und das muss für alle Anbieter gelten, unabhängig davon, ob sie Anbieter der besuchten Website (first party) oder Werbeanbieter (third party) sind.

5.5 Hinter verschlossenen Türen: ICANN und die neuen Verträge mit den Registraren

Weitgehend unbemerkt werden die Verträge zwischen ICANN und den Registrierungsstellen überarbeitet und um zusätzliche Pflichten erweitert – leider auch zu Lasten des Datenschutzes.

Die wenigsten Internetnutzer wissen, wer ICANN ist und was diese Stelle tut. Kurz gesagt: Die Internet Corporation for Assigned Names and Numbers ist eine nicht auf Gewinn ausgerichtete Organisation mit Sitz in den USA und koordiniert die Vergabe von Namen und Adressen im Internet. Registrierungsstellen in den verschiedenen Ländern – oftmals sind dies Internetzugangsanbieter – übernehmen als letztes Glied die lokale Vergabe von Domainnamen und die Verteilung von IP-Adressen an Personen und Organisationen. Zu diesem Zweck schließt ICANN mit den Registraren Verträge ab, in denen unter anderem geregelt ist, welche Daten von den Endkunden erhoben, gespeichert und in den WhoIs-Datenbanken veröffentlicht werden müssen.

Diese Verträge werden derzeit überarbeitet. An dem Prozess sind neben den Registraren auch Vertreter der Strafverfolgungsbehörden und – nur beratend – der Regierungsbeirat GAC (Governmental Advisory Committee) beteiligt, der einen ständigen Sitz bei der EU-Kommission hat. Datenschützer haben keine Stimme.

Es verwundert daher nicht, dass insbesondere die „Wünsche“ der Strafverfolger berücksichtigt und in die neuen Verträge aufgenommen werden sollen: die jährliche Reverifizierung von Kontaktdaten der Registranten (E-Mail-Adresse, Telefonnummer), die beide auch in der WhoIs-Datenbank veröffentlicht werden sollen, und die Speicherung von personenbezogenen Daten, die weit über das für betriebliche Zwecke erforderliche Maß hinausgehen, wie z. B. zusätzliche Bankdaten, IP-Adressen, Logfiles etc. Diese Daten sollen die Arbeit der Strafverfolger erleichtern, damit die zunehmenden illegalen Handlungen und Geschäfte im Internet, wenn nicht verhindert, so doch zumindest aufgeklärt werden können.

Ein wesentlicher Grund für die vielfach falschen Angaben in WhoIs-Datenbanken ist ICANN seit langem bekannt: Richtige Kontaktdaten, vor allem von Privatpersonen, sind eine Quelle für Spammer, und daher werden bei der Registrierung zum eigenen Schutz falsche Daten angegeben. Dem könnte z. B. durch Einführung des OpoC-Models (Operational Point of Contact) abgeholfen werden, was bisher nicht geschehen ist. Anfragen berechtigter Stellen würden dann von einer vertrauenswürdigen Stelle beantwortet, die die WhoIs-Daten verwaltet. Dieses Modell würde die öffentlichen WhoIs-Datenbanken ersetzen und damit auch den Interessen der Privatpersonen am Schutz ihrer Daten Rechnung tragen.

Die Artikel-29-Gruppe hat sich im September 2012 mit einem Schreiben an ICANN gewandt und sich gegen die Erweiterungen in den Verträgen ausgesprochen, da sie nach europäischem Recht unzulässig seien. Denn Registrare dürfen nicht vorsorglich und ohne Rechtsgrundlage Daten für Strafverfolgungszwecke sammeln und vorhalten, die weder für vertragliche Zwecke noch für die Erbringung des Dienstes erforderlich sind. Würden sie dazu vertraglich von ICANN verpflichtet, verstießen sie gegen europäisches Recht.

Ob ein Kompromiss gefunden werden kann und es eine Ausnahmeregelung für EU-Registrare geben wird, ist offen. Eine solche wurde jedenfalls in dem Antwortschreiben von ICANN in Aussicht gestellt. Die Verhandlungen dauern noch an.

5.6 IPv6 – Wird wirklich gut, was lange währt?

Die schöne neue Welt der geänderten Kennzeichenpflicht auf der Datenautobahn hat zwei Seiten. Dem „paranoiden" Nutzer stechen zunächst das ungeheure Überwachungspotential und die Identifizierbarkeit des Einzelnen ins Auge. Dabei bietet die Neuordnung der IP-Adressen auch Raum für datenschutzfreundliche Lösungen und somit letztlich unbeschwerte „Ausfahrten" auf der Datenautobahn.

Technologien und Trends im und um das Internet herum verbreiten und entwickeln sich in der Regel rasend schnell, viel schneller als wir es je in anderen Bereichen gewohnt waren. Allerdings scheint es auch beim Internet immer wieder Ausnahmen zu geben, die diese Regel bestätigen. Schon wenige Jahre nach der Einführung der aktuellen Version vier des Internetprotokolls (IPv4) im Jahre 1983 zeichnete sich durch den sprunghaften Anstieg der Nutzer ab, dass der zur Verfügung stehende Adressumfang sehr bald zur Neige gehen würde. Allerdings wäre man 1998, als man mit der Standardisierung des Nachfolge-Protokolls begann, sicher überrascht gewesen, dass erst zu Beginn des Jahres 2012 der letzte Adressblock in Europa ausgegeben wurde.

Die Nachfolgerversion sechs (IPv6) vergrößert im Vergleich zu IPv4 den Adressraum um den unglaublichen Faktor 2 hoch 96. Insgesamt bietet IPv6 einen Adressvorrat von ca. 340 Sextillionen Adressen. Dies bedeutet, dass jeder Quadratmeter der Erdoberfläche in etwa mit 655 570 793 348 866 943 898 599 Adressen ausgestattet werden kann. Würde jede Adresse (ganz gleich ob IPv4 oder IPv6) durch ein Sandkorn dargestellt, ergäbe die Gesamtheit der Adressen von IPv4 einen handlichen Ball mit 8 cm Durchmesser, wohingegen alle IPv6-Adressen die Größe eines stattlichen Asteroiden mit einem Durchmesser von 350 km erreichen würden. Im Gegensatz zu ihrem Vorgänger teilt sich eine IPv6-Adresse in zwei gleich große Teile (je 64 bit). Der „vordere" Teil der Adresse, das sog. *Präfix*, dient im Wesentlichen der Identifikation des Netzsegmentes (beispielsweise des spezifischen Hausanschlusses). Der „hintere" Teil, der *Interface Identifier*, komplettiert die Adresse und ist die Identifikation der einzelnen Netzwerkkarte (vgl. Kasten a zu Nr. 5.6).

Anhand der zuvor genannten Zeiträume ist die Tatsache, dass die Internetadressen des derzeitigen Internetprotokolls (IPv4) knapp werden, ja schon lange bekannt. Dennoch hat die „plötzliche" Gewissheit der Vergabe der letzten Adressblöcke zu Beginn des Jahres 2012 in Unternehmen und Behörden eine gewisse Hektik hervorgerufen und die Anstrengungen zur Verwendung des gar nicht mehr so neuen Protokolls IPv6 verstärkt. Problematisch daran ist: Mit der Erweiterung des Adressraumes ändert sich auch die grundlegende Strategie der Adressverteilung. Es ist (grundsätzlich) zukünftig möglich, jedes an das Internet angeschlossene Gerät mit einer eigenen dauerhaften Adresse zu versehen, quasi ein Kennzeichen für jeden Computer, jede Kaffeemaschine und jeden Stromzähler. Angesichts dessen mögen sich jene schon die Hände reiben, deren Geschäfte auf der möglichst lückenlosen Registrierung des Nutzerverhaltens und der Bildung von Verhaltensprofilen basieren.

Jedoch war das bisher allenfalls Theorie, denn bekommen konnte man das Protokoll am hauseigenen Internetanschluss nur sehr schwer. Verfügbar wurde das Produkt erst durch die stille Einführung eines großen Providers, der IPv6 nicht als Neu-Produkt, sondern als technischen Fortschritt bestehender Produkte sieht. Hier bekommt jeder Neukunde bei Beantragung eines Internetzugangs seit September 2012 einen IPv6-basierten Anschluss, und den meisten dürfte es nicht mal auffallen. Von Beginn der Einführung an wurde auf die sofortige Neuvergabe des Präfixes bei der Trennung und dem Wiederaufbau der Verbindung Wert gelegt und diese auch realisiert. Bislang jedoch nötigt die fehlende Zwangstrennung den Liebhaber wechselnder Adressen, sich das neue Präfix manuell durch Ausschalten oder halbautomatisch durch eine Zeitschaltuhr an der Stromversorgung des Routers zu organisieren. Jedoch sind hier schon bald deutlich komfortablere Lösungen zu erwarten: ein Knopf auf der Konfigurationsoberfläche, mit dem ein neues Präfix erzwungen werden kann, sowie eine Funktion, die dies automatisiert in bestimmten Intervallen erledigt.

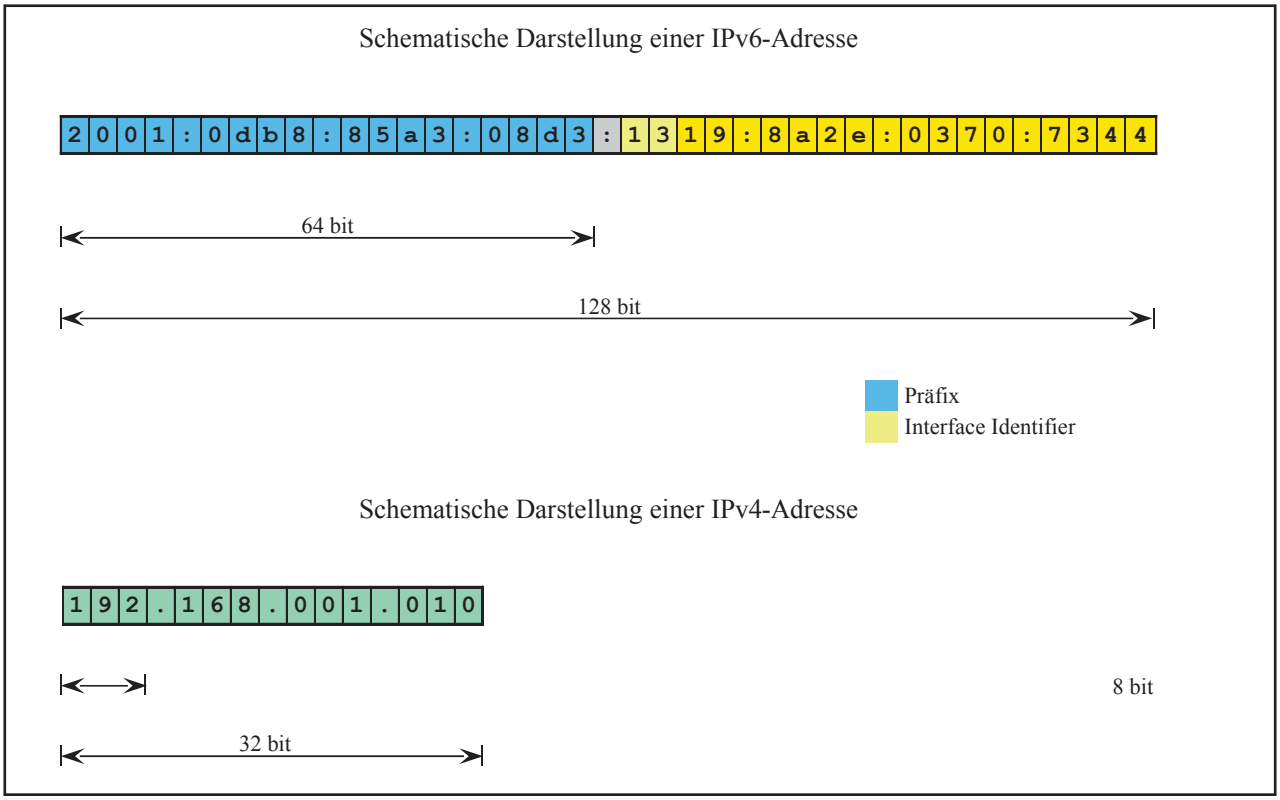
Meine Umfrage im Jahr 2011 ergab, dass knapp ein Drittel der 33 angefragten Anbieter von Internetzugängen im Berichtszeitraum nicht über eine Einführung von IPv6 nachdachten. Von den restlichen zwei Dritteln ließen die Planungen zu diesem Zeitpunkt bereits die Aussage zu, dass die Präfixvergabe an den Endkunden dynamisch erfolgen würde. Dass dies, wie der Brachenschnellste zeigt, auch tatsächlich so umgesetzt wird, habe ich wohlwollend zur Kenntnis genommen.

Die Umstellung auf das „neue" Protokoll wurde in diversen nationalen und internationalen Gremien hinsichtlich der datenschutzfreundlichen Einführung und Ausgestaltung diskutiert (vgl. Kasten b zu Nr. 5.6).

Darüber hinaus hat der Arbeitskreis Technische und Organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe „Datenschutz bei IPv6" erarbeitet, die sich an Hersteller und Provider im Privatkundengeschäft richtet und die wichtigsten Themen rund um die Änderungen bei der Einführung aufgreift.

Um auszuleuchten, welche Folgen die Umstellung auf das neue Internetprotokoll haben wird, habe ich im November 2011 in Berlin ein Symposium mit dem Titel „Internetprotokoll Version 6 (IPv6) – Wo bleibt der Datenschutz?" veranstaltet. Mir ging es insbesondere darum, eine breit angelegte Diskussionsrunde über die Branchen hinweg zu etablieren und die daraus entstehenden Synergieeffekte zu nutzen. Die eingeladenen Referenten aus Wissenschaft und Wirtschaft sorgten mit ihren Vorträgen und der Beteiligung an der Diskussionsrunde für Transparenz und klärten über die Vor- und Nachteile einer schleichenden Umstellung der Protokolle auf. Die dort gehaltenen Vorträge sowie die anschließende Diskussionsrunde wurden in Form eines Tagungsbandes dokumentiert, der auf meiner Website (www.datenschutz.bund.de) abgerufen werden kann.

Kasten a zu Nr. 5.6



Kasten b zu Nr. 5.6

Es haben sich sowohl die 82. und 84. nationale als auch die 33. internationale Datenschutzkonferenz mit dem Thema IPv6 beschäftigt und im Wesentlichen folgende Forderungen festgehalten:

- Die Provider sollten den Kunden grundsätzlich ein dynamisches Präfix ohne Aufpreis zuweisen; ein statisches Präfix nur auf expliziten Kundenwunsch.
- Sollte eine dynamische Vergabe nicht möglich sein, muss es eine Möglichkeit der Einflussnahme des Kunden geben, die zum Wechsel des Präfixes führt.
- Interface Identifier und Präfix sollten synchron gewechselt werden.
- Verwürfelung des Interface Identifiers („Privacy Extensions“) sollte flächendeckend eingesetzt werden.
- Im Bezug auf die Reichweitenmessung sollten nicht benötigte Adressteile gelöscht werden (nur die ersten 4 Bytes sind nötig).
- Der gemeinsame Betrieb von IPv6 und IPv4 („Dual-Stack-Betrieb“) sollte vermieden werden; dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle.

Die Entschließungen sind abrufbar unter www.datenschutz.bund.de.

5.7 Internetangebote der Bundesbehörden

Auch bei der elektronischen Kontaktaufnahme mit Behörden müssen die Bürgerinnen und Bürger sicher sein, dass ihre Daten geschützt werden. Ich musste leider feststellen, dass dies nicht immer der Fall war.

Auf vielen Internetangeboten von Bundesbehörden können Bürgerinnen und Bürger unkompliziert mit den Behörden in Kontakt treten, um z. B. Informationsmaterial anzufordern oder Fragen zu stellen. Dabei werden mittels der eingebundenen Kontaktformulare auch personenbezogene Daten erhoben, die nach § 9 BDSG verschlüsselt übertragen werden müssen; dies war nicht immer der Fall.

Im November 2010 erfuhr ich durch die Eingabe eines Petenten, dass das Internetangebot der Antidiskriminierungsstelle des Bundes die geltenden Datenschutzbestimmungen nicht einhalte. In diesem Fall wurden personenbezogene Daten wie z. B. Name, Anschrift und E-Mail-Adresse, die auf der Homepage dieser Behörde über das Kontaktformular erhoben wurden, unverschlüsselt übertragen. Dies habe ich zum Anlass genommen, stichprobenartig Prüfungen bei anderen Bundesbehörden vorzunehmen. Dabei entdeckte ich weitere vergleichbare Fälle. Dies verstößt gegen die Anlage zu § 9 BDSG, nach der zu gewährleisten ist, „dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports […] nicht unbefugt gelesen, kopiert […] oder verändert werden können“.

Im Januar 2011 habe ich die behördlichen Datenschutzbeauftragten der Obersten Bundesbehörden um entsprechende Prüfung aller Internetangebote sowohl ihrer eigenen Stellen als auch der jeweils nachgeordneten Behörden gebeten. Von den angeschriebenen 43 behördlichen Datenschutzbeauftragten wurden bis zum März 2011 insgesamt 77 Internetseiten benannt, die von Bundesbehörden betrieben werden.

Laut diesen Rückmeldungen gab es dabei 22 verschlüsselte sowie 34 unverschlüsselte Kontaktformulare. Von den unverschlüsselten Formularen war aber bei sieben eine entsprechende Verschlüsselung bereits in der Vorbereitung. Bei weiteren 20 Internetangeboten waren gar keine Kontaktformulare vorhanden. Positiv ist auch anzumerken, dass allein aufgrund meiner Anfrage einige Formulare auf den verschlüsselten Betrieb umgestellt wurden und ein unverschlüsseltes Formular unmittelbar entfernt wurde. Im April 2011 habe ich die behördlichen Datenschutzbeauftragten der Obersten Bundesbehörden über das Abfrageergebnis informiert und dazu aufgefordert, bei allen noch unverschlüsselt betriebenen Kontaktformularen geeignete Verschlüsselungsmaßnahmen umgehend zu etablieren. Nach meinem jetzigen Kenntnisstand ist dieses Verfahren überall abgeschlossen.

Ergänzend zu meinem o. g. Schreiben habe ich im Januar 2011 auch darauf hingewiesen, dass die Verwendung des „Facebook-Like-Buttons“ aus datenschutzrechtlicher Sicht bei Internetangeboten der Bundesbehörden nicht akzeptiert werden kann. Zu diesem Zeitpunkt war auf den Internetseiten der Bundesbehörden noch kein „Facebook-Like-Button“ implementiert; lediglich eine Bundesbehörde plante die Einbindung dieses Social-Plugins (vgl. auch Nr. 5.8.3).

Ich werde auch zukünftig die Internetangebote der Bundesbehörden auf die Einhaltung des Datenschutzes kontrollieren. Aufgrund der Vielzahl sowie der stetigen Erweiterungen und Anpassungen der betriebenen Internetangebote wird mir eine flächendeckende und aktuelle Kontrolle aber leider auch in Zukunft nicht möglich sein.

5.8 Soziale Netzwerke

Auch in dieser Berichtsperiode haben sich die Nutzerzahlen und die Bedeutung interaktiver Internetdienste weiter verstärkt. Dabei sind soziale Netzwerke von besonderer Bedeutung – nicht allein wegen des schieren Umfangs der Mitgliederzahlen, sondern auch wegen der Art ihrer Nutzung. Stehen für den Privatnutzer die Möglichkeiten zur Kontaktpflege mit „Freunden“ (… dabei kann es sich sogar um echte Freunde handeln oder aber auch nur um entfernte Bekannte) im Vordergrund, ergeben sich für kommerzielle und behördliche Nutzer neue Wege, mit ihrer Kundschaft bzw. mit den Bürgerinnen und Bürgern in Kontakt zu treten. Diese neuen Möglichkeiten werden aber mit Risiken für den Datenschutz erkauft. Grund genug, sich mit diesen Diensten weiterhin kritisch auseinanderzusetzen und auf datenschutzfreundliche Lösungen zu drängen.

Unter den sozialen Netzwerken ist Facebook das erfolgreichste weltweit und wohl auch das beliebteste. Ob die Millionen von Nutzern die – aus Datenschutzsicht – richtige Wahl getroffen haben, sollte eine Prüfung zeigen, die einen Blick in die Verarbeitung der Nutzerdaten erlaubte. Interesse an einem solchen Audit bestand bei allen europäischen Datenschutzbehörden gleichermaßen, kamen doch immer wieder neue „Streiche“ ans Licht. Das Audit wurde durch die irische Datenschutzbehörde durchgeführt.

5.8.1 Alles gut? Facebook nach dem Audit

Die irische Datenschutzbehörde hat das soziale Netzwerk Facebook geprüft und die Ergebnisse in einem Bericht veröffentlicht. Trotzdem bleiben viele datenschutzrechtliche Fragen unbeantwortet.

Manch einer wird sich sicherlich fragen, warum die irische Datenschutzbehörde ein US-amerikanisches soziales Netzwerk prüft und dabei auch die notwendige Unterstützung durch das Netzwerk erhält. Und warum nicht deutsche Datenschutzbehörden dies in gleicher Weise tun können. Die Antwort ist einfach und lässt doch viele Fragen offen: Facebook Ltd. in Irland sei die verantwortliche Stelle für die Datenverarbeitung in Europa, die Datenverarbeitung selbst erfolge in deren Auftrag durch Facebook Inc. in den USA. Sagt Facebook Inc.

Will man dieses Konstrukt anerkennen, so ergibt sich aus der EU-Datenschutzrichtlinie 95/46/EG und dem BDSG die Anwendbarkeit des irischen Datenschutzrechts und damit die Kontrollzuständigkeit der irischen Datenschutzbehörde. Eine alleinige Zuständigkeit beansprucht diese jedoch nicht. Auch aus diesem Grunde konnten die europäischen Datenschutzbehörden in der Artikel-29-Gruppe die Probleme aus den eigenen Ländern ansprechen und den irischen Datenschutzbeauftragten um Berücksichtigung bitten.

Wenig Zustimmung findet die Position von Facebook bei einigen deutschen Landes-Aufsichtsbehörden, die auch ihre Zuständigkeit gegeben sehen, weil Daten von Facebook-Nutzern in Deutschland erhoben und verwendet werden. Facebook beharrt jedoch auf seiner Position, und so blieben Forderungen aus den deutschen Datenschutzgesetzen letztendlich immer dann unberücksichtigt, wenn vergleichbare Regelungen im irischen Recht nicht bestehen.

Dies ist z. B. der Fall bei der sog. Klarnamenpflicht, die Facebook in seinen Nutzungsbedingungen festgeschrieben hat. Die Begründung: Die Idee des sozialen Netzwerks sei, dass jeder wisse, mit wem er es zu tun habe. Und: Die Sicherheit müsse gewährleistet werden. Das deutsche Telemediengesetz sieht nun aber vor, dem Nutzer eine anonyme Nutzung oder die Verwendung eines Pseudonyms zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Im irischen Datenschutzrecht fehlt eine solche Vorschrift, die Klarnamenpflicht wurde daher bei der Prüfung nicht beanstandet. Solche und ähnliche Probleme, die durch die globalisierte Informationsverarbeitung bei unterschiedlichen oder fehlenden nationalen

Gesetzen entstanden sind, sollen durch die EU-Datenschutz-Grundverordnung gelöst werden (vgl. Nr. 2.1), die ja einen stärker harmonisierten Rechtsrahmen gewährleisten soll.

Um seine „Namensrichtlinie“ durchzusetzen, hat Facebook die Nutzer aufgerufen, solche Nutzer zu melden, die unter falschem Namen angemeldet sind. Die Folge einer solchen Meldung ist eine Sperre des Accounts, bis der Betroffene seine (wahre) Identität durch die Übersendung einer Ausweiskopie offenlegt. Dieses „harte Durchgreifen“ war Anlass für eine deutsche Aufsichtsbehörde, gegen Facebook eine Anordnung zu erlassen, durch die Facebook verpflichtet werden soll, die pseudonyme Nutzung zu ermöglichen und gesperrte Accounts wieder freizuschalten. Das Verfahren war bei Redaktionsschluss noch nicht abgeschlossen.

Möglicherweise lässt sich im weiteren Diskussionsprozess mit Facebook ein Kompromiss durchsetzen, der von der Artikel-29-Gruppe in ihrer Stellungnahme zu sozialen Netzwerken (WP 163) als datenschutzfreundliche Lösung vorgestellt wurde: Bei der Registrierung müssen die richtigen Daten angegeben werden, der Nutzer kann sich aber im Netzwerk unter einem Pseudonym bewegen.

Die irische Datenschutzbehörde veröffentlichte im Dezember 2011 den Bericht über das Audit, das in Anwendung des irischen und EU-Rechts über mehrere Monate durchgeführt worden war. Danach hatte Facebook die Möglichkeit, Stellung zu nehmen und Änderungen und Nachbesserungen durchzuführen. Eine Überprüfung durch die irische Datenschutzbehörde schloss sich an und der entsprechende abschließende Bericht wurde im September 2012 veröffentlicht.

Insgesamt hat die Prüfung zu Verbesserungen für die Nutzer geführt. So wurden die Nutzungsbedingungen und Datenverwendungsrichtlinien im Sinne einer größeren Transparenz übersichtlicher und detaillierter gestaltet, die Kontrolle des Nutzers über seine Einstellungen erhöht und die Zugriffsmöglichkeit des Nutzers auf seine Daten verbessert. Ein großer Erfolg ist das Abschalten der Gesichtserkennung für alle Nutzer in der EU. Dies geht jedoch nicht nur auf das Konto der irischen Datenschutzbehörde, sondern ist auch dem Einsatz hiesiger Aufsichtsbehörden zu verdanken.

Neben dem Problem der Klarnamenpflicht gibt es die Forderung, datenschutzfreundliche Voreinstellungen anzubieten. Dies ist zwar gesetzlich nicht festgeschrieben, wird aber auch von der Artikel-29-Gruppe als wesentliches Element einer vorbildlichen Datenschutzpolitik angesehen und sollte daher zur Unterstützung der Nutzer umgesetzt werden. Die irische Datenschutzbehörde wird sich bei den weiteren Beratungsgesprächen mit Facebook dafür einsetzen. Denn leider tut sich (auch) Facebook noch schwer. Also doch (noch) nicht alles gut?

5.8.2 Dürfen Behörden Facebook-Fanpages nutzen?

Immer wieder erreichen mich Anfragen nach der Zulässigkeit behördlicher Fanpages. Leider ist eine pauschale Antwort nicht möglich.

Viele private Firmen und Unternehmen betreiben mittlerweile auf Facebook eigene Fanpages, um z. B. neue Produkte vorzustellen oder für sich zu werben. Von besonderem öffentlichen Interesse war im Berichtszeitraum die Verwendung von Fanpages durch Polizeibehörden für Fahndungszwecke (vgl. Nr. 7.4.7). Dabei scheint Facebook für die Verantwortlichen das geeignete Medium zu sein, um ganz gezielt ein jüngeres Publikum zu erreichen und interaktiv mit den Nutzern in Verbindung zu treten. Diese neuen Möglichkeiten werden auch zunehmend von den Bundesbehörden entdeckt, die entweder bereits eigene Fanpages betreiben oder dies planen. Bei allem Verständnis dafür, über Fanpages ein spezielles Zielpublikum erreichen zu wollen, muss natürlich der Datenschutz beachtet werden.

Bei einer Fanpage handelt es sich um eine Art von Homepage, die durch Facebook publiziert („gehostet“) wird. Für den Inhalt dieser Fanpage ist nicht Facebook, sondern deren Betreiber, also die jeweilige Behörde, verantwortlich. Zur Erstellung dieser Seite muss sich der potentielle Fanpagebetreiber zunächst als Nutzer bei Facebook anmelden. Erst dann kann seine Seite erstellt und auch betreut werden. Somit ist die bei Facebook registrierte Person bzw. Stelle einerseits Nutzer von Facebook und durch den Betrieb der Fanpage andererseits Diensteanbieter im Sinne des Telemediengesetzes.

Bei der Prüfung der Zulässigkeit solcher Fanpages ist zu beachten, dass es sich bei Facebook zwar um ein US-amerikanisches Unternehmen handelt, der europäische Markt jedoch von Facebook Ireland Limited bedient wird. Insoweit liegt die Datenschutzaufsicht für Facebook beim irischen Datenschutzbeauftragten. Dieser hat im Rahmen eines Datenschutzaudits sowie einer Nachprüfung die Einhaltung des Datenschutzes überprüft bzw. wirkt auf diese hin (vgl. Nr. 5.8.1). Obwohl im Zuge dieses Audits Facebook wesentliche datenschutzrechtliche Anpassungen vorgenommen bzw. die Umsetzung zugesagt hat, sehe ich einige Punkte wie z. B. die Übertragung von Nutzerdaten in die USA kritisch. Sobald die datenschutzrechtliche Anpassung des Internetangebotes von Facebook abgeschlossen ist, werde ich prüfen, ob und unter welchen Rahmenbedingungen der Betrieb von Fanpages durch Bundesbehörden unter datenschutzrechtlichen Gesichtspunkten akzeptabel ist.

Unabhängig von der grundsätzlichen Zulässigkeit müssen die Behörden ihre Angebote auf sozialen Netzwerken datenschutzgerecht ausgestalten. Dies bedeutet etwa, dass eine Bundesbehörde oder Krankenkasse die Nutzer nicht dazu einladen dürfen, sensible Informationen über die Fanpage beim sozialen Netzwerk preiszugeben. Manche Probleme lassen sich auch dadurch vermeiden, dass die Nutzer von der Fanpage direkt auf ein von der Behörde gehostetes eigenes Angebot weitergeleitet werden. Auf jeden Fall sollte die direkte Kommunikation mit dem Bürger über sichere Kanäle abgewickelt werden, etwa über ssl-verschlüsselte Formulare oder über De-Mail (vgl. Nr. 3.2.4). „Persönliche Mitteilungen“ über ein technisch außerhalb Europas abgewickeltes System sollten dabei nach Möglichkeit vermieden werden.

5.8.3 Datenschutzgerechte Einbindung von „Social Plugins“

In vielen Internetangeboten sind mittlerweile sog. Social Plugins eingebunden, eines der bekanntesten davon ist der „Facebook-Like-Button“. Dessen Verwendung ohne besondere Vorkehrungen verstößt gegen geltendes Datenschutzrecht. Technisch, etwa durch ein „zwei-Klick-Verfahren“, lassen sich derartige Probleme entschärfen.

Durch die Einbindung von Social Plugins bekannter sozialer Netzwerke in die eigenen Websites versprechen sich die Betreiber höhere Zugriffszahlen, da über diese Portale Seitenempfehlungen ausgetauscht werden. Auch bei Bundesbehörden gibt es Bestrebungen, durch Einbindung von Social Plugins in die Internetangebote auf sich aufmerksam zu machen. Datenschutzrechtlich ist dies kritisch zu sehen, wie das Beispiel des Facebook-Like-Buttons zeigt.

Beim Facebook-Like-Button bindet Facebook selbst auf der Website ein sog. Facebook-Frame in den Quellcode ein. Hierdurch wird bei jedem Aufruf dieser Internetseite auf dem Rechner ein Facebook-Cookie mit einer Gültigkeitsdauer von zwei Jahren gesetzt. Zusätzlich wird beim Seitenaufruf der „Referer“ (die Internetadresse der Webseite, von der der Benutzer durch Anklicken eines Links zu der aktuellen Seite gekommen ist) und die dazugehörige URL an den Facebook-Server geschickt. Damit erfährt der Diensteanbieter, welche Webseite ein Nutzer gerade aufgerufen hat. Somit ist eine Nutzerbeobachtung auch von solchen Personen möglich, die gar nicht Mitglied bei Facebook sind. Wenn die Seite von einem angemeldeten Facebook-Mitglied aufgerufen wird, wird durch das Skript zusätzlich die Sitzungs-ID an Facebook übertragen und kann dort der jeweiligen Person direkt zugeordnet werden. Für diesen Personenkreis ist dem Unternehmen eine umfassende namentliche Registrierung der Internetnutzung und eine Profilbildung möglich.

Diese Datenübertragung steht im Widerspruch zu § 13 Absatz 1 TMG (vgl. Kasten zu Nr. 5.8.3).

Zur datenschutzgerechten Einbindung von Social Plugins hat ein deutscher Verlag im November 2011 die sog. 2-Klick-Lösung vorgestellt. Bei diesem Ansatz sind Social Plugins bei Aufruf der Seite zunächst inaktiv, so dass keine Datenübertragung stattfindet. Erst bei Anklicken der Plugins können diese aktiviert werden. Bei diesem zweistufigen Verfahren erhält der Nutzer nach Anklicken zunächst den Hinweis gemäß TMG, dass personenbezogene Informationen an das entsprechende soziale Netzwerk übertragen und unter Umständen auch im nichteuropäischen Ausland gespeichert werden. Der Nutzer kann also selbst darüber entscheiden, ob er dies möchte. Erst danach ist das eingebettete Programm wie oben beschrieben aktiv. Aus meiner Sicht stellt das Verfahren einen gangbaren Weg dar, Social Plugins datenschutzgerecht in Internetangebote einzubinden.

Kasten zu Nr. 5.8.3

§ 13 Absatz 1 TMG

Pflichten des Diensteanbieters

Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

5.9 Kampf mit Giganten

Die Prüfung der neuen Datenschutzerklärung von Google ist abgeschlossen. Sie wurde als Pilot-Projekt „einer für alle“ der Artikel-29-Gruppe durch die französische CNIL durchgeführt. Nun wird auch die Prüfung des geänderten Nutzungsvertrags und der Datenschutzerklärung von Microsoft vorbereitet.

Google hatte Ende Januar 2012 angekündigt, seine neue Datenschutzerklärung zum 1. März 2012 in Kraft zu setzen. Sie sollte umfassend überarbeitet und natürlich im Sinne der Nutzer verbessert worden sein: einfach, klar und transparent. Die Aufforderung der Artikel-29-Gruppe, den Termin zu verschieben und so eine datenschutzrechtliche Prüfung zu ermöglichen, wurde abgelehnt. Die Begründung überraschend: Die Nutzer hätten mehr als einen Monat Zeit gehabt, die neue Privacy Policy zu lesen und zu verstehen. Und man sei zuversichtlich, dass die Anforderungen der europäischen Datenschutzgesetze erfüllt seien.

Was dann der Öffentlichkeit präsentiert wurde, entsprach aber in wesentlichen Punkten keineswegs den Anforderungen des EU-Datenschutzrechts. Dies ergab schon eine erste Analyse, die federführend von der französischen Datenschutzbehörde (CNIL) im Auftrag der Artikel-29-Gruppe umgehend nach Bekanntwerden der Datenschutzerklärung durchgeführt wurde. Zwar konnte es als Verbesserung angesehen werden, dass die zahlreichen Datenschutzerklärungen – immerhin 70 an der Zahl – nun in einem einzigen Dokument zusammengefasst worden waren, das einigermaßen übersichtlich und für den normalen Internetnutzer verständlicher daherkam. Aber dabei blieben Genauigkeit und Detailtiefe auf der Strecke, an deren Stelle sich nun allgemeine Formulierungen befinden, etwa:

„Wir erfassen möglicherweise gerätespezifische Informationen (beispielsweise das von Ihnen verwendete Hard-

ware-Modell, die Version des Betriebssystems, eindeutige Gerätekennungen und Informationen über mobile Netzwerke, einschließlich Ihrer Telefonnummer). Google verknüpft Ihre Gerätekennungen oder Telefonnummer gegebenenfalls mit Ihrem Google-Konto."

„Wir nutzen diese Informationen außerdem, um Ihnen maßgeschneiderte Inhalte anzubieten – beispielsweise um Ihnen relevantere Suchergebnisse und Werbung zur Verfügung zu stellen."

Derartige Formulierungen bieten viel Raum für beliebige Auslegungen, sicherlich zum Vorteil für Google. Den Nutzer lässt dies letztendlich ratlos und genau so schlau wie vorher zurück.

Die Information des Nutzers ist nicht ausreichend, er erfährt nicht, welcher Zweck, welche Daten, welche Zugriffsrechte für einen bestimmten Dienst relevant sind, den er gerade nutzen will. Weit schwerwiegender, weil weitreichender und unkontrollierbar, ist die Verknüpfung und Auswertung aller Daten eines Nutzers aus den verschiedenen Diensten, die Google ohne Wenn und Aber einführt: keine detaillierten Informationen und vor allem keine Einwilligung – nicht einmal eine Widerspruchsmöglichkeit ist vorgesehen. Damit räumt sich Google nicht nur die Möglichkeit ein, umfassende Nutzerprofile zu erstellen, sondern diese diensteübergreifend zu Metaprofilen zusammenzuführen. Google-Chef Larry Page rechtfertigt die Verknüpfung der Daten damit, dass nur so innovative Angebote mit Mehrwert für die Nutzer möglich seien. Eine indirekte Botschaft an die Datenschützer, dass sie mit Überregulierung und Verboten die technische Entwicklung hemmen? Bei der Debatte um die ambitionierte europäische Datenschutzreform (vgl. Nr. 2.1) hört man dies auch von anderen Lobbyisten.

Die CNIL begann umgehend nach Inkraftsetzen der Privacy Policy mit der detaillierten datenschutzrechtlichen Untersuchung. Was dann ablief, war ein Frage-und-Antwort-Spiel, in dem Google zwar rein formal seinen Kooperationswillen bestätigte, im Inhaltlichen aber zu oft den Kernfragen auszuweichen versuchte. Die europäischen Datenschutzbeauftragten der Artikel-29-Gruppe waren in den gesamten Prozess eng eingebunden.

Die Ergebnisse der Prüfung wurden Google im Oktober 2012 mitgeteilt. Zusammenfassend kann gesagt werden, dass Google die wesentlichen Datenschutz-Prinzipien – Zweckbegrenzung, Datenminimierung, Verhältnismäßigkeit, Recht auf Widerspruch – nicht beachtet. Für die Überarbeitung der Datenschutzerklärung und die erforderlichen Änderungen in der Praxis wurde eine Frist bis Mitte Februar 2013 gesetzt. Trotz erklärter Bereitschaft zur Kooperation lassen die Erfahrungen aus vergangenen Verfahren vermuten, dass Google durch fortlaufenden Briefwechsel und immer neu verpackte Argumentation das Verfahren verschleppen wird. Die Artikel-29-Gruppe wird darauf vorbereitet sein und reagieren.

Microsoft hat im September 2012 seinen „Vertrag über Microsoft-Dienste" (*Services Agreement)* geändert, eine weitere Überarbeitung ist angekündigt. Da sich dies auch auf die *Privacy Policy* auswirkt und zahlreiche Dienste von Microsoft betroffen sind, hat die Artikel-29-Gruppe beschlossen, eine ähnliche Prüfung wie bei Google durchzuführen. Die Federführung wird der Datenschutzbeauftragte von Luxemburg (CNPD), unterstützt von der CNIL, übernehmen. Microsoft wurde Mitte Dezember 2012 über die geplante Prüfung informiert und um einen Aufschub der Revision bis zum Ende des Verfahrens gebeten.

5.10 Zahlen, bitte

Was früher der Dialer tat, erledigt heute die App. Zahlen muss aber immer noch der Kunde!

Sie sind ja ach so niedlich, wenn nicht gar noch praktisch, diese kostenlosen Apps für unsere unverzichtbaren Begleiter, die Smartphones. Man kann damit die Kinder beschäftigen oder aber auch mal eben ein Regal akkurat ausrichten. Ärgerlich wird es nur, wenn man – mangels dritter Hand – beim Handwerken statt der Bedienknöpfe der Smartphone-Wasserwaage das Werbebanner trifft. In diesem Fall könnte die Anschaffung eines richtigen Werkzeugs billiger gewesen sein.

Hinter vielen Werbeeinblendungen in kostenlosen Applikationen von Smartphones verbirgt sich, wie Petenten mir berichteten, eine perfide Masche, dem Kunden das Geld aus der Tasche zu ziehen. Ich habe diese Eingaben zum Anlass genommen, das Thema genauer zu beleuchten.

In der App-Branche ist es üblich, durch die Reservierung von Werbeflächen innerhalb der App einen Teil der Entwicklungskosten zu decken. Diese Werbeflächen werden meist von Werbenetzwerken mit Kontext gefüllt, auf den die Entwickler keinen Einfluss haben. Ziel dieser Vermarktungsstrategie ist es, sowohl den Anbieter des Werbeplatzes als auch den Werbenden am Kunden verdienen zu lassen. Berührt man ein solches Banner, wird man häufig auf eine sog. Landing Page, eine speziell hergerichtete Internetseite, geleitet, die über das Angebot des Banners informieren soll. Entscheidend ist allerdings nicht, welche Seite man aufruft, sondern welche (unsichtbaren) Informationen diesem Aufruf anhänglich sind.

Auf Nachfrage teilten mir die Telekommunikationsunternehmen mit, dass hierbei häufig die Mobile Subscriber ISDN Number (MSISDN), also die weltweit eindeutige Rufnummer des Kunden an die Anbieter von Mehrwertdiensten übergeben wird, damit diese ihre Dienste über den Telefonanbieter abrechnen können. Dies wird schon seit über zehn Jahren so praktiziert. Auch die Kunden werden bei Vertragsabschluss darüber informiert – die Daten gehen ausschließlich an die vertraglich gebundenen Mehrwertdiensteanbieter. Verwunderlich dabei ist allerdings die Renaissance eines längst ausgestorben geglaubten Protokolls – Wireless Application Protocol (WAP). Einst der Vorreiter des „mobilen Internets", wie wir es heute kennen, hat es nie eine breite Verwendung gefunden und ist schließlich (zunächst) in der Versenkung verschwunden. Dieses Protokoll nutzte schon jeher die Weitergabe von Daten wie die MSISDN zum komfortablen Erwerb von Leistungen und Diensten. Da es nun aber

verdeckt im Hintergrund genutzt wird, sind sich viele Kunden der Tatsache nicht bewusst, dass sie bereits mit dem Berühren eines Banners einen Kauf getätigt haben – ob es sich dabei jedes Mal wirklich um einen wirksamen Vertragsabschluss handelt, ist zumindest zweifelhaft.

Zudem zeigte sich, dass auch moderne Internetprotokolle nicht ganz unberührt von dieser Industrie bleiben. So wird in der Literatur berichtet, dass auch über das bzw. mittels des Hypertext Transfer Protocol (HTTP) ähnliche personenbezogenen Daten innerhalb der Protokollkopfdaten übertragen werden. Ich habe mir diese Thematik für Kontrollen im nächsten Berichtszeitraum vorgemerkt, damit ich mir ein eigenes Bild von den Technologien und Verfahren machen kann.

Über den reinen Verfahrensaspekt hinaus birgt dieses Thema Diskussionsbedarf bezüglich der Rechtsgrundlage der Übermittlung von personenbezogenen Daten. Diesem Themenkomplex hat sich die Bundesnetzagentur angenommen und im Jahr 2011 eine Umfrage bei den betreffenden Anbietern gestartet. Derzeit stellt sich die Lage, ohne dass das Verfahren abgeschlossen ist, wie folgt dar: § 97 Absatz 5 TKG (vgl. Kasten zu Nr. 5.10) greift im Falle der Übermittlung der MSISDN nicht, da das Geschäftsmodell den Forderungsverkauf vorsieht und somit nicht die Forderung eines Dritten, sondern eine eigene abgerechnet wird. In Übereinstimmung mit der Bundesnetzagentur bedarf die Datenübermittlung hier stets einer gültigen Einwilligung des Nutzers. Ohne Einwilligung wäre die Übermittlung ohne Rechtsgrundlage und damit unzulässig.

Kasten zu Nr. 5.10

§ 97 TKG (Auszug)

Entgeltermittlung und Entgeltabrechnung

(5) Zieht der Diensteanbieter mit der Rechnung Entgelte für Leistungen eines Dritten ein, die dieser im Zusammenhang mit der Erbringung von Telekommunikationsdiensten erbracht hat, so darf er dem Dritten Bestands- und Verkehrsdaten übermitteln, soweit diese im Einzelfall für die Durchsetzung der Forderungen des Dritten gegenüber seinem Teilnehmer erforderlich sind.

6 Telekommunikation und Post

6.1 Die Vorratsdatenspeicherung – eine unendliche Geschichte?

Seit nunmehr über sechs Jahren scheiden sich an der Vorratsdatenspeicherung die Geister. Die Bedenken verschiedener europäischer Gerichte dürfen nicht ignoriert werden. Das „Was“ und „Wie“ einer neuen Regelung sind allerdings nach wie vor unklar.

In meinem letzten TB habe ich gefragt: „Vorratsdatenspeicherung: Quo vadis?“ (vgl. 23. TB Nr. 6.1). Zwei Jahre später ist trotz vieler Diskussionen nicht erkennbar, in welche Richtung sich der europäische und der deutsche Gesetzgeber bewegen werden.

So hat die Europäische Kommission im April 2011 einen Evaluierungsbericht über die der Vorratsdatenspeicherung (VDS) zu Grunde liegende Richtlinie 206/24/EG veröffentlicht. Darin listete sie gleich eine ganze Reihe von Mängeln auf, die sich fast auf sämtliche Aspekte der getroffenen Regelungen beziehen. So konnte die durch die Richtlinie bezweckte Harmonisierung des europäischen Telekommunikationsmarktes offensichtlich nicht erreicht werden. Ebenso wurde kritisiert, dass Statistiken, die zu einer umfänglichen Bewertung der Umsetzung der Richtlinie in den Mitgliedstaaten eigentlich erforderlich gewesen wären, nur spärlich, nicht aussagekräftig und in einigen Fällen sogar gar nicht von den Mitgliedstaaten zur Verfügung gestellt worden seien. Darüber hinaus wurden unterschiedliche Mankos beispielsweise bei Definitionen oder Vorgaben zur Zweckbindung der Datenverwendung festgestellt. Schließlich ist deutlich geworden, dass die in der Richtlinie vorgesehene maximal zulässige Speicherdauer von zwei Jahren viel zu lang bemessen ist, da die von den Sicherheitsbehörden abgefragten Daten zu 70 Prozent nicht älter als drei und nur zu 10 Prozent älter als sechs Monate waren.

Angesichts dieser unübersehbaren und erheblichen Probleme hat mich die Erklärung der Europäischen Kommission überrascht, die Richtlinie habe sich grundsätzlich bewährt und bedürfe lediglich einer Überarbeitung. Hierzu wurden im Laufe des Jahres 2011 mehrere Workshops mit Interessenvertretern von Wirtschaft, Regierungen, Nichtregierungsorganisationen und Datenschutzaufsichtsbehörden durchgeführt, auf denen einzelne Lösungsansätze diskutiert wurden. Ebenso gab die Kommission mehrere Studien in Auftrag, unter anderem über die Möglichkeit, „Quick-Freeze“-Verfahren im Zusammenhang mit der VDS einzusetzen. Ergebnisse wurden allerdings bislang nicht präsentiert, stattdessen aber der Termin für die Veröffentlichung des Entwurfs einer überarbeiteten Richtlinie immer wieder verschoben. War ursprünglich eine erste Version bereits für Ende 2011 angekündigt, hat EU-Innenkommissarin Malmström im Oktober 2012 verkündet, sie könne noch nicht absehen, wann mit einer Veröffentlichung zu rechnen sei. Als Grund für die Verzögerung benannte sie unter anderem die technische und rechtliche Komplexität des Themas. Dies erscheint umso bemerkenswerter, als die Kommission, die sich selbst nicht in der Lage sieht, die als mangelhaft bewertete Richtlinie zeitnah zu überarbeiten, gleichzeitig von den Mitgliedstaaten verlangt, diese Richtlinie in nationales Recht umzusetzen. Deutschlands gesetzgeberische Bemühungen im Nachgang der Nichtigerklärung des ersten Umsetzungsgesetzes durch das Bundesverfassungsgericht im Frühjahr 2010 gingen der Kommission jedenfalls nicht schnell genug, so dass sie im Mai 2012 eine Nichtumsetzungsklage vor dem Europäischen Gerichtshof gegen die Bundesrepublik erhob.

Zwar hatte das Bundesjustizministerium im Juli 2011 meinen Vorschlag aufgegriffen und einen ersten Diskussionsentwurf für ein „Quick-Freeze“-Gesetz („Gesetz zur

Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet“) vorgestellt. Dieser hat bislang aber nicht den Weg ins Kabinett gefunden, da das Bundesinnenministerium weiterhin an einer umfassenden Vorratsdatenspeicherung festhält. Ziel des Entwurfs war die Schaffung einer Rechtsgrundlage, nach der Strafverfolgungsbehörden Telekommunikationsunternehmen anweisen können, die Daten eines konkret im Verdacht stehenden Kunden vorübergehend nicht zu löschen. Um auch solche Verkehrsdaten „einfrieren“ zu können, die zu betrieblichen Zwecken nur kurz oder gar nicht gespeichert werden, sieht das Gesetz für einzelne Datenkategorien, wie beispielsweise dynamische IP-Adressen, zusätzlich eine befristete Speicheranordnung vor. Eine anlasslose flächendeckende Speicherung von Verkehrsdaten ist nach diesem Ansatz nicht notwendig, zumal diese in der Regel ohnehin für betriebliche Zwecke mehrere Monate gespeichert werden und somit Strafverfolgungsbehörden grundsätzlich zur Verfügung stehen (vgl. Nr. 6.7). Ich erachte dieses Verfahren nach wie vor als eine valide Alternative zur allumfassenden anlasslosen VDS, die 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.

Die Wiedereinführung einer flächendeckenden VDS erscheint auch deshalb als nicht zielführend, da ihre Erforderlichkeit auch nach über vier Jahren weder auf nationaler noch auf europäischer Ebene belegt werden konnte. Eine im Januar 2012 veröffentlichte Studie des Max-Planck-Instituts kommt sogar zu dem Ergebnis, dass der durch das Bundesverfassungsgericht mit seinem Urteil vom 2. März 2010 bewirkte Wegfall der VDS in Deutschland keinen wesentlichen Einfluss auf die Effektivität der Strafverfolgung gehabt habe. Vielleicht liegt das Schicksal der VDS aber gar nicht in den Händen der Kommission oder nationaler Gesetzgeber. Nach dem irischen High Court hat auch der österreichische Verfassungsgerichtshof 2012 ein Vorabentscheidungsersuchen an den Europäischen Gerichtshof gerichtet, in dem gebeten wird, die Vereinbarkeit der VDS-Richtlinie mit der europäischen Grundrechtecharta zu überprüfen. Ich halte es nicht für ausgeschlossen, dass das Gericht im Rahmen dieser Prüfung zumindest eine teilweise Unvereinbarkeit der Richtlinie mit den europäischen Grundrechten feststellen könnte. Ob eine solche Entscheidung dann tatsächlich das Ende der VDS besiegeln oder lediglich den Anfang einer neuen (unendlichen?) Geschichte darstellen wird, bleibt abzuwarten.

6.2 Von Doppeltüren und IP-Adressen – Der Beschluss des Bundesverfassungsgerichtes zur Bestandsdatenauskunft

Das Bundesverfassungsgericht sorgte für mehr Klarheit über die Schutzbedürftigkeit von IP-Adressen und löste gesetzgeberischen Handlungsbedarf aus.

Am 24. Januar 2012 hat das Bundesverfassungsgericht (BVerfG) einen Beschluss zur Verfassungsmäßigkeit der §§ 111 bis 113 Telekommunikationsgesetz (TKG) gefasst. Insbesondere die höchstrichterliche Entscheidung zur rechtlichen Einordnung von Auskunftsersuchen zu den Anschlussinhabern hinter dynamischen IP-Adressen sowie die Einführung des so genannten Doppeltürenmodells sollten sich als wichtige Meilensteine im Bereich des Datenschutzes im Telekommunikationsrecht erweisen.

Anlass für den Beschluss (1 BvR 1299/05) war eine Verfassungsbeschwerde aus dem Jahr 2005, mit der die im Zusammenhang mit dem Auskunftsverfahren über Bestandsdaten stehenden Normen des TKG angegriffen wurden. Nach Auffassung der Beschwerdeführer werde sowohl durch das Verfahren der Datenerhebung zu Zwecken der Abwicklung von Bestandsdatenauskünften (§ 111 TKG) als auch durch die jeweiligen Verfahren der automatischen (§ 112 TKG) und manuellen Auskunft (§ 113 TKG) gegen das Fernmeldegeheimnis sowie das Recht auf informationelle Selbstbestimmung verstoßen.

Diese Ansicht teilte das Gericht nur teilweise. So erklärte es die §§ 111 und 112 TKG für verfassungsgemäß und beanstandete lediglich die Vorschrift des § 113 TKG (vgl. auch die Leitsätze des Gerichtes im Kasten zu Nr. 6.2). So sei es nicht mehr mit dem Recht auf informationelle Selbstbestimmung zu vereinbaren, wenn § 113 Absatz 1 Satz 2 TKG den Sicherheitsbehörden ermögliche, Daten, die als Zugangssicherungscodes (wie Passwörter, PIN oder PUK) den Zugang zu Endgeräten und Speichereinrichtungen wie z. B. Mobiltelefonen oder E-Mail-Accounts sichern, unabhängig davon abrufen zu können, ob auch die Voraussetzungen für eine Nutzung der Sicherungscodes durch die Behörden gegeben sind.

Daneben sind aus datenschutzrechtlicher Sicht noch zwei weitere vom Gericht behandelte Themenbereiche von essentieller Bedeutung. Zum einen hat das Gericht klargestellt, dass sich bei einem Auskunftsersuchen zu Telekommunikationsdaten immer eine Ermächtigung zur Datenübermittlung für den Anbieter und eine hiermit korrespondierende Anspruchsgrundlage für die Datenabfrage der Behörden gegenüberstehen müssen. Wie das Gericht zur Verbildlichung dieses als „Doppeltürenmodell“ bezeichneten Grundsatzes ausgeführt hat, müsse zur Übergabe eines Datensatzes von einem Telekommunikationsdiensteanbieter an einen Bedarfsträger für jeden der Beteiligten eine Rechtsgrundlage in Form einer zu durchschreitenden Türe existieren, um die Datenübergabe vornehmen zu können. Konkret stellte das Gericht klar, dass die §§ 112 und 113 TKG lediglich die Ermächtigungsnormen zur Datenübermittlung für den Telekommunikationsdiensteanbieter darstellen und nicht zugleich die Anspruchsgrundlage für die Abfrage seitens der Bedarfsträger sind. Hierfür müssten grundsätzlich eigene Rechtsgrundlagen in den jeweiligen Fachgesetzen der Bedarfsträger geschaffen werden. Während beim Verfahren des § 112 TKG nach Ansicht des Gerichtes Vorschriften genügen, die allgemein zur Erhebung personenbezogener Daten ermächtigen, werden beim manuellen Auskunftsersuchen entsprechende spezielle Rechtsgrundlagen benötigt, die eine eindeutige Abrufermächtigung der Bedarfsträger für Daten nach § 113 TKG enthalten.

Zum anderen hat das BVerfG erstmals eine explizite Aussage zur Natur der Auskunft über Bestandsdaten des Anschlussinhabers getroffen, der sich hinter einer dynamischen IP-Adresse verbirgt. Damit hat es einen seit Jahren anhaltenden Streit (vgl. 22. TB Nr. 7.11) beendet. Wie das Gericht jetzt klarstellte, kann § 113 TKG in seiner gegenwärtigen Form keine Grundlage für ein entsprechendes Auskunftsrecht sein. Hierfür bedürfe es einer expliziten und normenklaren gesetzlichen Befugnis, die derzeit nicht existiere. Positiv sehe ich vor allem die Feststellung, dass die Telekommunikationsunternehmen für die Zuordnung von dynamischen IP-Adressen in einem Zwischenschritt Verkehrsdaten ihrer Kunden sichten und somit auf konkrete Kommunikationsvorgänge zugreifen müssten, die dem Schutz des Fernmeldegeheimnisses nach Artikel 10 Absatz 1 GG unterliegen. Soweit aber ein Zugriff auf dem Telekommunikationsgeheimnis unterliegende Daten als Vorfrage für eine Auskunft zwingend notwendig sei, erstrecke sich der Schutzbereich von Artikel 10 Absatz 1 GG entsprechend auf das gesamte Auskunftsverfahren.

Für die aufgrund des Urteils notwendigen Änderungen hat das Gericht dem Gesetzgeber eine Übergangsfrist bis zum 30. Juni 2013 eingeräumt. Ein entsprechendes Gesetzgebungsverfahren wurde bereits eingeleitet (vgl. Nr. 6.3). In jedem Fall hat das BVerfG mit der Entscheidung ein weiteres Mal den Datenschutz in der Telekommunikation gestärkt.

Kasten zu Nr. 6.2

Leitsätze des BVerfG-Beschlusses zur Bestandsdatenauskunft

1. In der Zuordnung von Telekommunikationsnummern zu ihren Anschlussinhabern liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung. Demgegenüber liegt in der Zuordnung von dynamischen IP-Adressen ein Eingriff in Artikel 10 Absatz 1 GG.
2. Der Gesetzgeber muss bei der Einrichtung eines Auskunftsverfahrens sowohl Rechtsgrundlagen für die Übermittlung als auch für den Abruf von Daten schaffen.
3. Das automatisierte Auskunftsverfahren der §§ 112, 111 TKG ist mit der Verfassung vereinbar. § 112 TKG setzt dabei für den Abruf eigene Ermächtigungsgrundlagen voraus.
4. Das manuelle Auskunftsverfahren der § 113 Absatz 1 Satz 1, § 111, § 95 Absatz 1 TKG ist in verfassungskonformer Auslegung mit dem Grundgesetz vereinbar. Zum einen bedarf es für den Abruf der Daten qualifizierter Rechtsgrundlagen, die selbst eine Auskunftspflicht der Telekommunikationsunternehmen normenklar begründen. Zum anderen darf die Vorschrift nicht zur Zuordnung dynamischer IP-Adressen angewendet werden.
5. Die Sicherheitsbehörden dürfen Auskünfte über Zugangssicherungscodes (§ 113 Absatz 1 Satz 2 TKG) nur dann verlangen, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind.

6.3 Neue Regeln für Auskunft über Telekommunikationsbestandsdaten

Nach einer Verfassungsgerichtsentscheidung muss der Gesetzgeber das Verfahren der Bestandsdatenauskunft bis zum 30. Juni 2013 ändern. Hierfür müssen neben dem Telekommunikationsgesetz (TKG) noch einige weitere Gesetze geändert werden.

In Folge der Entscheidung des BVerfG vom 24. Januar 2012 (vgl. Nr. 6.2) muss das Auskunftsverfahren über Telekommunikationsbestandsdaten teilweise neu geregelt werden. Neben Anpassungen im TKG werden Änderungen in der Strafprozessordnung sowie in den jeweiligen Gesetzen der Nachrichtendienste, des Bundeskriminalamtes, der Bundespolizei und des Zollfahndungsdienstes erforderlich (vgl. Kasten zu Nr. 6.3).

Da die Übergangsfrist des BVerfG, während der die aktuellen Vorschriften weiterhin wie bisher angewendet werden dürfen, bereits am 30. Juni 2013 ausläuft, war Eile geboten. Das BMI hat im Sommer 2012 die Umsetzung der Forderungen des BVerfG eingeleitet. Bei Redaktionsschluss war das Gesetzgebungsverfahren noch nicht abgeschlossen.

Im Wesentlichen beschränkt sich der vorliegende Entwurf darauf, die Vorgaben des Gerichts umzusetzen.

Ich habe das Gesetzgebungsverfahren von Anfang an begleitet und konnte einige Änderungsvorschläge durchsetzen. Auch wenn die geplanten Änderungen durchaus im Sinne des Datenschutzes sind, hätte ich mir gewünscht, dass aus diesem Anlass noch einmal die grundsätzliche Notwendigkeit und der sehr weit gefasste Umfang der Bestandsdatenauskunft hinterfragt wird. Ich werde daher den Fortgang des Verfahrens weiterhin kritisch begleiten und mich insbesondere dafür einsetzen, die Auskunft über IP-Adressen zur Verfolgung von Ordnungswidrigkeiten auf Fälle von besonderem Gewicht zu beschränken. Ebenso trete ich dafür ein, die Benachrichtigungspflichten der Behörden gegenüber den Betroffenen zu verbessern.

Kasten zu Nr. 6.3

Beim TKG liegt der Schwerpunkt auf der Neugestaltung des § 113, der nunmehr verständlicher werden soll. In Absatz 1 der Entwurfsfassung werden die Daten benannt, über die Telekommunikationsanbieter beim Vorliegen entsprechender Anfragen Auskunft erteilen müssen. Neben den auch in der aktuell gültigen Norm erwähnten Daten – also Bestandsdaten nach §§ 95 und 111 TKG sowie Daten, die den Zugriff auf Endgeräte oder andere Speichereinrichtungen schützen – ist nun erstmals auch explizit die Auskunft über den Anschlussinhaber einer zu einem bestimmten Zeitpunkt zu-

gewiesenen IP-Adresse geregelt. Demzufolge ist eine für diese Auskunft notwendige automatisierte Auswertung von Verkehrsdaten zulässig. Nach Absatz 2 der Entwurfsfassung ist eine Auskunftserteilung seitens der Telekommunikationsanbieter nur dann zulässig, wenn der Bedarfsträger bei seiner Anfrage auf eine gesetzliche Anspruchsgrundlage verweist, die eine Erhebung der entsprechenden Daten explizit gestattet. Hierdurch werden die Anforderungen des Gerichtes an das sog. Doppeltürenmodell umgesetzt, nach dem sich für eine Auskunftserteilung zwingend eine gesetzliche Abfrageermächtigung der Bedarfsträger und eine Übermittlungsbefugnis der Telekommunikationsanbieter korrespondierend gegenüber stehen müssen (vgl. Nr. 6.2). In den Absätzen 3 und 4 werden nunmehr die Kategorien von Bedarfsträgern genannt, die grundsätzlich ermächtigt sind, Auskünfte zu verlangen; außerdem müssen Telekommunikationsunternehmen über die Umstände der Auskunftserteilung schweigen. Die einzige beabsichtigte Neuerung, die nicht auf eine Vorgabe des Gerichts zurückgeht, findet sich in Absatz 5. Hier werden Unternehmen mit mehr als 100 000 Kunden verpflichtet, für die Abwicklung des Auskunftsverfahrens eine elektronische Schnittstelle zur Verfügung zu stellen. Hierdurch will man die Datenübermittlung sicherer gestalten und eine eindeutige Identifizierung der Bedarfsträger gewährleisten. Damit das Verfahren nicht zu einem verkappten automatisierten Auskunftsverfahren ausufert, wie bei § 112 TKG, sind die Telekommunikationsanbieter verpflichtet, jede Anfrage manuell zu prüfen, die sie über die elektronische Schnittstelle erhalten.

Für den Bereich der Strafverfolgung fügt der Gesetzentwurf einen neuen § 100j in die Strafprozessordnung (StPO) ein. Danach sollen die entsprechenden Daten (§ 113 TKG) angefordert werden können, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist. Für den Zugriff auf Endgeräte oder auf Speichereinrichtungen sollen die Daten nur verlangt werden dürfen, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Korrespondierend zur entsprechenden Regelung im TKG soll auch die Auskunft zu einer zu bestimmten Zeitpunkten zugewiesenen IP-Adresse geregelt werden (§ 100j Absatz 2 StPO-E).

Auch die Regelungen für die Abfragen durch die Bedarfsträger müssen in den Fachgesetzen entsprechend angepasst werden. So sieht der Gesetzentwurf vor, sowohl die Polizeigesetze auf Bundesebene (Bundeskriminalamtgesetz und Bundespolizeigesetz) als auch die Gesetze für die Nachrichtendienste (Bundesverfassungsschutzgesetz, Gesetz über den Militärischen Abschirmdienst und Gesetz über den Bundesnachrichtendienst) und das Zollfahndungsdienstgesetz zu ändern. Fast gleichlautende Regelungen sollen für die entsprechenden Zuständigkeitsbereiche die Abfrage der Bestandsdaten ermöglichen. Auch hier soll die Auskunft über Daten, die den Zugriff auf Endgeräte oder Speichereinrichtungen ermöglichen, nur erlaubt sein, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten erfüllt sind.

6.4 Telekommunikationsgesetz: Nicht alles, was länger dauert, muss auch besser sein!

Die Novellierung des Telekommunikationsgesetzes wurde erforderlich, weil zwei europäische Richtlinien umzusetzen waren. Dabei wurden zwar datenschutzrechtliche Verbesserungen vorgenommen, aber auch Änderungen, die eher problematisch sind.

Am 10. Mai 2012 ist das Gesetz zur Änderung telekommunikationsrechtlicher Regelungen in Kraft getreten (BGBl. I 2012 S. 958 ff.). Diese Novellierung des Telekommunikationsgesetzes (TKG) setzt europarechtliche Vorgaben um, die bereits am 19. Dezember 2009 in Kraft getreten waren und eigentlich bis zum 25. Mai 2011 hätten in nationales Recht transformiert sein sollen. Auf zwei zentrale Änderungen, die Einführung spezieller Meldepflichten für die Telekommunikationsunternehmen und Konkretisierungen bei der Vorschrift zur Regelung der Standortdaten, wird an anderer Stelle detailliert eingegangen (vgl. Nr. 3.5.3 und 6.5).

Ärgerlich ist, dass die im Gesetzentwurf der Bundesregierung vorgesehene Einführung einer einheitlichen Speicherfrist für die zum Zweck der Abrechnung zwischen den Diensteanbietern gespeicherten Verkehrsdaten in letzter Minute des Gesetzgebungsverfahrens gestrichen wurde, und zwar ohne (offizielle) Begründung. Auf meine Initiative hin sollte eine Speicherung dieser Daten nur für maximal drei Monate nach Versand der Rechnung an den anderen Diensteanbieter erlaubt sein. Leider bleibt es jetzt bei der bisherigen Regelung, und die Daten dürfen bis maximal sechs Monate nach Rechnungsversand gespeichert werden, sofern die Diensteanbieter die Erforderlichkeit belegen (vgl. auch Nr. 6.7).

Darüber hinaus führen einige Änderungen eher zu Unklarheiten. Eine dieser Änderung betrifft den Anwendungsbereich der datenschutzrechtlichen Vorschriften des TKG, nämlich die §§ 91ff TKG. Geschützt werden hiernach die personenbezogenen Daten von Teilnehmern und Nutzern, die im Zusammenhang mit der geschäftsmäßigen Erbringung eines Telekommunikationsdienstes von dessen Anbieter verarbeitet werden. Anbieter von geschäftsmäßigen Telekommunikationsdiensten ist wiederum jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt. Im Rahmen der Gesetzesnovellierung wurden die Legaldefinitionen der Begriffe Teilnehmer und Nutzer in § 3 Nummer 14 und Nummer 20 TKG insoweit geändert, dass lediglich auf die Inanspruchnahme von öffentlich zugänglichen Telekommunikationsdiensten eingegangen wird. Nach einhelliger Meinung stellt dies wohl ein gesetzgeberisches Versehen dar, dass der redaktionellen Anpassung an die europäischen Richtlinien geschuldet ist. Der nach der Gesetzessystematik eingeschränkte Anwendungsbereich ist im Wege einer Analogie dahingehend auszulegen, dass er grundsätzlich auch geschlossenen Benutzergruppen eröffnet und nicht auf Anbieter öffentlich zugänglicher Telekommunikationsdienste beschränkt bleibt. Dies ist deshalb von Bedeutung, weil man auch dann Diensteanbieter im Sinne des TKG ist, wenn das Angebot von Telekommunikationsdienstleistungen nur für geschlossene Benutzer-

gruppen erfolgt. So sind beispielsweise Betreiber von Hotels oder Cafés, die ihren Gästen einen Internetzugang anbieten, ebenso Diensteanbieter wie Arbeitgeber, die ihren Arbeitnehmern die private Nutzung der betrieblichen Telekommunikationsinfrastruktur erlauben.

Gestrichen wurde die Regelung des § 92 TKG, nach der Diensteanbieter personenbezogene Daten an ausländische Stellen nach Maßgabe des BDSG nur übermitteln durften, soweit dies für die Erbringung von Telekommunikationsdiensten, für die Erstellung und Versendung von Rechnungen oder für die Missbrauchsbekämpfung erforderlich war. Diese Vorschrift enthielt also eine bereichsspezifische Zweckbindung, die zusätzlich zu den Regelungen des BDSG zu beachten war. Künftig bemisst sich die Zulässigkeit einer entsprechenden Datenübermittlung nach den §§ 4b und 4c BDSG. Wie sich das konkret auswirken wird, ist noch nicht sicher zu beurteilen. Der Datenverkehr in und zwischen den Mitgliedstaaten der Europäischen Union ist nun genauso zu behandeln wie der inländische. Für eine Datenübermittlung in ein Land außerhalb der Europäischen Union, ein sog. Drittland, sind nunmehr die Vorgaben des BDSG maßgeblich. Ich gehe davon aus, dass auch in diesen Fällen das neue Verfahren keine datenschutzrechtlichen Standards absenkt, zumal ich nach § 4c Absatz 2 BDSG für Genehmigungen zuständig bin, falls personenbezogene Daten in einen Drittstaat übermittelt werden sollen.

6.5 Ortung per Handy

Die jüngste TKG-Änderung hat für Ortungsdienste Regelungen geschaffen, die einen Missbrauch signifikant erschweren – zumindest theoretisch.

Die Situation bei den Ortungsdiensten hatte ich in meinem 23. TB (Nr. 6.2) ausführlich dargestellt. Kritisch sah ich insbesondere die Möglichkeiten zur heimlichen Handy-Ortung. Mit der im Mai 2012 in Kraft getretenen Änderung von § 98 TKG wurden die rechtlichen Anforderungen an Ortungsdienste verschärft. Sie müssen bei jeder Feststellung des Standortes eine Informations-SMS an das Handy senden. Nur wenn der Standort ausschließlich auf dem Handy angezeigt wird, darf auf den SMS-Hinweis verzichtet werden.

Einige Monate nach dem Inkrafttreten der Neuregelung recherchierte ich im Internet stichprobenartig deren Umsetzung. Dabei fielen mir zwei Firmen auf, die offensichtlich noch Ortungen ohne Übersendung von SMS durchführten. Hierbei handelt es sich um einen bußgeldbewehrten Tatbestand, weshalb ich die Bundesnetzagentur als zuständige Bußgeldbehörde um weitere Prüfung bat.

Die Unternehmen beriefen sich darauf, dass es sich um „Eigenortungen“ handele, bei denen keine SMS zu versenden sei. Mich und die BNetzA überzeugte diese Einlassung nicht, denn der Standort wird ja nicht auf dem georteten Handy, sondern an anderer Stelle angezeigt – insofern gibt es keinen Rechtfertigungsgrund für den Verzicht auf die Info-SMS. Die BNetzA erließ einen Bußgeldbescheid, gegen den Widerspruch eingelegt wurde. Den weiteren Fortgang des Verfahrens werde ich mit Interesse verfolgen.

Bedeutsam ist eine weitere Änderung der datenschutzrechtlichen Vorgaben für die Ermittlung und Verwendung von Standortdaten. Bisher erfasste das TKG nur Standortdaten, die in einem Telekommunikationsnetz erhoben oder verwendet werden. In der TKG-Novelle wurden auch die Standortdaten aufgenommen, die von einem Telekommunikationsdienst erhoben oder verwendet werden (s. § 3 Nummer 19 TKG). Es sind nicht nur die Funkzellen umfasst, in denen ein Handy eingebucht ist, sondern ggf. auch die per Satelliten- oder WLAN-Ortung erfassten Standortdaten. Bisher sind die praktischen Konsequenzen dieser Änderung noch nicht abschließend abzuschätzen. Schon jetzt erkennbar sind jedoch zwei Problemkreise: Zum Einen ist vielfach eine klare Unterscheidung zwischen Telekommunikationsdienst und Telemediendienst schwierig, so dass unklar bleibt, ob jeweils das TKG oder das Bundesdatenschutz- bzw. Telemediengesetz anwendbar ist. Zum Anderen kann die Ortung durch einen Dienst erfolgen, der über das (mobile) Internet aus dem Ausland erbracht wird, so dass deutsche Vorschriften nur eingeschränkt gelten und durchsetzbar sind.

Unabhängig von diesen gesetzlichen Vorgaben trete ich dafür ein, die ausufernde Verwendung von Standortdaten, insbesondere mittels Smartphone-Apps, wirksam zu begrenzen und für die Betroffenen transparent zu gestalten. Die Verantwortung hierfür liegt bei den App-Anbietern, den Unternehmen, die Download-Plattformen bereitstellen und bei den Herstellern der Smartphone-Betriebssysteme. Von der in der Diskussion befindlichen Datenschutz-Grundverordnung (vgl. Nr. 2.1.1) erwarte ich hier deutliche Verbesserungen, insbesondere weil auch Anbieter aus Drittstaaten an die Vorgaben des europäischen Datenschutzrechts gebunden werden.

6.6 Notrufortung: Weihnachten kommt immer so überraschend …

Die Notrufortung sollte an Weihnachten 2012 umgesetzt worden sein – zumindest nach den Vorstellungen des Gesetzgebers. Technische Umsetzungsprobleme führen zu Verzögerungen.

Bereits seit 2004 sieht das Telekommunikationsgesetz (TKG) eine Übermittlung des Standortes eines Notrufenden zur Rettungsleitstelle vor. Nur so können Notrufe von Handys bearbeitet werden, wenn der Anrufer nicht in der Lage ist, seinen genauen Standort zu nennen. Bei Festnetzkunden kann der Standort vom Netzbetreiber alternativ auch anhand der Bestandsdaten ermittelt werden. Zur Umsetzung dieser Regelung des TKG waren die Notrufverordnung und die Technische Richtlinie Notruf (TR Notruf) erforderlich, die beide auf sich warten ließen. Die Björn-Steiger-Stiftung hatte daraufhin im Jahr 2006 die Initiative ergriffen und ein alternatives System zur Notrufortung aufgebaut. Dieses wurde inzwischen von der Allianz OnlineService GmbH (AOS) übernommen (vgl. 23. TB Nr. 6.2). Dieses System ermöglicht zwar eine Ortung von Notrufenden, entspricht aber nicht den Vorgaben des Gesetzgebers, und auch ein Missbrauch ist zumindest theoretisch nicht ausgeschlossen.

Nachdem die Notrufverordnung mit einiger Verzögerung 2009 erlassen und die TR Notruf schließlich am 22. Juni 2011 im Amtsblatt Nr. 12 der Bundesnetzagentur (Verfügung Nr. 42/2011) veröffentlicht wurde, war diese auf-

grund einer 18-monatigen Übergangsfrist bis zum 23. Dezember 2012 umzusetzen. Somit war ein den Vorgaben des Gesetzes entsprechender Betrieb der Notrufortung an Weihnachten 2012 zu erwarten.

Weil die Mobilfunknetzbetreiber bei der Implementierung technische Probleme feststellten, mussten einige Vorschriften der Notrufverordnung geändert werden (vgl. auch Bundesratsdrucksache 595/12). Obwohl sich alle Seiten um eine möglichst schnelle Umsetzung bemühten, konnte der Termin nicht gehalten werden. Da die Änderungen der Technischen Richtlinie erst spät an die Hersteller der Notrufabfragestellen weitergegeben wurden, muss mit einer Verzögerung von einigen Monaten gerechnet werden, bis die übermittelten Standortdaten in den Rettungsleitstellen ausgewertet werden können. Aus diesem Grunde habe ich einen zeitlich begrenzten Weiterbetrieb des Notrufortungssystems von AOS bis Ende März 2013 akzeptiert. Ich gehe davon aus, dass spätestens an Ostern die Notrufortung gesetzeskonform betrieben wird.

Einige Punkte in der TR Notruf sind noch offen. So wird gefordert, Standortinformationen auch bei Verbindungen zwischen Netzbetreibern zu übermitteln. Natürlich ist es sinnvoll, etwa bei der Internettelefonie (VoIP), den Standort des Anrufers zu ermitteln. Durch die mögliche „nomadische“ Nutzung muss der Standort aber nicht mit dem Wohnort des Nutzers übereinstimmen. Somit muss anhand der IP-Adresse der Internetanbieter ermittelt und um Auskunft zum Standort befragt werden. Wie dies für beliebige Internetanbieter mit wirtschaftlich vertretbarem Aufwand und gleichzeitig ausreichender Sicherung gegen Missbrauch durchgeführt werden kann, lässt die TR Notruf offen. Mir sind noch keine Lösungen bekannt.

In der TR Notruf wird auch ein optionales Verfahren geregelt, wie eine zusätzliche Übermittlung von Standortdaten durch ein Handy bei einem Notruf erfolgen kann. Diese Standortangaben, etwa von einer Satellitenortung, können deutlich genauer sein als die durch ein Mobilfunknetz ermittelten Standorte. Die zusätzliche Übermittlung wäre durchaus sinnvoll, da so bei einem Rettungseinsatz wertvolle Zeit gespart werden kann. Ein Anrufer sollte jedoch hierüber informiert sein und zumindest die Möglichkeit haben, diese Übermittlung im Einzelfall auszuschließen.

Weiterhin halte ich die Forderung, dass Notrufanschlüsse mit dem Leistungsmerkmal „Malicious Call Identification“ auszustatten sind, für problematisch. Dieses für sog. Fangschaltungen verwendete Leistungsmerkmal dürfte aufgrund der generellen Rufnummernanzeige bei Notrufanschlüssen zur Ermittlung von Spaßanrufern nur einen begrenzten Mehrwert bieten. Regelungen, wie lange hier Verkehrsdaten gespeichert werden sollen, sucht man in der Richtlinie vergebens. Somit ist zu erwarten, dass ich mich weiterhin mit der Notrufthematik zu beschäftigen habe.

6.7 Leitfaden zur Speicherung von Verkehrsdaten

Vom „Leitfaden zum Datenzugriff“ zum „Leitfaden zur Speicherung von Verkehrsdaten“. Er soll zu einer datenschutzgerechten und einheitlichen Auslegung des TKG führen.

Die Veröffentlichung des „Leitfadens zum Datenzugriff, insbesondere für den Bereich der Telekommunikation“ der Generalstaatsanwaltschaft München, hat großes öffentliches Interesse an der tatsächlichen Speicherdauer von Verkehrsdaten geweckt. Telekommunikationsanbieter standen in der Kritik, die zu einem Teil berechtigt war. Diese Thematik wurde deswegen beim „Jour Fixe Telekommunikation“ im Herbst 2011 diskutiert, einem regelmäßigen Treffen des BfDI mit Datenschutzbeauftragten der Netzbetreiber. Als Ergebnis habe ich gemeinsam mit der Bundesnetzagentur (BNetzA) einen Leitfaden zur Speicherung von Verkehrsdaten erarbeitet. Die Netzbetreiber wurden um Kommentierung eines im Frühjahr 2012 vorgelegten ersten Entwurfs gebeten. Der endgültige Leitfaden konnte im Herbst 2012 veröffentlicht werden. Er soll zu einer datenschutzgerechten und einheitlichen Auslegung des TKG – auch im Sinne von „Best Practices“ – führen und stellt für die Beurteilung des Begriffs der Erforderlichkeit einen Prüfungsmaßstab dar.

Den Leitfaden habe ich in meinem Internetangebot unter Informationsmaterial | Arbeitshilfen veröffentlicht, von der BNetzA erfolgte eine Veröffentlichung in deren Amtsblatt.

De facto sieben Tage

Ein Punkt, der sich fast schon als roter Faden durch den Leitfaden zieht, ist eine de-facto-Sieben-Tage-Regelung für die Speicherung nicht abrechnungsrelevanter Verkehrsdaten. Diese hat sich im Laufe der Jahre als praktikabler Weg herausgestellt, um einerseits den datenschutzrechtlichen Überlegungen zu genügen, andererseits aber den betrieblichen Anforderungen der Netzbetreiber zu entsprechen.

Damit können zumindest zeitnah gemeldete Störungen überprüft oder Vergleiche über mehrere Tage gemacht werden. In einer BGH-Entscheidung (vom 13. Januar 2011, III ZR 146/10) wurde diese Sieben-Tage-Frist für den Fall der Speicherung von dynamischen IP-Adressen gestützt. Soweit die Daten allerdings bereits vor Ablauf der sieben Tage nicht mehr zur Störungserkennung und -beseitigung gebraucht werden, müssen sie vom Unternehmen gelöscht werden. Insofern handelt es sich um eine Höchstfrist, von der jeweils im Lichte der konkreten Umstände nach unten abgewichen werden kann.

Ähnlich liegt die Problematik bei der Missbrauchserkennung. Hier dürfen, als Ausnahme von der Zweckbindung, Daten verwendet werden, die für andere Zwecke gespeichert sind. Für bestimmte Szenarien kann es auch angemessen sein, weitere Verkehrsdaten für begrenzte Zeit zu speichern. Die entsprechende Formulierung im TKG hat jedoch zu vielen Diskussionen geführt, aus § 100 Absatz 3 TKG kann jedenfalls keine unumstrittene Handlungsanweisung gewonnen werden. Hier wäre eine Konkretisierung wünschenswert. Einen dritten Anwendungsfall für die Sieben-Tage-Frist bildet die Speicherung von Rohdaten. Die Verpflichtung in § 97 Absatz 3 TKG, „unverzüglich“ die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln, kann man zunächst als „sofort“ verstehen. Dabei ist der Tatsache Rechnung zu tragen, dass die Daten in der Praxis im Regelfall in mehreren Verarbeitungsstufen in komplexen, oft historisch gewachsenen Datenverarbeitungssystemen verarbeitet werden, die mit vielen unterschiedlichen Tarifen zurecht kommen

müssen. Eine fehlerhafte Berechnung der Entgelte würde zu erheblichen Verlusten bei den Unternehmen führen. Deshalb werden die Rohdaten für eine begrenzte Zeit zwischengespeichert. Da bei einer sorgfältigen Kontrolle Probleme bei der Datenverarbeitung innerhalb weniger Tage auffallen sollten, halte ich auch hier eine Speicherfrist von maximal sieben Tagen für angemessen. Eine längere Speicherdauer kann ich nicht mehr als „unverzügliche Ermittlung“ ansehen.

Wie lange abrechnen?

Auch die Speicherdauer von abrechnungsrelevanten Daten wurde geprüft. In § 97 Absatz 3 TKG wird die Höchstfrist mit sechs Monaten nach Rechnungsversand angegeben. Diese ist aber oft nicht erforderlich, insbesondere wenn ein Anbieter die Reklamationsfrist für den Kunden in den AGB entsprechend § 45i Absatz 1 TKG auf acht Wochen nach Rechnungserhalt begrenzt. Insofern halte ich drei Monate (acht Wochen zuzüglich Brieflaufzeit und Bearbeitungszeit) im Regelfall für ausreichend – begründete Ausnahmen sind möglich, wobei auch Abweichungen nach unten erfolgen können und müssen, sofern die Daten nicht mehr für Abrechnungszwecke benötigt werden. Auch bei der Abrechnung zwischen Netzbetreibern halte ich die bei vielen Anbietern übliche sechsmonatige – und teilweise noch längere – Speicherung nicht für angemessen. Nach meinem Eindruck sprechen meist keine überzeugenden sachlichen Gründe für diese Speicherpraxis. Lediglich in besonders zu begründenden Sonderfällen, etwa bei bestimmten Mehrwertdiensten, könnte eine sechs Monate umfassende Speicherung erforderlich sein.

Was braucht man zum Abrechnen?

Ein weiterer Punkt betrifft den Inhalt der Datensätze. Gerade im Mobilfunkbereich sind viele Informationen in einem Abrechnungsdatensatz enthalten, wie zum Beispiel die verwendete Funkzelle oder die Seriennummer eines Handys. Die Speicherung der Funkzelle ermöglicht die Erstellung eines Bewegungsbilds des Nutzers, ist aber nur bei einem sehr kleinen Teil der Kunden für die Abrechnung erforderlich. Die Netzbetreiber verweisen auf die Kosten, die es verursachen würde, die oben erwähnten komplexen Systeme zu ändern. Hier gilt aber das Primat des Rechts: Daten, die für die zulässigen Zwecke nicht oder nicht mehr erforderlich sind, müssen gelöscht werden.

6.8 Erfahrungen bei Kontrollen im Telekommunikationsbereich

Die Durchführung von Kontroll- und Beratungsbesuchen ist eine meiner Kernaufgaben. Ohne entsprechende Prüfungen liefen datenschutzrechtliche Vorgaben Gefahr, in der Praxis nicht mit der gebotenen Sorgfalt umgesetzt zu werden.

Im Berichtszeitraum habe ich die Anzahl der Kontrollen bei Telekommunikationsanbietern und Behörden deutlich erhöht. Der Schwerpunkt lag bei Mobilfunknetzbetreibern, bei denen sowohl die Verarbeitung von Bestands- als auch von Verkehrsdaten geprüft wurde.

6.8.1 Allgemeines: Jeder Beratungs- und Kontrollbesuch ist anders

Beratungs- und Kontrollbesuche geben immer wieder interessante Einblicke in die Unternehmen und Behörden, insbesondere weil es trotz gleicher Thematik viele Besonderheiten und unterschiedliche Probleme gibt.

Die Mitarbeiter sämtlicher geprüfter Unternehmen und Behörden sind in der Mehrheit sehr kooperativ und bemüht, mir ausreichende Informationen über die Betriebsabläufe zu geben. Wegen der in der Regel guten Vorbereitung und Organisation der Termine konnten Beratungs- und Kontrollbesuche meistens im geplanten Umfang durchgeführt werden. Es gibt allerdings auch Einzelfälle, in denen selbst bei rechtzeitig angekündigtem Besuch seitens der geprüften Stelle keine erkennbaren Vorbereitungen getroffen wurden. In einem Fall hatte der einzige anfangs anwesende betriebliche Experte (der zudem nur für einen einzigen Aspekt des Dienstes zuständig war) lediglich einen halben Tag Zeit. Tiefergehende Fragen konnten nur zu einem begrenzten Teil beantwortet werden, da nur für eine weitere Problematik ein Experte zur Verfügung stand. Konsequenz: Diesem Unternehmen werde ich 2013 einen weiteren Besuch abstatten. Auch im Hinblick auf die Nachbereitung der Besuche – insbesondere das zeitnahe Nachliefern von Informationen und Unterlagen – gibt es bei einigen Unternehmen noch „Luft nach oben“.

Nach meinen Erfahrungen führen insbesondere ausführliche Kontrollen und die damit für die Unternehmen verbundene Notwendigkeit, sich intern mit ihren Verfahrensabläufen auseinanderzusetzen, zu deutlichen Verbesserungen. Die mit Prüfungen bewirkte Förderung des Verständnisses und Zusammenspiels von Fachabteilungen und betrieblichen Datenschutzbeauftragten ist eine der wichtigsten Voraussetzungen für Fortschritte beim Datenschutz. Gerade bei großen Telekommunikationsanbietern ist die frühzeitige Einbindung des betrieblichen Datenschutzbeauftragten besonders wichtig, um den Gedanken von „Privacy by Design“ umzusetzen, zumal nachträgliche Änderungen an Systemen oftmals viel Zeit benötigen.

Anders gelagert ist die Problematik bei vielen kleinen Telekommunikationsunternehmen. Einerseits können Missstände hier meist zeitnah korrigiert werden. Andererseits ist das Problembewusstsein oft nur sehr mangelhaft ausgeprägt. Als Beispiel hierzu möchte ich ein Unternehmen nennen, das neben seiner Haupttätigkeit zusätzlich als „Mini-Serviceprovider“ tätig ist und zeitweise einige tausend Mobilfunkverträge abgeschlossen hatte. Ich wurde durch eine Eingabe auf dieses Unternehmen aufmerksam und sah mich schließlich veranlasst, dort einen Prüfbesuch durchzuführen. Dabei fand ich, begründet durch Unkenntnis der Unternehmensvertreter über die Rechtslage, erhebliche datenschutzrechtliche Mängel vor. So lagen einem Vertrag zur Auftragsdatenverarbeitung ausschließlich mündliche Absprachen zugrunde, aber „immerhin“ wurde eine Papiertüte mit über hundert Daten-CD in einem Safe sicher aufbewahrt. Auf diesen CDs waren u. a. sämtliche Verkehrsdaten der Teilnehmer über einen Zeitraum von fast zehn Jahren gespeichert. Zwi-

schenzeitlich wurden verschiedene Maßnahmen durchgeführt, und ich gehe heute von einem rechtskonformen Betrieb aus.

Auch bei Behörden habe ich Beratungs- und Kontrollbesuche durchgeführt und dabei insbesondere die Verarbeitung der Verkehrsdaten in den Telefonanlagen geprüft. Obwohl hier zunehmend neue, auf IP-Technik basierende TK-Anlagen eingesetzt werden, sind die Probleme beim Betrieb altbekannt. Gegenüber meinen Feststellungen im 19. TB (Nr. 11.15) hat sich eigentlich nur die umzusetzende Vorschrift geändert, da anstelle der Dienstanschlussvorschriften inzwischen die Richtlinie Telekommunikation Bund (RLTk Bund) gilt. Bei fast allen Kontrollen fiel auf, dass entgegen den gesetzlichen Vorgaben Verkehrsdaten erhoben wurden oder diese zu lange gespeichert wurden. Weiterhin gibt es in diesem Bereich nach wie vor Verbesserungsbedarf bei der Gestaltung und Umsetzung der Dienstvereinbarungen zum datenschutzgerechten Betrieb der TK-Anlagen.

6.8.2 Fachliches: Neue und immer wieder alte Probleme

Kontrollen bei den Unternehmen vor Ort sind unumgänglich, können doch viele datenschutzrechtliche Probleme oftmals nur bei einem Blick auf die Praxis entdeckt werden.

Bei verschiedenen Anbietern bin ich auf Systeme gestoßen, bei deren Bezeichnung sich die Nackenhaare eines Datenschützers sträuben: das Data Warehouse (DWH). In einem Fall habe ich eigens einen Besuch dazu durchgeführt. Hier waren praktisch sämtliche Bestands- und Verkehrsdaten aus betrieblich genutzten Systemen nochmals als Kopie im DWH gespeichert. Die Systeme des DWH sind auf einen hohen Datendurchsatz optimiert, so dass man verschiedene Auswertungen effektiv durchführen kann. Dabei ist der Programmieraufwand deutlich geringer als bei den betrieblich genutzten Systemen. Das besuchte Unternehmen argumentiert, dass es sich um rechtmäßig gespeicherte Daten handele und diese entweder anonymisiert oder in zulässiger Weise verwendet würden. Bei den anonymisierten Anwendungen handelt es sich z. B. um Berichte zur Geschäftsentwicklung oder Statistiken für die Funknetzplanung. Personalisierte Anwendungen sind z. B. Auswertungen von Verkehrsdaten bei Kunden, die entsprechend § 96 Absatz 3 TKG darin eingewilligt haben, Auswertungen für spezielle Rabatte oder Einzelverbindungsnachweise für bestimmte Kundengruppen. Für die überwiegende Anzahl der Datensätze kann die Doppelspeicherung jedoch nicht auf Vorschriften des TKG gestützt werden. Eine pauschale Doppelung von Kundendaten für nicht festgelegte Zwecke, wie sie typischerweise in Data-Warehouse-Systemen erfolgt, ist unzulässig. Bei der Verarbeitung personenbezogener Daten hat sich die verantwortliche Stelle an die gesetzliche Zweckbindung zu halten. Die Diskussion mit diesem Anbieter hielt zum Redaktionsschluss noch an. Auch bei anderen Anbietern bestehen zu den „Warenhäusern“ noch offene Fragen, so dass sich das Thema im kommenden Tätigkeitsbericht sicherlich wiederfinden wird.

Eine weitere – für mich unerwartete – Verarbeitung von Verkehrsdaten ist mir gleich bei zwei großen Anbietern aufgefallen. Dort werden an verschiedenen Stellen in der Verarbeitungskette Daten nochmals erhoben, parallel verarbeitet und mit den eigentlichen Abrechnungssystemen verglichen, nur um die eigenen Abrechnungssysteme zu prüfen. Da der „Nachweis der Richtigkeit“ der Abrechnung der Entgelte explizit in § 97 Absatz 2 TKG als zulässiger Zweck aufgeführt wird, halte ich diese Verarbeitung grundsätzlich für legitim. Wenn ein Anbieter jedoch drei getrennte Systeme für verschiedene Prüfungen nutzt, natürlich jeweils mit eigener Datenspeicherung, stellt sich allerdings die Frage der Angemessenheit. Wenn mit solchen Systemen die Vollständigkeit der Abrechnung geprüft werden soll und unverarbeitete Rohdaten verarbeitet werden, die zum Teil nicht abrechnungsrelevant sind, müssen auch Speicherfristen eingehalten werden. Hier gibt es noch einige offene Fragen.

Auch an anderer Stelle versuchen die Unternehmen, „auf der sicheren Seite“ zu sein. Sowohl die Rohdaten aus den Vermittlungsstellen als auch die Ergebnisse von Zwischenschritten bei der Abrechnung werden gerne gesichert. Für bis zu sieben Tage halte ich dies noch für vertretbar (vgl. Nr. 6.7); zehn Wochen Speicherung der Rohdaten in der Vermittlungsstelle oder 90 Tage bei den Zwischenverarbeitungen sind aber definitiv zu lange. Dies habe ich den Unternehmen bereits mitgeteilt.

Eine ebenfalls legitime Verarbeitung von Verkehrsdaten dient dazu, Störungen zu erkennen, einzugrenzen und zu beseitigen. In Mobilfunknetzen gibt es Systeme, die die Verkehrsdaten direkt aus dem Signalisierungsverkehr gewinnen. Dumm nur, dass auch Inhalte, wie Inhalte von SMS, im Signalisierungskanal übertragen werden. Hier reicht es nicht aus, dass die Anbieter versprechen, die Inhalte nicht zu lesen – sie dürfen erst gar nicht gespeichert werden. Auch ein anderes System für die Fehlerbeseitigung hat mich überrascht: Hier wurden der Datenverkehr der Mobilfunknutzer kopiert und die daraus gewonnenen Verkehrsdaten – gemeint war auch die URL der angesurften Seiten – entgegen den gesetzlichen Vorgaben für eine Woche personenbezogen gespeichert. Auch zur Störungsbeseitigung gem. § 100 Absatz 1 TKG ist explizit nur die Verarbeitung von Bestands- und Verkehrsdaten gestattet, nicht die von Inhalten. Um solche handelt es sich – aus telekommunikationsrechtlicher Sicht – aber auch bei durch den Internetzugangsanbieter übertragenen URLs. Denn der Mobilfunkanbieter muss diese für die Erbringung seiner Leistung nicht verarbeiten, sondern kann sie unbesehen weiterleiten (vgl. 23. TB Nr. 6.5).

Bei der Kontrolle eines Systems für die Auskunft über Verkehrsdaten an Sicherheitsbehörden, das ich genauer geprüft habe, weil bei einem anderen Mobilfunkanbieter zu umfangreiche Auskünfte festgestellt wurden (vgl. Nr. 7.4.6), habe ich grundsätzlich einen positiven Eindruck gewonnen. Wie ich jedoch feststellen musste, hatte eine Löschroutine zwei Jahre zuvor für einige Monate versagt. Somit waren etliche Abfragen von Behörden, einschließlich der übermittelten Verkehrsdaten, noch im System gespeichert. Auch wenn ich diesen Vorfall nicht

zu hoch aufhängen möchte – zumal die betroffenen Daten kurzfristig nach meiner „Entdeckung“ gelöscht wurden –, ist es für mich nicht nachvollziehbar, weshalb dieser Fehler den Mitarbeitern bei ihrer täglichen Arbeit nicht aufgefallen war.

Viele Anbieter speichern auch Bestandsdaten zu umfangreich und zu lange. Bereits im letzten Tätigkeitsbericht (vgl. 23. TB Nr. 6.3) berichtete ich von einem Telekommunikationsanbieter, der entgegen den Vorschriften des TKG grundsätzlich keine Löschroutine für Bestandsdaten vorgesehen hatte. Trotz großer Bemühungen und Investitionen, von denen ich mich bei weiteren Kontrollbesuchen überzeugt habe, konnte das Unternehmen bis zum Redaktionsschluss aufgrund der komplexen Systemstruktur noch immer keine umfassende Löschung der Daten realisieren.

Darüber hinaus haben meine Kontrollen ergeben, dass bei fast allen kontrollierten Telekommunikationsanbietern zu viele, bisweilen auch falsche oder nicht mehr aktuelle Daten gespeichert werden. Neben nicht mehr aktuellen Bank- und Adressdaten stellen Ausweisdaten, wie die Personalausweisnummer, ausstellende Behörde oder Gültigkeitsdauer, hier das Hauptproblem dar. Nach § 95 TKG dürfen aber nur Bestandsdaten auf Dauer gespeichert werden, die für die Bereitstellung der Telekommunikationsdienstleistung benötigt werden. Obwohl Personalausweisnummern eindeutig nicht zu diesen Daten zählen, werden sie immer häufiger bei Vertragsschluss erhoben und dauerhaft gespeichert. § 95 Absatz 4 TKG gestattet es den Anbietern zwar, sich bei Vertragsschluss den Ausweis des Kunden vorlegen zu lassen und zur Identitätsüberprüfung auch eine Kopie davon anzufertigen. Diese muss allerdings umgehend nach erfolgreicher Prüfung wieder vernichtet werden. Einige Anbieter verzichten sogar vollständig auf die Anfertigung von Ausweiskopien. Ich halte die Erfassung und vorübergehende Speicherung dieser Ausweisdaten lediglich aus zwei Gründen für akzeptabel. Zum Einen, wenn im Zusammenhang mit Vertragsschlüssen Hardware, wie beispielsweise Mobiltelefone oder Router, per Post an den Kunden versandt werden und hierbei das Postidentverfahren genutzt wird. Zum Anderen, um bei Online-Vertragsabschlüssen eine „Echtheitsprüfung“ durchzuführen, bei der die Ausweisnummer einem automatisierten Plausibilitätstest unterzogen wird. In jedem Fall darf die Speicherung der Personalausweisnummer ausschließlich zweckgebunden erfolgen, so dass jeweils eine Löschung unmittelbar nach Wegfall des Zwecks erfolgen muss.

Obwohl die rechtlichen Vorgaben, wie über die datenschutzrechtlichen Wahl- und Gestaltungsmöglichkeiten der Kunden zu informieren ist, seit langem unverändert sind, musste ich immer wieder feststellen, dass Vertrags- und Antragsformulare bei vielen Unternehmen fehlerhaft sind. Häufig fehlen Hinweise auf die bei der Beantragung eines Einzelverbindungsnachweises abzugebende Mitbenutzererklärung. Ebenso sind die Gestaltungsmöglichkeiten der Einträge in Telefonverzeichnisse oder der Auffindbarkeit bei Auskunftsdiensten mangelhaft. Besonders negativ fiel auf, dass in vielen Antragsformularen Felder, in denen die Einwilligung zur Nutzung der Bestands- und Verkehrsdaten explizit eingeholt werden muss, bereits systemseitig vorbelegt waren. Gerade weil es sich hierbei um Verstöße gegen Vorschriften handelt, die den Unternehmen zwingend bekannt sein müssten, kann der Eindruck entstehen, die Vertragsgestaltung solle unter Umgehung der Kundenwünsche im Sinne des Unternehmensinteresses beeinflusst werden.

6.9 Zuständigkeit für Bußgeldverfahren immer noch ungeklärt!

Seit Jahren setze ich mich vergeblich dafür ein, im Telekommunikationsbereich die gesetzliche Zuständigkeit für Bußgeldverfahren bei Verstößen gegen das Bundesdatenschutzgesetz zu erhalten.

Wie ich bereits in meinem letzten Tätigkeitsbericht ausgeführt hatte, kann ich Verstöße von Telekommunikationsunternehmen gegen das BDSG nicht mit einem Bußgeld belegen. Da auch die Bundesnetzagentur (BNetzA) nur Sanktionen verhängen kann, wenn Verstöße gegen spezialgesetzliche Regelungen wie z. B. das Telekommunikationsgesetz (TKG) vorliegen, liegt eine bedeutende Regelungslücke vor (vgl. 23. TB Nr. 2.1 und 6.3).

Im Rahmen der Novellierungen des BDSG im Jahr 2009 wurden neue Bußgeldvorschriften eingeführt. Seither sind auch Verstöße gegen die §§ 11 oder 34 BDSG bußgeldbewehrt, die im Bereich der Telekommunikationsbranche regelmäßig relevant werden. In meiner Aufsichtstätigkeit nach § 115 Absatz 4 TKG ist es daher notwendig, bei Verstößen die Bußgeldvorschriften des § 43 BDSG anzuwenden. Die Übertragung dieser Aufgabe entspräche der Systematik des § 38 Absatz 5 BDSG, der den Datenschutzaufsichtsbehörden der Länder für den nicht-öffentlichen Bereich ebenfalls die Zuständigkeit für die Verhängung von Buß- und Zwangsgeldern überträgt. Dies trägt schließlich den zwingenden Vorgaben des europäischen Rechts (Artikel 8 Absatz 3 EU-Grundrechtecharta, Artikel 28 EG-Datenschutzrichtlinie 95/46/EG) Rechnung, wonach die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften und die Verhängung von Sanktionen im datenschutzrechtlichen Bereich unabhängigen Behörden zu übertragen ist.

In Ermangelung einer konkreten Zuständigkeitsregelung für diese Fälle im BDSG oder dem TKG hatte ich mich daher bereits im Herbst 2009 an das BMWi gewandt und darum gebeten, eine Klärung der Zuständigkeiten herbeizuführen. Dies sollte ursprünglich im Zuge der seinerzeit anstehenden Novelle des TKG (vgl. Nr. 6.4) erfolgen. Eine zunächst im Referentenentwurf aufgenommene Regelung wurde aber aus mir nicht bekannten Gründen plötzlich wieder gestrichen und auch im späteren Verlauf des Gesetzgebungsverfahrens nicht wieder aufgenommen, obwohl ich die zuständigen Ausschüsse des Deutschen Bundestages auf diese Problematik aufmerksam gemacht habe. Es bleibt also bei dem unhaltbaren Zustand, dass Ordnungswidrigkeiten nach dem BDSG im

Bereich der Telekommunikationsunternehmen praktisch überhaupt nicht geahndet werden.

Mangels einer speziellen gesetzlichen Zuständigkeitsregelung gehe ich momentan von einer Anwendbarkeit des § 36 Absatz 1 Nummer 2 lit. b OWiG (vgl. Kasten zu Nr. 6.9) aus. Dabei ist als „fachlich zuständig" dasjenige Bundesministerium anzusehen, zu dessen Geschäftsbereich die das Gesetz ausführende Bundesbehörde gehört. Nach meiner – von der Bundesregierung offenbar nicht geteilten – Auffassung liegt die primäre Zuständigkeit für den Telekommunikationsbereich beim BMWi. Diesem werde ich entsprechende Bußgeldverfahren zur weiteren Bearbeitung vorlegen.

Ich empfehle nochmals dringend, mir die Zuständigkeit für die Verfolgung von nach dem BDSG bußgeldbewehrten Verstößen durch Telekommunikationsunternehmen zu übertragen. Diese Lösung ist nicht nur aufgrund praktischer Erwägungen sinnvoll, sondern vielmehr auch europarechtlich geboten.

Kasten zu Nr. 6.9

§ 36 OWiG (Auszug)

Sachliche Zuständigkeit der Verwaltungsbehörde

(1) Sachlich zuständig ist

1. die Verwaltungsbehörde, die durch Gesetz bestimmt wird,
2. mangels einer solchen Bestimmung
   a) die fachlich zuständige oberste Landesbehörde oder
   b) das fachlich zuständige Bundesministerium, soweit das Gesetz von Bundesbehörden ausgeführt wird.

…

(3) Das nach Absatz 1 Nr. 2 Buchstabe b zuständige Bundesministerium kann seine Zuständigkeit durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, auf eine andere Behörde oder sonstige Stelle übertragen.

6.10 Gesprächsaufzeichnungen in Callcentern

Eine Gesprächsaufzeichnung ohne vorherige Einwilligung des Kunden ist nicht zulässig. Die Möglichkeit, einer Aufzeichnung zu widersprechen, erfüllt nicht die datenschutzrechtlichen Anforderungen. Ein Thema auch für den Beschäftigtendatenschutz.

Es ist gängige Praxis in der Telekommunikationsbranche, sich zur Bearbeitung von Kundenanliegen so genannter Callcenter zu bedienen. Von großer datenschutz- und strafrechtlicher Relevanz ist hierbei die Frage, ob Kundengespräche mit den jeweiligen Beratern des Callcenters durch z. B. einen Teamleiter mitgehört oder aufgezeichnet werden dürfen, um die Qualität der Kundenbetreuung zu überprüfen.

Einvernehmlich mit den Datenschutzaufsichtsbehörden der Länder vertrete ich die Auffassung, dass eine Aufzeichnung von Gesprächen nur nach vorheriger Einwilligung des Kunden und des Mitarbeiters in Betracht kommt. Eine Aufzeichnung ohne eine solche Einwilligung ist grundsätzlich nach § 201 Strafgesetzbuch als „Verletzung der Vertraulichkeit des Wortes" strafbar. Beim reinen Mithören eines Kundengespräches zur Qualitätskontrolle oder zu Ausbildungszwecken empfehle ich, den Anrufer und den Mitarbeiter des Callcenters vorher darüber zu informieren. Der Anrufer kann dann selbst entscheiden, ob er das Telefonat fortsetzt oder beendet.

Im Berichtszeitraum haben meine Mitarbeiter bei ihren Beratungs- und Kontrollbesuchen festgestellt, dass einige Unternehmen diese Einwilligungslösung bereits praktizieren, andere hingegen noch auf eine Widerspruchslösung setzen, wonach der Kunde einer Aufzeichnung explizit widersprechen muss. Sowohl bei den Kontrollen als auch auf den regelmäßigen Jours Fixes mit Teilnehmern der Telekommunikationsbranche habe ich die Unternehmen aufgefordert, die Einwilligungslösung umzusetzen.

Mit geringem technischem Aufwand ist es möglich, bei Inboundgesprächen (der Kunde ruft an) die Einwilligung vom Kunden über die Tastatur des Endgerätes oder über die Sprachsteuerung der Telefonanlage *vor* Gesprächsbeginn einzuholen. Bei Outboundgesprächen (das Unternehmen ruft den Kunden an) muss der Kunde vom Mitarbeiter des Callcenters direkt angesprochen werden.

Die Gesprächsaufzeichnung bei Callcentern war auch ein Thema, das bei der ins Stocken geratenen Reform des Beschäftigtendatenschutzes (vgl. Nr. 13.1) kontrovers diskutiert wurde. Die von den Regierungsfraktionen vorgeschlagenen deutlich erweiterten Befugnisse zum heimlichen Mithören und Aufzeichnen von Gesprächen lehne ich ab.

6.11 Datenschutz auch beim Betrieb des neuen digitalen Behördenfunks

Nach jahrzehntelangen Vorarbeiten wird der analoge Behördenfunk durch ein bundesweit einheitliches Digitalfunksystem für alle Behörden und Organisationen mit Sicherheitsaufgaben (BOS) sukzessive abgelöst. Als datenschutzrechtlich problematisch erwies sich der Umgang mit Verkehrsdaten dieses Telekommunikationssystems.

Zurzeit befindet sich der digitale BOS-Behördenfunk in der Aufbau- und Inbetriebnahmephase und soll den technisch veralteten analogen BOS-Funk bis zum Jahr 2014 ablösen. Anders als der Analogfunk wird das BOS-Digitalfunksystem zentral von einem Netzbetreiber für alle Bundes- und Landes-BOS betrieben und steht (nach flächendeckendem Aufbau) deutschlandweit zur Verfügung. Damit wird erstmals ein bundesweites Funksystem zur Verfügung stehen, bei dem die Sprachübertragung durchgehend verschlüsselt ist. Die Übermittlung von personenbezogenen Daten über das Funksystem (Beispiele: Übermittlung von Namen und Anschrift bei Personen- und

Kfz-Halterabfragen der Polizei) ist so gegen unbefugtes Mithören geschützt.

Für den Aufbau und Betrieb des BOS-Funksystems ist zentral die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) zuständig. Nutzbar gemacht wird der Digitalfunk für die BOS (z. B. Beschaffung, Freischaltung und Inbetriebnahme von Funkgeräten, technische Betreuung) durch die sog. Autorisierten Stellen von Bund und Ländern, die als „Service-Provider“ auftreten. Bei Beratungs- und Kontrollbesuchen habe ich sowohl die BDBOS als auch die Autorisierte Stelle Bund für den Digitalfunk (AS Bund) aufgesucht, um mich über die konkreten Aufgaben und die Einhaltung des Datenschutzes zu informieren.

Beratungs- und Kontrollbesuche bei der BDBOS

Im Rahmen des BDBOS-Gesetzes (BDBOSG) wurde von der BDBOS ein privates Unternehmen mit dem Aufbau und dem technischen Betrieb der Systemtechnik beauftragt. Da beim Betrieb personenbezogene Daten (Teilnehmernummern) erhoben, gespeichert und verarbeitet werden, musste die BDBOS dafür auch einen Vertrag zur Auftragsdatenverarbeitung schließen, der die Einhaltung des Datenschutzes beim technischen Netzbetrieb sicherstellt. Während diese Beauftragung datenschutzrechtlich nicht zu beanstanden war, halte ich jedoch die pauschale Speicherung sämtlicher Verkehrsdaten für einen Zeitraum von drei Monaten (und im Einzelfall sogar von bis zu 120 Tagen) in Form von Call Data Records (CDR) für unzulässig. Begründet wird die lange Speicherdauer damit, dass im Fehlerfall eine Analyse auch rückwirkend durchgeführt werden können müsse. Aus meiner Sicht rechtfertigt dies jedoch nicht die pauschale Speicherung der durchaus sensiblen Verkehrsdaten ohne konkrete Zweckbindung. In diesem Zusammenhang habe ich auch Bedenken gegen die pauschale Herausgabe dieser Verkehrsdaten an die Autorisierten Stellen des Bundes und der Länder, insbesondere deshalb, weil hier zurzeit keine verbindlichen Dienstanweisungen existieren. Hierzu bin ich weiter im Gespräch mit der BDBOS, um eine datenschutzgerechte Lösung herbeizuführen, die die speziellen Aspekte dieses Funksystems berücksichtigt. Bei meinem letzten Besuch bei der BDBOS ist mir aufgefallen, dass die behördliche Datenschutzbeauftragte nur nach vorheriger Anmeldung Zutritt zum Netzbetriebszentrum des privatwirtschaftlichen Unternehmens erhält, was im Gegensatz zu ihrer Aufsichtspflicht steht. Eine Anpassung an die Vorgaben des BDSG wurde mir hier bereits zugesagt.

Beratungs- und Kontrollbesuche bei der Autorisierten Stelle Bund für den Digitalfunk

Die beim Bundespolizeipräsidium angesiedelte Autorisierte Stelle Bund (AS Bund) ist verantwortlich für die Nutzbarmachung des Digitalfunks für alle Bundesbehörden (auch ressortübergreifend). Zusätzlich trägt die AS Bund die Verantwortung für die Einführung und Nutzung des digitalen Behördenfunks innerhalb der Bundespolizei.

Wie ich bei meiner Kontrolle festgestellt habe, ist durch die technischen Teilnehmernummern des zugrunde liegenden TETRA-Funksystems und die namentliche Erfassung der Beschäftigten bei Ausgabe von Funkgeräten ein Personenbezug möglich und der jeweilige Nutzer bestimmbar. Dieser datenschutzrechtliche Aspekt war den Verantwortlichen vorher nicht klar. Ich habe verdeutlicht, dass es sich deswegen beim Funkverkehr bzw. der Nutzung eines Funkgerätes um einen Umgang mit personenbezogenen Daten handelt, deren Erhebung, Verarbeitung und Nutzung nur zulässig ist, soweit eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Eine entsprechende Rechtsgrundlage konnte mir aber zum Zeitpunkt meines letzten Besuches nicht genannt werden; eine Einwilligungslösung scheidet hier wegen der dienstlichen Verwendung des TK-Systems aus. Hier muss der Gesetzgeber nachbessern.

Ich habe ferner auf die strikte Einhaltung der Zweckbestimmung beim Umgang mit diesen Daten und auf die erforderliche Beteiligung der zuständigen Personalvertretung hingewiesen, da die Verkehrsdaten zur Verhaltens- und Leistungskontrolle der Digitalfunk nutzenden Beschäftigten verwendet werden könnten. Die von mir bereits während meines ersten Besuchs im November 2011 angeregte Dienstanweisung zur Nutzung des Digitalfunks wurde kurz vor meinem zweiten Besuch im November 2012 in Kraft gesetzt. Zu dieser Dienstanweisung habe ich während meines Besuchs im Detail datenschutzrechtliche Änderungs- und Ergänzungsempfehlungen gegeben.

Obwohl der digitale BOS-Funk aufgrund der verschlüsselten Sprachübertragung eindeutige Datenschutzvorteile gegenüber dem analogen BOS-Funk bei der täglichen Anwendung aufweist, müssen auch die datenschutzrechtlichen Anforderungen hier ausreichende Berücksichtigung finden.

6.12 Deutsche Post AG

6.12.1 Konzerndatenschutzrichtlinie der Deutschen Post DHL – ein langer Weg

Die Konzerndatenschutzrichtlinie regelt die datenschutzkonforme Übermittlung von Daten aus der Europäischen Union in Drittstaaten. Die Umsetzung der erteilten Genehmigung dauert länger als erwartet.

In meinem letzten Tätigkeitsbericht (vgl. 23. TB Nr. 10.1) hatte ich über den Abschluss des Genehmigungsverfahrens auf europäischer Ebene berichtet. Spätestens nachdem ich im Februar 2011 die „Deutsche Post DHL Data Privacy Policy (Konzerndatenschutzrichtlinie)“ gebilligt und das Genehmigungsschreiben dem Vorstand überreicht hatte, ging ich von einer zügigen Umsetzung innerhalb des Konzerns aus. Die Deutsche Post DHL (DP-DHL) war nun berechtigt, personenbezogene Daten nach Maßgabe ihrer Data Privacy Policy ins Ausland zu übermitteln, ohne dafür im Einzelfall eine Genehmigung einzuholen. Sie war damit das erste deutsche Unternehmen, dessen verbindliche unternehmensweite Datenschutzregelung (BCR – Binding Corporate Rules) nach einem

umfassenden Konsultationsverfahren zwischen den Datenschutzbehörden der Europäischen Union anerkannt wurde.

Mit meiner Billigung wurde ein (vermeintlich) wesentlicher Schritt auf dem langen Weg bis zur endgültigen Umsetzung der BCR zurückgelegt. Offensichtlich war das unternehmensinterne Verfahren aber so zeitaufwändig, dass mir erst zum Ende des Berichtszeitraums die „Deutsche Post Data Privacy Policy“ in einer Form präsentiert werden konnte, die im Gesamtunternehmen verteilt und dort den geltenden Datenschutzstandard festlegen wird. Im November 2012 hat die letzte Umsetzungsphase, nämlich der Versand der Beitrittserklärungen an die internationalen Konzerngesellschaften, begonnen. Erst im Laufe des Jahres 2013 wird nach den Planungen der DP AG die endgültige Umsetzung der Konzerndatenschutzrichtlinie abgeschlossen sein. Ich bin mir, nicht zuletzt wegen der gegebenen Zusicherung der DP AG, sicher, dass es soweit kommen wird; Prognosen zum zeitlichen Verlauf gebe ich aber keine mehr ab.

6.12.2 Können Packstationen unbesorgt genutzt werden – Kontrollerfahrungen

Der Datenschutz ist gewährleistet, aber Vorsicht bei Phishing-Attacken!

Die überwiegende Zahl der Beschwerden über die Deutsche Post AG (DP AG) betreffen Falschzustellungen, unberechtigte Rücksendungen an den Absender oder die Aufbewahrung von Briefsendungen. Zahlreiche Eingaben, in denen mir Phishing-Attacken bei der Nutzung von Packstationen mitgeteilt wurden, habe ich zum Anlass genommen, mich detailliert vor Ort zu informieren.

Bei den Packstationen handelt es sich um Paketautomaten, an denen Kunden der DP AG Sendungen unabhängig von Öffnungszeiten abholen oder einliefern können. Zur Nutzung dieser Anlage (Ausnahme: Einlieferung von Sendungen) muss sich jeder Kunde zunächst in einem zweistufigen Verfahren registrieren. Dies erfolgt im ersten Schritt durch Ausfüllen eines Online-Registrierungsformulars, in dem u. a. die E-Mail-Adresse und die Mobilrufnummer anzugeben sind; über diese Kontaktkanäle wird der Kunde über abholbereite Sendungen informiert. Im zweiten Schritt werden diese Angaben im Postidentverfahren verifiziert, danach erhält der Kunde persönlich die Unterlagen zur Nutzung der Packstationen („Begrüßungsset“).

Die Petenten berichteten, dass sie per E-Mail um Herausgabe ihrer Authentisierungsdaten (Postnummer und PIN) gebeten wurden. Diese E-Mails erweckten den Anschein, als würde es sich um Anschreiben der DP AG handeln. Auf diesem Weg versuchten unbekannte Dritte, illegal Zugriff auf die in den Packstationen lagernden Sendungen zu erhalten.

Die DP AG teilte mir auf meine Nachfrage mit, sie sei über diese Angriffe und Manipulationsversuche informiert und habe als Gegenmaßnahme Hinweise auf mögliche Phishing-Angriffe und zum sicheren Umgang mit den Zugangsdaten im Begrüßungsset aufgenommen. Der Kunde werde eindeutig darauf hingewiesen, dass die zur Warenabholung notwendigen Daten auf keinen Fall weitergegeben werden dürften. Zur Eindämmung der Phishing-Problematik gründete die DP AG zudem ein sog. Anti-Phishing-Response-Team, das Angriffe analysieren und die Sperrung der entsprechenden Internetseiten veranlassen soll. Weiter wurde das Authentisierungsverfahren zur Warenabholung mittels Postnummer und PIN umgestellt. Nun ist zusätzlich seit dem 2. Quartal 2011 eine Magnetstreifenkarte zur Abholung notwendig.

Seit November 2012 wurde die Magnetstreifenkarte durch eine mobile TAN (mTAN) ersetzt, die der Kunde per SMS erhält. Da die mTAN eine transaktionsbezogene Nummer mit begrenzter Gültigkeit ist, wird so ein potentieller Missbrauch zusätzlich erschwert. Aufgrund dieser Sicherheitsmechanismen greifen Phishing-Mails nicht mehr.

Auch wenn keine hundertprozentige Sicherheit gewährt werden kann, sehe ich das aktuelle Verfahren beim Abholen von Sendungen an den Packstationen mittels PIN und mTAN als datenschutzkonform an. Auch die Prüfung der Identität bei der Anmeldung zu diesem Verfahren entspricht den datenschutzrechtlichen Vorgaben.

Aufgrund weiterer Eingaben habe ich mir darüber hinaus auch in einem Verteilzentrum und in einem Zustellstützpunkt einen persönlichen Eindruck davon verschafft, ob und wie die datenschutzrechtlichen Vorgaben dort eingehalten werden. Trotz umfangreicher Schulungsmaßnahmen, die von Qualitätskontrollen bei der Zustellung begleitet werden, lassen sich Fehler beim Umgang mit Paket– und Briefsendungen leider nicht immer vermeiden. Mir ist durchaus bewusst, dass dies für den Betroffenen mit viel Ärger und manchmal sogar mit Nachteilen verbunden sein kann, aber auch hier gilt der Grundsatz „wo gehobelt wird, da fallen Späne“. Es ist jedoch zu berücksichtigen, dass sich diese unerfreulichen Versäumnisse der Anzahl nach im unteren Promillebereich bewegen.

Insgesamt bleibt festzustellen, dass sich die Dienstleistungen der DP AG auf einem hohen Datenschutz- und Qualitätsniveau bewegen. Die mir bekannt gewordenen Fehler mit Datenschutzrelevanz sind durchweg auf einzelnes menschliches Fehlverhalten zurückzuführen und keinesfalls durch fehlerhafte Systemprozesse bedingt. Nach meiner Einschätzung kann der Datenschutz hier nur durch noch bessere Schulungs- und Sensibilisierungsmaßnahmen weiter verbessert werden.

6.13 Hohes Datenschutzniveau bei den Postdienstleistern

Auf dem Markt der Postdienstleister haben sich neben der Deutschen Post AG eine Reihe weiterer Lizenznehmer etabliert; dabei handelt es sich überwiegend um kleine und mittlere Unternehmen, die insbesondere auf regionalen Märkten tätig sind.

Auch zu diesen Unternehmen haben mich Eingaben erreicht, die in etwa die gleichen Probleme wie beim „gelben Bruder“ zum Gegenstand hatten. Thematisiert

wurden überwiegend Falschzustellungen, angeblich unberechtigterweise geöffnete Briefe sowie Missstände bei der Zwischenaufbewahrung von Postsendungen.

Im Unterschied zu den Beschwerden über die Deutsche Post AG wurden hier allerdings auch Versäumnisse bei der Sortierung beklagt. Jedoch zeigt die Anzahl der Eingaben hier ebenfalls – gemessen an dem riesigen Volumen des täglich zu transportierenden Brief- und Paketaufkommens –, dass sich die Beschwerden glücklicherweise im untersten Promillebereich bewegen. Dennoch bin ich natürlich auch diesen relativ wenigen Eingaben nachgegangen.

Wie ich mich bei mehreren Kontroll- und Informationsbesuchen überzeugen konnte, wird bei diesen Unternehmen datenschutzkonform gearbeitet. Wurden einmal kleinere Mängel festgestellt, so sind diese – unter Berücksichtigung meiner vor Ort gegebenen Hinweise – umgehend abgestellt worden. Oft führte alleine meine Besuchsankündigung schon zu einem höheren Datenschutzbewusstsein und zur Behebung von Datenschutzmängeln. Überwiegend sind die Beschwerden auf Unzulänglichkeiten bei der Qualität der Zustellung zurückzuführen, verursacht durch Fehlverhalten im menschlichen Bereich. Es ist nicht zuletzt der Mensch der Faktor, der datenschutzgerechte Leistungen erbringen muss.

Es bleibt aber festzustellen, dass große und kleine Postdienstleister ihre Aufgaben insgesamt datenschutzgerecht erfüllen.

7 Innere Sicherheit und Strafrecht

7.1 Evaluierung von Sicherheitsgesetzen

Die Evaluierung von Sicherheitsgesetzen bleibt eine der Kernforderungen des Datenschutzes. Das Terrorismusbekämpfungsergänzungsgesetz hat die Bundesregierung nur unzureichend evaluiert, die Evaluierung des Antiterrordateigesetzes ist noch nicht abgeschlossen. Für künftige Evaluierungen habe ich beim Deutschen Forschungsinstitut für öffentliche Verwaltung einen Leitfaden in Auftrag gegeben. Dieser steht nunmehr allen Interessierten zur Verfügung.

Sicherheitsgesetze enthalten Befugnisse, die oftmals intensiv in die Grundrechte der Betroffenen eingreifen. Beispiele sind verdeckte Ermittlungsmaßnahmen wie die Telekommunikationsüberwachung oder die umfassenden Befugnisse der Nachrichtendienste, bei denen die Rechtsschutzmöglichkeiten des Einzelnen nur eingeschränkt bestehen. Solche neuen Befugnisse werden oftmals unter dem Eindruck aktueller Ereignisse oder Gefahren mit großer Eile eingeführt. Daher ist es notwendig, in regelmäßigen Abständen gründlich zu überprüfen, ob die Befugnisse sich als effektiv, notwendig und verhältnismäßig erwiesen haben. Immer wieder habe ich deswegen gefordert, die Sicherheitsgesetze umfassend zu evaluieren (vgl. ausführlich 23. TB Nr. 7.1.1). Wichtig ist dabei auch, die vom Gesetzgeber gewählten legislativen Mittel insgesamt in ihren Wechselwirkungen zu berücksichtigen und nicht nur die Folgen des einzelnen Gesetzes („Überwachungsgesamtrechnung“). Die Evaluierung muss anhand einer umfassenden Sachverhaltsauswertung die tatsächlichen – auch mittelbaren – Auswirkungen auf die Betroffenen analysieren. Eine Analyse des Ist-Zustandes kann auch im Vorfeld umfassender Reformen hilfreich sein. Zuerst muss geklärt werden, ob bestehende Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. Erst dann kann entschieden werden, ob und welche gesetzgeberischen Schritte notwendig sind (vgl. dazu Nr. 7.7.6).

Die Deutungshoheit darf dabei nicht bei den Stellen liegen, die mit zusätzlichen Befugnissen ausgestattet wurden. Vielmehr muss der Deutsche Bundestag auf Basis unabhängiger und nach wissenschaftlichen Kriterien durchgeführter Evaluationen darüber entscheiden, ob einmal beschlossene Möglichkeiten weiterhin gerechtfertigt sind. Kritisch sehe ich es deshalb, wenn die Bundesregierung oder eines ihrer Ressorts die Evaluierungen selbst durchführt.

So legte das Bundesministerium des Innern 2011 einen von ihm selbst erstellten Evaluierungsbericht zum Terrorismusbekämpfungsergänzungsgesetz (TBEG) vor, für den es sich nur externe Methodenberatung eingeholt hatte. Der Bericht war zudem inhaltlich unzureichend. Im Mittelpunkt der Analysen hatte nicht die Frage gestanden, welche Auswirkungen das Gesetz auf die Grundrechte der Betroffenen hatte. Genau das wäre aber notwendig gewesen, um die Verhältnismäßigkeit der Befugnisse beurteilen zu können. Der Evaluierungsbericht hätte also soweit wie möglich die Frage beantworten müssen, ob das Gesetz seine Ziele erreicht und der Gesetzgeber dabei das jeweils mildeste geeignete Mittel gewählt hat. Der vorliegende Bericht machte jedoch schon nicht hinreichend deutlich, auf welcher tatsächlichen Grundlage er beruht. Es ist insbesondere nicht zu erkennen, ob zumindest exemplarische Einzelfälle gründlich ausgewertet worden sind. Insgesamt haben sich die Autoren mit den Grundrechten der Betroffenen nur oberflächlich auseinandergesetzt. Für das Antiterrordateigesetz lag bis Redaktionsschluss noch kein abschließender Evaluierungsbericht vor. Die Frist dafür war am 31. Dezember 2011 abgelaufen. Zu den im Koalitionsvertrag vorgesehenen Evaluierungen (vgl. 23. TB Nr. 7.1.1) liegt bislang ebenfalls kein Bericht vor – die hierfür erst Anfang Januar 2013 eingesetzte Regierungskommission wird diese Aufgabe in der in dieser Legislaturperiode noch zur Verfügung stehenden Zeit kaum in der gebotenen Gründlichkeit erledigen können.

Immerhin hat der Gesetzgeber aufgrund der negativen Erfahrungen mit der Evaluierung des Terrorismusbekämpfungsergänzungsgesetzes eine neue Evaluierungsklausel geschaffen („Gesetz zur Änderung des Verfassungsschutzgesetzes“). Danach ist künftig ausdrücklich zu evaluieren, wie häufig und mit welchen Auswirkungen die Nachrichtendienste aufgrund der mit diesem Gesetz geschaffenen Befugnisse in die Grundrechte der Betroffenen eingegriffen haben. Dies ist mit der Frage abzugleichen, wie wirksam und effektiv mit Hilfe dieser Befugnisse terroristische Aktivitäten aufgespürt oder bekämpft

werden konnten. Ich hoffe, hierdurch werden zumindest für dieses Gesetz auch in der Praxis künftige Evaluierungen verbessert.

Als Hilfestellung für künftige Evaluierungen hatte ich beim Forschungsinstitut für öffentliche Verwaltung einen „Leitfaden zur Durchführung von ex-post-Gesetzesevaluationen unter besonderer Berücksichtigung der datenschutzrechtlichen Folgen“ in Auftrag gegeben. Der Leitfaden wurde Ende 2012 fertiggestellt. Er richtet sich an alle Stellen, die eine Gesetzesevaluation in Auftrag geben möchten oder mit ihr betraut sind, also insbesondere an Abgeordnete, Wissenschaftler und Beamte. Der Leitfaden setzt sich umfassend mit den Standards, Evaluationsinstrumenten und Methoden auseinander, die für die Evaluation gelten und stellt die verfassungsrechtlichen Rahmenbedingungen dar. Er gibt zudem einen praktischen Überblick über die notwendigen Abläufe bei den zu evaluierenden Stellen. Schon bevor eine Evaluierung in Auftrag gegeben wird, hilft der Leitfaden den Entscheidungsträgern, dafür die richtigen Bedingungen festzulegen.

Link zum Leitfaden Evaluierung: http://www.datenschutz.bund.de

7.2 Antiterrordatei

Kritische Nachfragen des Bundesverfassungsgerichts zum Antiterrordateigesetz (ATDG). Meine Kontrollen belegen: Auch in grundsätzlicher Hinsicht bestehen weiterhin erhebliche datenschutzrechtliche Defizite.

Am 6. November 2012 hat das Bundesverfassungsgericht eine Verfassungsbeschwerde über das ATDG verhandelt. Auf Aufforderung des Gerichts habe ich in der mündlichen Verhandlung meine Kritik an dem Gesetz (vgl. 21. TB Nr. 5.1.1) vorgetragen und über meine Kontrollerfahrungen berichtet. Insbesondere habe ich angeregt, den Gesetzgeber aufzufordern, zum Schutz unbescholtener (Kontakt-)Personen diverse Regelungen im ATDG enger, hinreichend bestimmt und verhältnismäßig auszugestalten. Das Gericht hat die Vertreter der Bundesregierung und der betroffenen Behörden auch zu den von mir kritisierten Regelungen kritisch befragt. Eine Entscheidung lag bei Redaktionsschluss noch nicht vor. Ich erwarte, dass das Urteil Auswirkungen auf die mit der Antiterrordatei (ATD) weitgehend inhaltsgleiche Rechtsextremismusdatei (RED – vgl. Nr. 7.3) haben wird.

Meine Kontrollen belegen: Es bestanden (vgl. 23. TB Nr. 7.1.2) und bestehen erhebliche datenschutzrechtliche Probleme. Diese kann ich – auch aus Gründen der Geheimhaltung – hier nur abstrakt und exemplarisch darlegen:

– Der Militärische Abschirmdienst (MAD) hat in der ATD Personen als „dolose“ Kontaktpersonen (also als Personen, die von der Planung oder Begehung einer Tat Kenntnis haben – vgl. 22. TB Nr. 4.2.2.2) gespeichert, ohne zu diesen Personen über eigene Erkenntnisse zu verfügen, die diese Speicherung und Bewertung (vgl. § 2 ATDG) gerechtfertigt hätten (vgl. zur Problematik der Kontaktpersonenspeicherung 22. TB Nr. 4.2.2.2 und 21. TB Nr. 5.1.1). Der MAD hat dies mit dem Hinweis begründet, eine andere Behörde habe die Betroffenen in der ATD als (dolose) Kontaktpersonen gespeichert. Diese Vorgehensweise widerspricht den Vorgaben des § 2 Satz 1 ATDG. Danach ist es erforderlich, dass ein in der ATD gespeichertes Datum von der speichernden Stelle selbst erhoben worden ist, wie sich auch aus der Begründung zum ATDG ergibt. Danach dürfen nur (weitergehende) Erkenntnisse gespeichert werden, über die die speichernde Stelle bereits verfügt. Nach Ansicht des MAD ist diese Vorgabe nicht aus der Gesetzesbegründung ableitbar. Die Diskussion hierzu dauert an.

– Der Bundesnachrichtendienst (BND) hatte in Freitextfeldern seiner ATD-Quelldatei unzulässige Daten gespeichert. Noch im Kontrolltermin hat er die Löschung und eine rechtskonforme Befüllung dieser Felder zugesagt, so dass ich von einer Beanstandung abgesehen habe.

  Wie ich bei meiner ATD-Kontrolle ferner festgestellt habe, hatte der BND einen bei einem deutschen Großunternehmen tätigen deutschen Staatsangehörigen sowohl in der ATD als auch in der entsprechenden Quelldatei des BND als dolose Kontaktperson gespeichert.

  Während meiner Prüfung musste der BND einräumen, dass zu diesem Fall keine Akten vorhanden seien. Auf Nachfrage teilte er im Kontrolltermin mündlich mit, es sei eine Anfrage des Großunternehmens erfolgt, ob der Betroffene beim BND bekannt sei. Er habe dies geprüft und dem Unternehmen gegenüber verneint. Weshalb der Betroffene aufgrund dieser Anfrage als dolose Kontaktperson gespeichert worden sei, sei nicht (mehr) erklärbar – zumal der BND über keine sonstigen Erkenntnisse zu dem Betroffenen verfügt habe.

  Obwohl ich den BND im Kontrolltermin um die Sperrung der Daten des Betroffenen bis zum Abschluss meiner Prüfung gebeten hatte, hat dieser aufgrund eines vermeintlichen Missverständnisses die Daten nach meiner Kontrolle abredewidrig gelöscht. Ein Zugriff auf die ATD-Protokolldaten dieses Falles wurde mir von dem zuständigen Bundeskriminalamt verwehrt.

  Abweichend von seinen Einlassungen im Kontrolltermin hat der BND den Sachverhalt nachträglich schriftlich wie folgt dargestellt: Es sei keine Anfrage des Großunternehmens erfolgt. Man habe dorthin auch keine Daten des Betroffenen übermittelt. Vielmehr sei die Anfrage von einer ausländischen öffentlichen Stelle erfolgt. Dorthin sei auch die Antwort übermittelt worden. Belege hierfür konnte der BND nicht vorlegen.

  Diese Änderung des Sachverhalts hat für den Betroffenen gravierende rechtliche Folgen. Während die Auskunft des BND an das Großunternehmen dem Betroffenen mitgeteilt werden muss, ist die Auskunft an eine öffentliche ausländische Stelle nicht mitteilungspflichtig.

Bei meiner Kontrolle hatte ich Ausdrucke (Screenshots) der von mir gesichteten Bildschirminhalte (zu den Datenspeicherungen des Betroffenen) erstellen lassen. Diese stützen inhaltlich die ursprünglichen, mündlichen Darlegungen des BND, wonach es sich um eine Anfrage des vorgenannten Großunternehmens gehandelt hat, die er beantwortet habe. Deswegen habe ich den BND aufgefordert, den Betroffenen hierüber in Kenntnis zu setzen. Während der BND mir dies nach intensiven Erörterungen zugesagt hatte, hat das Bundeskanzleramt als zuständige Fachaufsichtsbehörde eine Mitteilungspflicht verneint und den BND angewiesen, keine Mitteilung durchzuführen. Dem habe ich widersprochen. Eine Stellungnahme des Bundeskanzleramtes stand bei Redaktionsschluss noch aus.

Diese und weitere Ergebnisse meiner Kontrollen habe ich aufforderungsgemäß an das Bundesverfassungsgericht übermittelt. Auch mehrere Landesbeauftragte für den Datenschutz haben dem Gericht ihre Kontrollerfahrungen mitgeteilt.

7.3 Rechtsextremismusdatei

Die Datei zur Bekämpfung des Rechtsextremismus (RED) ist ebenso wie ihr Vorbild – die Antiterrordatei (ATD – vgl. Nr. 7.2) – eine gemeinsame Datei der Polizeien und Nachrichtendienste. Trotz einzelner Verbesserungen gegenüber der ATD sehe ich noch dringenden gesetzgeberischen Handlungsbedarf. Bei ersten Kontrollen habe ich bereits Verstöße festgestellt.

Gesetzliche Grundlage für diese Datei ist das Gesetz zur Bekämpfung des Rechtsextremismus (REDG), das weitgehend inhaltlich dem Antiterrordateigesetz (ATDG – vgl. 21. TB Nr. 5.1.1.) entspricht. Neu ist, dass die in der RED gespeicherten Daten projektbezogen ausgewertet werden dürfen (vgl. § 7 REDG). In Kraft getreten ist das REDG am 31. August 2012.

Nach einer Mitteilung des Bundesministeriums des Innern (BMI) soll die RED „als zweite zentrale Säule [neben dem GAR – vgl. Nr. 7.7.6] den Informationsaustausch zwischen Polizeien und Nachrichtendiensten verbessern“. Zu diesem Zweck verpflichtet das REDG 36 Sicherheitsbehörden des Bundes und der Länder (Bundeskriminalamt, Bundespolizei, Bundesamt für Verfassungsschutz, Militärischer Abschirmdienst, Landesverfassungsschutzbehörden und Landeskriminalämter), ihre Daten zum gewaltbezogenen Rechtsextremismus in der RED zu speichern. Das Bundeskriminalamt (BKA) führt die Datei, die am 19. September 2012 offiziell in Betrieb gegangen ist.

Für das BMI ist die RED „eine richtige Konsequenz aus der NSU-Mordserie, da an der einen oder anderen Stelle die Kommunikation zwischen den Behörden verbesserungsbedürftig“ gewesen sei. Angesichts der noch laufenden Untersuchungen zur Aufklärung der NSU-Taten sowie möglicher Defizite auf Seiten der Sicherheitsbehörden und der hierfür maßgeblichen Ursachen (vgl. Nr. 7.7.6) halte ich diese Aussage für gewagt. Sachgerechte Konsequenzen können sinnvoller Weise nur nach einer umfassenden und gründlichen Untersuchung aller Umstände und Ursachen gezogen werden. Wenn Mitarbeiter von Sicherheitsbehörden nicht erkennen (wollen), dass eine Tat einen rechtsextremistischen Hintergrund hat, werden sie diese Erkenntnis nicht in einer entsprechenden Fachdatei ihrer Behörde speichern. Folglich gelangen diese Erkenntnisse dann auch nicht in die RED. Daher muss man klar feststellen: Vollzugsdefizite können auch mit der RED nicht beseitigt werden.

Hierauf habe ich auch in meiner Stellungnahme als Sachverständiger in der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages zum REDG am 19. März 2012 hingewiesen (vgl. BT, Innenausschussdrucksache 17(4)460E). Zudem habe ich dort auch kritisiert, dass zur Begründung der RED auf die seit 2007 „erfolgreich“ betriebene ATD verwiesen wird. Für diese Bewertung sah ich keine valide Erkenntnisgrundlage, solange nicht die gesetzlich vorgeschriebene Evaluierung des ATDG (vgl. Nr. 7.1) durchgeführt worden ist.

Meine Bedenken richteten sich auch dagegen, dass das REDG vor der Entscheidung des Bundesverfassungsgerichts zu einer dort anhängigen Verfassungsbeschwerde zum ATDG gefallen ist (vgl. Nr. 7.2). Eine auch nur teilweise Verfassungswidrigkeit des ATDG hätte weitreichende Folgen für die inhaltsgleichen Regelungen des REDG.

Wie ich in meiner Stellungnahme vor dem Bundesverfassungsgericht ausgeführt habe, müssen insbesondere zum Schutz unbescholtener (Kontakt-)Personen auch im REDG einige Regelungen enger bzw. hinreichend bestimmter und verhältnismäßig gefasst werden.

Zudem habe ich über meine Kontrollerfahrungen bzgl. der RED berichtet. Bei den wenige Tage vor der mündlichen Verhandlung durchgeführten Kontrollen des REDG beim Bundeskriminalamt und Bundesamt für Verfassungsschutz (BfV) hatte ich festgestellt, dass das BfV alle Personen, die es in der RED als dolose Kontaktpersonen gespeichert hatte, nur als undolose Kontaktpersonen hätten führen dürfen (zur Frage, wann eine Kontaktperson als „dolos“ einzustufen ist vgl. 23. TB Nr. 7.1.2). Dies ist für die Betroffenen von erheblicher Bedeutung. Nur zu dolosen Kontaktpersonen dürfen über Identifizierungsangaben (sog. Grunddaten – z. B. Name, Vorname, Adresse, Geburtsdatum, etc. – vgl. § 3 Absatz 1 Ziffer 1 Buchstabe a ATDG) hinausgehende sog. erweiterte Grunddaten gespeichert werden (vgl. § 3 Absatz 1 Ziffer 1 Buchstabe b REDG; vgl. Kasten zu Nr. 7.3). Das BfV hat noch im Kontrolltermin unverzügliche Korrekturen zugesagt.

Wie ich bei meiner Prüfung ferner festgestellt habe, überträgt das BfV nach einem – mit anderen Behörden abgestimmten – Kriterienkatalog systematisch auch Daten in die RED, die dort nicht gespeichert werden dürfen. Da dieser Katalog als Verschlusssache eingestuft ist, darf ich hierüber nicht detaillierter berichten. Folglich darf ich auch die konkreten Daten (-Kategorien) hier nicht benennen. Ich kann jedoch sagen, dass es sich um äußerst sen-

sible Daten handelt und ich deren systematische Übertragung und Speicherung in der RED nicht erwartet hätte.

Diese Feststellungen erfordern – ebenso wie andere Punkte – weitergehende Kontrollen, auch um die Dimension der Problematik ermitteln zu können. Bis zum Redaktionsschluss konnte ich diese Prüfungen noch nicht durchführen. Eine abschließende Bewertung ist erst danach möglich.

Kasten zu Nr. 7.3

Erweiterte Grunddaten (§ 3 Absatz 1 Ziffer 1 Buchstabe b REDG)

Hierzu gehören sehr umfängliche Daten, wie z. B. eigene oder von Dritten genutzte Telekommunikationsanschlüsse und Telekommunikationsendgeräte, Adressen für elektronische Post, Bankverbindungen, Schließfächer, auf die Person zugelassene oder von ihr genutzte Fahrzeuge, Angaben zum Schulabschluss, zur berufsqualifizierenden Ausbildung und zum ausgeübten Beruf, Angaben zu einer gegenwärtigen oder früheren Tätigkeit in einer lebenswichtigen Einrichtung, Sprachkenntnisse, zusammenfassende besondere Bemerkungen, ergänzende Hinweise und Bewertungen sowie zahlreiche weitere Informationen (vgl. § 3 Absatz 1 Ziffer 1 Buchstabe b Doppelbuchstabe aa bis uu).

7.4 Bundeskriminalamt

7.4.1 Quellen-Telekommunikationsüberwachung

Bei der sog. Quellen-Telekommunikationsüberwachung habe ich Mängel festgestellt.

Ich habe die von Bundeskriminalamt, Zollkriminalamt und Bundespolizei durchgeführten Telekommunikationsüberwachungen datenschutzrechtlich kontrolliert (vgl. zum ZKA bereits 23. TB Nr. 7.4). Dabei habe ich Mängel bei der technischen Absicherung der Maßnahmen und den Löschungsmechanismen für Erkenntnisse aus dem Kernbereich privater Lebensgestaltung festgestellt. Bis zu meiner Kontrolle waren 40 Quellen-Telekommunikationsüberwachungen durchgeführt worden (vgl. Kasten zu Nr. 7.4.1).

Mangelhaft war die Absicherung der ausgeleiteten Datenströme. Diese waren mit einem unzureichenden Verschlüsselungsmechanismus versehen. Darüber hinaus war nicht ausreichend sichergestellt, dass sich die an den technischen Prozessen beteiligten Personen und Systeme hinreichend sicher authentisieren. Die vorhandenen Protokolle in Verbindung mit anderen Informationen ermöglichten zwar eine gute Nachvollziehbarkeit der Aktionen/Zugriffe, entsprechen aber nicht den Anforderungen des § 20l Absatz 2 Satz 2 i. V. m. § 20k Absatz 3 BKAG. Dies habe ich gegenüber dem Bundesministerium des Innern und dem Bundesministerium der Finanzen formell beanstandet. Durch die Infiltration des Computers können Sicherheitslücken geschaffen werden, die es auch Dritten ermöglichen, in das System einzudringen. Daher müssen Datenströme zum einen sicher verschlüsselt sein. Zum anderen dürfen nur legitimierte Personen und Systeme auf die Daten zugreifen können (Authentifizierung). Ich habe Anhaltspunkte dafür gefunden, dass beide Mechanismen unzureichend in der Überwachungssoftware implementiert wurden und der Schlüssel für Dritte leicht zu finden war.

Eine genaue technische Analyse war mir allerdings nicht möglich. Der Quellcode der eingesetzten Software war nicht dokumentiert. Das Bundeskriminalamt hat sich noch bemüht, auf den Hersteller der Software einzuwirken, um mir den Quellcode zur Verfügung zu stellen. Dieser hat jedoch von meinen Mitarbeitern verlangt, eine Verschwiegenheitserklärung zu unterschreiben. Zudem verlangte der Hersteller einen erheblichen Geldbetrag für seinen Personaleinsatz. Beides habe ich abgelehnt. Meine Prüfkompetenz kann nur durch Gesetz eingeschränkt werden. Eine vertragliche Geheimhaltungsvereinbarung würde zudem meine gesetzlichen Berichtspflichten beeinträchtigen, zum Beispiel gegenüber dem Deutschen Bundestag. Der Hersteller der Software ist weder mein Vertragspartner noch unterliegt er meiner datenschutzrechtlichen Kontrolle. Kann der Quellcode nicht von der geprüften Behörde für Zwecke der Datenschutzkontrolle zur Verfügung gestellt werden, endet meine datenschutzrechtliche Kontrollmöglichkeit.

Ich habe mir bei der Kontrolle neben dem technischen System auch die erlangten Informationen genau angesehen. Aus den eingesehenen Unterlagen und Dateien ergaben sich keine Anhaltspunkte dafür, die Behörden hätten mit der eingesetzten Software über die laufende Telekommunikation hinaus Daten erhoben oder die Nutzer weitergehend überwacht. Insbesondere fand ich keine Bildschirmfotos, Nutzerdateien oder dergleichen.

Rechtlich konnte ich die Maßnahmen nur begrenzt prüfen. Soweit die Behörden Maßnahmen im Auftrag von Staatsanwaltschaften der Länder durchführten, war ich nur insoweit kontrollbefugt, als die Bundesbehörden einen eigenen Entscheidungsspielraum hatten. Die notwendigen richterlichen Beschlüsse konnten mir vorgelegt werden. Wie sich aus diesen ergab, waren die Maßnahmen zulässig. Den Inhalt der Beschlüsse bewerte ich aus Respekt vor der richterlichen Unabhängigkeit nicht. In rechtspolitischer Hinsicht sehe ich im Bereich strafrechtlicher Ermittlungen aber keine Rechtsgrundlage für diese Maßnahmen. Die entsprechende Vorschrift der Strafprozessordnung sieht nicht vor, dass Computer heimlich mit einer Software infiltriert werden. Entsprechend gilt dies für die Vorschriften im Zollbereich.

Die gesetzlichen Bestimmungen beziehen sich nur auf die herkömmliche Form der Telekommunikationsüberwachung, bei der die Telekommunikationsanbieter die Gespräche auf Anordnung der Sicherheitsbehörden ausleiten. Auf die mit der Quellen-Telekommunikationsüberwachung verbundenen zusätzlichen Risiken hat das Bundesverfassungsgericht in seiner Entscheidung zur sog. Onlinedurchsuchung ausdrücklich hingewiesen und besondere gesetzliche Regelungen für derartige besonders

eingriffsintensive Maßnahmen gefordert. Eine entsprechende Befugnisnorm für die Onlinedurchsuchung und die Quellen-TKÜ hat der Bundesgesetzgeber bislang aber nur für das Bundeskriminalamt geschaffen, soweit es im Bereich des internationalen Terrorismus tätig wird, nicht aber in der für die Strafverfolgung einschlägigen StPO. Daraus ergibt sich die eigenartige Situation, dass die Befugnisse des BKA bei der Gefahrenabwehr weiter gehen als diejenigen für die Strafverfolgung.

Für unzureichend halte ich auch die technischen Löschungsmechanismen, soweit Inhalte aus dem Kernbereich privater Lebensgestaltung betroffen sind. Diese betreffen den intimsten Bereich höchstpersönlicher Kommunikation (z. B. Gespräche mit engsten Vertrauten über innere seelische Vorgänge). Derartige Inhalte habe ich in den Dateien des Bundeskriminalamts vorgefunden. Deren Löschung durfte ich nicht beurteilen, weil dies der Staatsanwaltschaft des betreffenden Landes vorbehalten war. Den zuständigen Landesbeauftragten für den Datenschutz habe ich informiert. Der Löschungsmechanismus selbst war aber vom Bundeskriminalamt zu verantworten. Danach konnte nur das gesamte Gespräch gelöscht werden, nicht jedoch gezielt der entsprechende kernbereichsrelevante Teil.

Das BMF hat meinen Bericht konstruktiv aufgenommen. Das BMI hat zu dem Bericht ebenfalls Stellung genommen, es teilt aber meine rechtlichen Bedenken nicht. Es sieht allerdings ebenfalls Verbesserungsmöglichkeiten bei der Software.

Bund und Länder arbeiten zurzeit an einer standardisierten Leistungsbeschreibung. Diese soll Eckpunkte festlegen und gelten, wenn Sicherheitsbehörden eine neue Software für Überwachungszwecke beschaffen oder selbst programmieren. Ich habe zu den bisher vorliegenden Entwürfen gegenüber dem BMI Stellung genommen. Darin halte ich insbesondere an meiner Position fest, dass der Quellcode den Datenschutzbehörden künftig bedingungsfrei zur Verfügung stehen muss, um die datenschutzrechtliche Kontrolle ausüben zu können. Darüber hinaus sollte die Funktionalität der Software klar geregelt sein. Dies gilt insbesondere für die Frage, was unter den Begriff der laufenden Telekommunikation fällt und was nicht.

Kasten zu Nr. 7.4.1

Bei dieser Maßnahme installieren die Ermittlungsbehörden heimlich eine Software auf dem Computer der Zielperson. Kommuniziert diese mit Hilfe des betroffenen Computers, werden die entsprechenden Daten an die Ermittlungsbehörden ausgeleitet. Dies betrifft beispielsweise verschlüsselt übertragene Gespräche, für die die Zielperson die IP-Telefoniesoftware „Skype“ benutzt. Die Maßnahme muss sich auf die laufende Telekommunikation beschränken. Die von der Polizeibehörde eingesetzte Software darf also nicht sonstige Inhalte des Computers, z. B. gespeicherte Texte, Bilder oder andere Dateien an die Polizeibehörde übertragen. Dadurch unterscheidet sich die Quellen-Telekommunikationsüberwachung von der sog. Onlinedurchsuchung.

7.4.2 Vorfeldmaßnahmen zur Terrorismusbekämpfung

Die neu geschaffenen Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus hat das Bundeskriminalamt bereits eingesetzt, allerdings nur in wenigen Verfahren.

Zum 1. Januar 2009 hat der Gesetzgeber dem Bundeskriminalamt (BKA) neue Aufgaben und Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus eingeräumt (§ 4a sowie §§ 20a bis 20t BKAG). Ich habe beim BKA angefragt, ob und ggf. in welchem Umfang dort bereits von diesen Befugnissen Gebrauch gemacht wird.

Das BKA hat mir mitgeteilt, dass bislang nur in wenigen Verfahren die neuen Befugnisse ausgeübt wurden. Dabei handelt es sich um größere Verfahren, bei denen das BKA eine Vielzahl von Maßnahmen durchgeführt hat, von denen es einen Teil niederschwellig ansieht. Dies gilt insb. für die in der Generalklausel zur Datenerhebung, Befragung, Identitätsfeststellung, Durchsuchung von Personen oder Sachen (§§ 20a bis 20f BKAG) vorgesehenen Befugnisse. Hierzu liegen keine statistischen Daten vor. Für Maßnahmen nach § 20g bis 20n BKAG hat das BKA mir konkrete Zahlen genannt. Besondere Mittel der Datenerhebung (z. B. längerfristige Observation, Abhören des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen) hat das BKA lediglich im zweistelligen Bereich eingesetzt, eine etwas höhere Anzahl gab es im Bereich der Telekommunikationsüberwachungsmaßnahmen und Verkehrsdatenabfragen. Außerdem hat es drei Wohnraumüberwachungen und sechs Onlinedurchsuchungen durchgeführt.

Zu den neu geschaffenen Befugnissen gehört auch die sog. Quellen-Telekommunikationsüberwachung. Dazu habe ich bereits eine erste datenschutzrechtliche Kontrolle durchgeführt (vgl. Nr. 7.4.1). Zu den übrigen Maßnahmen werde ich die Entwicklung weiter beobachten (vgl. auch Nr. 7.4.6).

7.4.3 Die Löschung erkennungsdienstlicher Daten durch das BKA

Nach heftiger Kritik hat das BKA sein Verfahren bei der Löschung erkennungsdienstlicher Daten der Länder im polizeilichen Informationssystem grundlegend überarbeitet (22. TB Nr. 16.21). Bei noch bestehenden Problemen ist eine Lösung absehbar.

Das Bundeskriminalamt (BKA) unterstützt als Zentralstelle die Polizeien der Länder bei der Verhütung und Verfolgung bestimmter Straftaten. Hierfür betreibt es mit dem polizeilichen Informationssystem (INPOL) einen elektronischen Datenverbund zwischen Bund und Ländern der auch zentrale erkennungsdienstliche Sammlungen umfasst, die sog. E-Gruppe. In diesen können die Landespolizeien z. B. Fingerabdrücke und Lichtbilder von Personen speichern. Hatte die Polizeibehörde eines Landes das Datum gelöscht, führte dies in der Vergangenheit nicht automatisch auch zur Löschung beim BKA. Der Vorgang wurde lediglich als „Besitzaufgabe“ durch

das Land angesehen. Diese Vorgehensweise hatte ich kritisiert (21. TB Nr. 5.2.4.1). Das mittlerweile geänderte Verfahren (22. TB Nr. 16.21) habe ich im Berichtszeitraum kontrolliert.

Anders als bisher speichert das Bundeskriminalamt die von den Ländern gelöschten Daten nur noch dann, wenn es über eigene Erkenntnisse verfügt. Praktisch funktioniert dies so: Geben die Länder den Besitz an ihren erkennungsdienstlichen Daten auf, wird dies in einer Liste der vom BKA zu bearbeitenden Datensätze aufgenommen. Anschließend prüft das BKA anhand der in INPOL und in den Papierkriminalakten vorhandenen Erkenntnisse in zwei Schritten, ob es die Daten zu der betreffenden Person weiter speichert oder löscht. Zunächst wird kontrolliert, ob

– eine nationale oder internationale Fahndung,

– eine Haftnotierung oder

– ein Prüfvermerk des BKA

zur jeweiligen Person vorliegen. In den verbliebenen Fällen prüft das BKA Erkenntnisse

– aus eigenen Ermittlungen sowie

– aus seiner Kontaktsstellenfunktion zu ausländischen Polizeibehörden.

Liegen keine Gründe für die weitere Speicherung vor, löscht das BKA die gesamte Kriminalakte einschließlich der erkennungsdienstlichen Daten. Andernfalls verlängert es das Aussonderungsprüfdatum. Etwa 80 Prozent der aufgelaufenen Daten hat das BKA nach Umstellung auf das neue Verfahren gelöscht.

Diese Vorgehensweise halte ich für datenschutzrechtlich zulässig, solange das BKA die von den Ländern gelöschten erkennungsdienstlichen Daten nur weiter speichert, wenn ihm eigene Erkenntnisse vorliegen, die darauf schließen lassen, dass der Betroffene künftig Straftaten begehen wird (sog. Negativprognose, § 8 Absatz 6 BKAG). Es gilt der Grundsatz: Die Stelle, die vorhandene erkennungsdienstliche Daten übernimmt, muss in jedem Einzelfall eine tragfähige rechtliche Entscheidung dafür getroffen haben.

Es bleiben noch Details zu klären. So sind in INPOL die verschiedenen Datengruppen auf unterschiedliche Weise miteinander verknüpft. Es kann passieren, dass erkennungsdienstliche Daten weiter gespeichert werden, weil ein Verbundteilnehmer noch andere Daten zu der Person gespeichert hat. Denn die erkennungsdienstlichen Daten sind technisch gesehen in die allgemeinen Prüffristen einbezogen. Hier wird darauf hinzuwirken sein, dass die Gruppe der erkennungsdienstlichen Daten ein gesondertes Aussonderungsprüfdatum erhält, also stärker „abgekoppelt“ wird. Dazu hat das BKA bereits ein Verfahren entwickelt, das sich derzeit in der Abstimmung befindet. Zudem existiert die Idee, ein besonderes Datenfeld einzuführen, mit dem die Polizeibehörden ihren Mitbesitz an den erkennungsdienstlichen Daten markieren können. Diese müssten dann den Einzelfall rechtlich prüfen und entscheiden. Ich werde das Verfahren weiter beobachten.

7.4.4 Die Zentraldatei „Politisch motivierte Kriminalität -links“ – noch viel zu tun!

Wie eine Kontrolle der Zentraldatei „Politisch motivierte Kriminalität -links“ („PMK-links-Z“) ans Licht brachte, sind viele personenbezogenen Speicherungen ohne hinreichende Rechtsgrundlage erfolgt. Einen Teil der Daten hat das Bundeskriminalamt (BKA) unmittelbar nach der Prüfung gelöscht.

Im Ergebnis hat der Beratungs- und Kontrollbesuch gezeigt, dass teilweise zu weitgehende Speicherungen in der Zentraldatei „PMK-links-Z“ erfolgt sind. Dies betraf oft Personen, die im Zusammenhang mit Versammlungen aufgefallen waren. In vielen Fällen war nicht ausreichend substantiiert dokumentiert, welche konkreten Handlungen ihnen vorgeworfen wurden und aus welchen Gründen die Speicherung erforderlich war. Für Zwecke der Gefahrenvorsorge darf das BKA gem. § 8 Absatz 2 BKAG eine Person nur speichern, wenn die die Prognose ergibt, dass sie auch zukünftig Straftaten begehen wird. Hierfür bedarf es einer ausreichenden Tatsachengrundlage.

Die Zentraldatei „PMK-links-Z“ dient dem BKA dazu, seine Aufgaben als Zentralstelle bei der Bekämpfung der politisch motivierten Kriminalität aus dem Phänomenbereich Links wahrzunehmen. Hierfür werden in der Datei Ereignisse auf einer grafischen Oberfläche mit Personen, Institutionen, Objekten und Sachen verknüpft. Daraus sollen Rückschlüsse auf Verflechtungen und Zusammenhänge gezogen werden. Personen werden entsprechend § 7 und § 8 BKAG in verschiedene Personenrollen unterteilt, dies sind u. a.:

– Beschuldigte,

– Verdächtige,

– sonstige Personen,

– Prüffälle.

In der Zentraldatei speichert das BKA sowohl eigene als auch Ländererkenntnisse, wobei ein wesentlicher Teil der Erkenntnisse von den Ländern stammt.

Bei meiner Kontrolle fiel mir auf, dass bei vielen als Beschuldigte bzw. Verdächtige gespeicherten Personen zweifelhaft ist, ob diese überhaupt an einer strafbaren Handlung beteiligt waren. Dies betrifft oft Fälle, in denen die Betroffenen Teil einer größeren Menschenmenge waren und nicht näher einer bestimmten Tätergruppe zugeordnet werden konnten. In solchen Fällen müssen jedoch tatsächliche Anhaltspunkte vorliegen, aus denen sich ergibt, weshalb eine festgestellte Person zum Täterkreis gehört bzw. ein entsprechender Verdacht hinsichtlich einer konkreten Straftat begründet werden kann. Grund für den unzureichenden Personenbezug war häufig auch die Form der Sachverhaltsdarstellung durch die Landespolizeien.

Im Zusammenhang mit der Speicherung von Veranstaltungsteilnehmern ist besonders auf die Verhältnismäßigkeit achten, wie das Bundesverfassungsgericht in einer aktuellen Entscheidung festgestellt hat (– 1 BvR 388/05 –), genießen auch Sitzblockaden grundsätzlich den Schutz der durch Artikel 8 des GG garantierte Versammlungsfreiheit. Bei der Anwendung des Nötigungsparagraphen ist

nach Auffassung des Gerichts in solchen Fällen eine äußerst differenzierte Betrachtung geboten (§ 240 Strafgesetzbuch). Ich sehe mich daher in meiner Einschätzung zur Zentraldatei „IgaSt“ bestätigt, wonach auch provokante Formen des Protests grundgesetzlich geschützt sind und daher die Teilnehmer nicht ohne Weiteres gespeichert werden dürfen (23. TB Nr. 7.2.2).

Ich habe auch festgestellt, dass Anmelder von Versammlungen als. „sonstige Personen“ in der Zentraldatei gespeichert waren. Bei „sonstigen Personen“ müssen bestimmte Tatsachen die Annahme rechtfertigen, dass sie in Zukunft Straftaten von erheblicher Bedeutung begehen werden (§ 8 Absatz 5 BKAG). In keinem der von mir geprüften Fälle lagen jedoch solche Tatsachen vor. Selbst Anmelder von Versammlungen, die in der Vergangenheit friedlich verliefen, wurden gespeichert. Ich habe das BKA auf Grund des gravierenden Verstoßes gegen datenschutzrechtliche Vorschriften unmittelbar nach der Kontrolle um sofortige Überprüfung der Speicherungen gebeten. Das BKA teilte mir daraufhin mit, die betreffenden Dateien seien in der Zwischenzeit nahezu vollständig gelöscht worden.

In der Zentraldatei werden auch sog. Prüffälle erfasst. Das BKA beruft sich hierbei auf die Generalklausel des § 7 Absatz 1 BKAG. Hierbei handelt es sich aber nur um eine Auffangvorschrift, mit deren Hilfe nicht die besonderen Vorschriften für die Speicherung zur Gefahrenvorsorge ausgehöhlt werden (§ 8 BKAG) dürfen. Bereits in der Vergangenheit habe ich mehrfach die Speicherung als Prüffall kritisiert. Sie führt dazu, dass Personen in den Fokus von Ermittlungen geraten, die an der Begehung von Straftaten nicht beteiligt oder gegebenenfalls nur zufällig anwesend sind (vgl. 22. TB Nr. 4.2.4). Durch die Kontrolle hat sich meine kritische Haltung bestätigt. Speicherungen zur Gefahrenvorsorge nach der Auffangvorschrift § 7 Absatz 1 i. V. m. § 2 Absatz 1 BKAG sind nur tolerabel, wenn die Personen nur für kurze Zeit erfasst werden. Dies darf lediglich geschehen, um die Voraussetzungen des § 8 Absatz 2 bzw. Absatz 5 BKAG prüfen zu können, etwa wenn das BKA zunächst ergänzende Informationen bei anderen Polizeibehörden einholen muss.

Um die o. g. Fehler zukünftig zu vermeiden kommt der Errichtungsanordnung der Zentraldatei eine wichtige Konkretisierungsfunktion zu (vgl. auch Nr. 7.4.5).

Die vom BKA festgelegten Aussonderungsprüffristen in der Zentraldatei „PMK-links-Z“ waren teils zu lang und nicht für jedes Ereignis gesondert festgelegt. Grund hierfür ist eine technische Einstellung in der Zentraldatei. Erkenntnisse, die das BKA dort speichert, werden aus dem Vorgangsbearbeitungssystem des BKA bzw. dem polizeilichen Informationssystem (INPOL) entnommen. Die Zentraldatei übernimmt aus diesen beiden Systemen auch automatisch das dort festgelegte höchste Aussonderungsprüfdatum. Daher muss in der Zentraldatei „PMK-links-Z“ zu einer Person jedes Ereignis manuell mit einem eigenen Aussonderungsprüfdatum versehen werden. Dies ist jedoch nicht durchgehend geschehen, so dass alte, nicht mehr erforderliche Daten weiterhin gespeichert blieben.

Bei meiner Kontrolle fiel mir auch auf, dass im Vorgangsbearbeitungssystem zu einer gespeicherten Person ein von ihr unabhängiges Dokument eingestellt war. Darin wurde eine Veranstaltung einer angesehenen internationalen Menschenrechtsorganisation beschrieben, obwohl keine Straftaten oder sonstige Störungen der öffentlichen Sicherheit registriert worden sind. Sogar der Anmelder der Veranstaltung war namentlich erkennbar. Ich habe mir die Frage gestellt, aus welchem Grund die Landespolizei die Informationen an das BKA übermittelt hat und den zuständigen Landesbeauftragten für den Datenschutz informiert.

Schließlich müssen auch Gerichtsentscheidungen, wie z. B. ein Freispruch, im Sinne von § 8 Absatz 3 BKAG, zur Löschung aus der Datei führen. Institutionen, die vom BKA Daten erhalten haben, sind hierüber zu informieren. Problematisch ist allerdings, dass das BKA oftmals selbst keine Information von den Staatsanwaltschaften der Länder über den Ausgang von Verfahren (insb. Entscheidungen über die Einstellung von Verfahren, Urteile) erhält. Es kann daher diese Informationen auch nicht an andere Behörden kommunizieren. Hier sehe ich vor allem die Staatsanwaltschaften und Polizeien der Länder in der Pflicht, durch bessere Kommunikation mit dem BKA die Rechte der Betroffenen zu stärken. Aus meiner Sicht könnte hier zudem gesetzgeberischer Handlungsbedarf bestehen. Schon das Bundesverwaltungsgericht hat bei seiner Entscheidung über die Datei „Gewalttäter Sport“ auf Defizite in diesem Bereich hingewiesen.

Ich habe mir nach der Kontrolle verschiedene Beanstandungen vorbehalten. Das BKA hat bis zum Redaktionsschluss noch nicht abschließend zu meinem Kontrollbericht Stellung genommen. Ich werde die dargestellten Sachverhalte weiter im Auge behalten.

7.4.5 Weiterentwicklung der polizeilichen Dateienlandschaft

Das polizeiliche Informationssystem (INPOL) wird stetig weiterentwickelt. Grundlegend wird der derzeit noch geplante polizeiliche Informations- und Analyseverbund (PIAV) die Dateienlandschaft verändern.

Mit dem Polizeilichen Informations- und Analyseverbund (PIAV) soll neben INPOL (vgl. Kasten zu Nr. 7.4.5) ein weiteres, eigenständiges Verbundsystem geschaffen werden. Ich mahne hier zur Vorsicht. Ein solcher umfassender Verbund birgt die Gefahr, die gegenwärtigen rechtlichen Grenzen zu überschreiten. Diese Grenzen sind auch von verfassungsrechtlicher Bedeutung. Wie das geplante System genau ausgestaltet werden wird, ist derzeit noch nicht abschließend geklärt. Aus den bislang vorliegenden Planungen ergibt sich jedoch: Das System wird einen sehr großen Datenbestand enthalten. Angedacht sind zudem umfassende Auswerte- und Analysemöglichkeiten. Diese sind jedoch bis zum Redaktionsschluss nur unscharf beschrieben. Folgende Eckpunkte sind aus Datenschutzsicht besonders wichtig:

– Das Verhältnis zwischen dem zentralen Verbundsystem INPOL und PIAV ist grundlegend klärungsbedürftig. Durch den parallelen Betrieb zweier Verbundsysteme besteht die Gefahr einer Doppelspeicherung mit voneinander abweichenden Daten und Fristen.

– PIAV dient nach meiner ersten Einschätzung vor allem der Gefahrenvorsorge bzw. der vorbeugenden Bekämpfung von Straftaten und darf die dafür geltenden besonderen Schwellen für die Speicherung nicht unterlaufen. Diese Schwellen sind im Bundeskriminalamtgesetz festgelegt. Die Speicherung der Daten von Beschuldigten und Tatverdächtigen setzt danach eine täter- bzw. tatbezogene Einzelprognose voraus (sog. Negativprognose). Die Daten sind erforderlich, wenn wegen der Art oder Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind. Stets muss eine hinreichende Tatsachengrundlage vorliegen, um eine derartige Negativprognose vorzunehmen. Für Kontakt- und Begleitpersonen, Zeugen, Opfer und sonstige Personen legt das Gesetz engere Grenzen fest.

– Der Umfang der zu speichernden Daten ist ebenfalls klärungsbedürftig. Die Rechtsverordnung über die Arten von Daten, die das BKA als Zentralstelle speichern darf, sieht entsprechende Grenzen vor (vgl. 23. TB Nr. 7.2.1). Dies schließt größtenteils aus, Volltextdokumente zur Gefahrenvorsorge in zentrale Verbunddateien zu übernehmen. Besonders kritisch sehe ich es, wenn die Recherche- und Analysefunktionen die Suche in Dateianhängen umfassen (vgl. dazu auch die Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, abgedruckt in: 23. TB Kasten zu Nr. 7.5.1).

Ich habe das Bundeskriminalamt um Stellungnahme gebeten. Diese lag bis Redaktionsschluss noch nicht vor.

Die Speicherung sog. personengebundener Hinweise (PHW) im INPOL-Verbund beschäftigt die Datenschutzbeauftragten des Bundes und der Länder schon seit langem. Die PHW dienen der Eigensicherung, teilweise aber auch dem Schutz der Betroffenen. Polizeibeamte sollen zum Beispiel rechtzeitig gewarnt werden, wenn eine Person als bewaffnet bekannt oder freitodgefährdet ist. Hierbei handelt es sich oft um sensible personenbezogene Daten. Sie können sich u. a. auf Krankheiten beziehen (z. B. „Ansteckungsgefahr“). Die Datenschutzbeauftragten haben immer wieder darauf gedrängt, klare Kriterien zu schaffen. Diese müssen festlegen, welche PHW die Polizeibehörden geben dürfen, und klar bestimmen, unter welchen Voraussetzungen dies geschehen darf. Das Bundeskriminalamt hat in Zusammenarbeit mit den Ländern nun einen Leitfaden erarbeitet. Dieser legt die Speicherkriterien nun ausführlicher fest. Vergibt eine Polizeibehörde einen PHW, muss sie die Gründe dafür dokumentieren. Ich hätte mir allerdings gewünscht, dass auch klare Kriterien für eigenständige Laufzeiten der PHW festgelegt worden wären. Dies ist nicht der Fall, obwohl INPOL richtigerweise ein eigenes Feld für das Aussonderungsprüfdatum von PHW enthält. Aktuell ist eine weitere Entwicklung geplant. Neben den Hinweisen zur Eigensicherung sind sog. ermittlungsrelevante Hinweise (EHW) vorgesehen. Dies werde ich beobachten. Insbesondere wird der Zweck dieser Hinweise und deren Abgrenzung zu den PHW zu klären sein.

Bei den Errichtungsanordnungen des Bundeskriminalamts fällt auf, dass diese zu einzelnen Punkten oft nur den Gesetzeswortlaut wiedergeben. Damit beschreiben sie nach meiner Auffassung vor allem den Kreis der zu speichernden Personen nur unzureichend. Die Errichtungsanordnung soll gerade dazu dienen, das Gesetz zu konkretisieren. Der Bearbeiter muss klar entscheiden können, ob er eine Person in der jeweiligen Datei speichern darf oder nicht.

Mit dem Bundesministerium des Innern und dem Bundeskriminalamt konnte eine Verfahrensweise gefunden werden, mit der die Arbeitsgruppe INPOL der Datenschutzbeauftragten des Bundes und der Länder bei der Weiterentwicklung der polizeilichen Verbundsysteme beteiligt wird. Das begrüße ich sehr.

Kasten zu Nr. 7.4.5

INPOL

Das polizeiliche Informationssystem INPOL ist ein elektronischer Datenverbund zwischen Bund und Ländern. Das Bundeskriminalamt ist die Zentralstelle dieses Verbundes.

INPOL besteht aus verschiedenen Dateien. Zu den wichtigsten zählen: der Kriminalaktennachweis – KAN, die Personenfahndung, die Sachfahndung, die Haftdatei, der Erkennungsdienst, die DNA-Analyse-Datei.

An dem Informationssystem sind neben dem Bundeskriminalamt und den Landeskriminalämtern sonstige Polizeibehörden der Länder, die Bundespolizei sowie die mit der Wahrnehmung grenzpolizeilicher Aufgaben betrauten Behörden der Zollverwaltung und das ZKA mit dem Recht beteiligt, Daten in das System im automatisierten Verfahren einzugeben und daraus abzurufen.

In INPOL werden polizeilich relevante Angaben über Straftäter, Beschuldigte, Verdächtige, potenzielle Straftäter, aber auch von Kontakt- und Begleitpersonen, Zeugen, Hinweisgebern, Opfern und vermissten Personen gespeichert.

7.4.6 Funkzellenabfragen

Auch beim BKA sind Daten von Funkzellenabfragen gespeichert.

Beim Bundeskriminalamt (BKA) habe ich nachgefragt, in welchem Umfang es Funkzellenabfragen (vgl. Kasten zu Nr. 7.4.6; Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juli 2011) durchgeführt und in welchem Umfang es Daten aus solchen Maßnahmen gespeichert hat. Es hat mir sehr ausführlich geantwortet, weshalb ich eine ursprünglich geplante datenschutzrechtliche Kontrolle zunächst verschoben habe. Gleichzeitig hat mich das Bundeskriminalamt um datenschutzrechtliche Beratung in Bezug auf die Speicherung

von Daten aus Funkzellenabfragen in verschiedenen Dateien gebeten, die es im Laufe aktueller Ermittlungen in einem Großverfahren angelegt hat. Diese Beratung dauert noch an. Das BKA speichert Daten aus Funkzellenabfragen u. a. in verschiedenen Amtsdateien, die dazu dienen, einzelne Ermittlungsverfahren zu bearbeiten. Einige dieser Dateien enthalten eine größere Menge von Verkehrsdaten, die zum Großteil bereits von Landespolizeibehörden erhoben worden sind, bevor das BKA die Ermittlungen übernommen hat. Diese Daten werden erst nach Abschluss des jeweiligen Ermittlungsverfahrens gelöscht. Dies ist regelmäßig erst nach einem rechtskräftigen Urteil oder einer endgültigen Einstellung der Fall. Das BKA weist darauf hin, dass dies für das jeweilige Verfahren von der zuständigen Staatsanwaltschaft zu entscheiden ist.

Der Sächsische Datenschutzbeauftragte hatte mich im Rahmen seiner Ermittlungen zur Funkzellenabfrage gebeten, einige Informationen zu den übermittelten Daten bei den Netzbetreibern abzufragen. Das Ergebnis fiel wie erwartet aus: Nur bei Telekommunikationsvorgängen werden Daten erfasst und werden nur die Verkehrsdaten ohne Bestandsdaten übermittelt. Insofern war ich sehr überrascht, als mich mein sächsischer Kollege kurz darauf darüber informierte, dass ein Mobilfunknetzbetreiber 2009 auch in erheblichem Umfang Bestandsdaten bei den Funkzellenanfragen übermittelt hätte. Auf meine Rückfrage bestätigte das Unternehmen dies. Erst bei der Umsetzung der Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung 2010 seien durch eine Verfahrensänderung keine Bestandsdaten mehr bei Verkehrsdatenabfragen übermittelt worden. Erstaunlicherweise konnte das Unternehmen nicht klären, seit wann die Bestandsdaten unaufgefordert mit übermittelt worden sind. Zumindest seit 2005 wäre dies so praktiziert worden. Ich habe deshalb gegen das Unternehmen eine formale Beanstandung gegenüber der Bundesnetzagentur ausgesprochen.

Kasten zu Nr. 7.4.6

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juli 2011

Funkzellenabfrage muss eingeschränkt werden!

Die Strafverfolgungsbehörden in Dresden haben mit einer sog. Funkzellenabfrage anlässlich von Versammlungen und dagegen gerichteter Demonstrationen am 19. Februar 2011 Hunderttausende von Verkehrsdaten von Mobilfunkverbindungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmerinnen und Versammlungsteilnehmer, darunter Abgeordnete von Landtagen und des Deutschen Bundestages, Rechtsanwältinnen und Rechtsanwälte, sowie Journalistinnen und Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohnerinnen und Anwohner der dicht besiedelten Dresdener Innenstadt, in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden.

Dieser Vorfall verdeutlicht die Schwäche der gesetzlichen Regelung.

Rechtsgrundlage der nichtindividualisierten Funkzellenabfrage ist bisher § 100g Absatz 2 S. 2 StPO, wonach im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation ausreichend sein soll, um Verkehrsdaten bei den Telekommunikationsdiensteanbietern erheben zu dürfen. Diese Aussage wird mit einer allgemeinen Subsidiaritätsklausel verknüpft. Diese 2001 in die Strafprozessordnung eingefügte Regelung ist unzureichend, da sie weder hinreichend bestimmt ist noch den heutigen technischen Gegebenheiten entspricht. Aktuelle Geräte erzeugen durch ihren Datenverkehr ohne aktives Zutun des Besitzers eine Vielzahl von Verkehrsdaten, die später in einer Funkzellenabfrage erhoben werden können.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis (Artikel 10 GG). Sie richtet sich unterschiedslos gegen alle in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur – wie etwa eine Telekommunikationsüberwachung nach § 100a StPO – gegen bestimmte einzelne Tatverdächtige. Sie offenbart Art und Umstände der Kommunikation von u. U. Zehntausenden von Menschen, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben. Sie schafft damit des Weiteren die Möglichkeit, diese Personen rechtswidrig wegen Nicht-Anlasstaten, etwa Verstößen gegen das Versammlungsgesetz, zu verfolgen. Sie ist bezogen auf einzelne Personen ein Instrument der Verdachtsgenerierung. Die Strafprozessordnung regelt nicht näher, wie die Behörden mit den erhobenen Daten umzugehen haben, insbesondere nicht, über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiter verwendet werden dürfen.

Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt. Verkehrsdaten können das soziale Netz des Betroffenen widerspiegeln; allein aus ihnen kann die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen deutlich werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Bundesgesetzgeber auf, den Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken (etwa durch die Pflicht zur unverzüglichen Reduzierung der erhobenen Daten auf das zur Strafverfolgung oder gerichtlichen Auseinandersetzung Erforderliche) sowie die Löschungsvorschrift des § 101 Absatz 8 StPO zu präzisieren.

7.4.7 Öffentlichkeitsfahndung im Internet

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit der Öffentlichkeitsfahndung im Internet, insbesondere in sozialen Netzwerken beschäftigt. Auch das Bundeskriminalamt betreibt eine Fahndungsseite bei „Facebook“.

Zahlreiche Behörden von Bund und Ländern betreiben eigene Websites, einige haben eine „Fanpage“ bei Facebook (vgl. Nr. 5.8.2.). Für Diskussionen sorgten dabei besonders Polizeibehörden, die das soziale Netzwerk zu Fahndungsausschreibungen einsetzen. Die Öffentlichkeitsfahndung greift besonders intensiv in die Persönlichkeitsrechte der Betroffenen ein. Im Internet werden Informationen weltweit einem unbeschränkten Empfängerkreis bekannt gegeben. Nach derzeitigem Stand ist ein „Rückholen“ der im Internet verbreiteten Informationen unmöglich. Daher ist eine Öffentlichkeitsfahndung im Internet stets Ultima Ratio. Sie kommt nur bei besonders schwerwiegenden Delikten in Betracht. Besonders kritisch wäre es, wenn im Internet nicht nur nach Verdächtigen sondern auch nach Zeugen gefahndet würde. Die dort veröffentlichten Informationen sind stets auf das Notwendigste zu beschränken. Äußerst bedenklich ist auch, wenn Hinweise aus der Bevölkerung im Internetauftritt der Ermittlungsbehörde öffentlich einsehbar sind (z. B. in Foren, Chats, sozialen Netzwerken o. Ä.). Werden auf diese Weise Verdachtsmomente veröffentlicht, belastet dies den Betroffenen stets in unangemessener Weise, insbesondere, wenn sich später seine Unschuld herausstellt.

Das BKA betreibt eine Fanseite bei „Facebook“. Es zeigt dabei aber große Zurückhaltung, denn bislang hat es diese Seite nur in dem Ermittlungsverfahren gegen Mitglieder des „Nationalsozialistischen Untergrunds (NSU)“ genutzt. Dabei geht es um besonders schwerwiegende Delikte. Bei Facebook-Fahndungen sind jedoch nicht nur die besonderen strafprozessualen Anforderungen zu beachten. Vor allem ist zu fragen, wie mit den Daten derjenigen umgegangen wird, die das Angebot aufrufen (Nutzerdaten). Das BKA hat Maßnahmen getroffen, um die datenschutzrechtlichen negativen Auswirkungen zu begrenzen. Deaktiviert sind Pinnwand- und Teilenfunktion in den Fahndungsaufrufen und das Senden von Nachrichten. Zu den eigentlichen Fahndungen verlinkt die Facebook-Seite auf die Website des BKA, enthält also nicht selbst die Fahndungsinformation. Dadurch werden zwar die Daten der Besucher minimiert. Allerdings kann so nicht verhindert werden, dass Cookies gesetzt und über den „Gefälltmir“-Knopf IP-Adressen an Facebook übertragen werden. Auch ungefragt wird die Nutzungsanalyse mit Hilfe von „Facebook Insights“ durchgeführt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat gegenüber der Innenministerkonferenz und der Justizministerkonferenz in einem Schreiben auf wesentliche Eckpunkte hingewiesen:

– Die Polizeibehörden müssen vorrangig prüfen, ob sie eigene Internetseiten schalten können, bevor sie soziale Netzwerke in Anspruch nehmen.
– Falls sie dies nicht für ausreichend erachten, müssen sie einen Betreiber auswählen, der deutsches Datenschutzrecht einhält.
– Die jeweilige Polizeibehörde bzw. Staatsanwaltschaft muss ihre datenschutzrechtliche Verantwortung wahrnehmen können (Herrin des Verfahrens). Dies gilt sowohl für die Erstveröffentlichung des Fahndungsaufrufs als auch für die weitere Behandlung (z. B. Löschung). Es muss vollständig erkennbar sein, welche Daten der Anbieter des Netzwerks verarbeitet.

7.4.8 Darf das BKA bei datenschutzrechtlichen Auskunftsersuchen Ausweiskopien verlangen?

Das Bundeskriminalamt verlangt für Auskünfte an die Betroffenen eine beglaubigte Ausweiskopie. Dies ist nicht zu beanstanden.

Jeder Bürger hat einen Auskunftsanspruch über zu seiner Person beim Bundeskriminalamt (BKA) gespeicherte Daten. Das BKA verlangt hierfür eine beglaubigte Kopie des Personalausweises oder Reisepasses der Betroffenen. Es lässt auch eine polizeilich bestätigte Kopie der o. g. Ausweise als Nachweis gelten. Diesen Nachweis erhalten Betroffene bei ihrer örtlichen Polizeidienststelle. Dort können Betroffene zu den täglichen Bürozeiten von ihren o. g. Ausweisdokumenten eine Kopie und das Original vorlegen und sich ihre Identität auf der Kopie von der Polizei bestätigen lassen. Nur die Polizeidienststellen in Berlin vergeben diesen Nachweis nicht. Da das Bundeskriminalamt nicht alle Merkmale des Ausweises zur Identifizierung benötigt, können die Seriennummer und das Passbild geschwärzt werden. Ich habe dieses Verfahren akzeptiert, da es dem Nachweis der Identität von Betroffenen und der Vermeidung von Verwechslungen dient. Dadurch soll auch vermieden werden, dass sensible Daten unter Umständen an Personen versandt werden, die zu deren Empfang nicht berechtigt sind. Das BKA darf diese Ausweiskopien nicht dauerhaft aufbewahren und nur zu dem Zweck verwenden, zu dem sie angefordert worden sind.

Zukünftig könnten Betroffene ggf. auch mittels der eID-Funktion des neuen Personalausweises (vgl. Nr. 8.5) gegenüber Behörden ihre Identität nachweisen; Ausweiskopien und andere Identitätsnachweise wären dann nicht mehr erforderlich. Soweit ist das BKA aber noch nicht.

7.4.9 Forschungsdaten

Das Bundeskriminalamt möchte Fingerabdruckdaten für ein Forschungsprojekt weitergeben und hat mich um datenschutzrechtliche Beratung gebeten.

Bevor das Bundeskriminalamt (BKA) Fingerabdruckdaten für Forschungszwecke weitergab, hat es sich mit mir in Verbindung gesetzt. Gemeinsam konnten wir eine datenschutzgerechte Lösung finden.

Fingerabdruckdaten sind personenbezogene Daten. Dies gilt auch dann, wenn sie nicht mit weiteren, identifizierenden Daten verbunden sind (z. B. Personennamen). Denn

Fingerabdruckdaten dienen schon für sich genommen der Identifizierung einer Person. Sie sind – im wahrsten Sinne des Wortes – nicht von der Person trennbar. Daher muss das BKA datenschutzrechtliche Anforderungen auch dann beachten, wenn es reine Fingerabdruckdaten weitergibt, ohne sonstige Angaben.

Nach den Vorschriften des Bundeskriminalamtgesetzes (BKAG) kann das Amt personenbezogene Daten für Forschungszwecke übermitteln (§ 29 BKAG). Diese setzt insbesondere voraus, dass das Forschungsinteresse das schutzwürdige Interesse der Betroffenen erheblich überwiegt. Bei dieser Abwägung war zu berücksichtigen, dass sich das BKA nach Diskussion mit mir für die Forschungsarbeit ein besonderes Verfahren überlegt hatte. Die Daten sollen den Forschern nämlich nur innerhalb der Räume des BKA zur Verfügung gestellt werden. Auf Rechnern, die das BKA bereitgestellt hat und die von Technikern des BKA kontrolliert werden, können die Forscher die Daten auswerten. Nur die abstrakten Forschungsergebnisse ohne Personenbezug werden den Forschern am Ende übergeben. Damit trägt das Verfahren den schutzwürdigen Interessen der Betroffenen sehr weitgehend Rechnung, denn die Risiken für sie werden minimiert. Auf diese Weise kann das Forschungsvorhaben datenschutzkonform durchgeführt werden.

7.5 Zoll

7.5.1 Beschäftigtenscreenings bei der AEO-Zertifizierung der Zollverwaltung

Das von den Zollverwaltungen häufig ohne konkreten Anlass angeordnete Beschäftigtenscreening bei der sog. AEO-Zertifizierung (AEO – Authorised Economic Operator = zugelassener Wirtschaftsbeteiligter) erweist sich weiterhin als problematisch. Auch eine aktuelle Entscheidung des Bundesfinanzhofs (BFH) räumt diese Bedenken nicht aus.

Die AEO-Zertifizierung soll die Zollabfertigung erleichtern. Betroffen sind in der Europäischen Union ansässige, im grenzüberschreitenden Warenverkehr tätige Unternehmen. Ein AEO-Zertifikat „Zollrechtliche Vereinfachungen/Sicherheit“ (das sog. AEO-F-Zertifikat) kann jedem in der Europäischen Union niedergelassenen Wirtschaftsbeteiligten auf Antrag erteilt werden, der die Kriterien zur Einhaltung der Zollvorschriften – angemessene Führung seiner Geschäftsbücher, Zahlungsfähigkeit und angemessene Sicherheitsstandards – erfüllt.

Im Rahmen der AEO-Zertifizierung verlangen die Zollverwaltungen von den Unternehmen umfangreiche Beschäftigtenscreenings, teilweise sogar wiederholt und in sehr kurzen Abständen, was ich bereits mehrfach kritisiert habe (vgl. z. B. 23. TB Nr. 13.7). Dabei werden die Bediensteten des antragstellenden Wirtschaftsbeteiligten einer Sicherheitsüberprüfung durch Abgleich mit den sog. Antiterrorlisten unterzogen. Der Abgleich erfolgt anhand der in den EG-Antiterrorverordnungen (Verordnungen [EG] Nummer 2580/2001 und Nummer 881/2002) genannten Sanktionslisten (Namenslisten von Personen, die im Verdacht stehen, Mitglied einer terroristischen Vereinigung zu sein). Die den EG-Verordnungen zu Grunde liegenden UN-Terrorlisten sind aber aus rechtsstaatlicher Perspektive bedenklich, da ihr Zustandekommen intransparent ist und die Listung nur eingeschränkt gerichtlich überprüft werden kann (vgl. EuGH, Urteile vom 15. November 2012, Rs. C-539/10; C-550/10 P; C-417/11 P). Wegen dieser Fehleranfälligkeit und den gravierenden Folgen, die bei einem Treffer für den Betroffenen eintreten können, sind verfahrensrechtliche Sicherungen in Form von datenschutzrechtlichen Betroffenenrechten unerlässlich.

Im Frühjahr 2011 habe ich die Praxis eines Hauptzollamtes (HZA) bei der Erteilung des o. g. AEO-F-Zertifikats geprüft und beanstandet. Dort wurde das Zertifikat nur bewilligt, wenn die antragstellenden Unternehmen den Nachweis über einen regelmäßigen systematischen Abgleich aller Beschäftigten mit den sog. EG-Antiterrorlisten erbracht hatten. Mit dieser Praxis hatte das HZA gegen Nr. 253 der Dienstanweisung „Zugelassener Wirtschaftsbeteiligter – AEO“ vom 22. Juni 2010 verstoßen, mit der die Überprüfung auf Beschäftigte in sicherheitsrelevanten Bereichen begrenzt wird, und damit zugleich den Grundsatz der Verhältnismäßigkeit verletzt. Nach Mitteilung seiner Aufsichtsbehörde, des Bundesministeriums der Finanzen, hat die geprüfte Behörde den Fehler inzwischen eingeräumt und behoben.

Mit dem Beschluss vom 22./23. November 2011 setzt sich auch das Koordinierungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (Düsseldorfer Kreis) für eine wirksame Begrenzung des Beschäftigtenscreenings ein und fordert Datenscreenings in Unternehmen nicht pauschal und anlasslos durchzuführen (vgl. Kasten zu Nr. 7.5.1).

Inzwischen liegt mit dem Urteil des BFH (Urteil vom 19. Juni 2012, VII R 43/11) die erste höchstrichterliche Klärung einiger Streitpunkte zum Thema Beschäftigtenscreening vor, die gleichwohl aus datenschutzrechtlicher Perspektive nicht überzeugt. Denn der BFH kommt in seiner Entscheidung zu dem Ergebnis, der datenschutzrechtliche Erlaubnistatbestand des § 32 Absatz 1 Satz 1 BDSG ermögliche es, einen Abgleich der personenbezogenen Daten der Bediensteten des Arbeitgebers, der sich um ein AEO-Zertifikat bemüht, mit den Antiterrorlisten durchzuführen. Zwar hat der BFH das Screening auf Beschäftigte begrenzt, die im sicherheitsrelevanten Bereich eingesetzt werden oder werden sollen. Dennoch wird dadurch meine Kritik an den von Zollverwaltungen ohne konkreten Anlass angeordneten pauschalen, massenhaften Beschäftigtenscreenings nicht ausgeräumt, denn es bestehen bereits grundlegende Zweifel an dem Verfahren. So halte ich es für fragwürdig, ob die unternehmensinternen Abgleiche angesichts der unbaren Gehaltszahlungen einen zusätzlichen Beitrag zur Terrorbekämpfung leisten können, obgleich schon die Banken nach § 25c Kreditwesengesetz Abgleiche ihrer Kundendaten mit den Antiterrorlisten vornehmen. Schließlich mangelt es für diesen Massendatenabgleich an einer tragfähigen Rechtsgrundlage. Weder die EG-Antiterrorverordnungen noch die einschlägigen UN-Beschlüsse enthalten entsprechende Verpflichtungen. Auch erscheint eine Anwendung der Generalklausel des § 32 BDSG hier nicht tragfähig.

Kasten zu Nr. 7.5.1

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

(Düsseldorfer Kreis am 22./23. November 2011)

Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen

Der Düsseldorfer Kreis hat sich bereits mehrfach mit dem Problem des Mitarbeiterscreenings befasst, zuletzt durch Beschluss vom 23./24.April 2009. Es gibt Anlass, die Problematik erneut aufzugreifen.

In den letzten Jahren ist insbesondere die Zollverwaltung im Rahmen der Bewilligung des zollrechtlichen Status eines „zugelassenen Wirtschaftsbeteiligten“ (AEO-Zertifizierungen) dazu übergegangen, von den Unternehmen umfangreiche Screenings von Mitarbeitern – und gegebenenfalls Daten Dritter – zu verlangen. Diese Screenings werden zum Teil in Abständen von wenigen Wochen ohne konkreten Anlass und undifferenziert durchgeführt. In diesem Geschäftsfeld betätigen sich bereits spezialisierte Dienstleister, die sich die bestehende Unsicherheit bei den Unternehmen zunutze machen. Dies ist auch der Grund, warum diese Screenings immer häufiger durchgeführt werden. Nach den praktischen Erfahrungen der Aufsichtsbehörden mangelt es an klaren Regelungen, wie mit den Ergebnissen von Datenscreenings umzugehen ist (Treffermanagement). Das Bundesministerium der Finanzen hat zwar am 14. Juni 2010 anlässlich dieser Praxis einschränkende Vorgaben erlassen, diese werden jedoch von den zuständigen Zollbehörden nicht einheitlich umgesetzt.

Der Düsseldorfer Kreis hält in seinem vorgenannten Beschluss derartige Screenings nur aufgrund einer speziellen Rechtsgrundlage für zulässig. Eine solche Rechtsgrundlage fehlt.

Weder die geltenden EU-Antiterrorverordnungen noch andere Sanktionslisten erfüllen die Anforderungen an eine solche spezielle Rechtsgrundlage. Diese Verordnungen enthalten lediglich die allgemeine Handlungspflicht, den in den Anlagen genannten Personen und Institutionen keine rechtlichen Vorteile zu gewähren, verpflichten jedoch nicht zu Screenings von Mitarbeitern, Kunden oder Lieferanten.

Auch die Bundesregierung ist der Auffassung, dass die Terrorismusverordnungen keinen systematischen, anlassunabhängigen Abgleich von Mitarbeiterdateien mit den Sanktionslisten verlangen. Allenfalls nach Maßgabe von Sorgfaltspflichten und differenzierend nach verschiedenen Verkehrskreisen und Risikolagen seien solche Abgleiche zulässig. Es bleibe den Unternehmen überlassen, wie sie die Einhaltung der Terrorismusverordnungen sicherstellen (Bundestagsdrucksache 17/4136 vom 3. Dezember 2010).

Vor diesem Hintergrund empfiehlt und fordert der Düsseldorfer Kreis:

- Unternehmen sollten Datenscreenings nicht pauschal und anlasslos durchführen. Da die Lohnzahlung nur unbar erfolgt, die Kreditinstitute nach § 25c Kreditwesengesetz (KWG) ohnehin Abgleiche mit den Terrorlisten vornehmen, ist ein Datenabgleichverfahren innerhalb des Unternehmens mit Mitarbeiterdaten nicht geboten.
- Die Zollbehörden werden aufgefordert, die rechtsstaatlichen Vorgaben im Rahmen der AEO-Zertifizierung zu beachten. Eine einheitliche Praxis nach diesen Vorgaben gibt den Unternehmen Rechtssicherheit.
- Die Bundesregierung wird gebeten, die derzeitige AEO-Zertifizierungspraxis einer baldigen und umfassenden Evaluation zu unterziehen.

7.5.2 Das IT-Verfahren „PARIS“ – Eine Risikoanalyse

Das IT-Verfahren „PARIS“ (Pre-Arrival Risk Analysis) des Zollfahndungsdienstes steckt noch in den Kinderschuhen. Es stellt in der derzeitigen Fassung kein Risiko für den Datenschutz dar.

Nicht erst seit den vereitelten „Paketbomben-Anschlägen“ aus dem Jemen im Jahr 2010 bemühen sich Sicherheitsbehörden darum, den stetig wachsenden Strom an Fracht, der die Europäische Union (EU) passiert, genauestens zu kontrollieren. Seit dem 19. März 2012 nutzt der Zollfahndungsdienst hierfür nun ein neues Sicherheitsinstrument: das IT-Verfahren „PARIS“. Es dient der Risikoeinschätzung von Warenbewegungen, unter Berücksichtigung der daran beteiligten Personen sowie Organisationen und wird bei allen Einfuhren aus Drittstaaten in die EU angewendet.

Bestimmte Waren, die aus Drittstaaten in die EU unmittelbar nach oder über Deutschland transportiert werden, müssen beim Zoll angemeldet werden (Artikel 36a Zollkodex). Die hierfür in einem elektronischen Formular eingegebenen Daten werden an „PARIS“ übermittelt. „PARIS“ führt automatisiert anhand von europaweit einheitlich festgelegten Prüfkriterien eine Risikoeinschätzung dazu durch, ob von der versandten Ware oder den daran beteiligten Personen oder Unternehmen eine Gefahr ausgeht.

Die personenbezogenen Daten werden nicht in „PARIS“ selbst automatisiert geprüft, sondern an das IT-Verfahren

„ADA“ (Automatisierter Datenabgleich) übermittelt. Dort werden sie mit verschiedenen Bestandsdatenbanken abgeglichen. Gibt es bei der automatisierten Prüfung von Waren, Organisationen oder personenbezogenen Daten einen Treffer, wird dieser durch Mitarbeiter des Zollfahndungsdienstes in einem zweiten Schritt nochmals manuell untersucht. So soll sichergestellt werden, dass nicht bereits ein Treffer im automatisierten Verfahren eine Kontrollmaßnahme auslöst. Erst wenn die Risikoprüfung durch den Mitarbeiter des Zollfahndungsdienstes Anhaltspunkte für eine tatsächliche Gefahr ergibt, übermittelt dieser eine Kontrollempfehlung an den vor Ort zuständigen Zollmitarbeiter.

Bei meiner Prüfung habe ich festgestellt, dass dieses Verfahren bei der automatisierten Prüfung viele Treffer anzeigt, welche sich dann bei der manuellen Prüfung aber als „falscher Alarm“ herausstellen.

Die Entwicklung von „PARIS“ ist noch nicht abgeschlossen. Beabsichtigt sind sowohl die Vernetzung mit anderen Sicherheitsbehörden als auch den umfassenden Abgleich mit den Datenbanken des Zollfahndungsdienstes. Die Eingriffsintensität des neuen Verfahrens halte ich in seiner gegenwärtigen Form für moderat: Speicherungen zu geringfügigen zollrechtlichen Delikten können keinen Treffer erzeugen. In „PARIS“ werden keine Risikoprofile zu den an der Einfuhr beteiligten Personen erstellt. Zudem werden – jedenfalls bislang – keine personenbezogenen Daten anderer Sicherheitsbehörden in die Risikoeinschätzung einbezogen. Ich werde „PARIS“ weiterhin – insbesondere im Hinblick auf die geplanten Funktionserweiterungen – kritisch beobachten.

7.6 Bundespolizei

7.6.1 Elektronische Kriminalakte bei der Bundespolizei

Bereits in meinem letzten Tätigkeitsbericht (23. TB Nr. 7.3.3) habe ich darüber berichtet, dass die Bundespolizei zukünftig ihre Kriminalakten weitgehend von der Papierform in die elektronische Form überführen wird. Dabei stellen sich einige wichtige datenschutzrechtliche Fragen.

Dass Behörden von der papiermäßigen Akten- und Karteiführung zu elektronischen Systemen wechseln, ist an und für sich nichts ungewöhnliches (vgl. Nr. 3.2.1). Insbesondere bei Systemen, in denen in großem Umfang höchst sensible Daten gespeichert werden, stellen sich mit der Umstellung nicht immer einfach lösbare datenschutzrechtliche Fragen.

Ein solcher Fall ist die „elektronische Kriminalakte“ (eKA). Die Kriminalakte ist eine personenbezogene kriminalpolizeiliche Sammlung bei der Bundespolizei, die wesentliche Erkenntnisse zu bestimmten natürlichen Personen enthält. Im zweiten Halbjahr 2013 will die Bundespolizei die bisher in Papierform geführten Kriminalakten größtenteils in die elektronische Form überführen. Dies ist mit datenschutzrechtlichen Risiken verbunden.

Die in der“eKA“ gespeicherten Daten überschneiden sich inhaltlich zum Teil mit den Daten in der Datei „Bundespolizeiaktennachweis“ (BAN). Mir ist bewusst, dass beide Dateien unterschiedliche Zwecke verfolgen und eine Überschneidung der jeweils gespeicherten Daten unvermeidbar ist. Dennoch sollte bei der weiteren Einführung der „eKA“ die Doppelspeicherung von Daten so gering wie möglich gehalten werden. Dies reduziert auch den Arbeitsaufwand der Bundespolizei.

Bundespolizisten können auf Daten der „eKA“ leichter zugreifen als dies bisher bei der (Papier-)Kriminalakte möglich war. Alle Nutzer des Vorgangsbearbeitungssystems der Bundespolizei „@rtus-Bund“ können die in der „eKA“ enthaltenen Daten einsehen, ohne dass es – wie bisher – eines Ersuchens um Übersendung der (Papier-) Kriminalakte bedarf. Hierdurch besteht die Gefahr einer unverhältnismäßigen Ausweitung von Zugriffsrechten. Als Schutzmaßnahme ist deshalb vorgesehen, dass die Bundespolizisten vor dem Zugriff auf die „eKA“ die Notwendigkeit der Nutzung begründen müssen. Alle Zugriffe werden zudem protokolliert. Eine stichprobenartige Kontrolle durch den behördlichen Datenschutzbeauftragten des Bundespolizeipräsidiums ist vorgesehen, der u. a. für diese Aufgabe mit zusätzlichem Personal ausgestattet worden ist. Ob durch dieses Konzept der Zugriff auf die „eKA“ tatsächlich auf das erforderliche Maß reduziert wird, muss der praktische Betrieb zeigen.

In der „eKA“ sollen auch detaillierte Informationen zur Persönlichkeit der Betroffenen gespeichert werden. Hier deutet sich etwas Neues an. Denn während herkömmliche Dateien zur Gefahrenvorsorge zwar auch „personengebundene Hinweise“ und Angaben über Beziehungen zu anderen Personen enthalten, scheint es der Bundespolizei nunmehr gerade auf eine verstärkte Beschreibung der Persönlichkeit des Betroffenen anzukommen, die bei Erfassung in der „eKA“ grundsätzlich allen Nutzern von @rtus-Bund zugänglich sind. Gegen diese Form der Persönlichkeitsbeschreibung habe ich erhebliche Bedenken. Als Rechtsgrundlage für die Speicherung solcher Daten kommt m. E. nur § 29 Absatz 2 Satz 3 Nummer 2 Bundespolizeigesetz (BPolG) in Betracht. Danach ist die Speicherung von weiteren personenbezogenen Daten u. a. zulässig, soweit dies erforderlich ist, z. B. weil wegen der Persönlichkeit des Betroffenen Grund für die Annahme weiterer Strafverfahren besteht. Die Bundespolizei ist danach zumindest verpflichtet, die Angaben zur Persönlichkeit des Betroffenen in der „eKA“ auf das erforderliche Maß zu begrenzen. Eine von mir geforderte entsprechende Anweisung an alle Nutzer der „eKA“ hat die Bundespolizei bereits formuliert.

Außerdem ist sicherzustellen, dass der Beurteilung Tatsachen und nicht Vermutungen zugrunde liegen. Inwieweit die Mitarbeiter der Bundespolizei die Dokumentation dieser Tatsachen auch bei unübersichtlichen Situationen sicherstellen können, wird sich zeigen. Ggf. ist hierfür eine entsprechende Schulung notwendig.

Wie mir bei meiner Prüfung auffiel, plante die Bundespolizei, in die „eKA“ auch gefährdete Personen aufzunehmen, darunter Hilflose, Vermisste und Suizidgefähr-

dete. Zudem sollten „Personen, die in die Verarbeitung ihrer Daten eingewilligt haben (insbesondere Geschädigte und Zeugen für zukünftige Strafverfahren) sowie personenbezogene Daten der Angehörigen von Dienststellen“ in der „eKA“ gespeichert werden. Hierfür sehe ich keine hinreichende Rechtsgrundlage, denn gerade bei derartigen, für hoheitliche Zwecke geführten Datensammlungen scheidet die Einwilligung als Rechtsgrundlage weitgehend aus. Zudem sind im Kriminalaktennachweis (KAN) und im BAN solche Personenkategorien nicht vorgesehen. Auf einen entsprechenden Hinweis hin hat mir die Bundespolizei zugesagt, diese Personenkategorien nicht in der „eKA“ zu speichern.

Bei der Löschung von Daten aus der „eKA“ halten sich die Aussonderungsprüffristen zwar im gesetzlichen Rahmen und sehen eine gewisse Abstufung angesichts der Schwere der Tat vor. Sie gehen allerdings über die im BAN vorgesehene regelmäßige Speicherdauer erheblich hinaus. Dies ist für mich nicht nachvollziehbar. Ich halte insofern eine Verkürzung der Aussonderungsprüffristen für geboten; sie sollten die im BAN enthaltenen Fristen nicht übersteigen.

Positiv sehe ich das Verfahren zum Löschen von Daten aus der „eKA“. Wird zu einer natürlichen Person eine „eKA“ angelegt, wird jedes einzelne Delikt in einem gesonderten virtuellen „Merkblatt“ gespeichert. Jedes Merkblatt hat ein eigenes Aussonderungsprüfdatum und kann unabhängig von ggf. weiteren bestehenden Merkblättern gelöscht werden. Außerdem setzt die Verlängerung jedes Aussonderungsprüfdatums grundsätzlich voraus, dass neue Erkenntnisse in der Zwischenzeit hinzugekommen sind. Die Verlängerung muss immer begründet und dokumentiert werden.

Ich werde die zukünftige Entwicklung und praktische Nutzung der „eKA“ auch weiterhin kritisch begleiten.

7.6.2 Unzulässige Übermittlung personenbezogener Daten an Europol

Die Bundespolizei hat jahrelang rechtswidrig personenbezogene Daten von geschleusten Personen an das Europol-Informationssystem (EIS) übermittelt.

Das Europäische Polizeiamt „Europol“ betreibt zur Erfüllung seiner Aufgaben verschiedene Informationsverarbeitungssysteme (vgl. Nr. 2.2.2). Eines davon ist das Europol-Informationssystem (EIS). Dort dürfen nur solche Personen gespeichert werden, die verdächtig oder verurteilt sind oder bei denen faktische Anhaltspunkte für die zukünftige Begehung einer Straftat vorliegen, die in den Zuständigkeitsbereich von Europol fallen muss (Artikel 12 Absatz 1 i. V. m. Artikel 4 des Europol-Beschlusses (2009/371/JI)).

Wie meine bei der Bundespolizei durchgeführte Kontrolle gezeigt hat, lagen den an Europol übermittelten Daten ausschließlich Fälle von „Schleusungsdelikten“ zugrunde. Dabei hat die Bundespolizei in sämtlichen (überprüften) Sachverhalten nicht nur die der Schleusung verdächtigen Personen, sondern ganz überwiegend geschleuste Personen im EIS ausgeschrieben. Dies ist mit dem Europol-Beschluss nicht vereinbar. Ursache dieses Fehlers war das seinerzeit genutzte wenig flexible technische Verfahren, das es nur ermöglichte, entweder alle Personendaten eines relevanten Sachverhalts an Europol zu übermitteln oder gar keine. Der Bundespolizei hätte dieser Fehler bereits vor Jahren auffallen müssen, da ich sie seit 2007 immer wieder auf unzulässige Ausschreibungen im EIS hingewiesen hatte. Passiert war jedoch nichts.

Bei meiner Kontrolle musste ich zudem feststellen, dass auch die besondere Vorschrift zur Löschung von Daten im Europol-Beschluss keine Anwendung in der Praxis findet. Danach sind die Daten des Betroffenen zu löschen, wenn das Verfahren gegen ihn endgültig eingestellt oder er rechtskräftig freigesprochen wird (Artikel 12 Absatz 5 des Europol-Beschlusses). Eine Löschung erfolgte jedoch nicht, obwohl die Bundespolizei nach eigener Aussage in der Regel eine Mitteilung der Staatsanwaltschaft über den Ausgang des Verfahrens erhält. Auch hier musste Abhilfe geschaffen und die Anwendung spezieller Löschvorschriften gem. § 12 Absatz 5 Europol-Beschluss in allen Bundespolizeidirektionen sichergestellt werden.

Die Bundespolizei hat auf meine Kontrolle unmittelbar reagiert. Alle neuen Ausschreibungen im EIS sind sofort gestoppt worden. Außerdem wurden alle bisher an das EIS übermittelten Datensätze gelöscht. Zwischenzeitlich wurde das System angepasst, so dass es nun möglich ist, nur die zulässigen Personendaten an das EIS zu übermitteln. Alte wie neue Personendatensätze werden nun daraufhin überprüft, ob ihre Übermittlung an das EIS zulässig ist. Die Bundespolizei hat zudem sichergestellt, dass die Daten eines Betroffenen im EIS nun gelöscht werden, wenn das Verfahren gegen ihn endgültig eingestellt oder der Betroffene rechtskräftig freigesprochen wird.

Ich begrüße die sofortige und umfassende Reaktion der Bundespolizei auf meine Feststellungen. Dies hat mich auch dazu bewogen, von einer Beanstandung nach § 25 Absatz 2 BDSG abzusehen. Dennoch hätte insbesondere der technische Mangel des Systems deutlich früher aufgedeckt werden müssen. Dies hätte nicht nur Eingriffe in die Rechte der Betroffenen verhindert. Auch die Bundespolizei hätte sich einigen Ärger und Aufwand erspart.

7.7 Nachrichtendienste

7.7.1 „Need to Share“ für die Sicherheitsbehörden – „Need to Know“ im Datenschutz?

Der Paradigmenwechsel von „Need to Know“ zu „Need to Share“ und die damit verbundenen neuen Mechanismen des Datenaustauschs bei den Sicherheitsbehörden machen entsprechende übergreifende Kontrollbefugnisse bei den Kontrollgremien erforderlich.

Die staatliche Präventionslogik, die sich in der Auseinandersetzung mit dem islamistischen Terrorismus nach den Terroranschlägen 2001 verstärkte, führte zu zahlreichen neuen Befugnissen für Polizei, Strafverfolgungsbehörden und Nachrichtendiensten (vgl. Nr. 7.1 ff). Hinter fast allen neuen Befugnissen steht die Ablösung des alten Grundsatzes „Need to Know“, durch „Need to Share“. Dabei war „Need to Know“ praktisch dasselbe wie der Erforderlichkeitsgrundsatz im Datenschutzrecht: Eine

Behörde erhält nicht mehr und nicht weniger Informationen, als zur jeweiligen Aufgabenerfüllung erforderlich sind. „Need to Share“ ist das genaue Gegenteil: Ohne konkrete Anfrage werden Informationen mit allen anderen Stellen geteilt, die vielleicht etwas damit anfangen können – Datenübermittlung auf Vorrat.

In Deutschland ist der bekannteste Ausfluss dieses Paradigmenwechsels die Anti-Terror-Datei (ATD) (vgl. Nr. 7.2) Sobald eine der an dieser Datei beteiligten Behörden eine Person in der ATD gespeichert hat, müssen alle anderen angeschlossenen Stellen Informationen, die sie zu dieser Person besitzen, dazu speichern.

Völlig unabhängig von der Bewertung, inwieweit die neuen gemeinsamen Dateien und Kooperationsplattformen mit dem Trennungsgebot von Nachrichtendiensten und Polizei vereinbar sind: An dieser Stelle hat sich die Schere zwischen der Qualität des denkbaren Grundrechtseingriffs und den Möglichkeiten einer effizienten Datenschutzkontrolle weit geöffnet (zur Evaluationsnotwendigkeit vgl. Nr. 7.1.).

Zwar wurde für die gemeinsamen Dateien eine Inhalts- und Transaktionsvollprotokollierung implementiert. Außerdem hat der Deutsche Bundestag die lückenlose datenschutzrechtliche Kontrolle der Rechtsextremismusdatei gefordert, um so ein umfassendes und möglichst einheitliches und hohes Datenschutzniveau zu gewährleisten.

Die Praxis wird diesen Anforderungen jedoch nicht gerecht. Während Polizei und Nachrichtendienste, Landes- und Bundesbehörden über gemeinsame Dateien jederzeit auf die Gesamtheit der zu einem Betroffenen gespeicherten Daten zugreifen können, ist die Datenschutzkontrolle Stückwerk geblieben. Weder ich noch ein Landesbeauftragter für den Datenschutz erhalten aufgrund eigener Kompetenz einen vollständigen Überblick über Speicherung und Verwendung der Daten eines Betroffenen. Eine umfassende datenschutzrechtliche Prüfung wäre somit theoretisch nur mit erheblichem Koordinierungsaufwand aller zuständigen Datenschutzbehörden möglich und ist faktisch schon auf Grund fehlender Personalausstattung ausgeschlossen.

Darüber hinaus erfordert die Auswertung der Protokolldaten mit dem dazu vom BKA bereitgestellten Analysetool in aller Regel einen hohen technischen und zeitlichen Programmieraufwand. Für noch gravierender halte ich es, dass meine zu Datenschutzkontrollzwecken bestehende Nutzungsmöglichkeit der ATD-Protokolldaten (in der Praxis) unzulässig (weit) eingeschränkt wird, indem ich z. B. Protokolldaten, die von an der Datei beteiligten Landesbehörden generiert wurden, nicht einsehen darf. Auch bei der Prüfung der Dateien selbst wurde durch die kontrollierten Stellen die Auffassung vertreten, ich dürfe nur die Speicherungen sehen, die von den meiner Kontrolle unterfallenden (Bundes-)Behörden veranlasst wurden. Ich muss jedoch in der Lage sein, die Gesamtheit der personenbezogenen Daten zu sehen, die in den beim Bundeskriminalamt geführten Dateien zu einer Person gespeichert und verwendet werden.

Um einem Missverständnis vorzubeugen: Hier geht es nicht darum, dass ich die durch eine Landesbehörde gespeicherten Daten kontrollieren möchte. Wenn ich jedoch – sei es auf Ersuchen eines Betroffenen, sei es im Rahmen einer allgemeinen Kontrolle – eine Prüfung vornehme, kann es nicht sein, dass ich bei den Datenschutzbeauftragten aller Länder einzeln anfragen muss, ob die jeweils ihrer Kontrolle unterfallenden Stellen Speicherungen oder Abrufe vorgenommen haben, und dass ich dann die Antworten nach Art eines Puzzles zu einer Gesamtschau zusammenfügen muss.

Wenn dem Grundsatz „Need to Share“ die Erkenntnis zu Grunde liegt, nur die Gesamtschau aller zu einer Person vorhandenen Daten mache eine werthaltige Einschätzung eventueller Gefahren möglich, dann muss dies auch für den Datenschutz gelten. Die ansonsten unvermeidlichen datenschutzrechtlichen Kontrolldefizite dürfen nicht hingenommen werden und führen im Ergebnis zu einem verfassungswidrigen Zustand.

7.7.2 Vom Unterschied zwischen Kontrolle und Kenntnisnahme …

Mehrere Kontrollgremien führen faktisch zu kontrollfreien Räumen.

Die Kontrolle, ob Daten nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10), rechtmäßig erhoben und verwendet werden, unterliegt ausschließlich der G 10-Kommission des Deutschen Bundestages. Das darf aber nicht bedeuten, dass mir die Einsichtnahme in diese Daten verwehrt wird, wenn sie zur Beurteilung der Rechtmäßigkeit nachgelagerter Eingriffe in das informationelle Selbstbestimmungsrecht des Betroffenen erforderlich ist.

Nicht nur bei der Kontrolle gemeinsamer Datenbestände von Bund und Land bin ich im Berichtszeitraum an Grenzen gestoßen, die im Ergebnis kontrollfreie Räume markieren. Derzeit existieren drei unabhängige Kontrollorgane: Die G 10-Kommission, das Parlamentarische Kontrollgremium und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Nach dem Gesetz existieren keine kontrollfreien Räume – aber faktisch sieht die Sache anders aus.

So unterfallen gem. § 24 Absatz 2 Satz 3 BDSG personenbezogene Daten, die der Kontrolle durch die G 10-Kommission des Deutschen Bundestages unterliegen, nicht meiner Prüfung.

Diese Vorschrift des BDSG wird nun aber seitens der meiner Datenschutzaufsicht unterliegenden Stellen so interpretiert, dass mir nicht nur die Kontrolle, sondern darüber hinaus die Einsicht in Daten, die nach Artikel 10-Gesetz erhoben wurden, verwehrt wird. Personenbezogene Daten dürfen mit nachrichtendienstlichen Mitteln oder besonderen Befugnissen, wie Sie im Rahmen der Anti-Terror-Gesetzgebung neu für die Nachrichtendienste des Bundes geschaffen wurden, nur erhoben werden, wenn bestimmte Voraussetzungen vorliegen. Auch die weitere Verwendung personenbezogener Daten (z. B. die Speicherung in der Anti-Terror-Datei) ist nur dann datenschutzrechtlich nicht zu beanstanden, wenn gesetzlich vorgeschriebene Bedingungen erfüllt sind.

Sobald mir ein Nachrichtendienst bei einer Kontrolle erklärt, das Vorliegen legitimierender Voraussetzungen sei durch Informationen belegt, die im Rahmen einer G 10-Maßnahme gewonnen worden seien, werden mir diese Informationen vorenthalten. In der Praxis führt das dazu, dass ich die Gesetzmäßigkeit von Maßnahmen nach dem Bundesverfassungsschutzgesetz, die meiner ausschließlichen Kontrolle unterliegen, überhaupt nicht mehr prüfen kann.

Eine entsprechende Untersuchung kann aber auch nicht durch die G 10-Kommission erfolgen. Nach § 15 Absatz 5 Satz 2 Artikel 10-Gesetz erstreckt sich deren Kontrollbefugnis nur auf die Erhebung, Verarbeitung und Nutzung der nach dem Artikel 10-Gesetz erlangten personenbezogenen Daten durch Nachrichtendienste des Bundes. Aus diesen Erkenntnissen resultierende Maßnahmen nach Bundesverfassungsschutzgesetz darf die G 10-Kommission nicht beurteilen.

Die vorgenannte Problematik besteht in allen Bereichen, in denen G 10-Erkenntnisse (teilweise) Grundlage von nachrichtendienstlichem oder polizeilichem Handeln sind und mir die Überprüfung der Rechtmäßigkeit dieser Maßnahmen gesetzlich zugewiesen ist.

Eine gesetzliche Klarstellung ist erforderlich: Die G 10-Kommission des Deutschen Bundestages muss zur Beurteilung, ob eine Maßnahme zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses nach dem Artikel 10-Gesetz rechtmäßig ist, personenbezogene Daten sehen, die nach den spezialgesetzlichen Befugnissen der Nachrichtendienste oder mit polizeilichen Mitteln erhoben wurden. Ebenso muss ich solche G 10-Informationen sehen, die zur Legitimation der durch mich zu prüfenden Maßnahmen herangezogen wurden (vgl. hierzu auch Nr. 7.7.6). Nur so lassen sich die aufgetretenen Kontrolllücken schließen.

7.7.3 Eine Akte ist eine Akte ist eine Akte?

Handelt es sich bei einer elektronischen Akte um eine Datei oder eine Akte im herkömmlichen Sinne? An diese Frage knüpfen sich insbesondere bei den Nachrichtendiensten Rechtsfolgen für Speicherung und Löschung personenbezogener Daten.

Die Einführung elektronischer Aktensysteme wirft datenschutzrechtliche Fragen auf, die dringend beantwortet werden müssen (vgl. Nr. 3.2.1, 7.6.1). Dazu gehört auch die Unterscheidung zwischen „Akte“ und „Datei“. Nach dem Bundesdatenschutzgesetz erscheint die Angelegenheit recht einfach: Wird in besonderen Rechtsvorschriften des Bundes der Begriff Datei verwendet, ist dies entweder eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht automatisierte Datei). Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können. (§ 46 BDSG).

Wozu gehört also die elektronische Akte? Nach der Begriffsbestimmung des BDSG ist entscheidend, wie die elektronische Aktenführung erfolgt und was mit der elektronischen Akte gemacht werden kann. Lässt sie sich durch ein automatisiertes Verfahren umordnen und auswerten, handelt es sich um eine Datei. Damit hat der Gesetzgeber der Eingriffstiefe und dem erhöhten Missbrauchspotential Rechnung getragen, die mit der Verarbeitung personenbezogenen Daten in Dateien verbunden sind.

Deshalb dürfen die Nachrichtendienste nur einen Bruchteil der Daten, die sie in Akten sammeln dürfen, auch in Dateien speichern (vgl. Kasten zu Nr. 7.7.3). Automatisierte Dateien standen ursprünglich überhaupt nicht in Konkurrenz zu Akten, die in Papierform geführt wurden. Die technische Entwicklung, die auch zur Einführung der elektronischen Akte geführt hat, hat diese Differenzierung aufgehoben.

Gleichwohl vertreten Bundesamt für Verfassungsschutz (BfV) und Bundesministerium des Innern (BMI) bis heute die Auffassung, dass die elektronischen Akten den Regelungen für herkömmliche Akten unterfallen, insbesondere was die Speicherung und Löschung personenbezogener Daten angeht. Ich habe bereits unmittelbar nach der Einführung der elektronischen Akte im BfV (vgl. 20. TB Nr. 5.5.2; 19. TB Nr. 5.5.2; 18. TB Nr. 14.1) gefordert sicherzustellen, dass eine elektronische Recherche nur zu solchen Personen erfolgen kann, deren Daten nach geltendem Recht automatisiert gespeichert werden dürfen. Daraufhin wurde die Recherchebefugnis im BfV entsprechend geregelt. Das bedeutet, die Mitarbeiter dürfen unabhängig von den technischen Möglichkeiten die elektronische Akte nur nach solchen Personen auswerten, die nach dem Gesetz in Dateien gespeichert werden dürfen.

Eine derartige rechtliche Beschränkung genügt, insb. vor dem Hintergrund einer zunehmenden Automatisierung sämtlicher Verwaltungsprozesse, nicht den datenschutzrechtlichen Erfordernissen. Die Definition des § 46 BDSG stellt eindeutig darauf ab, ob eine automatisierte Auswertung möglich ist – ob sie gleichwohl durch eine (untergesetzliche) Regelung verboten ist, ist unerheblich.

Ich erlaube mir an dieser Stelle einen Vergleich: Niemand darf ohne entsprechende waffenrechtliche Genehmigung eine Schusswaffe besitzen – auch nicht, wenn er glaubhaft macht, dass er sie lediglich als Knüppel benutzt! Wenn eine elektronische Akte unter die datenschutzrechtliche Privilegierung der herkömmlichen Akte in Papierform fallen soll, ist daher technisch sicherzustellen, dass eine Auswertung durch automatisierte Verfahren allenfalls für solche personenbezogenen Daten möglich ist, die nach den gesetzlichen Befugnissen in Dateien gespeichert werden dürfen.

Der Militärische Abschirmdienst hat mit seiner elektronischen Akte im Sicherheitsüberprüfungsverfahren einen brauchbaren Ansatz entwickelt, nach dem er die enthaltenen Dokumente in einem weder recherchierbaren noch bearbeitbaren Format statisch stellt. Hierdurch könnten im Bereich der Nachrichtendienste sowohl der Grundsatz der Aktenwahrheit und -klarheit, als auch der Datenschutz gewährleistet werden.

Kasten zu Nr. 7.7.3

Bundesverfassungsschutzgesetz

§ 12 Berichtigung, Löschung und Sperrung personenbezogener Daten in Dateien

(1) Das Bundesamt für Verfassungsschutz hat die in Dateien gespeicherten personenbezogenen Daten zu berichtigen, wenn sie unrichtig sind.

(2) Das Bundesamt für Verfassungsschutz hat die in Dateien gespeicherten personenbezogenen Daten zu löschen, wenn ihre Speicherung unzulässig war oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Die Löschung unterbleibt, wenn Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden. In diesem Falle sind die Daten zu sperren. Sie dürfen nur noch mit Einwilligung des Betroffenen übermittelt werden.

(3) Das Bundesamt für Verfassungsschutz prüft bei der Einzelfallbearbeitung und nach festgesetzten Fristen, spätestens nach fünf Jahren, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind. Gespeicherte personenbezogene Daten über Bestrebungen nach § 3 Absatz 1 Nummer 1, 3 und 4 sind spätestens zehn Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen, es sei denn, der Behördenleiter oder sein Vertreter trifft im Einzelfall ausnahmsweise eine andere Entscheidung.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§ 13 Berichtigung und Sperrung personenbezogener Daten in Akten

(1) Stellt das Bundesamt für Verfassungsschutz fest, dass in Akten gespeicherte personenbezogene Daten unrichtig sind oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(2) Das Bundesamt für Verfassungsschutz hat personenbezogene Daten zu sperren, wenn es im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für seine künftige Aufgabenerfüllung nicht mehr erforderlich sind. Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr genutzt oder übermittelt werden. Eine Aufhebung der Sperrung ist möglich, wenn ihre Voraussetzungen nachträglich entfallen.

7.7.4 Technischer Fortschritt und strategische Fernmeldeüberwachung

Auch inländische Telekommunikation wird über Server im Ausland geleitet. Was bedeutet dies für die strategische Fernmeldeüberwachung des Bundesnachrichtendienstes (BND)?

Im Jahr 2001 wurde das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) geändert. Seitdem darf der BND auch internationale Telekommunikationsbeziehungen, d. h. Telefonate, E-Mails, SMS etc., überwachen, die von Deutschland ins Ausland und umgekehrt leitungsgebunden, d. h. via Kabel, gebündelt übertragen werden. Erforderlich hierfür ist die Anordnung einer sog. strategischen Beschränkung im Sinne des § 5 Absatz 1 G 10 (vgl. Kasten zu Nr. 7.7.4). Vor dieser Gesetzesänderung durfte der BND nur internationale nicht leitungsgebundene Telekommunikation (Satellitenverkehre, Richtfunkverkehre) erfassen. Mit der Änderung wollte der Gesetzgeber der gewandelten Telekommunikationstechnik Rechnung tragen. Es war nicht beabsichtigt, den Umfang der bisherigen Kontrolldichte zu erweitern (vgl. Bundestagsdrucksache 14/5655 S. 17).

Bereits seit Ende der 1990er Jahre wird die internationale Telekommunikation zunehmend nicht mehr über Richtfunk bzw. Satellit, sondern über die weltumspannenden Kabelnetze digital geführt. Aufgrund der Digitalisierung können in einem Kabel gleichzeitig zehntausende Verkehre übertragen werden. Diese werden an den großen Knotenpunkten des Welt – Telekommunikationsnetzes „gebündelt“. Technisch erfolgt die Übertragung in Form der Paketvermittlung („packet switching“). Hierbei wird ein Telekommunikationsverkehr, z. B. eine E-Mail, in verschiedene kleine Datenpakete zerlegt. Die Pakete werden mit Steuerungsinformationen versehen und einzeln computergesteuert auf verschiedenen Routen übertragen. Welche Route gewählt wird, ist für den Absender nicht vorhersehbar. Die Auswahl hängt u. a. von der Auslastung der Routen bzw. den dort eingesetzten Servern ab.

Bei der strategischen Beschränkung werden an ausgewählten Übertragungswegen maximal 20 Prozent (vgl. Kasten zu Nr. 7.7.4) der dort „gebündelt“ übertragenen Telekommunikationsverkehre nach den in der jeweiligen Anordnung festgelegten Suchbegriffen maschinell durchsucht und erfasst. Anschließend werden diese Daten durch den BND weiter gefiltert und ausgewertet.

Aufgrund des technischen Fortschritts werden auch inländische Telekommunikationsverkehre, d. h. Verkehre, bei denen sich Absender und Empfänger in Deutschland aufhalten, über im Ausland befindliche Routen geleitet. Dies hat zur Folge, dass auch dieser Verkehr über Übertragungswege gebündelt übertragen werden kann, die einer strategischen Beschränkung unterliegen. Demnach könnten auch diese Verkehre nach Suchbegriffen maschinell durchsucht und erfasst werden, obgleich es sich nicht um internationale Telekommunikationsbeziehungen im Sinne des § 5 Absatz 1 G 10 handelt.

Ich habe diese Problematik mit dem BND erörtert und darauf hingewiesen, dass derartige Verkehre nach der geltenden Rechtslage nicht erfasst werden dürfen. Sollte eine Erfassung (teilweise) technisch unvermeidbar sein, muss der BND gewährleisten, dass diese personenbezogenen Daten schnellstmöglich erkannt und gelöscht werden. Der BND teilt meine rechtliche Einschätzung. Aufgrund der ausschließlichen Kontrollkompetenz der G 10-Kommission des Deutschen Bundestages ist es mir allerdings nicht möglich, zu prüfen, ob eine Erfassung derartiger Daten erfolgt ist bzw. diese schnellstmöglich gelöscht worden sind (vgl. Nr. 7.7.2).

Kasten zu Nr. 7.7.4

Artikel 10-Gesetz:

Strategische Beschränkungen

§ 5 Voraussetzungen

(1) Auf Antrag des Bundesnachrichtendienstes dürfen Beschränkungen nach § 1 für internationale Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt, angeordnet werden. Die jeweiligen Telekommunikationsbeziehungen werden von dem nach § 10 Abs. 1 zuständigen Bundesministerium mit Zustimmung des Parlamentarischen Kontrollgremiums bestimmt. Beschränkungen nach Satz 1 sind nur zulässig zur Sammlung von Informationen über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr

1. eines bewaffneten Angriffs auf die Bundesrepublik Deutschland,
2. der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland,
3. der internationalen Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen sowie des unerlaubten Außenwirtschaftsverkehrs mit Waren, Datenverarbeitungsprogrammen und Technologien in Fällen von erheblicher Bedeutung,
4. der unbefugten gewerbs- oder bandenmäßig organisierten Verbringung von Betäubungsmitteln in das Gebiet der Europäischen Union in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland,
5. der Beeinträchtigung der Geldwertstabilität im Euro-Währungsraum durch im Ausland begangene Geldfälschungen,
6. der international organisierten Geldwäsche in Fällen von erheblicher Bedeutung oder
7. des gewerbs- oder bandenmäßig organisierten Einschleusens von ausländischen Personen in das Gebiet der Europäischen Union in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland
   a) bei unmittelbarem Bezug zu den Gefahrenbereichen nach Nr. 1 bis 3 oder
   b) in Fällen, in denen eine erhebliche Anzahl geschleuster Personen betroffen ist, insbesondere wenn durch die Art der Schleusung von einer Gefahr für ihr Leib oder Leben auszugehen ist, oder
   c) in Fällen von unmittelbarer oder mittelbarer Unterstützung oder Duldung durch ausländische öffentliche Stellen rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen. In den Fällen von Satz 3 Nr. 1 dürfen Beschränkungen auch für Postverkehrsbeziehungen angeordnet werden; Satz 2 gilt entsprechend.

(2) Bei Beschränkungen von Telekommunikationsbeziehungen darf der Bundesnachrichtendienst nur Suchbegriffe verwenden, die zur Aufklärung von Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich bestimmt und geeignet sind. Es dürfen keine Suchbegriffe verwendet werden, die

1. Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen, oder
2. den Kernbereich der privaten Lebensgestaltung betreffen.

Dies gilt nicht für Telekommunikationsanschlüsse im Ausland, sofern ausgeschlossen werden kann, dass Anschlüsse, deren Inhaber oder regelmäßige Nutzer deutsche Staatsangehörige sind, gezielt erfasst werden. Die Durchführung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.

Verfahren

§ 10 Anordnung

(4) In den Fällen der §§ 5 und 8 sind die Suchbegriffe in der Anordnung zu benennen. Ferner sind das Gebiet, über das Informationen gesammelt werden sollen, und die Übertragungswege, die der Beschränkung unterliegen, zu bezeichnen. Weiterhin ist festzulegen, welcher Anteil der auf diesen Übertragungswegen zur Verfügung stehenden Übertragungskapazität überwacht werden darf. In den Fällen des § 5 darf dieser Anteil höchstens 20 vom Hundert betragen.

(5) In den Fällen der §§ 3 und 5 ist die Anordnung auf höchstens drei Monate zu befristen. Verlängerungen um jeweils nicht mehr als drei weitere Monate sind auf Antrag zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.

7.7.5 Damit wir wissen, worüber wir sprechen …

Akte oder Datei? Löschfrist oder Aussonderungsprüffrist? Löschen oder schreddern? Auch beim Datenschutz steckt der Teufel oft im Detail! Wie wichtig hier die sorgfältige Anwendung der Begriffe ist, zeigt die Berichterstattung zum „Schredder-Skandal" beim Verfassungsschutz.

Kurz nachdem die rechtsextremistische Terrorgruppe „Nationalsozialistischer Untergrund" (NSU) Anfang November 2011 aufgeflogen war, wurde der damalige Präsident des Bundesamtes für Verfassungsschutz (BfV) in der Süddeutschen Zeitung zitiert: seine Behörde könne mögliche Versäumnisse im Bereich Rechtsterrorismus nicht vollständig aufarbeiten. Der Grund dafür sei, dass personenbezogene Akten nach fünf Jahren vernichtet würden. So schreibe es das Verfassungsschutzgesetz vor – und das hätten wiederum die Politiker zu verantworten. „Es wäre schön, wenn wir noch alle Akten hätten", zitiert ihn das Blatt. Der Artikel erläutert: Nur in besonderen Fällen sei es erlaubt, Akten zehn Jahre lang aufzubewahren. Allein bei Islamismus-Verdächtigen betrüge die Frist 15 Jahre.

Dieses Zitat suggeriert fälschlich, datenschutzrechtliche Vorgaben hätten zur Vernichtung von Daten geführt hätten, die für die Arbeit des Verfassungsschutzes erforderlich gewesen wären. Zum einen handelt es sich bei der erwähnten Fünf-Jahres-Frist nicht um eine Löschfrist, sondern um eine sogenannte „Aussonderungsprüffrist". Geregelt ist diese in § 12 Absatz 3 Satz 1 Bundesverfassungsschutzgesetz (BVerfSchG). Danach hat das BfV bei der Einzelfallbearbeitung und nach festgesetzten Fristen, spätestens nach fünf Jahren, zu prüfen, ob gespeicherte personenbezogene Daten in Dateien zu berichtigen oder zu löschen sind. Es gibt also keinen datenschutzrechtlichen Automatismus, Daten nach fünf Jahren zu löschen. Wenn das BfV bei der Prüfung zu dem Ergebnis gelangt, die Daten seien für die Aufgabenerfüllung noch erforderlich, unterbleibt die Löschung.

Dies habe ich auch in meinem Gutachten ausgeführt, dass ich im Auftrag des parlamentarischen Untersuchungsausschusses zur Terrorgruppe „NSU" erstellt habe. Dort habe ich dargelegt, dass nur§ 12 Absatz 3 Satz 2 BVerfSchG Fristen zur Löschung von Daten enthält. Danach sind personenbezogene Daten in Dateien spätestens zehn Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen, es sei denn, der Behördenleiter trifft im Einzelfall ausnahmsweise eine andere Entscheidung. Das heißt: Auch diese auf Dateien bezogene Löschfrist greift nicht, sofern die Daten noch benötigt werden. Es handelt sich daher keineswegs um unbedingte Löschfristen, wie sie z. B. im Bundeszentralregistergesetz gelten.

Im übrigen beziehen sich die Aussonderungsprüf- und Löschfristen nach § 12 BVerfSchG ausschließlich auf in Dateien gespeicherte Informationen. Die Speicherung personenbezogener Daten in Akten ist in § 13 BVerfSchG geregelt. Dieser sieht weder eine Aussonderungsprüffrist noch eine Löschfrist vor.

Übrigens sorgte auch der Begriff „löschen" in der Berichterstattung hier und da für Verwirrung, ob nun gerade Akten oder Dateien gemeint sind: Das Datenschutzrecht kennt für Akten und Dateien den Begriff „löschen", während man im allgemeinen Sprachgebrauch bei Akten eher Begriffe wie „vernichten" oder „schreddern" verwendet.

Um jedwedes Missverständnis zu vermeiden: Meine Äußerungen sind kein Plädoyer für unbegrenzte Speicherungen beim Verfassungsschutz. Ich habe immer gefordert, dass personenbezogene Daten in Akten zu löschen sind, wenn die korrespondierenden Daten in der Verbunddatei der Verfassungsschutzbehörden (NADIS) gelöscht werden.

Durch unpräzise Darstellung und falsche Verwendung von Begriffen darf aber nicht der Eindruck entstehen, es gebe Gesetze, die die Löschung von Daten vorschreiben, die für die Aufgabenerfüllung des BfV noch erforderlich sind – sei es in Akten oder Dateien.

Wenn das BfV personenbezogene Daten in Dateien und/oder Akten löscht, liegt dem immer die Entscheidung zu Grunde, dass diese Daten für die Aufgabenerfüllung nicht mehr erforderlich sind. Von einem irgendwie gearteten Automatismus kann also nicht die Rede sein.

7.7.6 Reform des Verfassungsschutzes – aber wie?

Bei der Diskussion über die Konsequenzen aus dem Versagen der Sicherheitsbehörden gegen rechtsterroristische Aktivitäten geht Gründlichkeit vor Schnelligkeit. Verfassungsrechtliche Garantien dürfen nicht angetastet werden.

Die Erkenntnisse über die rechtsextremistische Terrorgruppe Nationalsozialistischer Untergrund (NSU) sind schockierend. Der Deutsche Bundestag untersucht, weshalb diese Terrorgruppe über viele Jahre unerkannt bleiben konnte und welche Folgen dies für die Sicherheitsbehörden hat. Ursachen und Fehlentwicklungen müssen gründlich ermittelt werden. Nur dann können sachgerechte Reformen erfolgen. Aktionismus ist nicht zielführend und kann Ursachen ungewollt verdecken. Erforderlich ist eine effiziente Kontrolle der Nachrichtendienste – ihr entgegenstehende praktische und gesetzliche Hindernisse müssen beseitigt werden.

Im Januar 2012 hat der Deutsche Bundestag einen Untersuchungsausschuss zur Aufklärung der „Mordserie der rechtsextremistischen Terrorgruppe „Nationalsozialistischer Untergrund (NSU)" (Bundestagsdrucksache 17/8453) eingesetzt. Dieser prüft, ob bzw. welche „Fehler oder Versäumnisse" auf Seiten der Sicherheitsbehörden vorliegen und „welche Schlussfolgerungen im Blick auf den Rechtsextremismus für die Struktur und Organisation der Sicherheits- und Ermittlungsbehörden […] gezogen werden müssen".

Für diese Untersuchungen hatte mich der Ausschuss um ein Gutachten gebeten, insbesondere zur rechtlichen Bewertung der im Bundesamt für Verfassungsschutz (BfV) durchgeführten Datenlöschungen (vgl. Nr. 7.7.5). Die Untersuchungen werden voraussichtlich bis zum Sommer 2013 andauern.

Im Dezember 2012 hat die Konferenz der Innenminister und -senatoren (IMK) des Bundes und der Länder auf-

grund der NSU-Ereignisse Beschlüsse zur Reform bzw. Neuausrichtung des Verfassungsschutzes gefasst. So soll ein verpflichtender wechselseitiger Informationsaustausch zu schnelleren und besseren Ergebnissen bei der Bekämpfung von Extremisten führen. Die Landesverfassungsschutzbehörden (LfV) müssen künftig unverzüglich alle relevanten Informationen an den Bund übermitteln. Das BfV koordiniert diesen Informationsfluss und unterrichtet seinerseits die LfV über relevante Erkenntnisse und Ergebnisse eigener Informationsauswertungen. Zudem sollen V-Leute nur noch nach bundesweit einheitlichen Standards eingesetzt und in einer zentralen Datei gespeichert werden. Auf diese Weise sollen die Verfassungsschutzbehörden untereinander wissen, wer welche V-Leute führt. Gewährleistet werden sollen auch eine umfassende parlamentarische Kontrolle sowie mehr Transparenz gegenüber der Öffentlichkeit.

Vorschläge der Fraktionen

Die Fraktionen des Deutschen Bundestages haben ebenfalls Reformvorschläge entwickelt. Von zentraler Bedeutung ist hierbei die Stärkung der parlamentarischen Kontrolle. So soll beispielsweise das Parlamentarische Kontrollgremium des Deutschen Bundestages (PKGr), das die Nachrichtendienste des Bundes umfassend kontrolliert, nach Auffassung der Fraktionen von CDU/CSU, SPD und BÜNDNIS 90/DIE GRÜNEN gestärkt werden. Die CDU/CSU-Fraktion befürwortet die Einsetzung eines Nachrichtendienstbeauftragten.

Die Fraktion BÜNDNIS 90/DIE GRÜNEN plädiert zudem für eine Stärkung der Datenschutzkontrolle als zentrales Element der Kontrolle der Nachrichtendienste. Dies begrüße ich.

Kontrollkompetenzen

Ebenso wie das PKGr kontrolliere auch ich die Nachrichtendienste des Bundes, jedoch nur, soweit diese personenbezogenen Daten erheben oder verwenden. Bedauerlicherweise musste ich den Aufsichtsbehörden und dem Deutschen Bundestag wiederholt berichten, dass ich meine Kontrollen (teilweise) nicht bzw. nicht effizient durchführen konnte. Ursachen hierfür waren geltend gemachte Quellenschutzerwägungen, der vermeintliche Schutz anderer Nachrichtengeber (z. B. ausländischer Nachrichtendienste) sowie das (teilweise) Bestreiten meiner Prüfkompetenz (vgl. 23. TB Nr. 7.1.6).

Gravierende Kontrolllücken ergeben sich in der Praxis auch aus den unterschiedlichen Kompetenzen der Kontrollorgane (G 10-Kommission des Deutschen Bundestages, PKGr und meine Behörde). So ist z. B. die G 10-Kommission allein zuständig für die Kontrolle der personenbezogenen Daten, die nach dem Artikel 10-Gesetz (G 10) erhoben worden sind. Dadurch entsteht faktisch ein kontrollfreier Raum – und zwar generell in allen Fällen, in denen G 10-Erkenntnisse (teilweise) zur Legitimierung von nachrichtendienstlichen Maßnahmen dienen und mir die Überprüfung der Rechtmäßigkeit dieser Maßnahmen gesetzlich zugewiesen ist (vgl. Nr. 7.7.2).

Lösbar ist dieses Problem durch eine gesetzliche Klarstellung in Artikel 15 Absatz 5 G 10 oder § 24 Absatz 4 Bundesdatenschutzgesetz (BDSG). Dort könnte geregelt werden, dass ich für meine Kontrollen auch G 10-Erkenntnisse einsehen darf. Die Kompetenz der G 10-Kommission bliebe unberührt. Sie wäre weiterhin allein berechtigt, die Beachtung der Vorgaben des G 10 zu prüfen.

Gemeinsames Abwehrzentrum

Bereits wenige Wochen nach Bekanntwerden der Straftaten des NSU hatte der Bundesminister des Innern am 16. Dezember 2011 als Konsequenz dieser Ereignisse das „Gemeinsame Abwehrzentrum gegen Rechtsextremismus“ (GAR) eröffnet. Dieses ist keine neue Behörde. Ebenso wie das Gemeinsame Terrorismusabwehrzentrum (GTAZ – vgl. 21. TB Nr. 5.1.4) ist es eine Informations- und Kommunikationsplattform. Dort tauschen die Experten der beteiligten Behörden zur Abwehr des Rechtsextremismus/-terrorismus bzw. der politisch motivierten Kriminalität (PMK-rechts) ihre Informationen in verschiedenen Arbeitsgruppen aus. Dabei arbeiten sie nach den für sie jeweils geltenden Aufgaben und Befugnissen. Auf diese Weise soll das Fachwissen der Behörden gebündelt und ein möglichst lückenloser und schneller Informationsfluss gewährleistet werden. Beteiligt am GAR sind auf Bundesebene das Bundeskriminalamt, das BfV, der Bundesnachrichtendienst, die Bundespolizei, der Generalbundesanwalt und der Militärische Abschirmdienst. Teilnehmer auf Landesebene sind die Landeskriminalämter sowie die LfV. Ebenfalls beteiligt ist das Europäische Polizeiamt (Europol).

Im November 2012 hat das „Gemeinsame Extremismus- und Terrorismusabwehrzentrums (GETZ)“, in dem das GAR aufgegangen ist, seine Arbeit aufgenommen. Sitz des GETZ sind die Standorte des Bundesamtes für Verfassungsschutz und Bundeskriminalamtes in Köln und Meckenheim. Die Zusammenarbeit der Sicherheitsbehörden ist dadurch weiter ausgebaut worden. Sie beschränkt sich nicht mehr auf den Bereich des Rechtsextremismus und -terrorismus. Das GETZ fungiert als eine Informations- und Kommunikationsplattform zur Abwehr aller Arten des Extremismus und Terrorismus.

Reaktion der Datenschutzbeauftragten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom November 2012 (vgl. Kasten zu Nr. 7.7.6) darauf hingewiesen, dass eine Reform der Sicherheitsbehörden nur nach einer gründlichen Aufklärung der Ursachen und Fehlentwicklungen erfolgen darf. Bei diesen Untersuchungen ist zu berücksichtigen, dass bereits weitgehende gesetzliche Pflichten und Berechtigungen für umfassende Datenübermittlungen innerhalb der Polizeien und Nachrichtendienste sowie zwischen diesen Behörden existieren. Vollzugsdefizite aufgrund fehlender Kenntnis oder Nichtbeachtung dieser Vorschriften sowie Mentalitätsprobleme bei MitarbeiterInnen der Sicherheitsbehörden können neue Gesetze oder Dateien nicht beseitigen. Hierfür bedarf es anderer Maßnahmen, insbesondere effizienter Kontrollen.

Kasten zu Nr. 7.7.6

Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. November 2012 in Frankfurt (Oder)

Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist Versuche zurück, vermeintlich „überzogene“ Datenschutzanforderungen für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen.

Sie fordert die Bundesregierung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfassungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden.

In datenschutzrechtlicher Hinsicht geklärt werden muss insbesondere, ob die bestehenden Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. In diesem Zusammenhang ist auch zu untersuchen, ob die gesetzlichen Vorgaben den verfassungsrechtlichen Anforderungen genügen, also verhältnismäßig, hinreichend klar und bestimmt sind. Nur wenn Ursachen und Fehlentwicklungen bekannt sind, können Regierungen und Gesetzgeber die richtigen Schlüsse ziehen. Gründlichkeit geht dabei vor Schnelligkeit.

Schon jetzt haben die Sicherheitsbehörden weitreichende Befugnisse zum Informationsaustausch.

Die Sicherheitsgesetze verpflichten Polizei, Nachrichtendienste und andere Behörden bereits heute zu umfassenden Datenübermittlungen. Neue Gesetze können alte Vollzugsdefizite nicht beseitigen.

Bei einer Reform der Sicherheitsbehörden sind der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten.

Eine effiziente Kontrolle schützt die Betroffenen und verhindert, dass Prozesse sich verselbständigen, Gesetze übersehen und Ressourcen zu Lasten der Sicherheit falsch eingesetzt werden. Nur so kann das Vertrauen in die Arbeit der Sicherheitsbehörden bewahrt und gegebenenfalls wieder hergestellt werden.

Datenschutz und Sicherheit sind kein Widerspruch. Sie müssen zusammenwirken im Interesse der Bürgerinnen und Bürger.

7.8 Sicherheitsüberprüfungsgesetz

7.8.1 Novelle des Sicherheitsüberprüfungsgesetzes

Bei der geplanten Änderung des Sicherheitsüberprüfungsgesetzes muss das erforderliche Datenschutzniveau im Geheim- und Sabotageschutz gewahrt bleiben.

Seit Herbst 2012 erörtert die Bundesregierung erste Entwürfe zur Reform des Sicherheitsüberprüfungsgesetzes (SÜG). An diesen internen Beratungen nehme ich teil.

Das Sicherheitsüberprüfungsverfahren stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen dar. Gleichzeitig ist es für den personellen Geheimschutz und damit für die Sicherheitsinteressen des demokratischen Rechtsstaates unverzichtbar. Ein hohes Datenschutzniveau, das auch die Akzeptanz des Verfahrens bei den Betroffenen gewährleistet, ist dabei unerlässlich. Im Zentrum meines Interesses stehen hierbei:

– Eine lückenlose und effiziente Datenschutzkontrolle der im Rahmen der Sicherheitsüberprüfung erhobenen Daten sowie ihrer Verwendung zu gewährleisten. Dies heißt auch: Bestehende Beschränkungen, die eine wirksame Kontrolle behindern, müssen aufgehoben werden (vgl. auch Nr. 7.7.6);

– keine Aufweichung der strengen Zweckbindung für im Rahmen der Sicherheitsüberprüfung erhobene personenbezogene Daten;

– die Beibehaltung restriktiver Bestimmungen, für die elektronische Verarbeitung der Sicherheits- und Sicherheitsüberprüfungsunterlagen. Insbesondere ein automatisierter Zugriff auf Volltextbestände wäre aus Sicht des Datenschutzes nicht tragbar.

Zum Zeitpunkt des Redaktionsschluss war das Gesetzgebungsverfahren noch nicht abgeschlossen.

7.8.2 „Kunst und Wissenschaft sind frei …“

Die Erforderlichkeit von Sicherheitsüberprüfungen bei Künstlern und Wissenschaftlern habe ich in zwei konkreten Fällen hinterfragt – mit unterschiedlichen Ergebnissen.

Im ersten Fall hat mich ein Künstler auf eine Ausschreibung aufmerksam gemacht: Beim Wettbewerb „Offene Kunst am Bau“ für die gemeinsame Schule von Bundesamt für Verfassungsschutz (BfV) und Bundesnachrichtendienst (BND) wurde als Voraussetzung für die Realisierung des Kunstwerkes die Durchführung einer Sicherheitsüberprüfung gem. § 8 Sicherheitsüberprüfungsgesetz (SÜG) genannt.

Auch wenn es sich dabei um die niedrigste Stufe der Sicherheitsüberprüfung (Ü1) handelt, so stellt diese Maßnahme doch bereits einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen dar. In der Sicherheitserklärung muss dieser umfangreiche Angaben machen – unter anderem wird er zu seiner finanziellen Situation befragt. Dann werden Bundeszentralregister, Bundeskriminalamt, Bundespolizei, Bundesnachrichtendienst, Militärischer Abschirmdienst, und die Landesämter für Verfassungsschutz angefragt, ob dort Informationen zu dem Betroffenen gespeichert sind. Schließlich werden Daten des Überprüften im NADIS, der Verbunddatei der Verfassungsschutzbehörden gespeichert.

Gegenüber der zuständigen Stelle, in diesem Fall das Bundesamt für Bauwesen und Raumordnung (BBR), habe ich darauf hingewiesen, dass ich diesen Eingriff für unverhältnismäßig halte. Der BND gilt zwar auf Grund des Umfanges und der Bedeutung dort anfallender Verschlusssachen durchgehend als Sicherheitsbereich. Gleichwohl kann die zuständige Stelle von der o. g. Überprüfung absehen, wenn Art oder Dauer der Tätigkeit dies zulassen. Nach meiner Auffassung wäre die Durchführung einer Sicherheitsüberprüfung bei einem Künstler, der sich für einen begrenzten Zeitraum zur Installation eines Kunstwerks in einem begrenzten räumlichen Bereich einer BND-Liegenschaft aufhalten soll, datenschutzrechtlich nicht gerechtfertigt, zumal mit dessen Begleitung bzw. Beaufsichtigung ein milderes Mittel zur Erreichung des mit der Sicherheitsüberprüfung verfolgten Zwecks zur Verfügung steht. Das BBR ist dieser Einschätzung erfreulicher Weise gefolgt.

In einem weiteren Fall sollten Historiker, die im Rahmen des Forschungsprojekts zur „Organisationsgeschichte des Bundesamtes für Verfassungsschutz 1950 bis 1975, unter besonderer Berücksichtigung der NS-Bezüge früherer Mitarbeiter in der Gründungsphase“ mit der Vergangenheitsaufarbeitung des BfV betraut wurden, nach der höchsten Überprüfungsstufe gem. § 10 SÜG (Ü3), überprüft werden. Hierbei werden die Partner der Betroffenen in die Maßnahme einbezogen und zusätzlich zu den oben genannten Dateiabfragen Referenz- und Auskunftspersonen zu den Überprüften befragt.

Ich hatte gegenüber dem Bundesministerium des Inneren (BMI) angeregt, dass das BfV als die zuständige Stelle von der Durchführung einer Ü3 absehen sollte, da ich hier eine einfache Sicherheitsüberprüfung nach § 8 SÜG (Ü1) oder eine erweiterte Sicherheitsüberprüfung ohne Sicherheitsermittlungen gem. § 9 SÜG – Ü2) für ausreichend hielt.

- Die Wissenschaftler sollten laut Ausschreibung ausschließlich Zugang zu Verschlusssachen bis zur Einstufung GEHEIM erhalten.

- Zudem soll lediglich die Organisationsgeschichte des BfV von 1950 bis 1975 erforscht werden. Die für das Projekt auszuwertenden Unterlagen wären mithin mindestens 36 Jahre alt so dass eine sorgfältige Prüfung, in welchem Umfang der ggf. zur Zeit noch bestehende VS-Grad der in Frage kommenden Unterlagen aufrechterhalten werden müsste, vorrangig durchzuführen wäre. Dies wäre auch im Hinblick auf die Verwertbarkeit der Daten im Rahmen der historischen Forschung zielführend.

Das BfV ist meiner Anregung leider nicht gefolgt. Ich werde nach Abschluss des Geschichtsprojektes prüfen, inwieweit seine Argumentation stichhaltig war.

7.9 Bundeszentralregister

7.9.1 Forschungsdaten aus dem Bundeszentralregister

Die Übermittlung von Daten zu Forschungszwecken ist im Bundeszentralregistergesetz enger geregelt worden.

Personenbezogene Daten aus dem Bundeszentralregister sind für bestimmte Forschungsvorhaben notwendig. Dies gilt etwa, wenn eine Universität die langfristige Entwicklung der Kriminalität in einem bestimmten Bereich erforschen möchte. Um etwa Rückfallhäufigkeiten zu erfassen, kommt es bisweilen dazu, dass für ein Forschungsvorhaben in längeren Abständen mehrfach Daten übermittelt werden. In solchen Fällen darf aber kein umfassender „Parallelbestand“ zum Bundeszentralregister bei einer forschenden Stelle aufgebaut werden. Der Gesetzgeber hat deshalb die entsprechende Forschungsklausel des Bundeszentralregistergesetzes (§ 42a BZRG) überarbeitet. Danach gelten höhere Anforderungen, wenn personenbezogene Daten aus diesem Register mehrfach zu derselben Person oder Personengruppe übermittelt werden sollen. Dabei bin ich zu beteiligen. Umfassende Datenübermittlungen bleiben aber problematisch. Sofern etwa umfassende Statistiken erstellt werden sollen, wäre eine statistikrechtliche Regelung notwendig.

7.9.2 Wo stelle ich meinen Antrag auf ein Führungszeugnis?

Nach § 30 Absatz 1 Bundeszentralregistergesetz (BZRG) wird jeder Person, die das 14. Lebensjahr vollendet hat, auf Antrag ein Zeugnis über den sie betreffenden Inhalt des Registers (Führungszeugnis) erteilt. Klingt einfach, ist es aber nicht immer.

Haben Sie schon einmal ein Führungszeugnis beantragt? Nach § 30 Absatz 2 BZRG ist der Antrag bei der Meldebehörde zu stellen, in deren Zuständigkeitsbereich die antragstellende Person amtlich gemeldet ist. Für die meisten Menschen ist das unproblematisch.

Allerdings haben sich auch Petenten an mich gewandt, die Schwierigkeiten hatten, ein solches Führungszeugnis zu erhalten. Dabei handelte es sich um Menschen, für die keine Meldepflicht besteht. Dies sind Mitglieder ausländischer diplomatischer Missionen oder ausländischer konsularischer Vertretungen, bzw. in Deutschland stationierte Angehörige ausländischer Streitkräfte. Auch ausländische Staatsangehörige, die sich nur vorübergehend in Deutschland aufhielten, oder Menschen ohne festen Wohnsitz hatten Probleme, ein Führungszeugnis zu beantragen. Wenn diese Personen bei den Meldebehörden an ihrem Wohn- bzw. Aufenthaltsort vorsprachen, wurden sie darauf verwiesen, den Antrag unmittelbar beim Bundesamt für Justiz (BfJ) zu stellen. Das BfJ wiederum verwies auf die Meldebehörde.

Denn beim BfJ können nur Betroffene ein Führungszeugnis beantragen, die sich tatsächlich im Ausland aufhalten. Für alle anderen ist das BfJ nicht zuständig. Wer von der Meldepflicht befreit ist, kann und muss den Antrag bei der Meldebehörde stellen, in deren Bezirk er sich gewöhnlich aufhält.

Ich habe zusammen mit den Datenschutzbeauftragten der Länder, die die Datenschutzaufsicht über die kommunalen Stellen führen, eine entsprechende Information für die Meldebehörden herausgegeben. Seitdem hat mich niemand mehr wegen dieses Problems um Unterstützung ersucht.

7.10 Geldwäschegesetz

Im Geldwäscherecht gab es eine Vielzahl von Änderungen, die aus datenschutzrechtlicher Perspektive durchaus problematisch sind.

Die Novelle 2011 des Geldwäschegesetzes (GwG)

Durch das Gesetz zur Geldwäscheprävention vom 22. Dezember 2011 (BGBl. I S. 2959) fand eine umfangreiche Novellierung des GwG statt, um vor allem die von der bei der OECD angesiedelte Financial Action Task Force on Money Laundering (FATF) festgestellten Defizite zu beseitigen. Zudem erreichten die Verdachtsanzeigen nach dem GwG im Jahr 2011 einen neuen Höchststand (12 868).

Im Wesentlichen hat die Novelle zu einer Verschärfung und Ausweitung der Sorgfalts- und Meldepflichten, des Verpflichtetenkreises, der internen Sicherungsmaßnahmen sowie einer Absenkung der Verdachtsstufen geführt. Im Zuge der Verschärfung der Sorgfaltspflichten (u. a. Identifizierungspflicht des Vertragspartners) wurden die Datenspeicherungs- bzw. Datenerhebungspflichten der nach dem GwG Verpflichteten deutlich ausgeweitet (vgl. Kasten zu Nr. 7.10). Die erheblichen Bußgeldandrohungen bei Verletzungen von Sorgfaltspflichten dürften zudem den Druck erhöhen, auch überobligatorisch Daten zu sammeln und an das Bundeskriminalamt (BKA) und andere Strafverfolgungsbehörden weiterzuleiten.

So sind die Sorgfaltspflichten (und die daran anknüpfenden Meldepflichten) nun bereits dann zu erfüllen, wenn ein Geldtransfer außerhalb einer Geschäftsbeziehung einen Betrag im Wert von 1 000 Euro oder mehr ausmacht. Auch verzichtet das GwG jetzt auf konkrete Anhaltspunkte, die auf eine Geldwäschetat oder Terrorismusfinanzierung schließen lassen; es reicht bereits das Vorliegen von Tatsachen, die auf solche Taten hindeuten. Die Verpflichteten sollen zudem darüber hinaus bei allen aus ihrer Sicht ungewöhnlichen und auffälligen Geschäftsbeziehungen mit Geldwäscherelevanz frühzeitig eine Meldung an das BKA und die zuständige Strafverfolgungsbehörde erstatten. In „Niedrigrisikofällen“ kann auch nicht mehr von der Meldung abgesehen werden, da lediglich der Umfang der Identitätsprüfung und der Überwachung reduziert werden kann.

Verstärkte Sorgfaltspflichten bei politisch exponierten Personen

Auch bei den sog. politisch exponierten Personen (PEP) greifen nach der Gesetzesnovelle verstärkte Sorgfaltspflichten ein, wobei der Anwendungsbereich erheblich ausgeweitet wurde. Bereits im Gesetzgebungsverfahren hatte ich dagegen datenschutzrechtliche Bedenken geltend gemacht. So lassen sich aus meiner Sicht diese verstärkten Sorgfaltspflichten nur für Fälle rechtfertigen, in denen tatsächlich von einem erhöhten Risiko auszugehen ist. Im Gesetzgebungsverfahren wurde meinen Forderungen nach einer grundrechtsfreundlicheren Lösung – zumindest bezogenen auf PEP, die ihr Amt im Inland ausüben – teilweise Rechnung getragen.

Äußerst kritisch sehe ich auch die in der Praxis verbreiteten „PEP-Listen“, denn diese werden von kommerziellen Anbietern zusammengestellt und veräußert. Die PEP-Listen setzen sich regelmäßig aus verschiedenen Informationen zusammen (z. B. Name, Aliasname, Geburtsdatum, Nationalität, Wohnort, Werdegang, gegenwärtige Position, familiäre und geschäftliche Beziehungen, Fotografien etc.). Bei von ausländischen Anbietern erstellten Listen ist eine Kontrolle durch europäische Datenschutzbehörden nicht möglich, so dass auch die Rechtsstaatlichkeit der Datenerfassung nicht kontrolliert werden kann. Die Auslegungs- und Anwendungshinweise des Zollkriminalamts stellen zwar fest, dass keine Verpflichtung besteht, derartige kommerzielle PEP-Listen zu benutzen. Dennoch werden die ausländischen Listen in der Praxis regelmäßig verwendet.

Änderungen im E-Geld-Geschäft

Auch für den E-Geld-Verkehr wurde der Verpflichtetenkreis erweitert und die Möglichkeiten des anonymen elektronischen Bezahlens erheblich eingeschränkt. Immerhin habe ich im Gesetzgebungsverfahren erreichen können, dass die ursprünglich vorgesehene umfangreiche Pflicht zur Identifizierung von Kunden beim Kauf von E-Geld (insbesondere Prepaid-Karten) abgemildert wurde. Da-

nach greifen die Identifikations- und besonderen Sorgfaltspflichten nur, wenn der auf einem E-Geld-Träger gespeicherte E-Geld-Betrag mehr als 100 Euro pro Kalendermonat beträgt. Bei der Ermittlung des Höchstbetrags 100 Euro bestehen indes immer noch einige Unsicherheiten, die dazu führen könnten, dass überobligatorisch personenbezogene Daten gesammelt werden. Eine Klarstellung durch die BaFin, wie in der Praxis verfahren wird, wäre sicherlich sinnvoll.

Geldwäscheprävention auch beim legalen Glückspiel

Auch die Anbieter legaler Glückspiele im Internet und die von ihnen beauftragten Kredit- und Zahlungsinstitute haben nach dem Geldwäscheergänzungsgesetz eine flächendeckende Kontrolle zu gewährleisten. Die Verschärfung von Sorgfalts- und Meldepflichten sowie der Sanktionsmechanismus nach der o. g. GwG-Novelle werden damit auf den Bereich des Glücksspiels erstreckt.

Kasten zu Nr. 7.10

§ 6 Geldwäschegesetz – Verstärkte Sorgfaltspflichten

(1) Soweit erhöhte Risiken bezüglich der Geldwäsche oder der Terrorismusfinanzierung bestehen können, haben Verpflichtete zusätzliche, dem erhöhten Risiko angemessene verstärkte Sorgfaltspflichten zu erfüllen. § 3 Abs. 4 Satz 2 und Abs. 6 findet entsprechende Anwendung.

(2) Insbesondere in folgenden Fällen ist von einem erhöhten Risiko auszugehen und sind die nachstehend jeweils aufgeführten verstärkten Sorgfaltspflichten zu erfüllen:

1. Ein Verpflichteter hat angemessene, risikoorientierte Verfahren anzuwenden, mit denen bestimmt werden kann, ob es sich bei dem Vertragspartner und, soweit vorhanden, dem wirtschaftlich Berechtigten um eine natürliche Person handelt, die ein wichtiges öffentliches Amt ausübt oder ausgeübt hat, oder um ein unmittelbares Familienmitglied dieser Person oder eine ihr bekanntermaßen nahestehende Person im Sinne des Artikels 2 der Richtlinie 2006/70/EG der Kommission vom 1. August 2006 mit Durchführungsbestimmungen für die Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates hinsichtlich der Begriffsbestimmung von ‚politisch exponierte Personen' und der Festlegung der technischen Kriterien für vereinfachte Sorgfaltspflichten sowie für die Befreiung in Fällen, in denen nur gelegentlich oder in sehr eingeschränktem Umfang Finanzgeschäfte getätigt werden (ABl. L 214 vom 4. August 2006, S. 29). Hierbei gelten öffentliche Ämter unterhalb der nationalen Ebene in der Regel nur dann als wichtig, wenn deren politische Bedeutung mit der ähnlicher Positionen auf nationaler Ebene vergleichbar ist. Soweit ein Verpflichteter abklären muss, ob der Vertragspartner oder der wirtschaftlich Berechtigte einer Person, die wichtige öffentliche Ämter ausübt, nahesteht, ist er hierzu nur insoweit verpflichtet, als diese Beziehung öffentlich bekannt ist oder der Verpflichtete Grund zu der Annahme hat, dass eine derartige Beziehung besteht; er ist jedoch nicht verpflichtet, hierzu Nachforschungen anzustellen. Handelt es sich bei dem Vertragspartner oder dem wirtschaftlich Berechtigten um eine politisch exponierte Person in diesem Sinne, so gilt Folgendes:

   a) Die Begründung einer Geschäftsbeziehung durch einen für den Verpflichteten Handelnden ist von der Zustimmung eines diesem vorgesetzten Mitarbeiters abhängig zu machen,

   b) es sind angemessene Maßnahmen zu ergreifen, mit denen die Herkunft der Vermögenswerte bestimmt werden kann, die im Rahmen der Geschäftsbeziehung oder der Transaktion eingesetzt werden, und

   c) die Geschäftsbeziehung ist einer verstärkten kontinuierlichen Überwachung zu unterziehen.

   Für den Fall, dass der Vertragspartner oder der wirtschaftlich Berechtigte erst im Laufe der Geschäftsbeziehung ein wichtiges öffentliches Amt ausübt oder der Verpflichtete erst nach Begründung der Geschäftsbeziehung von der Ausübung eines wichtigen öffentlichen Amts durch den Vertragspartner oder dem wirtschaftlich Berechtigten Kenntnis erlangt, tritt an die Stelle der Zustimmung des für den Verpflichteten handelnden vorgesetzten Mitarbeiters dessen Genehmigung zur Fortführung der Geschäftsbeziehung. Der Vertragspartner hat dem Verpflichteten die für die Abklärung notwendigen Informationen zur Verfügung zu stellen und die sich im Laufe der Geschäftsbeziehung ergebenden Änderungen unverzüglich anzuzeigen. Soweit es sich bei dem Vertragspartner oder dem wirtschaftlich Berechtigten um eine politisch exponierte Person handelt, die ihr wichtiges öffentliches Amt im Inland oder als im Inland gewählte Abgeordnete des Europäischen Parlaments ausübt, oder soweit der Vertragspartner oder der wirtschaftlich Berechtigte seit mindestens einem Jahr kein wichtiges öffentliches Amt mehr ausgeübt hat, gelten vorbehaltlich einer Risikobewertung im Einzelfall die allgemeinen Sorgfaltspflichten nach § 3.

(…)

8 Innere Verwaltung und Rechtswesen

8.1 Statistik

8.1.1 Zensus 2011 – War da was?

Am 9. Mai 2011 war Stichtag der Volkszählung in Deutschland. Hauptsächlich als Registerzählung konzipiert, hat der Zensus 2011 viele gar nicht unmittelbar berührt. Dass aber hinter den Kulissen die praktische Durchführung des Zensus 2011 beim Statistischen Bundesamt ganz überwiegend datenschutzgerecht abläuft, davon habe ich mich überzeugt.

Die in mehrjährigem Rhythmus durchgeführten Volkszählungen sind die statistischen Großereignisse schlechthin. Bisweilen erregen sie auch die Gemüter – wie die letzte (west-)deutsche Volkszählung, die zunächst für 1983 geplant, auf Grund der Monita des Bundesverfassungsgerichts aber erst 1987 durchgeführt wurde. Das Volkszählungsurteil vom 19. Dezember 1983 (BVerfGE 65, 1, S. 1 – abrufbar unter www.zensus2011.de) ist seither die „Bibel" aller Datenschützer. Wie kein zweites Ereignis haben die Volkszählung und das Volkszählungsurteil des Bundesverfassungsgerichts den rechtlichen Rahmen und das Verständnis für den Datenschutz in Deutschland geprägt.

Wer allerdings gedacht hätte, dass der Zensus 2011 vergleichbare Aufmerksamkeit und Proteste auf sich ziehen würde, sah sich getäuscht. Die neue – registergestützte – Volkszählung lief im Großen und Ganzen unspektakulär ab und beschäftigte die Öffentlichkeit nur am Rande. Für mich und meine Mitarbeiterinnen und Mitarbeiter war dies aber kein Grund, weniger genau hinzusehen. In einer Vielzahl von Beratungsgesprächen und bei Prüfungen vor Ort habe ich darauf geachtet, dass die gesetzlichen und verfassungsrechtlichen Vorgaben eingehalten werden. Da die Durchführung des Zensus vor Ort durch die Statistischen Landesämter erfolgt, liegt die datenschutzrechtliche Kontrollzuständigkeit dafür bei den Landesbeauftragten für den Datenschutz, mit denen ich mich vor, während und nach dem Zensus abgestimmt habe.

Zum Stichtag hatten sämtliche Meldebehörden Datensätze über alle Einwohnerinnen und Einwohner an die Statistischen Ämter übermittelt. Auch von der Bundesagentur für Arbeit kamen umfangreiche Daten. Sämtliche Eigentümer bzw. Verwalter der Gebäude und Wohnungen in Deutschland wurden im Rahmen einer Gebäude- und Wohnungszählung zu diesen befragt. Lediglich bei 9,6 Prozent der Bevölkerung – immerhin noch fast 8 Millionen – fand darüber hinaus eine Haushaltebefragung statt, wobei die Auskunftspflichtigen in etwa dieselben Merkmale anzugeben hatten wie bei der Vollerhebung 1983 sämtliche Bürgerinnen und Bürger. Rechtsgrundlage für diese Erhebungen ist das Gesetz über den registergestützten Zensus im Jahre 2011 (Zensusgesetz 2011 – ZensG 2011, vgl. 23. TB Nr. 8.1.1).

Das Statistische Bundesamt hat für den Zensus einen so genannten Referenzdatenbestand aufgebaut. Dieser setzt sich zusammen aus dem Anschriften- und Gebäuderegister und dem Melde- und Erwerbsdatenregister (vgl. Kasten zu Nr. 8.1.1).

Ein Zugriff auf die Daten ist im Statistischen Bundesamt nur in einem speziell gesicherten Bereich und nur durch eigens dafür autorisierte Personen möglich. Bei einem Kontrollbesuch habe ich mir die Arbeitsplätze in diesem gesicherten Bereich zeigen lassen. Mir wurden der Aufbau der beim Statistischen Bundesamt vorhandenen Register bzw. Datenbestände sowie das Verfahren der Zentralen Benutzer- und Rechteverwaltung erläutert und praktisch am Arbeitsplatz vorgeführt. Wie ich dabei feststellen konnte, hat das Statistische Bundesamt die Herausforderungen des Zensus 2011 für den Datenschutz und die Datensicherheit erkannt und technische sowie organisatorische Lösungen für eine datenschutzgerechte Umsetzung gefunden, die einen Datenmissbrauch weitgehend ausschließen.

Trotz dieses guten Eindrucks ist leider auch der Zensus 2011 nicht gänzlich von Problemen verschont geblieben.

Einer der statistikrechtlichen Grundsätze, der sich sowohl im Bundesstatistikgesetz als auch speziell im ZensG 2011 findet, betrifft die Trennung und Löschung der so genannten Hilfsmerkmale. Hilfsmerkmale sind Angaben, die der technischen Durchführung der Statistik dienen, wie beispielsweise der Name und die Anschrift der Person. Sie sind zu löschen, sobald die Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist. Die Aufbereitung der Daten durch die statistischen Ämter hat länger gedauert als ursprünglich vorgesehen. Dadurch kommt es auch zu Verzögerungen bei der Löschung der Hilfsmerkmale. Dies ist sehr bedauerlich! Beim aktuellen Zensus müssen die statistischen Ämter die Hilfsmerkmale so schnell wie möglich löschen. Ich werde mich zu gegebener Zeit davon überzeugen, dass das Statistische Bundesamt dieser Verpflichtung nachkommt.

Die Gründe für die Verzögerungen müssen näher untersucht werden, um zu verhindern, dass sich dies beim für 2021 vorgesehenen nächsten Zensus wiederholt.

Kasten zu Nr. 8.1.1

Das Anschriften- und Gebäuderegister besteht aus den Daten der Vermessungsregister, den Anschriftenmerkmalen der Bundesagentur für Arbeit sowie aus Daten der Melderegister. Die in den Melderegistern vorhandenen personenbezogenen Daten finden sich dort allerdings nicht wieder. Diese wurden für das Anschriften- und Gebäuderegister lediglich als Strukturmerkmale verwendet, so zum Beispiel die Anzahl der Personen, die an einer Anschrift wohnen. Das Melde- und Erwerbsdatenregister wiederum enthält die Melderegisterdaten nach § 3 Absatz 1 sowie die erwerbsstatistischen Daten nach §§ 4, 5 ZensG 2011. Die Übernahme und Zusammenführung der Daten obliegt grundsätzlich den Statistischen Landesämtern.

8.1.2 Verwaltungsdaten für die amtliche Statistik?

Der Entwurf eines Gesetzes über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes (Bevölkerungsstatistikgesetz – BevStatG) bringt auch datenschutzrechtliche Verbesserungen mit sich.

Die Statistiken nach dem BevStatG sind als sogenannte Sekundärerhebungen ausgestaltet. Die erforderlichen Daten werden der Statistik von den Verwaltungsbehörden geliefert. Dagegen habe ich keine grundlegenden datenschutzrechtlichen Vorbehalte. Bedenklich wird es aber dann, wenn die Verwaltungsbehörden Daten für die amtliche Statistik erheben, die sie für ihre eigenen Zwecke nicht benötigen. Zunächst widerspricht dies dem im Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1, 1) ausdrücklich betonten Prinzip der Trennung von Statistik und Verwaltung. Denn durch die Erhebung der Statistikmerkmale erfahren die Verwaltungsmitarbeiter Informationen, die sie für die Wahrnehmung ihrer Aufgaben nicht benötigen und deshalb nicht erheben dürften.

Des Weiteren stellt sich die Frage nach der rechtlichen Konstruktion eines solchen Verfahrens. Erhebt die Verwaltungsbehörde nämlich Daten nicht für eigene Zwecke, sondern gleichsam als verlängerter Arm der Statistik, ist sie als Auftragnehmer einer Auftragsdatenverarbeitung anzusehen. Das hätte die Anwendbarkeit von § 11 BDSG mit allen Rechten und Pflichten zur Folge, die eine Auftragsdatenverarbeitung mit sich bringt; zum Beispiel Weisungsrechte und Kontrollpflichten. Ferner dürfte denjenigen, die zu Angaben gegenüber der Verwaltungsbehörde verpflichtet sind, nur schwer vermittelbar sein, dass einige Daten nur für Zwecke der amtlichen Statistik erhoben werden.

Der Gesetzentwurf sieht nun vor, dass die Verwaltungsbehörden nur solche Daten an die amtliche Statistik übermitteln, die dort bereits vorhanden sind. Daher entfallen insbesondere die Erhebungsmerkmale Körpergewicht und Körperlänge für die Statistik über lebend- und totgeborene Kinder sowie das Erhebungsmerkmal rechtliche (Nicht-) Zugehörigkeit zu einer Religionsgemeinschaft. Dies sehe ich positiv und werde mich im weiteren parlamentarischen Verfahren dafür einsetzen, dass insoweit keine Änderungen an dem Entwurf vorgenommen werden.

8.2 Bundesmeldegesetz – zentrales Bundesmelderegister konnte verhindert werden; Vermittlungsausschuss wurde angerufen

Das vom Deutschen Bundestag am 28. Juni 2012 beschlossene Gesetz zur Fortentwicklung des Meldewesens (MeldFortG) wies gegenüber dem Regierungsentwurf, den ich intensiv datenschutzrechtlich begleitet hatte, erhebliche Verschlechterungen auf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daraufhin durch eine Initiative gegenüber dem Bundesrat mit dazu beigetragen, dass dieser dem Gesetz nicht zugestimmt, sondern den Vermittlungsausschuss angerufen hat.

Mit der Föderalismusreform des Jahres 2006 ist dem Bund die ausschließliche Gesetzgebungskompetenz für das Meldewesen übertragen worden. Seit dem Jahre 2007 begleite ich intensiv das Gesetzgebungsvorhaben für das Bundesmeldegesetz (vgl. 22. TB Nr. 5.2 und 6.5). Dabei ist es insbesondere gelungen, die Einführung eines zentralen Melderegisters zu verhindern.

Nachdem ein Regierungsentwurf für eine neue gesetzliche Grundlage in der vorherigen Legislaturperiode nicht zustande gekommen war, hat die Bundesregierung nun am 31. August 2011 einen Gesetzentwurf beschlossen.

Der von der Bundesregierung dem Deutschen Bundestag vorgelegte Entwurf eines Gesetzes zur Fortentwicklung des Meldewesens (MeldFortG) vom 16. November 2011 – Bundestagsdrucksache 17/7746 – enthielt aus datenschutzrechtlicher Sicht einige Verbesserungen gegenüber früheren Referentenentwürfen (insbes. Verzicht auf ein zentrales Bundesmelderegister) und teilweise auch gegenüber der geltenden Rechtslage (insbes. Einwilligungslösung bei einfachen Melderegisterauskünften für Zwecke der Werbung und des Adresshandels). Gleichwohl bestanden noch wesentliche datenschutzrechtliche Bedenken und Forderungen, die im Rahmen der Ressortabstimmung nicht berücksichtigt worden waren. Diese betrafen:

- (weitere) Stärkung der Rechte des Meldepflichtigen bei Melderegisterauskünften,
- Abschaffung der Hotelmeldepflicht,
- keine Wiedereinführung der Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters.

Der Deutsche Bundestag hat in seinem Gesetzesbeschluss am 28. Juni 2012 nicht nur diese Forderungen nicht berücksichtigt, sondern auf Vorschlag des Innenausschusses hin Änderungen beschlossen, die die im Regierungsentwurf enthaltenen Datenschutzbestimmungen deutlich verschlechtern und zum Teil sogar hinter das geltende Recht zurückfallen. Dabei geht es im Wesentlichen um folgende Punkte:

- Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels:
  Die im Regierungsentwurf vorgesehene Einwilligungslösung wurde durch eine bloße Widerspruchslösung ersetzt, die zudem durch eine Ausnahme für Daten, die ausschließlich zur Bestätigung oder Berichtigung bereits vorhandener Daten verwendet werden, erheblich aufgeweicht wird.
- Einfache Melderegisterauskünfte zu sonstigen gewerblichen Zwecken:
  Beschränkung der ursprünglich vorgesehenen Zweckbindungsregelung für sämtliche gewerbliche Zwecke auf Zwecke der Werbung und des Adresshandels.
- Streichung des Widerspruchsrechts gegen die Erteilung einfacher Melderegisterauskünfte im Wege des automatisierten Abrufs über das Internet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 22. August 2012 (vgl. Kasten zu Nr. 8.2) und einer gemeinsamen fachlichen Stellungnahme an den Bundesrat auf die erheblichen datenschutzrechtlichen Defizite hingewiesen und den Bun-

desrat aufgefordert, dem Gesetz nicht zuzustimmen, damit im Vermittlungsverfahren die erforderlichen datenschutzgerechten Verbesserungen erfolgen können.

Der Bundesrat ist dem gefolgt und hat in seiner Sitzung am 21. September 2012 beschlossen, die Einberufung des Vermittlungsausschusses zu verlangen. Allerdings hat er dabei nicht alle datenschutzrechtlichen Bedenken aufgegriffen.

Der Vermittlungsausschuss hat im Berichtszeitraum allerdings noch keinen Vermittlungsvorschlag vorgelegt.

Kasten zu Nr. 8.2

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. August 2012

Melderecht datenschutzkonform gestalten!

Das vom Deutschen Bundestag am 28. Juni 2012 beschlossene neue Melderecht weist erhebliche datenschutzrechtliche Defizite auf. Schon die im Regierungsentwurf enthaltenen Datenschutzbestimmungen blieben zum Teil hinter dem bereits geltenden Recht zurück. Darüber hinaus wurde der Regierungsentwurf durch das Ergebnis der Ausschussberatungen des Bundestages noch einmal deutlich verschlechtert.

Bei den Meldedaten handelt es sich um Pflichtangaben, die die Bürgerinnen und Bürger gegenüber dem Staat machen müssen. Dies verpflichtet zu besonderer Sorgfalt bei der Verwendung, insbesondere wenn die Daten an Dritte weitergegeben werden sollen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher den Bundesrat auf, dem Gesetzentwurf nicht zuzustimmen, damit im Vermittlungsverfahren die erforderlichen datenschutzgerechten Verbesserungen erfolgen können. Dabei geht es nicht nur darum, die im Deutschen Bundestag vorgenommenen Verschlechterungen des Gesetzentwurfs der Bundesregierung rückgängig zu machen, vielmehr muss das Melderecht insgesamt datenschutzkonform ausgestaltet werden. Hierfür müssen auch die Punkte aufgegriffen werden, die von den Datenschutzbeauftragten im Gesetzgebungsverfahren gefordert worden sind, aber unberücksichtigt blieben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere in den folgenden Punkten Korrekturen und Ergänzungen für erforderlich:

– Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels bedürfen ausnahmslos der Einwilligung des Meldepflichtigen. Dies gilt auch für die Aktualisierung solcher Daten, über die die anfragenden Stellen bereits verfügen und die Weitergabe der Daten an Adressbuchverlage.

  Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwerbungszwecken und an Presse oder Rundfunk über Alters- und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.

– Der Meldepflichtige muss sonstigen einfachen Melderegisterauskünften widersprechen können. Die Übermittlung hat bei Vorliegen eines Widerspruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.

– Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.

– Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis der einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.

– Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.

– Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.

– Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu vernachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür – wie auch bei der Hotelmeldepflicht – außer Verhältnis zum Nutzen.

8.3 Fortbildung und Zertifizierung behördlicher Datenschutzbeauftragter

Bei der Entwicklung des Fortbildungslehrgangs „Behördliche Datenschutzbeauftragte Basis (Bund)“ habe ich die Bundesakademie für öffentliche Verwaltung fachlich beraten.

Um den steigenden Anforderungen an das Fachwissen behördlicher Datenschutzbeauftragter Rechnung zu tragen und zugleich Standards für die Ausbildung und Zertifizierung behördlicher Datenschutzbeauftragter in der Bundesverwaltung zu schaffen, hat die Bundesakademie für öffentliche Verwaltung (BAköV) den Fortbildungslehrgang „Behördliche Datenschutzbeauftragte Basis (Bund)“ entwickelt. Diesen Prozess habe ich beratend begleitet. Das Fortbildungsangebot, das den Erwerb einer gleichnamigen Zertifizierung einschließt, richtet sich an behördliche Datenschutzbeauftragte in der Bundesverwaltung oder diejenigen, die für diese Funktion vorgesehen sind.

Die Fortbildung bietet die Möglichkeit, die erforderlichen Grundkenntnisse auf den Gebieten des Datenschutzes und der Datensicherheit einfach und bequem zu erlernen und durch die Zertifizierung auch belegen zu können. Ich begrüße es, dass das auf 15 Tage angelegte Basisseminar den Teilnehmern genügend Raum lässt, den erlernten Stoff zu verinnerlichen. Die Ausbildung zum Datenschutzbeauftragten ist nicht im Schnellverfahren möglich.

Der modulare Aufbau des Lehrgangs bietet den Teilnehmern zudem größtmögliche Flexibilität. Die Zertifizierung als behördlicher Datenschutzbeauftragter, die eine Projektarbeit sowie den Abschlusstest umfasst, ist insbesondere nicht an den Besuch des Basisseminars geknüpft. Alle Teilnehmer können auf der Grundlage eines Selbsteinschätzungstests frei entscheiden, ob und in welchem Umfang sie das Basisseminar oder den ebenfalls angebotenen Kompaktkurs besuchen. Diese Wahlfreiheit wird insbesondere für erfahrene Datenschutzbeauftragte, die ihr Fachwissen in erster Linie zertifizieren lassen wollen, interessant sein.

Von der Zertifizierung erwarte ich eine Aufwertung der Funktion des behördlichen Datenschutzbeauftragten, der nun erstmals seine Kenntnisse und seine Ausbildung mit einem Zertifikat belegen kann. Ich wünsche der BAköV bei der weiteren Umsetzung der Fortbildung – ein erster Pilotdurchgang ist für Sommer 2013 geplant – viel Erfolg und regen Zulauf. Ich bin gerne bereit, das Fortbildungsprojekt bei Bedarf auch weiterhin fachlich beratend zu begleiten.

8.4 Anlaufschwierigkeiten bei der Herstellung des neuen Personalausweises

Anlaufschwierigkeiten bei der Herstellung des neuen Personalausweises in der Bundesdruckerei konnten abgestellt werden.

Nachdem die Presse über Probleme bei der Produktion des neuen Personalausweises berichtet hatte, habe ich dessen Herstellung – vom Auftragseingang bis zur Auslieferung – bei der Bundesdruckerei überprüft (vgl. Kasten zu Nr. 8.4).

Ein Problem, mit dem ich mich bei meiner Kontrolle befasst habe, stellte die Ausgabe von Personalausweisen mit nicht personalisiertem Chip dar. Die Ursache für diesen Fehler lag darin, dass bei der Maschine, die die Personalisierung und Prüfung des Chips übernimmt, versehentlich beide Funktionen gleichzeitig ausgeschaltet waren. Um derartige Pannen künftig auszuschließen, hat die Bundesdruckerei die elektrische Abschaltung deaktiviert und zusätzliche Prüffunktionen eingeführt.

Ein weiteres Problem stellte die doppelte Produktion von Personalausweisen dar, die auf einen Softwarefehler zurückzuführen war. Dieser Fehler wurde ebenfalls behoben. Auf Grund eines Verfahrensfehlers wurde als ausstellende Behörde immer die gleiche Stelle auf die betroffenen Personalausweise gedruckt, obwohl diese von unterschiedlichen Behörden ausgestellt worden waren. Auch dieser Fehler konnte beseitigt werden.

Darüber hinaus führte die Vielfalt der in den Kommunen und den zwischengeschalteten Rechenzentren eingesetzten IT-Infrastruktur anfänglich zu Instabilitäten, Fehlermeldungen und Wartezeiten, die die Bundesdruckerei durch nachträgliche Software-Updates beheben konnte.

Schließlich habe ich mir den Umgang mit fehlerhaft produzierten Ausweisen angesehen. Wie ich dabei feststellen konnte, hat die Bundesdruckerei durch entsprechende technische und organisatorische Maßnahmen eine datenschutzgerechte Vernichtung sichergestellt.

Kasten zu Nr. 8.4

In den Verantwortungsbereich der Bundesdruckerei fallen insbesondere

- die Entwicklung, die Bereitstellung und der Betrieb der Softwarekomponenten zur Erfassung der Daten der Ausweisinhaber in den Meldebehörden, der Komponenten zur sicheren, verschlüsselten Übertragung der persönlichen Daten des Bürgers in die Bundesdruckerei sowie der Hard- und Software zum Auslesen, Anzeigen und Ändern der im Chip gespeicherten Daten,
- die Entwicklung des Ausweiskartenkörpers aus unterschiedlichen Lagen mit neuen Sicherheitsmerkmalen,
- die Entwicklung, der Aufbau, die Inbetriebnahme und das Hochfahren der Produktion sowie
- die Entwicklung und Bereitstellung von Hauptkomponenten der IT-Infrastruktur zur Nutzung der elektronischen Identität.

8.5 Aufgaben des Bundesverwaltungsamtes bei der eID-Funktion des neuen Personalausweises

Das Bundesverwaltungsamt führt Sperrlisten und vergibt elektronische Berechtigungszertifikate. Die Prüfung vor Ort ergab keinen Grund zur Beanstandung.

Der neue Personalausweis unterscheidet sich von dem Vorgängermodell im Wesentlichen durch den integrierten Chip. Dieser Chip unterstützt drei Funktionen: Die hoheitliche Identitätskontrolle mittels biometrischer Merkmale (elektronisches Passfoto und – auf freiwilliger Basis – Fingerabdruck), die qualifizierte elektronische Signatur und den elektronischen Identitätsnachweis (eID-Funktion), mit dem der Inhaber sich elektronisch über das Internet ausweisen kann. Damit sollen sowohl elektronische Behördengänge als auch Onlinedienstleistungen, etwa das E-Banking, sicherer werden (vgl. 23. TB Nr. 3.2).

Dem Bundesverwaltungsamt (BVA) wurden bei der Realisierung des elektronischen Identitätsnachweises wichtige Aufgaben zugewiesen. Im Berichtszeitraum habe ich geprüft, ob das BVA sich dabei an die datenschutzrechtlichen Vorgaben hält.

Bei der Vergabestelle für Berechtigungszertifikate beantragen Diensteanbieter die Berechtigung, die für ihre Aufgaben erforderlichen Daten im Wege des elektronischen Identitätsnachweises mittels eines Berechtigungszertifikates anfragen zu dürfen.

Diensteanbieter können Behörden aber auch private Unternehmen sein. Entscheidend ist, dass die Übermittlung bestimmter im neuen Personalausweis hinterlegter Daten für den jeweiligen „Geschäftszweck“ erforderlich ist. In seinem Antrag auf eine solche Berechtigung hat der Diensteanbieter daher unter anderem die Datenkategorien zu benennen, auf die zugegriffen werden soll und dabei für jede Datenkategorie zu begründen, warum es für den dargelegten Zweck erforderlich ist, die Daten zu erheben. Die Prüfung der Erforderlichkeit bildet einen Schwerpunkt bei der Antragsprüfung durch die Vergabestelle für Berechtigungszertifikate. Zum Nachweis der Erforderlichkeit haben die Diensteanbieter ihre Geschäftsprozesse detailliert zu erläutern. Hierzu habe ich mir Anträge angesehen, bei denen sich aus einem Flussdiagramm eindeutig ergab, in welchem Stadium des Prozesses welche Daten wofür benötigt werden. Unter Vorlage des positiven Bescheids der Vergabestelle kann der Diensteanbieter von einem Berechtigungszertifikateanbieter (BerCA) das elektronische Berechtigungszertifikat erwerben.

Als Sperrlistenbetreiber hat das BVA jedem Diensteanbieter eine für ihn errechnete, aktuelle Liste bereitzustellen, die die Sperrmerkmale abhandengekommener Personalausweise mit eingeschaltetem elektronischem Identitätsnachweis enthält. Für Zwecke des Sperrmanagements führt das BVA eine so genannte Referenzliste, in der die Sperrsummen und Sperrschlüssel sämtlicher hergestellter Ausweise gespeichert sind. Erfolgt eine Sperrmeldung des Ausweisdokuments unter Mitteilung der Sperrsumme, wird mit Hilfe der Referenzliste der zugehörige Sperrschlüssel ermittelt und die Sperrsumme als gesperrt gekennzeichnet. Mit Hilfe des Sperrschlüssels wird das Sperrmerkmal nach den Vorgaben in den Technischen Richtlinien TR-03110 und TR-03111 berechnet und in der globalen Sperrliste in der Datenbank beim BVA gespeichert. Zweimal täglich wird die globale Sperrliste aus der Datenbank exportiert und als Kopie für die BerCA auf einem Downloadserver zur Verfügung gestellt. Der BerCA berechnet aus der zur Verfügung gestellten Kopie nach den Vorgaben in der TR-03110 eine diensteanbieterspezifische Sperrliste, welche die Diensteanbieter abrufen. Während des Authentisierungsprozesses bei der Nutzung der Online-Ausweisfunktion berechnet der Chip im Personalausweis ein diensteanbieterspezifisches Merkmal. Wird dieses in der diensteanbieterspezifischen Sperrliste gefunden, ist der Personalausweis gesperrt.

Sowohl die Vergabe der Berechtigungszertifikate als auch die Erstellung der Sperrlisten habe ich bei einer Kontrolle des BVA überprüft. Erfreulicherweise habe ich keine Datenschutzmängel festgestellt.

8.6 Forschungsprojekte der Bundesregierung zur Aufarbeitung des Umgangs mit der NS-Vergangenheit von Mitarbeiterinnen und Mitarbeitern in Bundesministerien

Gesetzliche Änderungen sind erforderlich, um die NS-Vergangenheit in Bundesbehörden wissenschaftlich aufarbeiten zu können.

Die Aufarbeitung der NS-Vergangenheit ist in den letzten Jahren zu Recht ein wichtiges Thema für zahlreiche Bundesbehörden geworden und hat auch den Deutschen Bundestag beschäftigt.

Wenn Forschungsaufträge vergeben werden, mit denen das Vorleben ehemaliger Mitarbeiter untersucht werden soll, ist es regelmäßig erforderlich, auch Daten aus Personalakten zu verwenden. Nur so werden sich die Forscher ein umfassendes Bild von den Mitarbeitern und deren eventuellen Verstrickungen in NS-Unrecht machen können.

Nach dem Bundesbeamtengesetz gilt für Bundesbeamte – wie analog auch für Tarifbeschäftigte – das Personalaktengeheimnis. Dieses sieht einen Zugang zu Personalakten nur unter sehr engen Voraussetzungen vor. Der Zugang zu Forschungszwecken ist nicht vorgesehen. Sofern kein archivrechtlicher Zugang möglich ist, sehe ich auch keine Möglichkeit, Forschern Personalakten aufgrund anderer Rechtsvorschriften zugänglich zu machen. Ein Forschungszugriff auf Personalaktendaten verstößt daher im Regelfall gegen das Personalaktengeheimnis (§ 107 Absatz 1 Bundesbeamtengesetz).

Ich halte dieses juristisch zwingende Ergebnis für unbefriedigend. Im Hinblick auf das gesellschaftliche Bedürfnis an einer wissenschaftlichen Aufarbeitung der NS-Vergangenheit von Bundesbehörden habe ich gegenüber der Bundesregierung angeregt, über eine entsprechende Änderung des Bundesbeamtengesetzes nachzudenken. Diese könnte sich inhaltlich an § 32 Stasi-Unterlagen-Gesetz orientieren, der eine ähnliche Interessenkollision angemessen regelt. Mit dieser modellhaften Regelung hat der Gesetzgeber eine ausgewogene Lösung des Konfliktes zwischen dem Anspruch der Allgemeinheit an einer historischen Aufarbeitung und dem Recht des Einzelnen auf informationelle Selbstbestimmung getroffen.

Leider hat die Bundesregierung meine Anregung nicht aufgegriffen. Es ist deshalb zu befürchten, dass die Aufarbeitung der NS-Vergangenheit durch – an sich vermeidbare – Rechtsstreitigkeiten behindert wird.

8.7 Nationales Waffenregister

Die gesetzliche Grundlage für ein Nationales Waffenregister (NWR) muss den datenschutzrechtlichen Anforderungen genügen.

Nach der europäischen Waffenrichtlinie (2008/51/EG) sind alle Mitgliedstaaten verpflichtet, bis spätestens 31. Dezember 2014 ein computergestütztes Waffenregister auf nationaler Ebene einzurichten und stets auf dem aktuellen Stand zu halten. Wie die Richtlinie weiter vorsieht, muss das nationale Register allen zuständigen Behörden Zugang zu den gespeicherten Daten gewähren. Der deutsche Gesetzgeber hat daraufhin beschlossen, das Nationale Waffenregister (NWR) bereits bis Ende des Jahres 2012 und damit zwei Jahre vor Ablauf der von der EU gesetzten Frist aufzubauen (§ 43a Waffengesetz). Ich habe das Projekt eines bundesweiten zentralen Nationalen Waffenregisters bereits in einem frühen Stadium begleitet (vgl. 23. TB Nr. 8.3).

Sowohl bei den Eckpunkten des BMI wie auch im eigentlichen Gesetzgebungsverfahren zum Errichtungsgesetz für das Nationale Waffenregister und zur entsprechenden Durchführungsverordnung habe ich datenschutzrechtliche Belange geltend gemacht. Im Ergebnis ist festzustellen, dass die notwendigen datenschutzrechtlichen Vorkehrungen sowohl in sachlicher als auch in technischer Hinsicht Berücksichtigung gefunden haben. Das Gesetz zur Errichtung eines Nationalen Waffenregisters (NWRG) und die Verordnung zur Durchführung des Nationalen-Waffenregister-Gesetzes (NWRG-DV) bilden jetzt eine solide Grundlage für das zum 1. Januar 2013 einzurichtende Register.

8.8 Der Umgang mit den Stasi-Unterlagen – ein Dauerthema

Neben den Anträgen auf Akteneinsicht war die Verwendung der Unterlagen für Forschungsvorhaben ein Kontrollschwerpunkt. Auch Fragen im Zusammenhang mit der manuellen Rekonstruktion zerrissener Stasi-Unterlagen waren Gegenstand meiner Beratung.

Im Berichtszeitraum wurden Beratungs- und Kontrollbesuche in der Zentrale sowie in einer Außenstelle des BStU durchgeführt. Ferner fand ein Informations- und Beratungsbesuch bei der Projektgruppe zur manuellen Rekonstruktion der Stasi-Unterlagen statt.

Als generelles Ergebnis meiner Prüfungen konnte ich erneut feststellen, dass die BStU-Mitarbeiter sich durch hohe Sachkunde und Gewissenhaftigkeit im Umgang mit den sensiblen personenbezogenen Unterlagen auszeichnen. An allen besuchten Stellen wird den Maßnahmen zur inneren und äußeren Sicherung der Stasi-Unterlagen, der sorgfältigen Dokumentation der Verfahrensabläufe und der restriktiven Kenntnisnahme der Inhalte hohes Gewicht beigemessen.

Der Beratungs- und Kontrollbesuch in der BStU-Zentrale galt der Verwendung der Unterlagen für Forschungsvorhaben. Zu unterscheiden ist zwischen Vorhaben, die von Externen beantragt werden (§ 32 StUG) und solchen, die der BStU selbst durchführt (im Rahmen der Aufgabenstellung nach § 37 Absatz 1 Nummer 5 StUG). Nach Darstellung des BStU sei entscheidender Aspekt für die Zulässigkeit der Herausgabe von Stasi-Unterlagen für diese Forschungszwecke die zweifelsfreie Feststellung, dass das Forschungsvorhaben der Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes oder einem sonstigen in § 32 Absatz 1 StUG genannten Forschungszweck diene – und nicht lediglich als Vorwand zur Ausforschung einzelner Personen. Anders als bei Anträgen auf Akteneinsicht, die konkret personenbezogen gestellt würden, stelle sich der Recherchevorgang bei themenbezogenen Forschungsvorhaben komplexer dar, weil die Herausgabe der Unterlagen nach dem Erforderlichkeitsgrundsatz konkret auf den Themenbezug zu beschränken sei. Auf dieser Grundlage würden dann die notwendigen Unterlagen herausgegeben – soweit nötig in anonymisierter Form – und diesbezüglich ein administrativer Nachweis dokumentiert. Insgesamt habe ich festgestellt, dass die Bereitstellung von Stasi-Unterlagen nach § 32 StUG datenschutzkonform erfolgt.

Die vom BStU selbst durchgeführten Forschungsvorhaben erfolgen im Rahmen der Aufgabenstellung nach § 37 Absatz 1 Nummer 5 StUG – Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes durch Unterrichtung der Öffentlichkeit über seine Struktur, Methoden und Wirkungsweise. Der BStU erklärte, dass auch bei der Einsichtnahme und Verwendung von Stasi-Unterlagen für interne Forschungszwecke die damit befassten Mitarbeiter nur projekt- und damit themenbezogen Zugang zu den Stasi-Unterlagen hätten. Dieser würde durch entsprechende Mechanismen vergleichbar den externen Antragstellern administrativ begleitet und nachgewiesen. Nach meinen Feststellungen stellt der BStU auch auf diesem Feld durch organisatorische Maßnahmen sicher, dass dem Schutz der Stasi-Unterlagen angesichts ihrer hohen Sensibilität großes Gewicht beigemessen wird.

Mein Informations- und Beratungsbesuch bei der Projektgruppe zur manuellen Rekonstruktion zerrissener Stasi-Unterlagen erstreckte sich schwerpunktmäßig auf Fragen der Sicherung der Unterlagen im Rahmen des Transportes von der Zentrale zur externen Projektdienststelle, auf die dortigen Sicherungsvorkehrungen sowie den Transport zurück. Auch hier konnte ich durch gezielte Nachfrage und Inaugenscheinnahme der baulichen Gegebenheiten und Zutrittsmechanismen feststellen, dass den Datenschutzerfordernissen in geeigneter Weise Rechnung getragen wird.

8.9 Visa-Warndatei und Datenabgleichverfahren

So erfreulich die datenschutzrechtlichen Verbesserungen für die künftige Visa-Warndatei sind, so kritisch sehe ich den zusätzlichen Abgleich von Daten aus dem Visum-Verfahren mit Daten aus der Antiterrordatei.

Seit langem wird über die Einrichtung einer Visa-Warndatei diskutiert. Nachdem ein entsprechendes Vorhaben in der letzten Legislaturperiode gescheitert war, sah der Koalitionsvertrag für die laufende 17. Legislaturperiode eine zentrale Visa-Warndatei vor. Sie soll Personen, die durch rechtswidriges Verhalten im Zusammenhang mit einem Visum-Verfahren oder mit sonstigem Auslandsbezug bereits auffällig geworden sind, für eventuelle weitere Visum-Verfahren erkennbar machen, um sie dann näher überprüfen zu können. Das Bundesministerium des Innern hatte hierfür zunächst einen Referentenentwurf vorgelegt, der aber insbesondere hinsichtlich der Sachverhalte, die eine Speicherung in der Visa-Warndatei auslösen sollten, und der zugriffsberechtigten Behörden über das erforderliche Maß hinaus ging (vgl. hierzu 23. TB Nr. 15.1).

Im Berichtszeitraum wurde der Entwurf überarbeitet und als „Gesetz zur Errichtung einer Visa-Warndatei und zur Änderung des Aufenthaltsgesetzes“ verabschiedet (Gesetz vom 22. Dezember 2011, BGBl. I S. 3037). Bei der Ausgestaltung der Visa-Warndatei, die beim Bundesverwaltungsamt geführt werden soll, enthält das Gesetz erhebliche datenschutzrechtliche Verbesserungen gegenüber dem ursprünglichen Entwurf. Dies gilt insbesondere für die deutliche Reduzierung der zu speichernden Warnsachverhalte sowie den Verzicht auf Zugriffsbefugnisse der Sicherheitsbehörden und Nachrichtendienste (einschließlich der Instrumente der Gruppenauskunft und des Suchvermerksverfahrens). Gleichwohl bleiben Zweifel: Ist es wirklich erforderlich, in der Visa-Warndatei Daten zu speichern, die bereits in anderen Dateien (z. B. dem Bundeszentralregister oder dem europäischen Visa-Informationssystem) enthalten sind? Meine Forderung, diese Frage vorab und nicht erst – wie in der Gesetzesbegründung vorgesehen (Bundestagsdrucksache 17/6643 S. 22) – im Rahmen der späteren Evaluierung des Gesetzes zu untersuchen, blieb im Gesetzgebungsverfahren leider unberücksichtigt.

Getrennt von der Visa-Warndatei führt das Gesetz ein zusätzliches Datenabgleichverfahren ein, mit dem besonderen sicherheitspolitischen Interessen im Visum-Verfahren Rechnung getragen werden soll. Künftig sollen in einer besonderen Organisationseinheit beim Bundesverwaltungsamt Daten aus dem Visum-Verfahren mit Daten aus der Antiterrordatei automatisiert abgeglichen werden. Dadurch soll eine Rückmeldung an die Visum-Behörden ermöglicht werden, wenn Personen aus dem terroristischen Umfeld eine Einreise nach Deutschland beabsichtigen. Gegen dieses Verfahren bestehen erhebliche datenschutzrechtliche Bedenken, die ich sowohl im Rahmen der Ressortabstimmung als auch gegenüber dem Innenausschuss des Deutschen Bundestages – letztlich erfolglos – geltend gemacht habe. Vorgesehen ist ein verdachtsloser Vollabgleich von sämtlichen Visum-Antragstellern, Einladern, Verpflichtungsgebern und sonstigen Referenzpersonen mit Angaben aus der Antiterrordatei. Ich habe Zweifel, ob dieses Abgleichverfahren, durch das weit überwiegend Personen betroffen sind, die sich rechtmäßig verhalten und keinen Anlass für eine Überprüfung gegeben haben, wirklich erforderlich ist; dies insbesondere vor dem Hintergrund, dass zur sicherheitsbehördlichen Überprüfung von Visum-Antragstellern aus bestimmten, als „kritisch“ eingestuften Herkunftsstaaten bereits das sog. Konsultationsverfahren (§ 73 Absatz 1 Aufenthaltsgesetz) existiert. Der Gesetzgeber hat an keiner Stelle dargelegt, das Konsultationsverfahren habe sich in der Vergangenheit nicht als ausreichend erwiesen. Ebenso fehlt eine Rechtfertigung für die Weite der betroffenen Personenkreise, deren Daten aus den beiden Dateien miteinander abgeglichen werden. Auch die technische und organisatorische Ausgestaltung des Abgleichverfahrens erschien während des Gesetzgebungsverfahrens noch nicht hinreichend durchdacht.

Das Gesetz wird am 1. Juni 2013 in Kraft treten. Zu diesem Zeitpunkt sollen sowohl die Visa-Warndatei als auch das Datenabgleichverfahren ihren Betrieb aufnehmen. Ich werde die technische Umsetzung insbesondere unter Datensicherheitsaspekten aufmerksam verfolgen.

8.10 Datenschutz bei THW und BBK

Bei Prüfungen beim Technischen Hilfswerk und beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe habe ich in einigen Punkten datenschutzrechtliche Defizite festgestellt. An Nachbesserungen wird gearbeitet.

Bundesanstalt Technisches Hilfswerk (THW)

Im Berichtszeitraum habe ich Beratungs- und Kontrollbesuche bei der Bundesanstalt Technisches Hilfswerk auf den verschiedenen Verwaltungsebenen durchgeführt. Diese erstreckten sich auf die THW-Leitung, die THW-Bundesschule, einen Landesverband, eine Geschäftsstelle und einen Ortsverband. Ich erfuhr, dass die THW-eigene Datenbank „THWin“ zentrales Speicher- und Informationsmedium über sämtliche Verwaltungsebenen darstellt. Von daher stellte sie den Schwerpunkt meiner Prüfungen dar.

Insbesondere ging es darum, inwieweit die Mitarbeiter der jeweiligen Verwaltungsebenen Zugriff auf Speicherinhalte der Datenbank haben bzw. diese mit Informationen beschicken können. Dies ist gerade mit Blick auf personenbezogene Daten von Bedeutung. Aus Datenschutzsicht ist es problematisch, dass die Datenbank sowohl personenbezogene Informationen als auch Informationen zu reinen Sachfragen beinhaltet. Nach Darstellung des THW ist dies darauf zurückzuführen, dass diese Datenbank bereits etwa 20 Jahre alt ist und aktuellen Erfordernissen folgend stets nur ergänzt wurde, ohne dass sie einem stringenten Konzept folgt. Auch liegt keine Dokumentation über die Datenbank vor. Ich habe daher das THW gebeten, eine Dokumentation über die Datenbank zu erstellen.

Meine Prüfungen ergaben, dass den Datenschutzerfordernissen aus praktischer Sicht Rechnung getragen wird und Zugriffsrechte auf der Grundlage eines Rechte- und Rollenkonzeptes nach dem Erforderlichkeitsprinzip organisiert sind. Meine Prüfungen erstreckten sich auch auf die Zutrittskontrollen zu den Liegenschaften und den zentra-

len Einrichtungen der Informationstechnik sowie die logische Zugangskontrolle zu den IT-Systemen.

Auch habe ich einzelne IT-Arbeitsplätze der Mitarbeiter geprüft. Hier besteht zum Teil Verbesserungsbedarf. Ich habe das THW aufgefordert, mir entsprechende Änderungsvorschläge vorzulegen.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

Im Berichtszeitraum habe ich ebenfalls den Datenschutz beim BBK geprüft. Meine Prüfungen erstreckten sich auf die verschiedenen datenschutzrelevanten Arbeitsbereiche, und zwar: Gemeinsames Lagezentrum von Bund und Ländern (GMLZ), Deutsches Notfallvorsorgeinformationssystem (deNIS), Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ), Psychosoziale Notfallversorgung (PSNV)/Koordinierungsstelle Nachsorge, Opfer- und Angehörigen-Hilfe (NOAH), den Bereich Öffentlichkeitsarbeit, das Fachinformationssystem (FIS) und den Bereich Forschung.

In den für das Bund-Länder-Krisenmanagement wesentlichen Bereichen GMLZ und deNIS habe ich keine datenschutzrechtlichen Unzulänglichkeiten festgestellt.

In den anderen Bereichen ergibt sich zum Teil ein Optimierungsbedarf, zu dem mir das BBK seine Vorschläge mitgeteilt hat. Diese prüfe ich derzeit und werde sie sodann mit der Behörde erörtern.

8.11 Auswärtiges Amt

Neben der datenschutzrechtlichen Kontrolle einer großen Auslandsvertretung ergab sich Gesprächsbedarf insbesondere zum Einsatz externer Dienstleister durch deutsche Botschaften und Konsulate im Ausland.

Zu Beginn des Berichtszeitraumes habe ich einen datenschutzrechtlichen Kontroll- und Beratungsbesuch nach § 24 BDSG bei einer großen deutschen Auslandsvertretung durchgeführt. Schwerpunkt der Kontrolle war die Verarbeitung personenbezogener Daten in der Rechts- und Konsularabteilung sowie die innerbehördliche Organisation des Datenschutzes.

Für diesen Besuch wurde auch der vor einigen Jahren erarbeitete Runderlass „Datenschutz im Auswärtigen Amt und an den Auslandsvertretungen“ herangezogen.

Neben einzelnen datenschutzrechtlichen Defiziten im Bereich der Prüfungsschwerpunkte, z. B. beim Verfahrensverzeichnis nach § 18 BDSG oder bei den Hinweisen auf Videoüberwachungsanlagen, zeigten sich größere Probleme bei der Verarbeitung personenbezogener Daten zur Abrechnung von Beihilfe-Leistungen. Das Verfahren umfasste die Verarbeitung teils sehr sensibler Daten nicht nur der Beamten selbst, sondern auch von deren Familienangehörigen, wobei die gebotene Vertraulichkeit medizinischer Daten verletzt wurde.

Beim Abschlussgespräch mit dem Leiter der Auslandsvertretung und im weiteren Dialog mit dem behördlichen Datenschutzbeauftragten des Auswärtigen Amtes habe ich auf eine datenschutzfreundliche Änderung des Abrechnungsverfahrens hingewirkt. Mittlerweile hat das Auswärtige Amt für alle Auslandsvertretungen ein geändertes Verfahren eingeführt, um Beihilfe-Leistungen abzurechnen. Dies begrüße ich.

Ein weiterer Schwerpunkt meiner Tätigkeit war die Frage, ob und unter welchen Bedingungen die Auslandsvertretungen einzelne Aufgaben des Visum-Verfahrens an externe Dienstleistungserbringer auslagern dürfen. An einigen Auslandsvertretungen mit sehr hohem Visum-Aufkommen sollen bestimmte Dienstleistungen des Visum-Verfahrens künftig durch externe Dienstleister erbracht werden; dies betrifft insbesondere die Vereinbarung von Terminen bei den konsularischen Abteilungen sowie die Entgegennahme von Visum-Anträgen und die Prüfung der Unterlagen auf Vollständigkeit. Ich sehe die Auslagerung dieser Aufgaben kritisch, denn sie ist mit Risiken für den Datenschutz von Visum-Antragstellern und anderen in den Unterlagen genannten Personen (etwa Angehörigen und Einladern) verbunden. Insbesondere in nicht-demokratischen Staaten besteht die Gefahr, dass die entsprechenden Angaben in die falschen Hände geraten und dass den Betroffenen hieraus erhebliche Nachteile entstehen.

Grundsätzlich erlaubt der Europäische Visa-Kodex (Verordnung [EG] Nr. 810/2009 des Europäischen Parlaments und des Rates vom 13. Juli 2009 über einen Visa-Kodex der Gemeinschaft; ABl. L 243 vom 15. September 2009) in Artikel 43 zwar das „Outsourcing“ bestimmter konsularischer Dienstleistungen. Derselbe Artikel 43 regelt jedoch auch, dass der hoheitliche Kernbestandteil im Visum-Verfahren in der Verantwortung der Auslandsvertretung verbleiben muss, d. h. die eigentliche Prüfung und die Entscheidung über einen Visum-Antrag müssen in jedem Falle durch die Auslandsvertretung selbst erfolgen. Bevor Dienstleistungen ausgelagert werden dürfen, ist außerdem zu prüfen, ob andere Mittel – z. B. eine engere Zusammenarbeit der vor Ort befindlichen Auslandsvertretungen der EU-Staaten, die an der gemeinsamen Visum-Politik teilnehmen – zur Verfügung stehen und ebenso geeignet sind, eine Entlastung der Botschaften und Konsulate zu erreichen. Ferner legt ein Anhang zum Europäischen Visa-Kodex (Anhang V) „Mindestanforderungen“ fest, „die im Falle einer Zusammenarbeit mit externen Dienstleistungserbringern in den Vertrag aufzunehmen sind“. Im Falle des Outsourcings sind die Auslandsvertretungen durch die Vorgaben des Europäischen Visa-Kodex verpflichtet, die vertragsgemäße Auftragserfüllung des Dienstleistungserbringers zu überwachen und zu diesem Zweck regelmäßig stichprobenartige Kontrollen in dessen Räumlichkeiten durchzuführen.

Für die Gewährleistung eines angemessenen Datenschutzniveaus kommt es selbstverständlich darauf an, dass die Anforderungen des Europäischen Visa-Kodex durch die Auslandsvertretung und insbesondere durch etwaige externe Dienstleister in der Praxis zu jeder Zeit und in vollem Umfang beachtet werden.

Bei meinen Gesprächen mit dem Auswärtigen Amt habe ich betont, dass höhere Effizienz bzw. Kosteneinsparun-

gen nicht zu Lasten des Grundrechtsschutzes gehen dürfen und dass auch im Visum-Verfahren – unabhängig von dessen Ausgestaltung vor Ort – das Recht auf den Schutz der personenbezogenen Daten und der Privatsphäre der Antragsteller immer im Blick sein muss. Ich werde daher auch künftig das Visum-Verfahren und die Verarbeitung personenbezogener Daten in den Dienststellen des Auswärtigen Amtes kritisch begleiten, ggf. vor Ort überprüfen und mich für bestmögliche Lösungen im Sinne des Datenschutzes einsetzen.

8.12 Internetabfrage aus dem Schuldnerverzeichnis

Seit dem 1. Januar 2013 kann jeder, der ein legitimes Interesse hat, das Schuldnerverzeichnis über das Internet einsehen.

Bereits 2009 war mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung durch eine Änderung der Zivilprozessordnung (ZPO) die gesetzliche Grundlage zur Einführung elektronischer Einsichten in das Schuldnerverzeichnis geschaffen worden. Es oblag dem Bundesministerium der Justiz (BMJ), die Einzelheiten zur elektronischen Einsicht durch eine Rechtsverordnung zu regeln (§ 882h Absatz 3 ZPO), was durch die Verordnung über die Führung des Schuldnerverzeichnisses (Schuldnerverzeichnisführungsverordnung – SchuFV) geschah, die am 1. Januar 2013 in Kraft getreten ist. Die ursprüngliche Fassung der SchuFV wies bei der sog. Jedermannsauskunft (§ 8 SchuFV) erhebliche datenschutzrechtliche Mängel auf. Die Regelung konnte jedoch durch eine gemeinsame Initiative mit den LfD (vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Februar 2012 – vgl. Kasten zu Nr. 8.12) verbessert werden.

Ursprüngliche hatte der Entwurf für private Gläubiger nur die Angabe von Nachnamen, Vornamen oder Wohnort des Schuldners sowie Sitz des zentralen Vollstreckungsgerichts vorgesehen, um anschließend alle passenden Treffer übermittelt zu bekommen. Bei der Angabe nur dieser wenigen Merkmale wäre es insbesondere in Großstädten und bei gebräuchlichen Nachnamen zur gleichzeitigen Übermittlung von Datensätzen vieler unterschiedlicher Schuldner kommen. Es wären Datensätze übermittelt worden, an denen kein Bedarf besteht, und für den Gläubiger wäre nicht erkennbar gewesen, welche Treffer sich auf die von ihm gesuchte Person bezögen.

Durch die gemeinsame Initiative mit den Landesdatenschutzbeauftragten konnte hier eine Verbesserung erzielt werden. Nunmehr muss der private Gläubiger mindestens Vor- und Nachnamen sowie den Wohn- bzw. Aufenthaltsort oder das zuständige zentrale Vollstreckungsgericht angeben. Sind nach Eingabe dieser Daten mehrere Treffer gegeben, so erfolgt noch keine Übermittlung, sondern der Gläubiger muss zunächst das Geburtsdatum und gegebenenfalls auch den Geburtsort eingeben. Nur wenn nach Eingabe dieser Daten immer noch mehrere Treffer vorliegen, werden diese dann alle an den Gläubiger übermittelt.

Bei der technischen Ausgestaltung der Einsicht müssen dazu die Vorgaben aus der Verordnung eingehalten werden. So sind durch die zuständigen Stellen bei Privatpersonen Name, Vorname, Wohnort, Geburtsdatum und Geburtsort des Schuldners in das elektronische Schuldnerverzeichnis einzugeben. Nur so kann bei Abrufen nach § 8 SchuFV eine Übermittlung von Datensätzen zu mehreren Schuldnern möglichst vermieden werden. Die Überwachung der elektronischen Einsichtnahme obliegt den Aufsichtsbehörden in den Ländern.

In diesem Zusammenhang begrüße ich auch den Beschluss des Bundesrates vom 15. Juni 2012, der dem BMJ aufgibt, die SchuFV nach zwei Jahren unter datenschutzrechtlichen Gesichtspunkten zu evaluieren und die LfD und mich über das Ergebnis zu unterrichten.

Zeitgleich mit Inkrafttreten der SchuFV am 1. Januar 2013 nahm das „Vollstreckungsportal“ seinen Betrieb auf, das die elektronische Einsichtnahme ermöglicht.

Kasten zu Nr. 8.12

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Februar 2012

Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert das Bundesministerium der Justiz auf, für einen besseren Datenschutz bei der geplanten Internetabfrage aus dem Schuldnerverzeichnis Sorge zu tragen. Es sollen möglichst nur diejenigen Personen angezeigt werden, auf die sich der Abfragezweck bezieht.

Wer eine Wohnung vermieten oder einen Ratenkredit einräumen will, möchte wissen, ob sein zukünftiger Schuldner Zahlungsschwierigkeiten hat. Er hat unter bestimmten Voraussetzungen ein legitimes Interesse an der Einsicht in das von den zentralen Vollstreckungsgerichten geführte Schuldnerverzeichnis. So können sich mögliche Geschäftspartner darüber informieren, ob ihr Gegenüber in wirtschaftliche Not geraten ist.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung aus dem Jahr 2009 will der Gesetzgeber die Stellung des Gläubigers stärken. Das Gesetz sieht unter anderem vor, dass der Inhalt des Schuldnerverzeichnisses ab dem 1. Januar 2013 über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden kann. Die Ausgestaltung der damit wesentlich erleichterten Einsicht wird derzeit vom Bundesministerium der Justiz durch eine Rechtsverordnung im Einzelnen vorbereitet.

Die gesetzliche Regelung erlaubt Privatpersonen die Einsicht in das Schuldnerverzeichnis nur für bestimmte Zwecke, die bei einer Anfrage darzulegen sind, zum Beispiel, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Dennoch ist es derzeit vorgesehen, dass bereits nach Eingabe eines Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Bundesland eingerichtet sind, erhielte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner, deren Kenntnis sie zum angestrebten Zweck nicht benötigt.

Es ist zu befürchten, dass beispielsweise Vermieter Mietinteressenten nicht berücksichtigen, weil im Schuldnerverzeichnis namensgleiche Personen stehen und es ihnen zu mühsam oder zu schwierig erscheint, anhand weiterer Angaben zu prüfen, ob es sich beim Mietinteressenten tatsächlich um eine der eingetragenen Personen handelt. Auch aus der Sicht der Gläubiger ist die Anzeige von derart umfangreichen Ergebnislisten wenig hilfreich, denn um den auf die Anfrage bezogenen Datensatz aus der Liste auswählen zu können, müssen ohnehin weitere Daten wie zum Beispiel der Vorname bekannt sein. Da es für Geschäftspartner erforderlich ist, mehr als nur den Nachnamen und den Sitz des zuständigen Vollstreckungsgerichts voneinander zu kennen, ist es auch nicht unangemessen, eine Einsicht von vornherein von weiteren Angaben abhängig zu machen.

Aus Sicht des Datenschutzes ist eine Anzeige von Schuldnerdaten, die nicht vom legitimen Abfragezweck erfasst werden, zu vermeiden. Deshalb halten es die Datenschutzbeauftragten des Bundes und der Länder für notwendig, bei der Regelung der Einsicht in das Schuldnerverzeichnis die zwingende Angabe weiterer Identifizierungsmerkmale vorzusehen.

8.13 Ausweitung des elektronischen Rechtsverkehrs

Spätestens ab 2022 sollen nach einem Regierungsentwurf an allen Gerichten elektronische Dokumente eingereicht werden können und insbesondere Rechtsanwälte und Behörden verpflichtet werden, den elektronischen Zugang zu nutzen. Einige datenschutzrechtliche Fragen sind dabei noch nicht befriedigend geklärt.

Der Grundstein für die Öffnung der Gerichte für die elektronische Kommunikation wurde 2001 mit dem Gesetz zur Anpassung der Formvorschriften an den modernen Rechtsgeschäftsverkehr (BGBl. I S. 1542) gelegt. Bundesregierung und Landesregierungen erhielten die Möglichkeit, in ihren Bereichen elektronische Dokumente zuzulassen, was bisher nicht in allen Ländern und Gerichtszweigen in gleichem Maße genutzt wurde.

Der am 19. Dezember 2012 beschlossene Regierungsentwurf zum elektronischen Rechtsverkehr enthält – abgesehen von der Strafgerichtsbarkeit, für die es einen gesonderten Entwurf gibt – für alle Gerichtsbarkeiten Regelungen, die spätestens bis 2022 bei allen Gerichten elektronische Dokumente zulassen. Ab 2022 wären zudem insbesondere Rechtsanwälte und Behörden verpflichtet, Dokumente ausschließlich elektronisch einzureichen. Privatpersonen bliebe auch künftig die Möglichkeit der Dokumentenvorlage in Papier.

Da im gerichtlichen Verfahren zahlreiche sensible personenbezogene Daten übermittelt werden, darf die Kommunikation zwischen Parteien und Gericht nur auf sichere Weise erfolgen. Dies setzt die Gewährleistung von Authentizität, Integrität und Vertraulichkeit voraus. Authentizität und Integrität der Daten wird in dem Gesetzentwurf Rechnung getragen, während Regelungen zur Vertraulichkeit fehlen. Auch wenn sich die Verpflichtung zur Verschlüsselung aus anderen Regelungen, wie dem Berufsgeheimnis der Rechtsanwälte oder dem Sozial- oder Steuergeheimnis ableiten lässt, hatte ich gegenüber dem Bundesministerium der Justiz (BMJ) die Aufnahme von Regelungen zur Vertraulichkeit empfohlen. Die Empfehlung wurde durch das BMJ nicht umgesetzt. In der überarbeiteten Begründung wird jedoch klargestellt, dass sich die Vertraulichkeit nach den berufs- und datenschutzrechtlichen Bestimmungen richtet.

Ich werde das Gesetzgebungsverfahren weiter begleiten.

8.14 Anti-Doping

Der Datenschutz bei der Bekämpfung des Dopings im Sport ist sowohl auf nationaler als auch auf internationaler Ebene weiterhin ein wichtiges und kontrovers diskutiertes Thema.

Aufgrund aktueller Entwicklungen im internationalen Bereich – zum einen die Bekanntmachung der Welt-Anti-Doping-Agentur (WADA), Anfang 2011 wesentliche Änderungen im Anti-Doping Administration and Management System (ADAMS) (vgl. 22. TB Kasten zu Nr. 5.9) vorgenommen zu haben, zum anderen der Beginn der Überarbeitung des WADA-Codes im Jahr 2012 – wurde die WADA-Subgroup der Artikel-29-Gruppe reaktiviert, an der auch meine Mitarbeiter mitwirken.

Im Februar 2012 hat die Artikel-29-Gruppe zunächst in einem von der WADA-Subgroup vorbereiteten Schreiben an die zuständige EU-Kommissarin die Datenschutzprobleme beim Anti-Doping-System der WADA dargelegt. Die EU-Kommission hatte sich zuvor für Dopingbekämpfung in Übereinstimmung mit dem EU-Recht und unter Wahrung der Grundrechte, darunter auch des Datenschutzes, ausgesprochen. Nach Ansicht der Artikel-29-Gruppe kann die Einwilligung der Sportlerinnen und Sportler in Dopingkontrollen nicht als Rechtsgrundlage für die Verarbeitung ihrer personenbezogenen Daten herangezogen werden. Zudem weist sie darauf hin, dass Datenübermittlungen aus der EU an die ADAMS-Datenbank und eine

Weiterübermittlung der Daten an andere Drittstaaten nur dann erfolgen könnten, wenn in dem jeweiligen Staat ein angemessenes Datenschutzniveau gewährleistet sei oder die Ausnahmetatbestände des Artikel 26 der Datenschutzrichtlinie erfüllt seien. Sehr kritisch sieht die Gruppe weiterhin, dass aufgrund von Dopingverstößen verhängte Strafmaßnahmen im Internet veröffentlicht werden. Dies sei weder erforderlich noch verhältnismäßig. Schließlich fordert sie die WADA auf, die Verhältnismäßigkeit der Erhebung „Whereabouts" (Aufenthaltsdaten zur Ermöglichung von Spontankontrollen) zu überprüfen und zumindest die Speicherzeit dieser Daten zu verkürzen.

Seit Beginn des Jahres 2012 werden nun sowohl der WADA-Code als auch die dazugehörigen Standards, insbesondere auch der International Standard for the Protection of Privacy and Personal Information (ISPPI) überarbeitet. Dies soll Ende 2013 abgeschlossen sein. Im Rahmen des Überarbeitungsprozesses wird die Artikel-29-Gruppe prüfen, ob ihre Kritik aus früheren Stellungnahmen (Working Paper 156 vom 1. August 2008 und Working Paper 162 vom 6. April 2009) in dem Entwurf für eine Überarbeitung der Regelungswerke aufgegriffen wurde, und wird gegebenenfalls verbleibende datenschutzrechtliche Bedenken in einem Brief an die WADA geltend machen.

9 Finanzwesen

9.1 Steuerdaten-CD

Die Diskussion um die Nutzung rechtswidrig erlangter Steuerdaten-CDs dauert an. Ob die Einführung eines Straftatbestands der Datenhehlerei für Abhilfe sorgen kann, erscheint zweifelhaft.

Ohne Zweifel ist der Ankauf im Ausland befindlicher Steuerdaten fiskalisch sehr lukrativ und sorgt für erhebliche Mehreinnahmen des Staates in Zeiten der Finanzkrise. Auch im Hinblick auf den verfassungsrechtlich garantierten Grundsatz der Steuergerechtigkeit sind Ziel und Durchsetzung einer dem Gleichheitssatz des Artikel 3 Absatz 1 GG entsprechenden Besteuerung ein Grund, der auf den ersten Blick für den Ankauf von Steuerdaten-CDs sprechen könnte, da so der Steuerflucht ins Ausland in gewissem Umfang Einhalt geboten und die Steuerhinterziehung effektiv verfolgt werden kann.

Dabei sind aber die Grenzen des Rechtsstaats zu beachten, denn der Staat bedient sich letztlich der Hilfe Krimineller, die die eigentliche Datenerhebung durch „Datendiebstahl" vornehmen. Ich habe bereits mehrfach die Erforderlichkeit einer speziellen Rechtsgrundlage betont, damit die widerstreitenden Interessen und Rechtsgüter in einen angemessenen Ausgleich gebracht werden können (vgl. zuletzt 23. TB Nr. 9.1). Hieran ändert auch nichts, dass die Verwertbarkeit der Steuerdaten-CDs im strafrechtlichen Ermittlungsverfahren vom Bundesverfassungsgericht (Beschluss vom 9. November 2010, 2 BvR 2101/09) und im Besteuerungsverfahren von der Finanzgerichtsbarkeit (FG Köln, Beschluss vom 15. Dezember, 14 V 2484/10; FG Hamburg, Beschluss vom 12. Oktober 2011, 3 V 117/11) grundsätzlich nicht beanstandet wurde. Denn der Ankauf der Steuerdaten-CDs findet nach wie vor in einer rechtlichen Grauzone statt und ist nicht unbeträchtlichen strafrechtlichen Risiken ausgesetzt, wie erst jüngst Haftbefehle aus der Schweiz gegen deutsche Steuerfahnder belegt haben.

Eine höchstrichterliche Klärung dieser Frage fehlt bislang. Die deutschen Instanzgerichte sind bisher davon ausgegangen, dass die betroffenen Finanzbeamten weder deutsches Strafrecht noch Völkerrecht verletzen (vgl. LG Düsseldorf, Beschluss vom 11. Oktober 2010, 4 Qs 50/10; LG Bochum, Beschluss vom 7. August 2009, 2 Qs/09). So soll insbesondere der Ankauf der Daten durch die deutschen Finanzbehörden aufgrund der allgemeinen Ermittlungsbefugnis möglich sein. Eine solche extensive Auslegung dieser Befugnisse ist aus datenschutzrechtlicher Perspektive jedoch problematisch und schafft Raum für behördliche Willkür. Die Heranziehung von allgemeinen Ermittlungsbefugnissen zur Rechtfertigung des Ankaufs der Steuerdaten kann angesichts der schweren Beeinträchtigung vertraulicher personenbezogener Daten nicht überzeugen und würde den Datendiebstahl zwangsläufig bagatellisieren. Rechtsstaatliche Vorgaben und allgemeine Prinzipien des Datenschutzes verlangen, dass der Gesetzgeber bei der Ausgestaltung einer Eingriffsgrundlage den Verwendungszweck bereichsspezifisch und präzise bestimmt und die Daten für diesen Zweck geeignet und erforderlich sind (BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209/83 u. a.).

Die momentan erwogene Ergänzung des Strafgesetzbuches um einen Tatbestand der Datenhehlerei (§ 259a StGB-E) in der Fassung, die der hessische Justizminister vorgeschlagen hat, überzeugt mich aber nicht. Zwar ist es aus datenschutzpolitischer Sicht durchaus zu begrüßen, den strafrechtlichen Schutz rechtswidrig erlangter personenbezogener Daten wie auch anderer Daten (z. B. Passwörter oder sonstige Sicherungscodes) zu verbessern und im Strafgesetzbuch eine zentrale ergänzende Norm zu schaffen. Eine auch im allgemeinen Strafrecht verankerte Strafbarkeit des Ankaufs und Erwerbs illegal erhobener Daten kann daher neben den bisher schon bestehenden Regelungen (§§ 43, 44 BDSG) sinnvoll sein. Für schwer vermittelbar halte ich es aber, dass staatliches Handeln vom Tatbestand der Datenhehlerei ausgenommen werden soll – eine Lex Steuer-CD?

9.2 Steueridentifikationsnummer

In Bestrebungen, den Anwendungsbereich der Steueridentifikationsnummer (Steuer-ID) weiter auszudehnen, sehe ich die Gefahr, dass diese sich doch zu einem verfassungswidrigen allgemeinen Personenkennzeichen entwickelt.

Immer wieder habe ich mich in früheren Tätigkeitsberichten mit der datenschutzrechtlichen Problematik der Steueridentifikationsnummer (Steuer-ID) auseinandersetzen müssen (vgl. zuletzt 23. TB Nr. 9.2). Auch jetzt besteht wieder Veranlassung dazu. Die Steuer-ID dient der ein-

deutigen Identifizierung der Steuerpflichtigen im Besteuerungsverfahren. Vor dem Hintergrund der stetig zunehmenden elektronischen Übermittlung von steuerlichen Daten an die Finanzverwaltung soll sie die unverwechselbare Zuordnung dieser Daten zu einer bestimmten Person ermöglichen (z. B. bei Rentenbezugsmitteilungen oder Kontrollmitteilungsverfahren). Ziel ist die Gewährleistung einer gleichmäßigen Besteuerung und die Verhinderung etwaigen Missbrauchs.

In diesem Zusammenhang hat der Bundesfinanzhof die Steuer-ID als verfassungsgemäß eingestuft, da das Interesse der Allgemeinheit an einer gleichmäßigen Besteuerung den Eingriff in das Recht auf informationelle Selbstbestimmung rechtfertige (BFH, Urteil vom 18. Januar 2012, II R 49/10), wobei aber der strikte Grundsatz der Zweckbindung und die Erforderlichkeit beachtet werden müssten. Dem Gesetzgeber steht es daher nicht frei, den Einsatz der Steuer-ID beliebig zu erweitern, da sich aus den datenschutzrechtlichen Anforderungen, die auch in § 139b Absatz 2 bis 5 Abgabenordnung bereichsspezifisch verankert wurden, strikte Grenzen ergeben.

Doch schon jetzt können andere Stellen wie Arbeitgeber, Rentenversicherungsträger, Träger der Sozialleistungen, Krankenkassen, Kreditinstitute und Kindergeldkassen die Steuer-ID in – allerdings eng umgrenzten – Fällen verwenden. Ich werde mich auch weiterhin gegen die weitere Ausdehnung des Verwendungsbereichs der Steuer-ID einsetzen. Immerhin habe ich unlängst gemeinsam mit dem Bundesministerium der Justiz erreichen können, dass in einen Referentenentwurf des Bundesministeriums der Finanzen für eine Verordnung zum Erlass und zur Änderung steuerlicher Verordnungen die Verwendung der Steuer-ID mangels Erforderlichkeit doch nicht aufgenommen wurde.

Neuvergabe der Steuer-ID bei Adoptionen und Zeugenschutzprogrammen

Nach der bisherigen Gesetzeslage soll die Steuer-ID für jede natürliche Person nur einmal vergeben werden, um so eine hinreichende Beständigkeit und Eindeutigkeit der Zuordnung zu gewährleisten. Dieser Grundsatz ist zwar durchaus sinnvoll, er kann in bestimmten Fällen aber auch erhebliche Risiken bergen, sofern in Ausnahmekonstellationen nicht von ihm abgewichen werden kann. Gerade bei Adoptionen oder Transsexuellen oder Personen, die dem Zeugenschutz unterfallen wäre eine Rückverfolgbarkeit zur alten Identität aufgrund der weiter bestehenden Steuer-ID grundsätzlich möglich. Dies widerspricht aber dem besonderen Schutz dieser sensiblen Daten, wie er etwa im BDSG, im Zeugenschutz-Harmonisierungsgesetz, im Transsexuellengesetz und auch durch das Adoptionsgeheimnis gewährleistet wird.

Das Recht auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 Grundgesetz (GG) enthält auch das Recht des selbst gesteuerten Identitätsmanagements. Bei Sachverhalten, die durch eine besondere Schutzbedürftigkeit der jeweiligen personenbezogenen Daten gekennzeichnet sind, können weitere Verfassungswerte (Adoption – Artikel 6 GG; Zeugenschutz – Artikel 2 Absatz 2 GG) den Schutzanspruch erhöhen, sodass angemessene gesetzgeberische Maßnahmen zu treffen sind. Die lebenslange Beibehaltung der gleichen Steuer-ID kann in den vorstehend geschilderten Sachverhalten zu empfindlichen Schutzeinbußen führen, vor allem da eine weitreichende Streuung und Nutzung der Steuer-ID alles andere als ausgeschlossen ist. Gerade eine solche Rekonstruktion soll aber in Fällen der berechtigten Änderung von Identitätsmerkmalen nicht möglich sein, wie sich eindeutig aus den gesetzlichen Wertungen ergibt. Dementsprechend erachte ich es in den vorgenannten Fällen (Adoption, Transsexuelle, Zeugenschutz) für geboten, eine mögliche Neuvergabe der Steuer-ID gesetzlich zu verankern.

Steuer-ID: Keine Löschung unter dieser Nummer?

Die Löschung einer irrtümlich vergebenen Steuer-ID erweist sich momentan noch als unnötig schwierig. Ein Petent, der seit 1997 ausschließlich die französische Staatsangehörigkeit besitzt, bat mich, für ihn die Löschung der Steuer-ID beim Bundeszentralamt für Steuern (BZSt) durchzusetzen. Dem Petenten war auf Hinweis seiner Krankenversicherung vom BZSt irrtümlich eine Steuer-ID zugeteilt worden, obwohl er nicht mehr in Deutschland steuerlich geführt wurde und eine Steuer-ID dementsprechend auch nicht hätte vergeben werden dürfen.

Ich habe daher das BZSt darum gebeten, eine Löschung dieser Steuer-ID vorzunehmen und den Petenten hierüber zu informieren. Zwar hat das BZSt dies zugesagt, aber gleichzeitig darauf verwiesen, eine Löschung sei momentan noch nicht möglich, da sich ein entsprechendes Verfahren erst in der Vorbereitung befinde. Wie § 20 Absatz 2 Nummer 1 BDSG unmissverständlich vorgibt, sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist. Um eine Umsetzung dieser Verpflichtung zu gewährleisten, ist die jeweilige verantwortliche Stelle gehalten, entsprechende Verfahren vorzuhalten. Diese technischen und organisatorischen Maßnahmen sind erforderlich, um eine gesetzeskonforme Durchsetzung des Datenschutzes zu gewährleisten. Eine endgültige Antwort des BZSt zur Löschung der Steuer-ID steht noch aus. Ich werde das Verfahren weiterhin kritisch begleiten.

9.3 Jahressteuergesetz 2013 – Kirchensteuerabzug nicht datenschutzkonform

Das automatisierte Verfahren für den Kirchensteuerabzug auf Kapitalerträge ist auch in seiner derzeitigen Ausgestaltung datenschutzrechtlich problematisch.

In meinem 23. TB (Nr. 9.5) habe ich Mängel des automatisierten Verfahrens für den Kirchensteuerabzug auf Kapitalerträge eingehend dargestellt. Da es sich bei der Religionszugehörigkeit um ein besonders sensibles persönliches Merkmal handelt (vgl. § 3 Absatz 9 BDSG), sind auch entsprechend hohe datenschutzrechtliche Anforderungen an den Umgang damit zu stellen.

Im Rahmen der Beratungen des Entwurfes des Jahressteuergesetzes 2013 habe ich darauf hingewiesen, dass die vorgesehene Regelung (vgl. § 51a Absatz 2c und 2e Einkommensteuergesetz – EStG) nicht den datenschutzrechtlichen Anforderungen im Umgang mit den besonders sensiblen personenbezogenen Merkmalen der Religionszugehörigkeit gerecht wird. So hat nach § 51a Absatz 2c Nummer 3 EStG der Kirchensteuerabzugsverpflichtete unter Angabe der Steueridentifikationsnummer (Steuer-ID) des Schuldners der Kapitalertragsteuer einmal jährlich im Zeitraum vom 1. September bis 31. Oktober beim Bundeszentralamt für Steuern (BZSt) anzufragen, ob der Betroffene am 31. August des betreffenden Jahres (Stichtag) kirchensteuerpflichtig war (Regelabfrage). Da die Regelabfrage nur für den Zeitraum vom 1. September bis 31. Oktober vorgesehen ist, wird eine Änderung (z. B. Kirchenaustritt), die danach eintritt, nicht erfasst. Es wird weiterhin ein Kirchensteuerabzug vorgenommen und die steuerliche Belastung dauert somit fort. Auch besteht nicht die Möglichkeit der Anlassabfrage, denn diese ist nach § 51a Absatz 2c Nummer 3 Satz 3 EStG nicht für alle die Religionszugehörigkeit betreffenden Änderungen vorgesehen, sondern nur für Kapitalerträge (vgl. § 51a Absatz 2c Nummer 3 Satz 2 EStG).

Die Regelung berücksichtigt damit nicht ausreichend die höchstpersönliche Entscheidung des Steuerpflichtigen. So hat es bereits das Bundesverfassungsgericht für verfassungswidrig erachtet, wenn im Falle eines Kirchenaustritts der Steuerpflichtige noch bis zum Ende des laufenden Steuerjahres zur Kirchensteuer herangezogen wird (vgl. BVerfG, Beschluss vom 8. Februar 1977, 1 BvR 329/71). Diese Wertung ist auf den vorliegenden Sachverhalt übertragbar, sodass hier dringender Anpassungsbedarf besteht. Der bloße Verweis auf die Einkommenssteuererklärung reicht nicht aus, um einen ausreichenden Schutz zu gewährleisten.

Ich werde das zum Redaktionsschluss noch nicht abgeschlossene Gesetzgebungsverfahren zum Jahressteuergesetz 2013 weiterhin kritisch begleiten und darauf drängen, dass das automatisierte Verfahren für den Kirchensteuerabzug datenschutzkonform ausgestaltet wird.

9.4 Darf ich Steuerakten nur im Finanzamt prüfen?

Die Finanzverwaltung darf mein Prüfungsrecht nicht auf Einsichtnahme vor Ort beschränken – Grund für eine Beanstandung.

Aufgrund einer Eingabe habe ich unter Hinweis auf meine Kontroll- und Prüfbefugnisse nach § 24 Absatz 1 i. V. m. Absatz 4 BDSG eine Familienkasse der Bundesagentur für Arbeit (BA) um Übersendung einer Kindergeldakte zur Prüfung gebeten. Die mit der Gewährung des Kindergeldes nach dem Einkommensteuergesetz (EStG) betraute Familienkasse der BA lehnt dies auf Weisung des Bundesministeriums für Finanzen (BMF) bis heute ab. Es bestehe lediglich ein Anspruch auf Akteneinsicht vor Ort, nicht aber auf Übersendung der konkreten Akte. Wegen eines finanzgerichtlichen Verfahrens könne meiner Bitte aber auch tatsächlich nicht nachgekommen werden.

Ich habe deshalb eine Verletzung meiner Kontroll- und Prüfbefugnisse nach § 24 Absatz 1 i. V. m. Absatz 4 BDSG nach § 25 Absatz 1 Nummer 1 BDSG beanstandet. Denn es besteht eine umfassende Unterstützungspflicht der zu kontrollierenden öffentlichen Stellen, um eine effektive Kontrolle im Interesse des Schutzes des betroffenen Bürgers zu ermöglichen. Diese Unterstützungspflicht schließt auch die konkrete Durchführung mit ein, die meinem Ermessen obliegt.

Auch nach der Beanstandung habe ich das BMF wiederholt zur kurzfristigen Vorlage der bei der Familienkasse der BA geführten vollständigen Kindergeldakte auffordern müssen. Sollte die Akte der Familienkasse weiterhin aufgrund der benannten finanzgerichtlichen Auseinandersetzung nicht verfügbar sein, besteht für die Beteiligten nach § 78 Absatz 1 Finanzgerichtsordnung (FGO) ein Akteneinsichtsrecht sowie nach § 78 Absatz 2 FGO ein Recht auf Erteilung von Abschriften und daher die Möglichkeit, mir den betreffenden Akteninhalt zukommen zu lassen. Im Interesse der Petentin habe ich anlässlich einer Kontrolle bei der entsprechenden Familienkasse der BA die Kopie der Kindergeldakte vor Ort eingesehen.

Eine dem § 24 Absatz 1 i. V. m. Absatz 4 BDSG entsprechende Wahrung meines Einsichtsrechts werde ich aber weiterhin beim BMF einfordern.

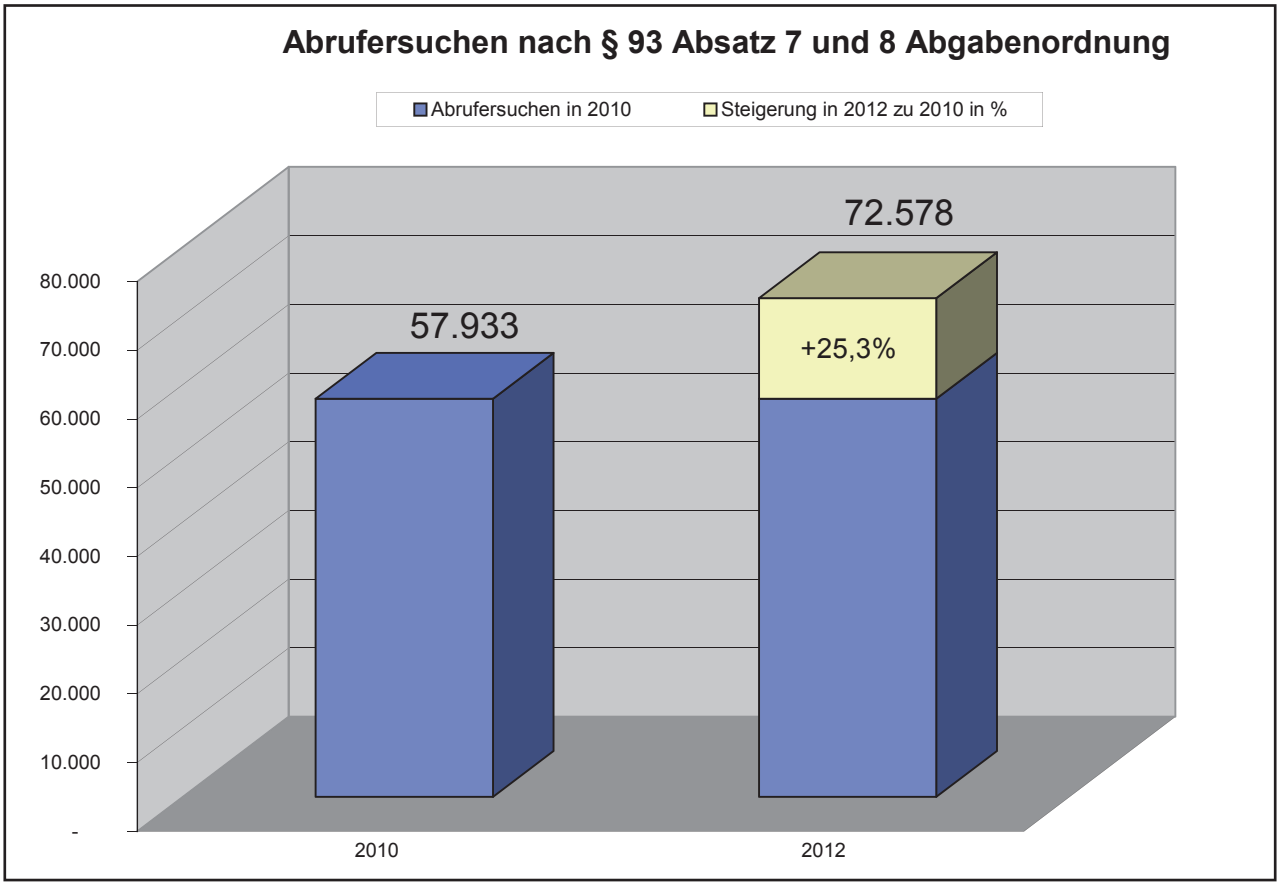
9.5 Immer mehr Kontenabrufe

Das automatisierte Kontenabrufverfahren wird ständig erweitert. Dies betrifft den Kreis der Abrufberechtigten ebenso wie die Anzahl der getätigten Anfragen. Dies steht mit der ursprünglichen Absicht des Gesetzgebers nicht in Einklang.

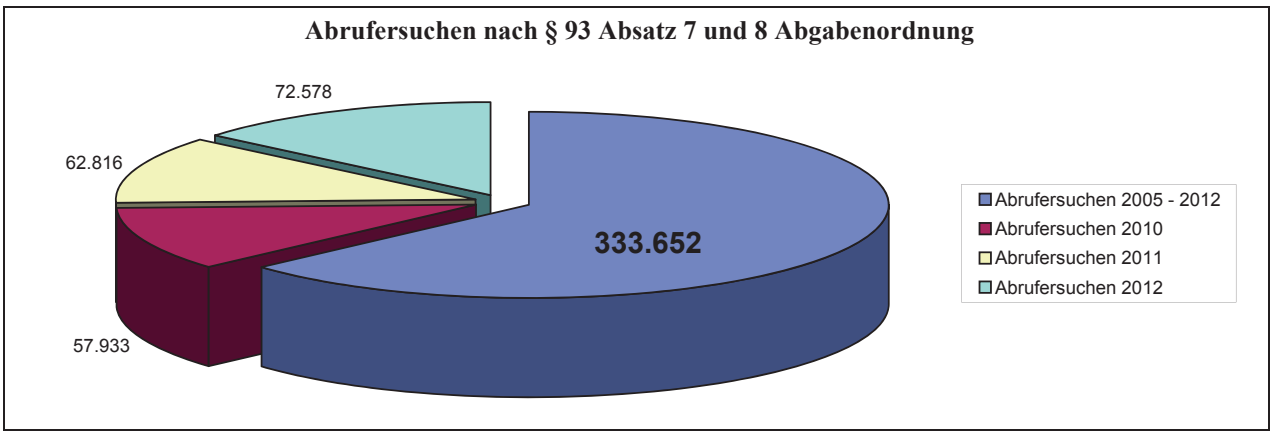
Die Nutzung des automatisierten Kontenabrufverfahrens nach § 93 Absatz 7 und 8 i. V. m. § 93b Abgabenordnung (AO) nimmt stetig zu, wie ein Blick auf die Statistiken des Bundeszentralamts für Steuern (BZSt) zeigt. Lag im Jahr 2010 die Anzahl der Kontenabrufe noch bei 57 933, waren es im Jahr 2012 bereits 72 578 Kontenabrufe, das entspricht einer Zunahme um ein Viertel im Berichtszeitraum. Insgesamt wurden seit Beginn des Kontenabrufverfahrens im Jahr 2005 bis zum 31. Dezember 2012 333 652 Kontenabrufe verzeichnet (vgl. Kasten a und b zu Nr. 9.5).

Auch der Kreis der Berechtigten, die eine Abfrage von Bankkundendaten vornehmen können, ist in den letzten Jahren zunehmend erweitert worden. Mittlerweile können etwa die Gemeinden in den Fällen des § 1 Absatz 2 AO die Kontenabfrage ebenso nutzen wie die Behörden, die zuständig sind für Grundsicherung für Arbeitssuchende nach dem SGB II, für Sozialhilfe nach dem SGB XII, für Ausbildungsförderung nach dem Bundesausbildungsförderungsgesetz, für Aufstiegsfortbildungsförderung nach dem Aufstiegsfortbildungsförderungsgesetz und für Wohngeld nach dem Wohngeldgesetz. Der Gesetzgeber hat mit

Kasten a zu Nr. 9.5



Kasten b zu Nr. 9.5



§ 93 Absatz 8 Satz 2 AO eine weitere Öffnungsklausel geschaffen, wonach ein Kontenabruf in anderen Fällen erfolgen darf, wenn dies durch Bundesgesetz ausdrücklich zugelassen ist, sodass ab dem 1. Januar 2013 auch Gerichtsvollzieher ein Ersuchen stellen können (vgl. § 802l Zivilprozessordnung). Es ist daher zu erwarten, dass auch andere öffentliche Stellen bald ihr Interesse anmelden werden.

Diese Ausdehnung ist schon deswegen kritisch zu sehen, weil die Zugriffsmöglichkeiten ursprünglich für die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und die Strafverfolgungsbehörden vor dem Hintergrund der Bekämpfung der Terrorismusfinanzierung geschaffen worden sind. Ursprünglich verfolgtes Ziel war die Austrocknung der Finanzströme des Terrorismus. Die nunmehr verfolgten Zwecke stehen hiermit in keiner Verbindung und sind in ihrer Wertigkeit auch nicht mit der Terrorismusbekämpfung gleichzusetzen. Wenn bereits zum Zeitpunkt der Kontoeröffnung die Kontostammdaten automatisch als Datensatz gespeichert und dieser durch das Kontenabrufverfahren verfügbar gemacht werden kann, erfolgt letztlich eine anlasslose Erfassung grundsätzlich aller Kontoinhaber in Deutschland. Da somit der Datensatz bereits vorliegt, obwohl noch keine Erklärungspflicht des Steuerpflichtigen besteht, ist von einer erheblichen Eingriffsintensität auszugehen, die weit über die ursprünglichen Absichten des Gesetzgebers hinaus das Recht auf informationelle Selbstbestimmung tangiert.

9.6 Datenpannen bei der Finanzagentur

Die Finanzagentur versandte fast 12 000 fehlerhafte Jahreskontoauszüge von Gemeinschaftskonten. Mindestens 169 Jahreskontoauszüge inkl. der Jahressteuerbescheinigungen 2011 gingen auf dem Postweg verloren.

Das Bundesministerium der Finanzen (BMF) als Fachaufsicht und die Bundesrepublik Deutschland Finanzagentur GmbH (Finanzagentur) unterrichteten mich darüber, dass ihnen aufgrund von Kundenrückmeldungen zu bei der Finanzagentur geführten Gemeinschaftskonten 11 965 Fälle bekannt geworden seien, in denen Jahreskontoauszüge 2011 mit falsch ausgewiesener Eigentumsquote zugesandt bzw. Eigentumsquoten auf den Jahreskontoauszug anderer Kunden gedruckt worden waren.

Die Finanzagentur will als Konsequenz ihre internen Richtlinien dahingehend ändern, dass neue Komponenten in ihren IT-Systemen besser getestet, interne Zuständigkeiten neu geordnet und zusätzliche Kontrollen eingeführt werden. Die Empfänger der fehlerhaften Jahreskontoauszüge wurden von der Finanzagentur inzwischen über den Fehler aufgeklärt und um Vernichtung des fehlerhaften Jahreskontoauszugs bzw. um Rücksendung in einem beigelegten Rückumschlag an die Finanzagentur gebeten.

Wie mich die Finanzagentur weiter informierte, haben sich bei ihr bis Ende August 2012 169 Kunden gemeldet, die keinen Jahreskontoauszug 2011 erhalten hatten. Es sei deshalb davon auszugehen, dass jedenfalls in den gemeldeten Fällen versandte Jahreskontoauszüge inkl. der Jahressteuerbescheinigungen 2011 auf dem Postweg verloren gegangen sind. Der Finanzagentur liegen keine Hinweise vor, die verlorenen Sendungen könnten in die Hände Dritter gelangt sein. Sie gibt die gedruckten und kuvertierten Briefsendungen an ihren Postdienstleister, der die weitere Verteilung der Sendungen über seine Briefzentren veranlasst. In einer Vielzahl der bekannten Verlustfälle haben die Empfänger außerhalb von dessen Einzugsbereich gewohnt. Dieser habe die Briefe deswegen an einen anderen Postdienstleister weitergereicht. Weitergehende Nachforschungen bei dem anderen Postdienstleister seien nicht möglich, da die Sendungen als Standardbriefe versandt worden seien. Im Rahmen der Neuausschreibung der Postdienstleistung will die Finanzagentur zur Minimierung von Zustellungsverlusten die Qualitätsanforderungen an die Ausschreibungsteilnehmer weiter präzisieren.

Das BMF und die Finanzagentur haben mich in den geschilderten Fällen aktiv informiert und meine Rückfragen zeitnah und umfassend beantwortet. Aufgrund der geführten Gespräche und der Stellungnahmen kann davon ausgegangen werden, dass die Finanzagentur in Abstimmung mit mir und ihrer Fachaufsicht das jeweils Erforderliche zur Schadensbegrenzung getan und geeignete Konsequenzen gezogen hat, um weitere Falschversendungen zu unterbinden. Aus den genannten Gründen habe ich in den geschilderten Fällen von einer formellen Beanstandung nach § 25 BDSG abgesehen. Ich werde das Verfahren weiterhin kritisch begleiten.

9.7 Zoll im Reality-TV?

Die Kontrolleinheit Verkehrswege (KEV) eines Hauptzollamtes (HZA) hat mehrere von einem Fernsehsender ausgestrahlte Produktionen einer Reality-TV-Sendung unterstützt, ohne den Schutz der Persönlichkeitsrechte der Betroffenen sicherzustellen.

Ein Petent machte mich auf mehrere von einem Fernsehsender ausgestrahlte Beiträge einer Reality-TV-Sendung aufmerksam, die mit Unterstützung der KEV eines HZA produziert worden waren und in denen es um Zigaretten- und Rauschgiftschmuggel sowie um Fälle mit waffenrechtlichem Hintergrund ging. Dabei wurden die betroffenen Privatpersonen in negativen Situationen – wenn auch verfremdet – dargestellt. Die Drehgenehmigungen wurden der Produktionsfirma von der dem HZA vorgesetzten Bundesfinanzdirektion (BFD) unter Hinweis auf datenschutzrechtliche Vorschriften und die Persönlichkeitsrechte der Betroffenen erteilt. Soweit Bild- und Tonaufnahmen von Zollbeamten/innen oder beteiligten Dritten gemacht würden, sei zur Wahrung der Persönlichkeitsrechte deren vorherige Zustimmung einzuholen. Hinweise, die eine Identifizierung von Personen ermöglichten, seien auf geeignete Weise (z. B. Pixeln) zu anonymisieren.

Die Datenschutzbeauftragten des Bundes und der Länder hatten auf ihrer 78. Konferenz am 8./9. Oktober 2009 die Mitwirkung von Behörden an „Reality-TV“-Reportagen nicht vollständig abgelehnt, jedoch von der Erfüllung der in der Erklärung genannten Grundsätze zum Schutz der Persönlichkeitsrechte der Betroffenen abhängig gemacht

(vgl. Kasten zu Nr. 9.7). Ich habe deshalb anlässlich der Eingabe dem Bundesministerium der Finanzen (BMF) als Fachaufsichtsbehörde nahegelegt, den Betroffenen die für die Sendung abschließend bearbeiteten Aufnahmen zur Freigabe zur Kenntnis zu geben. Ein derartiges Verfahren könnte sich an die gängige Praxis der Autorisierung von Interviews anlehnen. Das BMF hat die BFD daraufhin angewiesen, Dreharbeiten in Reality-TV/Dokutainment-Formaten künftig nur noch bei Vorliegen einer vorab erteilten, schriftlich dokumentierten Einwilligung zuzulassen. Aber auch ein solches Verfahren dürfte aufgrund der bei den Dreharbeiten gegebenen Überraschungssituationen keinen wirksamen Schutz der Persönlichkeitsrechte der betroffenen Privatpersonen garantieren. Denn in was sollte ein Betroffener angesichts der ihn erwartenden Unvorhersehbarkeiten im Voraus einwilligen?

Auf meine Intervention hin hat das BMF schließlich entschieden, dass die Zollverwaltung unabhängig von den rechtlichen Hintergründen die Mitwirkung an Dreharbeiten in Reality-TV/Dokutainment und ähnlichen Formaten bis auf weiteres aussetzen werde. Meine Zweifel, dass bei den betroffenen Privatpersonen der Schutz der Persönlichkeitsrechte gewährleistet ist, konnten bislang nicht ausgeräumt werden. Ich werde die weitere Entwicklung aufmerksam verfolgen.

Kasten zu Nr. 9.7

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009

„Reality-TV“ – keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

„Reality-TV“-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige „Lieferanten“ für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen Haftbefehl gegen einen Schuldner zu vollziehen – wobei auch schon einmal eine Wohnung zwangsgeöffnet wird – oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mitverfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleiben oder gar ausfällig werden. Aufgrund des Erfolgs derartiger „Unterhaltungssendungen“ ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

Presse- und Öffentlichkeitsarbeit sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und den Informationsanspruch der Öffentlichkeit zu erfüllen. Dabei muss aber das Persönlichkeitsrecht der Betroffenen gewahrt werden, gerade wenn Unterhaltung und Befriedigung von Sensationslust im Vordergrund stehen.

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit ihrer Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb alle Behörden auf, grundsätzlich von der Mitwirkung an solchen „Reality“-Reportagen Abstand zu nehmen.

10 Wirtschaft und Verkehr

10.1 Smarte Stromzähler nur mit intelligentem Datenschutz

Für den Einsatz „intelligenter“ digitaler Stromzähler sind datenschutzgerechte Lösungen in Sicht. Der durch das Energiewirtschaftsgesetz vorgegebene Rahmen bedarf noch der Konkretisierung durch eine Rechtsverordnung.

Die Energiewende ist eine große ökonomische und ökologische Herausforderung. Durch den Einsatz intelligenter Messeinrichtungen (Smart Meter) wird sie auch zum Datenschutzthema. Aus den Verbrauchsdaten können Rückschlüsse auf die Lebensgewohnheiten der Nutzer gezogen werden. Deswegen setze ich mich für Lösungen ein, die – ohne Abstriche an der Funktionalität – auch dem Recht auf informationelle Selbstbestimmung der Nutzer Rechnung tragen.

Energiewirtschaftsgesetz

Zu den datenschutzrechtlichen Herausforderungen, die der Einsatz von Smart Metern für alle Beteiligten mit sich bringt, habe ich bereits berichtet (vgl. 23. TB Nr. 5.1). Die Novellierung des Energiewirtschaftsgesetzes (EnWG) im Juni 2011 war ein erster großer Schritt. Die Datenschutzregelungen im EnWG sehen eine enge Zweckbindung für den Umgang mit sensiblen Verbrauchsdaten sowie verbindliche Standards für die Datensicherheit vor. Ich konnte erreichen, dass § 21g EnWG einen abschließenden Katalog vorgibt, für welche Zwecke die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig ist. § 21g EnWG legt fest, welche Stellen zur Verwendung der Daten berechtigt sind und stellt klar, dass datenschutzrechtliche Grundsätze wie Datenvermeidung und Datensparsamkeit auch für den Umgang mit personenbezogenen Daten mit Hilfe intelligenter Messsysteme gelten.

Das EnWG gibt jedoch nur die datenschutzrechtlichen Rahmenbedingungen vor. Die konkrete Ausgestaltung ist in einer Rechtsverordnung zu regeln. Ich hoffe, dass es auch hier gelingen wird, datenschutzrechtliche Belange angemessen zu berücksichtigen.

Orientierungshilfe zum datenschutzgerechten Smart Metering

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Juni 2012 eine Entschließung und eine ergänzende Orientierungshilfe mit Hinweisen zum datenschutzgerechten Smart Metering verabschiedet (vgl. Kasten zu Nr. 10.1). Diese soll unter anderem dem Gesetzgeber bei der Erarbeitung der Rechtsverordnung Hilfestellung geben. Die Orientierungshilfe gibt Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering. Anhand so genannter Use Cases (Anwendungsfälle) wird beschrieben, wie die zentralen Forderungen des Datenschutzes nach Zweckbindung, Datensparsamkeit und Erforderlichkeit in der Praxis umgesetzt werden können.

Nicht nur in Deutschland wird über die Anforderungen an den Datenschutz diskutiert, die bei der Einführung intelligenter Energienetze und -zähler zu beachten sind. Im März 2012 hat die Europäische Kommission „Empfehlungen zu Vorbereitungen für die Einführung intelligenter Messsysteme“ (Com(2012) 1342 final) herausgegeben. Darin fordert sie, den Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten durch intelligente Messsysteme in vollem Umfang zu gewährleisten. Daneben hat die Kommission das Mandat der von ihr Ende 2009 eingesetzten Task Force „Smart Grids“ verlängert. Das Arbeitsprogramm der Expertengruppe 2 der Task Force für das Jahr 2012 sieht unter anderem die Entwicklung eines Data Protection Impact Assessments (DPIA) für Smart Grids vor – eine Datenschutzfolgenabschätzung für intelligente Netze.

Die Artikel-29-Gruppe nimmt, vertreten durch die Kollegen aus Frankreich, dem Vereinigten Königreich sowie dem Europäischen Datenschutzbeauftragten, als Beobachter an den Sitzungen der Expertengruppe teil und wird sich nach Fertigstellung der finalen Version des DPIA dazu äußern. Die Stellungnahme wird die Technology Subgroup unter meiner Leitung erarbeiten (vgl. hierzu Nr. 2.4.1.2).

Kasten zu Nr. 10.1

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juni 2012

Orientierungshilfe zum datenschutzgerechten Smart Metering

Intelligente Energienetze und -zähler sind ein zentraler Baustein zur Sicherstellung einer nachhaltigen Energieversorgung im Sinne einer ressourcenschonenden, umweltfreundlichen und effizienten Produktion, Verteilung und Nutzung von Energie. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe beschlossen, die Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering enthält. Kernstück der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung sog. Use Cases, d. h. Anwendungsfälle, für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, dass insbesondere folgende Punkte beachtet werden:

- Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.
- Die Ableseintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.
- Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.
- Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.
- Die Daten sollen an möglichst wenige Stellen übermittelt werden.
- Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.
- Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein. Er muss Zugriffe auf den Smart Meter erkennen und dies im Zweifel unterbinden können.
- Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.
- Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.
- Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI.
- Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

10.2 Speicherfristen für bonitätsbezogene Daten bei Wirtschaftsauskunfteien

Der Petitionsausschuss des Deutschen Bundestages hat empfohlen, die geltende Rechtslage für Speicherfristen bonitätsbezogener Daten bei Wirtschaftsauskunfteien zu ändern und diese tagesaktuell zu halten. Für die zügige Umsetzung dieses Vorschlags setze ich mich ein.

Wer ein Privatinsolvenzverfahren durchläuft, hat es in der Regel schwer, einen Kredit oder auch nur einen Handyvertrag zu bekommen – jedenfalls zu erschwinglichen Konditionen. Daran ändert auch die Erteilung der Restschuldbefreiung vorerst nichts, weil die Tatsache der Restschuldbefreiung von Wirtschaftsauskunfteien gespeichert und an die angeschlossenen Unternehmen gemeldet wird. Das Gesetz verpflichtet die Auskunfteien lediglich dazu, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung der Restschuldbefreiung folgt, die Erforderlichkeit der weiteren Speicherung zu prüfen (§ 35 Absatz 2 Satz 2 Nummer 4 BDSG).

Besonders ärgerlich wird es für die Betroffenen, wenn das Amtsgericht die Restschuldbefreiung zu Beginn eines Kalenderjahres erteilt. Denn das gesamte laufende Jahr wird nicht in die Fristberechnung einbezogen, weil die dreijährige Prüffrist des § 35 Absatz 2 Satz 2 Nummer 4 BDSG erst im folgenden Kalenderjahr beginnt. Der Betroffene ist in diesem Fall also um ein ganzes Jahr schlechter gestellt als ein Betroffener, dem die Restschuldbefreiung im Dezember des Vorjahres erteilt worden ist – auch wenn zwischen beiden Restschuldbefreiungen nur wenige Tage liegen. Auf den Zeitpunkt der Restschuldbefreiung hat der Betroffene nur geringen Einfluss, weil dieser auch von der jeweiligen Arbeitsbelastung der zuständigen Gerichte abhängt.

Der Petitionsausschuss des Deutschen Bundestages hat Bedenken an der geltenden Rechtslage im Hinblick auf das allgemeine Gleichbehandlungsgebot in Artikel 3 Grundgesetz geäußert: Da das BDSG eine taggenaue Löschung des Eintrags über die Erteilung der Restschuldbefreiung nach Ablauf von drei Jahren nicht vorsehe, sondern die dreijährige Überprüfungsfrist zur weiteren Speicherung erst am 1. Januar des der erstmaligen Speicherung folgenden Kalenderjahres beginne, hänge es von dem Datum der Restschuldbefreiung ab, ob jemand genau drei Jahre, drei Jahre und beispielsweise sechs Monate oder drei Jahre und elfeinhalb Monate lang mit dem Negativvermerk im Auskunfteidatenbestand gespeichert sei.

Das Petitum des Ausschusses, die Fristenregelung des § 35 Absatz 2 Satz 2 Nummer 4 BDSG zu überdenken, unterstütze ich nachdrücklich. Ich habe mich an das Bundesministerium des Innern (BMI) gewandt und mich für eine taggenau berechnete Speicherfrist, die mit dem Tag der Erteilung der Restschuldbefreiung beginnt, ausgesprochen. Nur ein solcher Gleichlauf der Speicherfristen führt zu der gebotenen Gleichstellung aller Betroffenen. Die Speicherdauer von Insolvenzdaten bei Auskunfteien darf insbesondere nicht davon abhängen, ob der Betroffene seinen Wohnsitz zufällig in einem Amtsgerichtsbezirk mit hoher Auslastung oder einem mit niedrigerer Arbeitsintensität hat.

Gegenüber dem Bundesministerium der Justiz habe ich angeregt, eine stärker fristenorientierte Entscheidung der Insolvenzgerichte über die Erteilung der Restschuldbefreiung bei Verbraucherinsolvenzen vorzusehen, um Verzögerungen bei der Erteilung der Restschuldbefreiung durch die Amtsgerichte weitgehend auszuschließen.

Das BMI hat sowohl dem Petitionsausschuss des Deutschen Bundestages als auch mir mitgeteilt, dass es keine Gründe sehe, an der bisherigen Fristenregelung festzuhalten und in Aussicht gestellt, eine Änderung des § 35 BDSG im Kontext eines bereits laufenden Gesetzgebungsverfahrens herbeizuführen.

10.3 Aus dem Düsseldorfer Kreis

Der Düsseldorfer Kreis wird auch nach seiner Eingliederung in die Organisationsstruktur der Datenschutzkonferenz auf die bundesweit einheitliche Auslegung des Datenschutzrechts im nicht-öffentlichen Bereich hinwirken.

In meinem letzten Tätigkeitsbericht hatte ich die Erwartung geäußert (vgl. 23. TB Nr. 10.4), die weitgehende Zusammenlegung der Datenschutzaufsicht im öffentlichen und nicht-öffentlichen Bereich auf Landesebene werde Änderungen in den bundesweiten Koordinierungsstrukturen nach sich ziehen. Dies hat sich als zutreffend erwiesen.

Mittlerweile ist der Düsseldorfer Kreis, vormals oberstes Abstimmungsgremium der Aufsichtsbehörden im nicht-öffentlichen Bereich, in die Datenschutzkonferenz integriert. Ich begrüße diese Neustrukturierung, weil sie zu einer Verschlankung der Arbeitsstrukturen auf bundesweiter Ebene führt, ohne dass der Name „Düsseldorfer Kreis“ als Markenzeichen aufgegeben wird. Erhebliche Entlastungseffekte verspreche ich mir durch die Zusammenlegung zahlreicher Arbeitsgruppen des Düsseldorfer Kreises mit Arbeitskreisen der Datenschutzkonferenz.

Als Arbeitskreis der Datenschutzkonferenz trägt der Düsseldorfer Kreis innerhalb seines weitgehend unveränderten Aufgabenfeldes weiterhin zur bundesweit einheitlichen Auslegung des Datenschutzrechts im nicht-öffentlichen Bereich bei. Als einziger Konferenz-Arbeitskreis kann er Beschlüsse fassen und nach außen vertreten, sofern es um einheitliche Rechtsanwendung geht. Datenschutzpolitische Entscheidungen obliegen aber allein der übergeordneten Datenschutzkonferenz.

Den Entschluss, neben dem Bundesministerium des Innern auch einen Vertreter der Innenministerien der Bundesländer mit einem Gaststatus im Düsseldorfer Kreis zu versehen, sehe ich positiv. Hierdurch wird der Informationsaustausch zwischen den Datenschutzbehörden und den Innenressorts des Bundes und der Länder weiter optimiert.

Deutlicher als in den Vorjahren hat sich die internetbasierte Datenverarbeitung als Schwerpunkt der Beratungen des Düsseldorfer Kreises herausgebildet. Unter anderem hat er zu den datenschutzrechtlichen Anforderungen an soziale Netzwerke, zur Nutzung von Smartphones und zu Cloud Computing-Diensten Stellung bezogen. In einem weiteren Beschluss hat der Düsseldorfer Kreis die Möglichkeit der anonymen und pseudonymen Nutzung des Internets angemahnt. Schließlich hat er sich auch mit den Anforderungen des kontaktlosen Auslesens von Geldkarten über den Einsatz der so genannten Near Field Communication-Technologie (NFC) befasst, mit denen das unberechtigte Auslesen der auf der Karte gespeicherten Daten verhindert werden kann. Alle Beschlüsse des Düsseldorfer Kreises im Berichtszeitraum sind aus dem Kasten zu Nr. 10.3 ersichtlich und auf meiner Internetseite abrufbar.

Kasten zu Nr. 10.3

Beschlüsse des Düsseldorfer Kreises in den Jahren 2011/2012:

- Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert
- Datenschutzgerechte Smartphone-Nutzung ermöglichen!
- Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen
- Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze
- Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing
- Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen
- Anonymes und pseudonymes elektronisches Bezahlen von Internetangeboten ermöglichen!
- Datenschutz in sozialen Netzwerken
- Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft
- Nearfield Communication (NFC) bei Geldkarten

10.4 Datenschutz in der Versicherungswirtschaft

Im Berichtszeitraum konnten wesentliche Verbesserungen beim Datenschutz in der Versicherungswirtschaft erreicht werden.

Über viele Jahre musste ich in meinen Tätigkeitsberichten feststellen, dass dringend notwendige Verbesserungen beim Datenschutz in der Versicherungswirtschaft auf sich warten lassen und die Gespräche zwischen den Datenschutzaufsichtsbehörden und dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) nur langsam vorankommen (vgl. 22. TB Nr. 3.4.7, 23. TB Nr. 10.7). Erfreulicherweise kann ich nun gleich zu mehreren Punkten über eine erfolgreiche Erhöhung des Datenschutzniveaus bei der Verarbeitung personenbezogener Daten durch Versicherungsunternehmen berichten.

Mit einer neuen Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung und Verwendung von Gesundheitsdaten, der Entwicklung von Verhaltensregeln für den Umgang mit personenbezogenen Daten nach § 38a BDSG sowie mit der Umstellung des Hinweis- und Informationssystems (HIS) auf eine neue rechtliche Grundlage wurden fundamentale Voraussetzungen für eine datenschutzgerechte Datenverarbeitung in der Versicherungswirtschaft geschaffen.

Neue Einwilligungs- und Schweigepflichtentbindungserklärung

Für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen ist weder im Bundesdatenschutzgesetz noch im Versicherungsvertragsgesetz eine Rechtsgrundlage enthalten. Aus diesem Grund bedarf es stets einer datenschutzrechtlichen Einwilligung des Versicherungsnehmers sowie einer Schweigepflichtentbindungserklärung. Die von den Versicherungsunternehmen bisher verwendete Musterklausel genügte schon seit langem nicht mehr den gesetzlichen Anforderungen des § 4a BDSG und entsprach auch nicht den Vorgaben, die das Bundesverfassungsgericht in einem Beschluss vom 23. Oktober 2006 für eine wirksame Schweigepflichtentbindungserklärung gemacht hat (vgl. 21. TB Nr. 9.6).

In langwierigen und zähen Verhandlungen haben sich die Datenschutzaufsichtsbehörden und der GDV gemeinsam bemüht, die Einwilligungs- und Schweigepflichtentbindungserklärungen nicht nur gesetzeskonform, sondern auch transparenter zu gestalten. Erst im Jahr 2011 konnte Einigung über eine neue Mustererklärung erzielt werden, die bei einwilligungsbedürftigen Datenerhebungs- und -verwendungsprozessen einzuholen ist. Nach den entsprechenden Anwendungshinweisen ist die Klausel zudem in regelmäßigen Abständen vom GDV und den Aufsichtsbehörden gemeinsam zu überarbeiten, um aktuelle Entwicklungen der Datenverarbeitung und gesetzliche Änderungen zu berücksichtigen. Der Düsseldorfer Kreis, ein Koordinierungsgremium aller Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, hat diese Mustererklärung mit Beschluss vom 17. Januar 2012 (s. Anlage 8) gebilligt und veröffentlicht.

Die neue Mustererklärung wird flankiert durch Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft (s. u.).

Hinweis- und Informationssystem (HIS)

Im 23. TB (Nr. 10.7) habe ich bereits über die vom GDV geplante Neukonzeption eines Hinweis- und Informationssystems (HIS) berichtet, die das alte Warnsystem „Uniwagnis“ ablösen und dazu beitragen sollte, einen datenschutzrechtswidrigen Zustand (vgl. 21. TB Nr. 9.5) zu beenden. Die Umstellung ist im Berichtszeitraum abgeschlossen worden. Am 1. April 2011 hat die Versicherungswirtschaft für die verschiedenen Versicherungssparten das in enger Abstimmung zwischen dem GDV und der AG Versicherungswirtschaft des Düsseldorfer Kreises entwickelte Hinweis- und Informationssystem (HIS) in Betrieb genommen, das als Auskunftei von der Firma informa Insurance Risk and Fraud Prevention GmbH in Baden-Baden betrieben wird.

Das HIS dient der Risikobeurteilung im Antragsfall, zur Sachverhaltsaufklärung bei der Leistungsprüfung sowie der Bekämpfung von Versicherungsmissbrauch. Rechtsgrundlagen sind § 28 Absatz 1 Nummer 2 BDSG für die Einmeldung personenbezogener Daten in das System und § 29 BDSG für die geschäftsmäßige Erhebung und Speicherung zum Zweck der Übermittlung. Liegen festgelegte Kriterien vor, werden in das System Auffälligkeiten aus Versicherungsfällen eingemeldet, z. B. atypische Schadenshäufigkeiten, besondere Schadensfolgen oder erschwerte Risiken.

Die Versicherungsunternehmen können Informationen zur Risikoprüfung im Antragsbereich und zur Schadensfallprüfung im Leistungsbereich im automatisierten Verfahren abrufen. Sämtliche Abfragen werden protokolliert und stichprobenartig überprüft. Antrags- und Leistungsbereich sowie die einzelnen Versicherungssparten sind streng voneinander getrennt. Besondere Arten von personenbezogenen Daten, wie z. B. Gesundheitsdaten, werden nicht an das HIS gemeldet.

Die Betroffenen werden von der Versicherung über die Einmeldung ihrer Daten benachrichtigt. Dadurch können sie frühzeitig bei der Auskunftei einen Antrag auf Selbstauskunft stellen, wenn sie Einzelheiten über die zu ihrer Person gespeicherten Daten wissen wollen.

Die zuständige baden-württembergische Datenschutzaufsichtsbehörde hat sich vor der Inbetriebnahme des Systems davon überzeugt, dass HIS den datenschutzrechtlichen Anforderungen Rechnung trägt.

Verhaltensregeln für den Umgang mit personenbezogenen Daten (Code of Conduct)

Parallel zu den Bemühungen um eine datenschutzgerechte Gestaltung der Einwilligungs- und Schweigepflichtentbindungserklärung (s. o.) wurden auch die Gespräche zwischen den Aufsichtsbehörden und dem GDV über Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft fortgesetzt. Über die Absicht, einen solchen so genannten Code of Conduct zu erstellen, hatte ich bereits im 22. TB (Nr. 3.4.7) berichtet.

Ausgangspunkt war die Überlegung, dass sich die neue Einwilligungs- und Schweigepflichtentbindungserklärung auf die tatsächlich einwilligungsbedürftigen Datenerhebungs- und -verwendungsprozesse beschränken soll, während in Verhaltensrichtlinien die weiteren, auf einer gesetzlichen Grundlage beruhenden Datenverarbeitungen konkretisiert werden sollen.

Im September 2012 haben alle Datenschutzaufsichtsbehörden dem endgültigen Entwurf zugestimmt. Daraufhin hat der GDV die Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft nach § 38a Absatz 2 BDSG der zuständigen Aufsichtsbehörde zur Überprüfung der Vereinbarkeit mit dem Datenschutzrecht vorgelegt. Mit Bescheid vom 2. November 2012 hat der zuständige Berliner Beauftragte für Datenschutz und Informationsfreiheit festgestellt, dass die Verhaltensregeln geeignet sind, die Durchführung der datenschutzrechtlichen Regelungen zu fördern, und nicht im Widerspruch zum geltenden Datenschutzrecht stehen.

Der Code of Conduct der Versicherungswirtschaft ist eines der wenigen Beispiele für eine gelungene Umsetzung des § 38a BDSG, der Wirtschaftsverbänden die Möglichkeit einräumt, den Datenschutzaufsichtsbehörden Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen zu unterbreiten (vgl. Nr. 3.4).

Die Verhaltensregeln enthalten insgesamt 31 Artikel, in denen die wichtigsten Verarbeitungen personenbezogener Daten im Zusammenhang mit der Begründung, Durchführung, Beendigung oder Akquise von Versicherungsverträgen erfasst werden, u. a. auch die Nutzung des Hinweis- und Informationssystems HIS. Eine Evaluierungsklausel gewährleistet, dass bei jeder den Regelungsgehalt betreffenden Rechtsänderung, spätestens aber nach fünf Jahren eine Überprüfung stattfindet.

Mit den Verhaltensregeln hat der GDV eine Vorreiterrolle übernommen und einen wesentlichen Beitrag zur Entwicklung der datenschutzrechtlichen Selbstregulierung in der Wirtschaft geleistet. Die dem GDV angeschlossenen Versicherungsunternehmen sind nunmehr dazu aufgerufen, mit ihrem Beitritt zu den Verhaltensregelungen ein hohes Datenschutzniveau in der Versicherungswirtschaft zu gewährleisten.

Die Verhaltensregeln waren bei Redaktionsschluss noch nicht veröffentlicht.

10.5 Zusammenarbeit zwischen deutschen und amerikanischen Abschlussprüferaufsichtsbehörden

Die deutsche Abschlussprüferaufsichtskommission (APAK) und die amerikanische Aufsichtsbehörde für Wirtschaftsprüfer (PCAOB) unterzeichnen eine Absichtserklärung zur Zusammenarbeit.

Seit 2005 übt die APAK weisungsfrei die öffentliche Fachaufsicht über die Wirtschaftsprüferkammer und insoweit über alle Wirtschaftsprüfer und vereidigten Buchprüfer aus. Die amerikanische Aufsichtsbehörde für Wirtschaftsprüfer, der Public Company Accounting Oversight Board (PCAOB), ist 2011 an mehrere europäische Länder mit dem Ziel herangetreten, eine bilaterale Vereinbarung abzuschließen, auf deren Grundlage Daten von europäischen Rechnungsprüferaufsichtsbehörden an den PCAOB übermittelt werden sollen.

Auf europäischer Ebene enthält die Richtlinie 2006/43/EG über Abschlussprüfungen Regelungen zur Zusammenarbeit mit zuständigen Stellen in Drittländern. Nach Artikel 47 der Richtlinie können die zuständigen Stellen der Mitgliedstaaten im Falle von Kontrollen und Untersuchungen bei Abschlussprüfern die Weitergabe von Arbeitspapieren an die zuständigen Stellen in Drittländern erlauben, sofern diese von der Europäischen Kommission für angemessen erklärt wurden.

Mit Beschluss vom 1. September 2010 (2010/485/EG) hat die Kommission eine bis zum 31. Juli 2013 befristete Entscheidung über die Angemessenheit der zuständigen Stellen in den USA getroffen und damit die erste Voraussetzung für den Informationsaustausch zwischen der APAK und dem PCAOB geschaffen (sog. Adäquanzentscheidung).

Nach Artikel 2 Absatz 4 des Beschlusses müssen die Mitgliedstaaten zudem durch bilaterale Vereinbarungen sicher stellen, dass bei der Übermittlung von Arbeitspapieren und Dokumenten an die zuständigen Stellen in den USA angemessene Maßnahmen zum Schutz der enthaltenen personenbezogenen Daten gewährleistet werden.

Die Artikel-29-Gruppe (vgl. Nr. 2.4.1) empfahl in einem Schreiben an die Kommission, wie sich Rechnungsprüferaufsichtsbehörden bis zum Vorliegen einer endgültigen einheitlichen europäischen Lösung verhalten sollen. Danach sollte ein „Memorandum of Understanding – MoU“ der Europäischen Rechnungsprüferaufsichtsbehörde (EGAOB) als Interimslösung genutzt werden.

Der PCAOB hat diese Lösung nicht akzeptiert und bereits im Laufe des Jahres 2011 mit einzelnen europäischen Staaten (Vereinigtes Königreich, Niederlande) bilaterale Vereinbarungen abgeschlossen. Er ist diesbezüglich auch an die deutsche APAK herangetreten. Die APAK hat mich über den Fortgang der Angelegenheit unterrichtet und am 12. April 2012 eine Vereinbarung mit dem

PCAOB unterzeichnet, die – basierend auf der niederländischen Lösung – einzelne weitere datenschutzrechtliche Modifikationen berücksichtigt. Die bisher von dem PCAOB abgeschlossenen bilateralen Vereinbarungen (einschließlich die Vereinbarung mit der APAK) sind bis zum 31. Juli 2013 befristet, weil zu diesem Zeitpunkt die Adäquanzentscheidung ausläuft.

Ich habe in der Unterarbeitsgruppe Finanzen der Artikel-29-Gruppe das Verfahren begleitet. Die Kommission hat zugesagt, zu prüfen, ob für den Zeitraum nach dem 1. August 2013 eine einheitliche europäische Lösung umsetzbar ist, und die Artikel-29-Gruppe über das Ergebnis zu unterrichten.

10.6 Kontrollbesuch beim Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz

Der behördliche Datenschutzbeauftragte ist Motor bei der Umsetzung von Datenschutz und Datensicherheit in der Praxis. Dies verdeutlichte ein Kontrollbesuch beim Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV).

Zum Zeitpunkt meiner Kontrolle war die Datenschutzbeauftragte des BMELV seit etwa neun Monaten im Amt. Die vorherige Vakanz auf diesem Posten hatte zu einem entsprechenden „Modernisierungsstau“ geführt, der erst nach Wiederbesetzung der Position des Datenschutzbeauftragten durch die heutige Amtsinhaberin sukzessive aufgelöst werden konnte. Dabei habe ich das BMELV während und nach meinem Kontrollbesuch unterstützt. Das BMELV teilte mir mit, dass die Position des Datenschutzbeauftragten künftig stets besetzt sein würde.

Einen Schwerpunkt bei der Aufarbeitung der Rückstände bildete die Aktualisierung des IT-Sicherheitskonzepts. Meine diesbezüglichen Hinweise wurden vom BMELV aufgegriffen.

Darüber hinaus hat das BMELV mit der Erstellung eines aktualisierten Datenschutzkonzepts begonnen und wird sich in Kürze mit der Überarbeitung einer Dienstvereinbarung mit seinem Personalrat bezüglich der elektronischen Verarbeitung von Personaldaten beschäftigen.

Außerdem wird das BMELV zeitnah eine Hausanordnung zur Sicherstellung des Datenschutzes im BMELV in Kraft setzen und die Präsidenten seiner Geschäftsbereichsbehörden bitten, entsprechende Hausanordnungen zu erlassen.

Die Mitarbeiterinnen und Mitarbeiter des BMELV werden auf dieser Basis in Fragen des Datenschutzes und der Datensicherheit im Rahmen von Inhouse-Schulungen fortgebildet.

Die vielfältigen Aktivitäten des BMELV zur Optimierung des Datenschutzes begrüße ich nachdrücklich. Ich bin davon überzeugt, dass sich damit die Situation im Bereich von Datenschutz und Datensicherheit beim BMELV nachhaltig verbessern wird, und hoffe, dass das BMELV Beispiel auch für andere Bundesressorts ist.

10.7 Kontrollbesuch beim Kraftfahrt-Bundesamt – ZEVIS-Protokolldaten

Beim Kraftfahrt-Bundesamt (KBA) habe ich mich über den Umgang mit den Protokolldaten im Bereich des Zentralen Verkehrsinformationssystems (ZEVIS) informiert. Aufgrund meiner Empfehlungen wurde die Arbeitsanweisung zur Bearbeitung von Anfragen auf Datennutzung überarbeitet.

Nach § 36 Absatz 6 Satz 1 Straßenverkehrsgesetz (StVG) hat das KBA die im automatisierten Verfahren mittels ZEVIS erfolgten Abrufe aus dem Zentralen Fahrzeugregister zu protokollieren. Die Protokolldaten müssen die zum Abruf verwendeten Daten, den Tag, die Uhrzeit, die Kennung der abrufenden Stelle und die abgerufenen Daten enthalten. Zusätzlich müssen nach § 36 Absatz 7 StVG Informationen protokolliert werden, aus denen sich der Anlass des Abrufs und die für den Abruf verantwortliche Person ergeben.

Die protokollierten Daten dürfen für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage verwendet werden (§ 36 Absatz 6 Satz 2 StVG). Liegen Anhaltspunkte vor, dass ohne die entsprechenden Daten die Verhinderung oder Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person wesentlich erschwert wäre, dürfen die Daten auch für diesen Zweck verwendet werden (§ 36 Absatz 6 Satz 3 StVG).

Die Mitarbeiter des KBA müssen bei jeder Anfrage auf Nutzung der Protokolldaten das Vorliegen dieser Voraussetzungen prüfen. Als Grundlage hierfür dient eine interne Arbeitsanweisung. Während der Kontrolle habe ich dem KBA diverse Empfehlungen zur Überarbeitung der Arbeitsanweisung gegeben. Insbesondere forderte ich, die Bearbeitung der Anfragen lückenlos zu dokumentieren. Es muss hieraus insbesondere das Ergebnis der Prüfung hervorgehen, ob der Anfragende gemäß § 36 Absatz 6 StVG hierzu berechtigt war und der schriftlichen Anfrage eine stichhaltige Begründung beigefügt ist. Aus ihr muss weiterhin hervorgehen, dass die Nutzung der Protokolldaten des KBA zwingend für einen der in § 36 Absatz 6 Sätze 2 und 3 StVG genannten Zwecke erforderlich ist.

Das KBA ist meinen Empfehlungen bezüglich der Arbeitsanweisung gefolgt. Sie bietet nun auch eine gute Grundlage für die Dokumentation bei der Bearbeitung der Anfragen.

10.8 Kontrollbesuch beim Kraftfahrt-Bundesamt – Zentrales Kontrollgerätkartenregister

Das Kraftfahrt-Bundesamt (KBA) führt das zentrale Kontrollgerätkartenregister (ZKR) und personalisiert die zum Betrieb der Kontrollgeräte erforderlichen Chipkarten. Bei einer Kontrolle beim KBA habe ich keine Datenschutzmängel festgestellt.

Zentrales Kontrollgerätkartenregister (ZKR)

Das ZKR wird auf der Basis des Fahrpersonalgesetzes (FPersG) und der Fahrpersonalverordnung (FPersV) seit 1. Mai 2005 beim KBA geführt. Das Register wird benötigt, weil bei der Personen- und Güterbeförderung mit Fahrzeugen über 3,5 Tonnen zulässigem Gesamtgewicht grundsätzlich ein digitales Kontrollgerät mitgeführt werden muss. Das ZKR wird ausschließlich elektronisch geführt und enthält Informationen zu den in Deutschland ausgegebenen Kontrollgerätkarten.

Fahrerkarten, auf denen neben den Personalien des Fahrers, dessen Führerscheinnummer und seine Lenk- und Ruhezeiten gespeichert werden.

Werkstattkarten, mit denen das Kontrollgerät geprüft, repariert und kalibriert wird. Sie enthalten Informationen über die autorisierte Werkstatt, den Kontrollgeräteherstellers, den Fahrzeughersteller sowie personenbezogene Daten der dort jeweils verantwortlichen Personen.

Unternehmenskarten, mithilfe derer die im Kontrollgerät gespeicherten Daten angezeigt und heruntergeladen oder ausgedruckt werden können. Sie helfen dem Unternehmer bei der Organisation und internen Betriebskontrollen. Die Unternehmenskarten enthalten Informationen über das Unternehmen (z. B. Spedition, Busunternehmen) sowie personenbezogene Daten des verantwortlichen Unternehmers.

Die Kontrollkarte ermöglicht den kontrollbefugten Behörden (z. B. Bundesamt für Güterverkehr, Polizei und Zoll) den Zugriff auf alle im Kontrollgerät gespeicherten Daten, um die Einhaltung von Lenk- und Ruhezeiten zu überwachen. Auf der Kontrollkarte sind ausschließlich Informationen über die kontrollbefugte Behörde und damit keine personenbezogene Daten gespeichert.

Die Kontrollbehörden erhalten im Rahmen ihrer gesetzlichen Befugnisse im Online-Dialog-Verfahren Auskünfte über im ZKR gespeicherte Daten. Sie haben hierauf ausschließlich lesenden Zugriff. Lediglich die Ausgabestellen (i. d. R. Führerscheinstellen) haben die Befugnis, den „Kartenstatus“ im Falle des Verlustes einer Karte (z. B. Diebstahl, Zerstörung etc.) unmittelbar im Datenbestand des ZKR zu ändern. Anschließend muss der Inhaber der bisherigen Karte zwingend eine neue Karte auf elektronischem Weg beim KBA beantragen.

Ich habe mich davon überzeugt, dass die vom KBA ergriffenen technisch-organisatorischen Maßnahmen zur sicheren Datenübertragung dem Stand der Technik entsprechen. Das KBA beachtet auch die einschlägigen Vorschriften zur Registerführung.

Personalisierung der Gerätekarten

Das KBA personalisiert die Kontrollgerätkarten. Der Personalisierungsprozess umfasst sowohl den auf der Karte angebrachten und damit sichtbaren Teil (etwa Personalien und Bild des Karteninhabers), als auch die Digitalisierung des in den Karten etwa zur Speicherung der Lenk- und Ruhezeiten enthaltenen Mikrochips. Das KBA hat einen vom übrigen Teil seines Dienstgebäudes in Flensburg abgeschotteten und nach innen und außen besonders abgesicherten Bereich eingerichtet. Ich konnte mich davon überzeugen, dass sowohl datenschutzrechtlich als auch datensicherheitstechnisch der gesamte Personalisierungsprozess bis hin zum abschließenden Versand der Kontrollgerätkarten optimal umgesetzt wurde.

Teilnahme am Informationsaustausch

Ebenfalls einwandfrei verläuft die Teilnahme des KBA am Telematics Network for the Exchange of Information Concerning the Issuing of Tachograph Cards (TACHOnet). TACHOnet ist eine von der EU-Kommission in Brüssel auf einem dortigen Server betriebene Plattform für den elektronischen Informationsaustausch zwischen den zur Ausstellung von Fahrerkarten zuständigen Behörden der EU/EWR-Staaten auf der Basis der bei ihnen geführten nationalen Datenbanken. Für Deutschland ist dies das ZKR.

Auf der TACHOnet-Plattform wird vor Ausstellung einer Fahrerkarte abgefragt, ob der Antragsteller eine solche Karte nicht bereits besitzt. Hierdurch wird sichergestellt, dass jeder Betroffene nur eine gültige Fahrerkarte hat, auf deren Mikrochip die Lenk- und Ruhezeiten aufgezeichnet werden. Dadurch können die Kontrollbehörden die Einhaltung der Vorschriften effektiv überwachen.

10.9 Eisenbahn-Bundesamt

Im Rahmen eines Beratungs- und Kontrollbesuchs habe ich das Eisenbahn-Bundesamt bei der datenschutzkonformen Einrichtung des neuen Triebfahrzeugführerscheinregisters beraten.

Mit der Richtlinie 2007/59/EG vom 23. Oktober 2007 wurde mit dem Triebfahrzeugführerschein eine europaweit einheitliche Fahrerlaubnis für Eisenbahnfahrzeuge mit eigenem Antrieb eingeführt. Dieser Führerschein soll sukzessive entsprechende nationale Fahrerlaubnisse ablösen. Ich habe das Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS) bei der Umsetzung der EU-Richtlinie in deutsches Recht durch die Triebfahrzeugführerscheinverordnung (TfV) von 2011 intensiv beraten.

Triebfahrzeugführerscheinregister

Anschließend habe ich auch das Eisenbahn-Bundesamt (EBA) bei der ihm durch die TfV übertragenen Führung des Triebfahrzeugführerscheinregisters beraten. Alle Daten, die für die Erteilung, den Entzug und zur Information über den aktuellen Status eines Triebfahrzeugführerscheins erforderlich sind, werden in diesem Register gespeichert. Dessen Aufbau erfolgt in drei Schritten. Zum Zeitpunkt meines Besuchs hatte das EBA im ersten Schritt erst rund 100 Führerscheine ausgestellt. Ab Ende Oktober 2013 wird es im zweiten Schritt etwa weiteren

8 000 Triebfahrzeugführern einen entsprechenden Führerschein aushändigen. Mit dem Vollaufbau des Registers ab Ende Oktober 2018 werden im dritten Schritt etwa 30 000 Triebfahrzeugführer über einen entsprechenden Führerschein verfügen. Der Führerschein muss vom Inhaber schriftlich beantragt werden. Alle erforderlichen Vordrucke und Ausfüllhinweise finden sich auf der Homepage des EBA. Diese wurden aufgrund meiner Empfehlungen optimiert.

Die Registerführung, sowie die Erteilung und der Entzug der Triebfahrzeugführerscheine wird durch die eigens hierfür eingerichtete Triebfahrzeugführerscheinstelle des EBA vorgenommen. Zum Zeitpunkt meines Besuchs wurde das Register noch in einer Excel-Anwendung geführt, die im Laufe des Jahres 2013 durch eine Oracle-Apex-Datenbankanwendung abgelöst werden soll. Die Excel-Tabelle enthielt wesentlich mehr Datenfelder als in der TfV vorgesehen und konnte noch nicht alle Funktionalitäten erfüllen, wie z. B. die erforderliche Darstellung von Historien der Datensätze. Angesichts der geringen Zahl von rund 100 gespeicherten Datensätzen, der zu ihrem Schutz gegen unbefugten Zugriff getroffenen technisch-organisatorischen Maßnahmen und der avisierten zeitnahen Implementierung einer Datenbanklösung, habe ich diese Behelfsversion übergangsweise akzeptiert. Ich habe das EBA aber zur Löschung der nicht erforderlichen Datenfelder aufgefordert und gebeten sicherzustellen, dass die Integrität des Registers beim Datentransfer von der Excel-Tabelle in die Oracle-Datenbank gewährleistet wird. Dies wurde mir vom EBA zugesagt. Von der Umsetzung meiner Empfehlungen werde ich mich überzeugen.

Triebfahrzeugführerscheine

Zu den Aufgaben des EBA nach der TfV zählen auch die Herstellung, Personalisierung und Lieferung von Triebfahrzeugführerscheinen. Diese Aufgaben lässt das EBA durch die Bundesdruckerei auf der Basis eines Rahmenvertrages erledigen. Die Verarbeitung personenbezogener Daten erfolgt im Wege der Auftragsdatenverarbeitung nach § 11 BDSG. Hinsichtlich der Ausgestaltung des Vertrages habe ich das EBA in datenschutzrelevanten Punkten um Präzisierung gebeten. Die im Rahmen des Vertragsvollzugs erforderliche Kommunikation des EBA mit der Bundesdruckerei erfolgt datenschutzkonform an einem hierfür besonders eingerichteten Arbeitsplatz im EBA.

Wie ich schließlich festgestellt habe, verlangt das EBA zur Prüfung der Voraussetzungen vom Antragsteller eine Kopie des Reisepasses oder des nationalen Personalausweises sowie eine Selbstauskunft aus dem Verkehrszentralregister („Punkteauskunft“). Da dies für die Aufgabenerfüllung des EBA erforderlich ist, toleriere ich das Verfahren unter der Voraussetzung, dass das BMVBS die hierfür erforderlichen Rechtsgrundlagen schafft. Der vorgelegte Entwurf zur Übermittlung von Daten aus dem Verkehrszentralregister an das EBA begegnet keinen datenschutzrechtlichen Bedenken. Die erforderlichen Rechtsgrundlagen für die Vorlage einer Kopie des Reisepasses oder des nationalen Personalausweises will das BMVBS im Frühjahr 2013 in Angriff nehmen.

10.10 Kontrollbesuch beim Bundesamt für Bauwesen und Raumordnung: Forschungsprojekte

Ein Kontrollbesuch beim Bundesamt für Bauwesen und Raumordnung offenbarte Problembewusstsein.

Im Berichtszeitraum habe ich einen Beratungs- und Kontrollbesuch beim Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR), einer Abteilung des Bundesamts für Bauwesen und Raumordnung (BBR), durchgeführt. Ich wollte mir anhand exemplarisch dargestellter Forschungsprojekte einen Überblick über die Arbeitsweise dieser Forschungseinrichtung verschaffen.

Die vorgestellten Projekte waren datenschutzrechtlich im Wesentlichen nicht zu beanstanden. Lediglich die Frage, unter welchen Voraussetzungen bei extern vergebenen Forschungsaufträgen mit dem Forschungsnehmer ein Vertrag zur Auftragsdatenverarbeitung geschlossen werden muss, wurde zunächst kontrovers diskutiert. Aufgrund meiner Hinweise hat das BBR einen Mustervertrag für Verträge nach § 11 BDSG erarbeitet, der künftig in den entsprechenden Fällen Verwendung finden soll.

Eines der vorgestellten Forschungsprojekte war das Projekt „Bestandsaufnahme und Wirkungsanalyse des Wohngeldes“. Wenn das Wohngeldgesetz (WoGG) geändert wird, gibt das BBR regelmäßig eine Studie zur Evaluation der jeweiligen Gesetzesänderung in Auftrag.

Darüber hinaus wertet das BBSR regelmäßig und auch kurzfristig (zur Beantwortung besonderer Fragestellungen des Bundesministeriums für Verkehr, Bau und Stadtentwicklung – BMVBS) die Stichprobe nach § 36 WoGG aus. Vereinzelt hat sie diese auch durch einen Auftragnehmer auswerten lassen, dessen Mitarbeiter dazu auch einen „Arbeitsplatz“ (Raum mit Rechner) erhalten hat.

Die Durchführung der Stichprobe durch Dritte ist generell unzulässig. Nach § 36 Absatz 2 WoGG dürfen die Einzelangaben der Stichprobe vom Statistischen Bundesamt nur an das Ministerium oder das BBR übermittelt werden. Dabei hat das BBR eine Organisationseinheit einzurichten, die räumlich, organisatorisch und personell von anderen Aufgabenbereichen zu trennen ist. Die in dieser Organisationseinheit tätigen Personen müssen Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sein. Diese gesetzlich vorgeschriebene räumliche, organisatorische und personelle Trennung innerhalb des BBR war bislang nicht vorhanden.

Das BBSR hat begonnen, meine Hinweise umzusetzen. So muss die Arbeit an den Stichprobendaten auf einem nur hierfür eingesetzten PC erfolgen. Der Rechner muss in einem mit zugangscodierter Schließvorrichtung versehenen Raum stehen, zu dem nur diejenigen Mitarbeiter Zutritt haben, die für die Bearbeitung zuständig sind. Die organisatorische Trennung könnte durch die Einrichtung einer Stabsstelle oder einer sonstigen von der üblichen Referatsstruktur abgetrennten Arbeitseinheit erreicht werden.

Die gleichzeitige Wahrnehmung von Aufgaben innerhalb der bisherigen Referatsstruktur ist nach meiner Auffassung dabei dann unschädlich, wenn sie außerhalb der für die Stichprobendurchführung zu schaffenden Strukturen und nicht mithilfe der dortigen Infrastruktur (z. B. PC) erfolgt. Ferner sind die Stichprobendaten unverzüglich nach Abschluss der diesbezüglichen Arbeiten zu löschen. Ich werde das BBSR in dieser Angelegenheit weiterhin unterstützen.

10.11 Neue Verkehrsunternehmensdatei

Die datenschutzgerechte Umsetzung europarechtlicher Vorgaben zum Aufbau eines elektronischen Unternehmensregisters für Kraftverkehrsunternehmer und zur Einrichtung einer nationalen Kontaktstelle für den Informationsaustausch mit den Mitgliedstaaten ist gelungen.

Durch die Verordnungen (EG) Nr. 1071/2009, 1072/2009 und 1073/2009 des Europäischen Parlaments und des Rates werden die Zulassung zum Beruf des Kraftverkehrsunternehmers, der Zugang zum Markt des grenzüberschreitenden Güterkraftverkehrs und der Zugang zum grenzüberschreitenden Personenkraftverkehrsmarkt grundlegend neu geregelt. Unter anderem werden die Mitgliedstaaten verpflichtet, einzelstaatliche elektronische Unternehmensregister aufzubauen und außerdem einzelstaatliche Kontaktstellen für den Informationsaustausch mit anderen Mitgliedstaaten einzurichten. Für Deutschland bedeutet dies eine Verbesserung der fachlich erforderlichen Kommunikation zwischen dem Bundesamt für Güterverkehr (BAG) und den für Güterkraftverkehr zuständigen Stellen der Länder einerseits und zwischen dem BAG als nationaler Kontaktstelle und den nationalen Kontaktstellen der übrigen EU-Mitgliedstaaten sowie den dort für Güterkraftverkehr zuständigen Stellen andererseits.

Im Berichtszeitraum habe ich das BMVBS bei der innerstaatlichen Umsetzung dieser Verpflichtung beraten. Dabei ging es insbesondere um das Gesetz zur Änderung des Güterkraftverkehrsgesetzes und des Personenbeförderungsgesetzes sowie die Verordnung zur Durchführung der Verkehrsunternehmensdatei nach dem Güterkraftverkehrsgesetz. Das BMVBS hat meine zahlreichen Vorschläge zur datenschutzrechtlichen Optimierung des Gesetzes und der Verordnungen dankenswerterweise übernommen. Die Regelungen sind mittlerweile in Kraft getreten.

Noch während der Pilotphase habe ich mich beim BAG über die Umsetzung der gesetzlichen Vorgaben informiert. So ist das BAG als registerführende Stelle und nationale Kontaktstelle insbesondere zuständig für die Verfügbarkeit, Vertraulichkeit und Integrität der gespeicherten Daten. Ebenso hat es Löschungsfristen und Protokollierungspflichten umzusetzen sowie technisch-organisatorische Maßnahmen nach der Anlage zu § 9 BDSG zu ergreifen. Für die inhaltliche Richtigkeit der zu speichernden Daten ist die eingebende Stelle (i. d. R. die für den Güterverkehr zuständigen Landesbehörden) verantwortlich.

Die vom BAG während meines Besuchs vorgestellte DV-Anwendung setzte alle datenschutzrechtlichen Vorgaben des Güterkraftverkehrsgesetzes und der Verkehrsunternehmensdatei-Durchführungsverordnung um, sowohl hinsichtlich der Registerführung als auch hinsichtlich der künftigen Funktion des BAG als nationale Kontaktstelle. Die vom BAG getroffenen technischen Vorkehrungen entsprechen hohen datenschutzrechtlichen Standards.

Im Anschluss an meinen Besuch teilte das BAG mir mit, dass der Wirkbetrieb der Registerdateien Mitte November 2012 begonnen hat und dass es seit 1. Januar 2013 seine Funktion als nationale Kontaktstelle ausübt.

10.12 Forschungsprojekte bei der Bundesanstalt für Straßenwesen

Die Bundesanstalt für Straßenwesen geht mit personenbezogenen Daten in Forschungsprojekten datenschutzgerecht um.

Bei einem Informations- und Beratungsbesuch bei der Bundesanstalt für Straßenwesen (BASt) habe ich mir einen Überblick über deren Forschungstätigkeit verschafft. Die BASt betreut jährlich etwa 200 eigene und 400 fremde Forschungsprojekte. Davon weist die überwiegende Anzahl keinen Personenbezug auf. Exemplarisch habe ich mir jeweils ein eigenes und ein fremdes Forschungsprojekt erläutern lassen, bei denen personenbezogene Daten verarbeitet und genutzt werden. Bei beiden konnte ich eine hohe Sensibilität der Mitarbeiter für den datenschutzgerechten Umgang mit den personenbezogenen Daten feststellen.

Hinsichtlich der Frage, unter welchen Voraussetzungen bei Forschungsprojekten zwischen Auftraggeber und Forschungsnehmer ein Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG geschlossen werden muss, bin ich mit der BASt noch im Gespräch. Ebenfalls ist meine Beratung in Bezug auf das Datenschutzkonzept, das IT-Sicherheitskonzept und das Verfahrensverzeichnis der BASt noch nicht abgeschlossen.

11 Gesundheit und Soziales

11.1 Krankenversicherung

11.1.1 Verschlechtert wirtschaftlicher Druck den Datenschutzstandard für die Versicherten?

Beim Zusammenschluss von Krankenkassen ist darauf zu achten, dass der jeweils höhere Datenschutzstandard der Fusionspartner übernommen wird.

Bei den regelmäßigen Beratungs- und Kontrollbesuchen der gesetzlichen Krankenkassen habe ich erfreulicherweise festgestellt, dass viele Krankenkassen die in zurückliegenden Tätigkeitsberichten dargelegten Vorgaben für den Datenschutz in ihrem Bereich umgesetzt haben. Dies gilt insbesondere bei den größeren Krankenkassen. Allerdings habe ich auch konstatieren müssen, dass das Erreichte alles andere als sicher ist und bestehende Datenschutzstandards insbesondere durch den verstärkten wirt-

schaftlichen Druck gefährdet sind, unter dem die Krankenkassen stehen. Dieser wirtschaftliche Druck führt zu unterschiedlichen datenschutzrechtlichen Problemen:

– Private Krankenversicherungen (PKV) und gesetzlichen Krankenkassen („Gesetzliche Krankenversicherung“ – GKV) arbeiten immer enger zusammen. Dies wird als „wichtiger Wettbewerbsvorteil“ beschrieben und beworben. Angestoßen wurde dies durch das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GMG) vom 14. November 2003 (BGBl. I S. 2190), über das ich in meinem 20. Tätigkeitsbericht ausführlich berichtet habe (Nr. 17.1.1 und 17.1.2). Dabei ist es zu Verstößen von Krankenkassen gegen datenschutzrechtliche Bestimmungen bei der Vermittlung privater Zusatzversicherungen gekommen (22. TB Nr. 10.2.4 und 23. TB Nr. 11.1.8, vgl. auch Nr. 16.10).

– Wie die Presse gegen Ende des Berichtszeitraums mitteilte, soll eine gesetzliche Krankenversicherung schwer kranke Versicherte zur Kündigung des Versicherungsverhältnisses gedrängt haben. Versicherte, gegen die wegen der Nichtzahlung des Zusatzbeitrages Mahnbescheide beantragt worden waren, wurden bei Vorliegen der Merkmale „schwere Krankheit“ und „geringes Einkommen“ telefonisch kontaktiert. Dem Hinweis der Krankenkassen, diese Merkmale seien lediglich als Filter verwendet worden, um säumigen Versicherten mit Stundung, Erlass oder Niederschlagung entgegenzukommen, stehen – mir vorliegende – Vermerke entgegen, die die Mitarbeiter der Krankenkasse über ihre Gespräche führten. Sie vermitteln den Eindruck, die Versicherten hätten dazu gebracht werden sollen, das Versicherungsverhältnis zu beenden. Die datenschutzrechtliche Prüfung ist allerdings in diesem Fall noch nicht abgeschlossen.

– Eine ganze Reihe Versicherter beschwerte sich bei mir, weil eine gesetzliche Krankenkasse anlässlich von Schulveranstaltungen oder sonstigen öffentlichen Veranstaltungen für Werbezwecke personenbezogene Daten bei ihren Kindern erhoben hat. Das OLG Hamm hat nun in einem Urteil vom 20. September 2012 (4 U 85/12) festgestellt, die bei einem Gewinnspiel anlässlich einer Jobmesse von einer gesetzlichen Krankenkasse vorgenommene Datenerhebung (Name, Geburtsdatum, Kontaktdaten) bei 15-Jährigen sei unzulässig. Das Urteil trägt hoffentlich dazu bei, die gesetzlichen Krankenkassen davon abzuhalten, bei Schulveranstaltungen Daten bei Minderjährigen zu erheben.

– Nach Fusionen von Krankenkassen habe ich feststellen müssen, dass sich die Harmonisierung beim Schutz der Sozialdaten häufig am schwächeren Datenschutzstandard eines der Fusionspartner orientiert. Oft glaubten dabei die eher an der Wirtschaftlichkeit des neu entstandenen „Unternehmens“ orientierten Vorstände, auf gesetzliche Vorgaben des Sozialdatenschutzes verzichten zu können. Bemerkbar macht sich dies u. a. dadurch, dass sich Eingaben der Versicherten wieder um Themen drehen, die man mit den jeweiligen Fusionspartnern teilweise bereits vor Jahren geklärt hatte. Dazu zählen z. B. auch die Themen Krankenhausentlassungsberichte und Selbstauskunftsbögen (vgl. auch Nr. 11.1.8).

– Auch organisatorisch haben Fusionen bei den gesetzlichen Krankenkassen Auswirkungen. So verlieren die bisherigen internen Datenschutzbeauftragten mit der Fusion ihrer Krankenkasse ihr Amt (vgl. Bundesarbeitsgericht, Urteil vom 29. September 2010 – 10 AZR 588/09).

Ich werde bei künftiger Beratungs- und Kontrolltätigkeit der Frage nachgehen, inwieweit einmal erreichte Datenschutzstandards eingehalten werden. Der verstärkte Wettbewerb im Gesundheitswesen darf nicht zu Lasten des Datenschutzes und der Persönlichkeitsrechte gehen.

11.1.2 Viel Lärm um die Hausarztzentrierte Versorgung

Bei der Einschaltung privater Rechenzentren für die Abrechnung der Hausarztzentrierten Versorgung habe ich mich besonders dafür eingesetzt, dass es keine Abstriche beim Datenschutz gibt.

Am 4. August 2011 trat § 295a SGB V in Kraft, der eine neue Rechtsgrundlage für die Einschaltung privater Dritter bei der Abrechnung der Hausarztzentrierten Versorgung schafft, nachdem die Verträge zur Hausarztzentrierten Versorgung, die auf der alten Rechtslage gründeten, in mehreren Bundesländern aufgrund einer obergerichtlichen Entscheidung ausgesetzt worden waren (vgl. 23. TB Nr. 11.1.1). Im Gesetzgebungsverfahren habe ich mich besonders dafür eingesetzt, dass das Datenschutzniveau bei der Abrechnung über private Stellen demjenigen bei der Abrechnung über die Kassenärztlichen Vereinigungen entspricht. Dies sollen verschiedene datenschutzrechtliche Mechanismen gewährleisten.

§ 295a Absatz 1 und 2 SGB V schafft die Rechtsgrundlage für eine Abrechnung zwischen drei verschiedenen Akteuren: Dies erlaubt den Datenfluss bei der Abrechnung zwischen „Leistungserbringern“ (Ärzten) und „Vertragspartnern auf Leistungserbringerseite“, etwa dem Hausärzteverband, sowie zwischen „Vertragspartnern auf Leistungserbringerseite“ und „anderen Stellen“, wie beispielsweise Rechenzentren. Beim Datenfluss zwischen Ärzten und ihren Vertragspartnern handelt es sich um eine Datenübermittlung, beim Datenfluss zwischen Vertragspartnern und von diesen beauftragten Rechenzentren um Auftragsdatenverarbeitung im Sinne des § 11 BDSG. In beiden Verhältnissen gilt nach der neuen gesetzlichen Regelung das Sozialgeheimnis nach § 35 SGB I entsprechend, auch soweit die Beteiligten keine Sozialleistungsträger sind und daher nicht unmittelbar an das Sozialgeheimnis gebunden wären. Für das Verhältnis zwischen Vertragspartnern und deren Rechenzentren ordnet § 295a SGB V an, dass hier statt § 11 BDSG der für das Sozialrecht zugeschnittene § 80 SGB X gelten soll. Dies hat zur Folge, dass auch hier der Sozialdatenschutz greift. Hierfür habe ich mich im Gesetzgebungsverfahren besonders eingesetzt.

Grundlage der Teilnahme an der hausarztzentrierten Versorgung ist die Einwilligung der Teilnehmer nach § 73b Absatz 3 SGB V. Diese Einwilligung umfasst auch die Abrechnung über private Stellen. Daher handelt es sich insoweit nicht um eine echte Einwilligung im Sinne des § 67b Absatz 2 SGB X. Der oder die Versicherte sind zuvor darüber zu informieren, dass die Einwilligung in das Versorgungsprogramm mit einer Abrechnung über private Dritte verbunden sein kann. Auch das war mir sehr wichtig. Im Verhältnis zwischen Hausärzteverband und Rechenzentrum habe ich mich zudem für einige Besonderheiten eingesetzt: So findet § 80 Absatz 5 SGB X keine Anwendung und Unterauftragsverhältnisse sind grundsätzlich ausgeschlossen. Die Datenschutzaufsicht richtet sich nach § 38 BDSG.

Die Grundsatzentscheidung, bei der Abrechnung von ärztlichen Leistungen private Dritte zu beteiligen, ist gesundheitspolitischer Natur und unterliegt der Entscheidungsprärogative des Gesetzgebers. Im Gesetzgebungsverfahren war mir deshalb besonders wichtig, dass die Datenübermittlungen durchgängig dem Sozialgeheimnis unterliegen und dass es nicht zu einer Absenkung des datenschutzrechtlichen Schutzstandards kommt. Diese rechtliche Absicherung ist auch vor dem Hintergrund zu begrüßen, dass die befristete Vorgängerregelung Rechtsstreitigkeiten nach sich gezogen hatte, die bundesweit zur Aussetzung der bestehenden Verträge zur Hausarztzentrierten Versorgung führte.

Die Vorschrift ist grundsätzlich neben § 295 Absatz 1b SGB V anwendbar, sodass die Ärzte nicht verpflichtet sind, private Dritte einzuschalten. Eine Abrechnung unmittelbar zwischen Arzt und Krankenkasse i. S. v. § 295 Absatz 1b SGB V bleibt danach möglich.

In vielen Bundesländern wurden auf Basis dieser geänderten Rechtslage neue Verträge zur Hausarztzentrierten Versorgung geschlossen. Mehrere gesetzliche Krankenkassen, die in meiner Zuständigkeit liegen, haben mir die entsprechenden Vertragsentwürfe vorgelegt. Datenschutzrechtliche Probleme haben sich hierbei bislang nicht ergeben.

11.1.3 Das GKV-Versorgungsstrukturgesetz

Die von mir im Gesetzgebungsverfahren zum GKV-Versorgungsstrukturgesetz vorgeschlagenen datenschutzrechtlichen Verbesserungen, insbesondere zu den Transparenzregelungen (§§ 303a ff. SGB V), wurden berücksichtigt.

Mit dem „Gesetz zur Verbesserung der Versorgungsstrukturen in der gesetzlichen Krankenversicherung (GKV-Versorgungsstrukturgesetz – GKV-VStG)“ vom 22. Dezember 2011 (BGBl. I S. 2983) soll dem Ärztemangel in ländlichen Regionen begegnet werden. Das Gesetz enthält auch eine Reihe wichtiger datenschutzrechtlicher Vorschriften, über die ich an anderer Stelle berichte (vgl. Nr. 4.1 und Nr. 11.1.4).

Von besonderer Bedeutung ist hier die Neufassung der seit dem 1. Januar 2004 bestehenden Transparenzregelungen (§§ 303a bis 303e SGB V). Danach dürfen Daten, die im Rahmen des morbiditätsorientierten Risikostrukturausgleichs (Morbi-RSA-Daten) erhoben worden sind, von den in § 303e SGB V genannten Einrichtungen (Krankenkassen, Kassenärztlichen Vereinigungen, Hochschulen, Patientenorganisationen, Bundesärztekammern, Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen etc.) verarbeitet und genutzt werden, wenn dies für die Erfüllung ihrer Aufgaben erforderlich ist. Dabei handelt es sich um Leistungs- und Abrechnungsdaten der Krankenkassen. Hiergegen habe ich keine grundsätzlichen Bedenken, vor allem, da die Daten lediglich anonymisiert zur Verfügung gestellt werden und eine öffentliche Datenaufbereitungsstelle bei jeder Anfrage die Erforderlichkeit prüft. Dabei geht es um eine Vollerhebung, in die alle 70 Millionen gesetzlich Versicherten einbezogen sind.

Das Nähere regelt die Verordnung zur Umsetzung der Vorschriften über die Datentransparenz (Datentransparenzverordnung – DaTraV) vom 10. September 2012 (BGBl. I S. 1895). An dem Datenaufbereitungsverfahren beteiligt sind drei Stellen: das Bundesversicherungsamt (BVA), die Vertrauensstelle und die Datenaufbereitungsstelle.

Zwar werden nach § 2 Absatz 1 und 2 DaTraV sowohl die Aufgaben der Vertrauensstelle als auch die Datenaufbereitungsstelle durch das Deutsche Institut für Medizinische Dokumentation und Information (DIMDI) wahrgenommen. Die datenschutzrechtlichen Bedenken hiergegen habe ich jedoch deshalb zurückgestellt, weil § 2 Absatz 3 DaTraV bestimmt, dass Vertrauensstelle und Datenaufbereitungsstelle räumlich, organisatorisch und personell jeweils eigenständig geführt werden müssen. Die Umsetzung dieser Vorgaben werde ich mir sehr genau ansehen.

Nach dem ursprünglichen Entwurf sollte die Vertrauensstelle die gesamten Morbi-RSA-Daten (Leistungsdaten und Pseudonyme) erhalten, diese erneut pseudonymisieren und anschließend an die Datenaufbereitungsstelle weiterleiten. Datenschutzfreundlicher ist jedoch das nunmehr umgesetzte Verfahren, bei dem das Bundesversicherungsamt die Leistungsdaten an die Datenaufbereitungsstelle und die Pseudonyme an die Vertrauensstelle jeweils getrennt voneinander übermittelt (vgl. Kasten zu Nr. 11.1.3).

Wichtig war mir auch, dass der Umfang, die Auswahl und das Verfahren der Übermittlung der Daten in den Transparenzvorschriften selbst oder zumindest in einer Rechtsverordnung hinreichend bestimmt sind. Dies betrifft vor allem den Umfang der vom Bundesversicherungsamt an die Vertrauensstelle zu übermittelnden Daten sowie die ausführliche Darstellung des Pseudonymisierungsverfahrens.

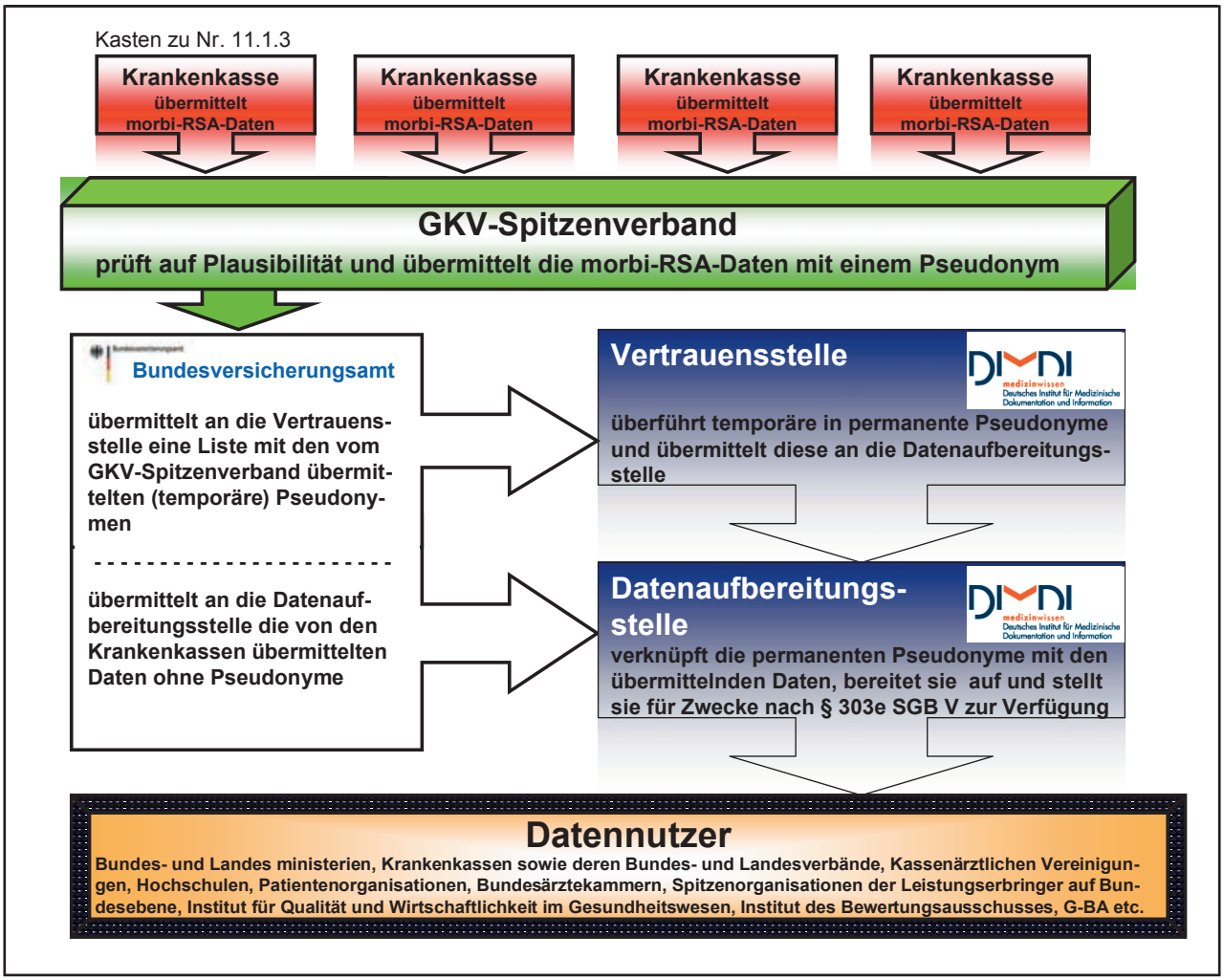
Ich begrüße die Klarstellung, dass die Aufgaben der Datentransparenz öffentliche Stellen des Bundes wahrnehmen sollen. Die Vertrauensstelle und die Datenaufbereitungsstelle nach §§ 303c, 303d SGB V unterliegen meiner Datenschutzaufsicht. Beteiligt bin ich nun auch an der Auswahl der Daten, die für strukturierte Behandlungsprogramme erforderlich sind. Bislang wurde dies durch Rechtsverordnung des Bundesgesundheitsministe-

riums geregelt, nun sollen Richtlinien des Gemeinsamen Bundesausschusses, an deren Entstehen ich nach § 91 Absatz 5a SGB V zu beteiligen bin (vgl. Nr. 11.1.4), diese Daten festlegen.

Weiter gibt es jetzt eine Übermittlungsbefugnis für den Austausch von Sozialdaten zwischen Krankenkassen bzw. Kassenärztlichen Vereinigungen für die Fehlverhaltensbekämpfung im Gesundheitswesen (§ 197a und § 81a Absatz 3a SGB V). Die Erforderlichkeit einer Zusammenarbeit ergibt sich sowohl im Bereich der Ermittlungen als auch im bei der Rechtsverfolgung. Da seit Einführung der Fehlverhaltensbekämpfungsstellen eine entsprechende Übermittlungsbefugnis fehlte, hatte sich ein Widerspruch ergeben zwischen dem datenschutzrechtlich Zulässigen und dem praktisch für die Fehlverhaltensbekämpfung im Gesundheitswesen Erforderlichen. Dieser Widerspruch ist nunmehr beseitigt.

Insgesamt bin ich mit der geltenden Fassung des GKV-VStG aus datenschutzrechtlicher Sicht durchaus zufrieden. Gleichwohl wurden und werden von verschiedenen Seiten Wünsche geäußert, die genutzte Datenbasis zu erweitern oder datenschutzfreundliche Lösungen aufzuweichen. Ich werde darauf achten, dass das festgelegte Datenschutzniveau nicht unterschritten oder abgesenkt wird.

Kasten zu Nr. 11.1.3



11.1.4 Stellungnahme bei Beschlüssen des Gemeinsamen Bundesausschusses – eine neue Aufgabe

Seit dem 1. Januar 2012 ist mir bei Beschlüssen des Gemeinsamen Bundesausschusses, die die Erhebung, Verarbeitung oder Nutzung personenbezogener oder personenbeziehbarer Daten regeln oder voraussetzen, Gelegenheit zur Stellungnahme zu geben.

Der Gemeinsame Bundesausschuss (G-BA) wird von den Kassenärztlichen Bundesvereinigungen, der Deutschen Krankenhausgesellschaft und dem Spitzenverband Bund der Krankenkassen gebildet. Er beschließt insbesondere die zur Sicherung der ärztlichen Versorgung erforderlichen und verbindlichen Richtlinien über die Gewährung für eine ausreichende, zweckmäßige und wirtschaftliche Versorgung der Versicherten. Er legt damit fest, welche Leistungen der medizinischen Versorgung von der gesetzlichen Krankenversicherung erstattet werden. Darüber hinaus beschließt er Maßnahmen der Qualitätssicherung für den ambulanten und stationären Bereich des Gesundheitswesens. Im Einzelnen sind seine Aufgaben im Fünftem Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung (SGB V) geregelt.

Seit Anfang 2012 hat mir der G-BA – nach § 91 Absatz 5a SGB V – bei Beschlüssen, die die Erhebung, Verarbeitung oder Nutzung personenbezogener oder personenbeziehbarer Daten regeln oder voraussetzen, Gelegenheit zur Stellungnahme zu geben. Diese Stellungnahme ist in die Entscheidung einzubeziehen. Der Gesetzgeber hat sich zu dieser Regelung entschlossen, da bei Beschlüssen und Richtlinien des G-BA „die Erhebung, Verarbeitung und Nutzung personenbezogener oder -beziehbarer Daten eine immer größere Rolle“ spielen und deshalb „eine frühzeitige Berücksichtigung datenschutzrechtlicher Aspekte … sicherzustellen“ ist (Bundestagsdrucksache 17/6906 S. 68).

Im Rahmen dieser neuen Aufgabe habe ich u. a. Stellung genommen

- zur redaktionellen Gestaltung von Richtlinien und den „Tragenden Gründen“, nicht zuletzt, um die datenschutzrechtlich relevanten Regelungen auch für verständige Laien nachvollziehbarer zu gestalten,
- dazu, dass Regelungen durch den G-BA selbst zu treffen sind und eine Subdelegation an eine beteiligte dritte Stelle nicht in Betracht kommt,
- zur Statthaftigkeit einer vorgesehenen Datenerhebung nach dem SGB V und
- zur Zulässigkeit einer Datenerhebung aufgrund einer Einwilligung.

Die Prüfung und Stellungnahme zu den teilweise komplexen und sehr umfangreichen Beschlussvorlagen des G-BA binden als neue Aufgabe in meinem Hause erhebliche personelle Ressourcen, die für anderweitige wichtige Aufgaben nicht mehr zur Verfügung stehen.

11.1.5 Das Lichtbild auf der Gesundheitskarte

Die Aufforderung ihrer gesetzlichen Krankenkasse, ein Lichtbild für die neue elektronische Gesundheitskarte (eGK – vgl. Nr. 4.1) zu senden, stieß bei vielen Betroffenen auf Kritik.

Im Berichtszeitraum erreichten mich zahlreiche Eingaben zu diesem Thema. Im „Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG)“ vom 14. November 2003 (BGBl. I S. 2190) war bereits festgelegt worden, dass die Krankenversichertenkarte u. a. ein Lichtbild enthalten muss (§ 291 Absatz 2 SGB V). Von Gesetzes wegen hätte „die Erweiterung der Krankenversichertenkarte um das Lichtbild … spätestens bis zum 1. Januar 2006 … erfolgen“ müssen (§ 291 Absatz 2 a. E. SGB V). Die Aufnahme des Lichtbildes soll die eindeutige Zuordnung der Krankenversichertenkarte zum jeweiligen Karteninhaber verbessern, um damit Missbrauch zu verhindern (Bundestagsdrucksache 15/1525 S. 143). Später erfolgte eine gesetzliche Einschränkung insofern, als Versicherte bis zur Vollendung des 15. Lebensjahres sowie Versicherte, deren Mitwirkung bei der Erstellung des Lichtbildes nicht möglich ist, eine Krankenversichertenkarte ohne Lichtbild erhalten. Über § 291a Absatz 2 Satz 1 SGB V muss ein Lichtbild auch auf der neuen eGK (vgl. Nr. 4.1) sein.

Insoweit darf die zuständige Krankenkasse nach § 284 Absatz 1 Satz 1 Nummer 2 SGB V die Bilddaten ihrer Versicherten erheben und speichern, da dies für die Ausstellung der Krankenversichertenkarte auch in Form der elektronischen Gesundheitskarte erforderlich ist. Auf die Frage, wie lange die Bilddaten gespeichert werden dürfen, regelt § 304 Absatz 1 Satz 1 SGB V i. V. m. § 84 Absatz 2 SGB X: Sozialdaten sind danach zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Da die zuständige Krankenkasse aufgrund des bestehenden Versicherungsverhältnisses verpflichtet ist, im Falle des Defektes oder Verlustes eine Ersatzkarte auszustellen, erlischt die Pflicht, die Bilddaten zu speichern, endgültig erst mit der Beendigung des Versicherungsverhältnisses. Zu diesem Zeitpunkt muss die gesetzliche Krankenkasse die gespeicherten Bilddaten löschen.

In einem erstinstanzlichen Urteil hat das Sozialgericht Düsseldorf entschieden, dass die eGK in der vorgesehenen Form nicht auf verfassungsrechtliche Bedenken stoße (Urteil vom 28. Juni 2012 – S 9 KR 111/09 –). Das Urteil bezieht sich nach Aussagen des Gerichts zunächst auf die jetzt in Umlauf gebrachte eGK, die lediglich die bisherige Krankenversichertenkarte ersetzt. Nach Presseberichten hat der Kläger gegen dieses Urteil Berufung eingelegt.

11.1.6 Externe Beratungsstellen der Krankenkassen – Nicht alle Informationen sind zulässig

Eine große Krankenkasse berät ihre Mitglieder per Telefon nicht nur über Tarife und versicherungsrechtliche Fragen, sondern auch bei gesundheitlichen Problemen.

Diese Tätigkeit wurde einem externen Beratungsunternehmen übertragen.

Eine Krankenkasse bot ihren Mitgliedern an, dass sie sich rund um die Uhr an sieben Tagen in der Woche bei ihrem Ärztezentrum „zu allen Fragen rund um Medizin und Gesundheit“ informieren könnten. Sie hatte hierzu mit einem Unternehmen eine Vereinbarung zur medizinischen Beratung ihrer Mitglieder durch ärztliches Personal abgeschlossen und überließ dem Unternehmen die halbjährlich aktualisierten Stammdaten aller ihrer Mitglieder (Name, Adresse, Geburtsdatum, Telefonnummer, E-Mail-Adresse). Die Angaben sollten zu Abrechnungszwecken zwischen der Krankenkasse und dem Beratungsunternehmen erforderlich sein. Das Beratungsunternehmen wiederum meldete der Krankenversicherung, aus welchem Grund das Mitglied angerufen hatte. Die automatisierte Mitteilung enthielt Angaben darüber, ob das Mitglied einen Arzt/Zahnarzt oder ein Krankenhaus suchte oder eine medizinische, pharmakologische oder eine Beratung aus dem Bereich der Prävention wünschte. Weiterhin wurden Datum, Uhrzeit und Art des Kontaktes sowie der Anlass (versicherungsrechtliche oder medizinische Frage) mitgeteilt. Diese Informationen speicherte die Krankenkasse sechs Monate lang. Die ratsuchenden Versicherten blieben jedoch bei ihrem Anruf im Unklaren darüber, dass sie mit einem externen Unternehmen und nicht mit ihrer Krankenversicherung telefonierten.

Ich habe zwar keine grundsätzlichen Bedenken, wenn die Krankenkassen ihrer Verpflichtung aus § 1 SGB IX i. V. m. §§ 13 und 14 SGB I sowie § 11 Absatz 4 SGB V zur Beratung und Aufklärung der Bevölkerung auch durch Einschaltung geeigneter ärztlicher Beratungsunternehmen nachkommen. Dies darf aber nicht so weit gehen, dass die externen Berater alle Stammdaten der Versicherten der Krankenkasse jederzeit einsehen können.

Die gesetzliche Krankenkasse hat meiner Kritik an dem Verfahren Rechnung getragen. Die beratenden Ärzte können jetzt nur noch auf die absolut notwendigen Stammdaten des jeweiligen Anrufers zurückgreifen. Die Angaben, die der ärztliche Berater der Krankenkasse übermittelt, müssen sich ebenfalls auf das unbedingt notwendige Maß beschränken. Die Krankenkasse lässt sich nur noch Informationen dazu übermitteln, ob ein Rückruf des beratenden Arztes beim Versicherten erfolgte und ob das Krankenkassenmitglied eine versicherungsrechtliche oder eine medizinische Frage hatte. Diese Informationen werden getrennt von den allgemeinen Leistungsdaten zu Abrechnungszwecken mit dem Beratungsunternehmen gespeichert und nach sechs Monaten gelöscht. Angaben zu gesundheitlichen Verhältnissen der Anrufer dürfen auf keinen Fall weitergegeben werden.

Schließlich wird nun – auch auf meine Aufforderung hin – der Anrufer darüber informiert, dass er mit einem externen Unternehmen und nicht mit seiner Krankenkasse telefoniert. Gleichzeitig wird auf die datenschutzrechtlichen Gesichtspunkte hingewiesen, die auf der Internetseite der Krankenkasse veröffentlicht sind. Damit wird sowohl von Seiten der Krankenkasse als auch von Seiten des Unternehmens eine ausreichende Transparenz hergestellt, damit der Betroffene weiß, mit wem er telefoniert, welche Daten gespeichert werden, wer Zugang zu diesen Daten hat und welche Daten an die Krankenkasse übermittelt werden.

11.1.7 Wird der Medizinische Dienst der Krankenversicherung überflüssig?

Immer mehr Krankenkassen beauftragen externe Gutachterstellen mit Aufgaben, die das Sozialgesetzbuch dem Medizinischen Dienst der Krankenversicherung (MDK) zugewiesen hat.

In zahlreichen Eingaben, aber auch durch Hinweise von Verbänden und von Kollegen aus den Bundesländern wurde ich darauf aufmerksam gemacht, dass gesetzliche Krankenkassen immer häufiger externe Beratungsdienste damit beauftragen, Gutachten zu erstellen, die sie etwa bei Entscheidungen über Leistungsanträge unterstützen. Auch bei meinen Kontrollen im Berichtszeitraum habe ich dies feststellen müssen (vgl. auch Nr. 11.1.6, 11.1.8 und 11.1.10).

Die gesetzlichen Krankenkassen berufen sich hierbei entweder auf eine „Datenverarbeitung im Auftrag“ nach § 80 SGB X oder eine Beauftragung nach § 197b SGB V als Rechtsgrundlage. Bei einer „Datenverarbeitung im Auftrag“ handelt es sich lediglich um eine „Hilfsfunktion“, die mit einem Auftragsverhältnis im Sinne der §§ 662 ff. BGB nichts zu tun hat. Bei der Datenverarbeitung im Auftrag bleibt der Auftraggeber auch weiterhin für den Umgang mit den Daten verantwortlich. Eine Übermittlung findet nicht statt, da der Auftragnehmer kein Dritter i. S. d. Gesetzes ist (§ 3 Absatz 8 Satz 3 BDSG, § 67 Absatz 7 Satz 3 SGB X). Das Wesen eines Gutachters ist es aber gerade, dass er aufgrund der ihm zur Verfügung gestellten Daten eigenverantwortlich Schlussfolgerungen für die tatsächliche Beurteilung eines Geschehens oder Zustands ableitet. Dies geht also weit über eine „Hilfsfunktion“ hinaus. Es handelt sich datenschutzrechtlich um eine Funktionsübertragung und damit ist die Bekanntgabe personenbezogener Daten an einen Gutachter eine „Übermittlung“ im Sinne von § 3 Absatz 4 Nummer 3 BDSG und § 67 Absatz 6 Nummer 3 SGB X. Hiervon gehen auch das Bundesversicherungsamt (BVA) und die staatlichen Aufsichtsbehörden der Länder aus.

Nach § 197b SGB V können gesetzliche Krankenkassen ihnen obliegende Aufgaben grundsätzlich Dritten übertragen, wenn die Aufgabenwahrnehmung dadurch wirtschaftlicher ist, es im Interesse der Betroffenen liegt, die Rechte der Versicherten nicht beeinträchtigt werden und keine wesentliche Aufgabe zur Versorgung der Versicherten in Auftrag gegeben wird. Ich habe erhebliche Zweifel, ob diese Voraussetzungen hier vorliegen. So fragt sich schon, ob es wirtschaftlicher ist, eine zusätzliche Stelle mit einem Gutachten zu beauftragten, obwohl mit dem MDK eine Stelle vorhanden ist, die von den gesetzlichen Krankenkassen im Umlageverfahren finanziert wird (§ 281 Absatz 1 Satz 1 SGB V), zu deren gesetzlichen Aufgaben es gehört, sozialmedizinische Gutachten zur Klärung von Sachverhalten zu erstellen. Den Krankenkassen obliegt es zudem, den MDK so auszustatten, dass

er Prüfaufträgen in angemessener Zeit nachkommen kann. Zwar kann es in Einzelfällen notwendig sein, einen externen Gutachter heranzuziehen. Dies hat allerdings durch den MDK zu geschehen (§ 279 Absatz 5 Satz 1 2. Halbsatz SGB V), mit der Folge, dass die Gutachten an den MDK und nicht an die gesetzliche Krankenkasse zu erstatten sind. Sie unterliegen auch den Vorgaben des §§ 275 ff. SGB V. Eine Beauftragung von externen medizinischen Gutachtern durch die gesetzlichen Krankenkassen führt dagegen zur Umgehung dieser gesetzlichen Regelungen.

11.1.8 Rechtfertigt das „Krankenfallmanagement“ die Erhebung zusätzlicher Daten?

Arbeitsunfähige Versicherte werden von gesetzlichen Krankenkassen unzulässig ausgefragt – bisweilen wird versteckt mit Leistungsverweigerung oder -entzug gedroht.

In den vergangenen Monaten wurde in der Presse immer wieder kritisiert, dass gesetzliche Krankenkassen umfassend Daten über solche Versicherte erheben, die längere Zeit arbeitsunfähig sind oder bereits Krankengeld erhalten. Zu diesem Thema haben mich auch zahlreiche Eingaben erreicht. Danach rufen Krankenkassen Versicherte – teilweise wöchentlich – an, machen Hausbesuche oder nehmen Kontakt zu Arbeitgebern auf. Auch mit so genannten „Selbstauskunftsbogen“ erheben Krankenkassen beim Versicherten zusätzliche Daten. Die detaillierte Erhebung von Gesundheitsdaten rechtfertigten sie mit der Prüfung von Krankengeldansprüchen oder mit der Absicht, zur Genesung beizutragen.

Ein Versicherter hat mir Folgendes berichtet: Die Krankenkasse habe sich im Rahmen des Fallmanagements schriftlich an den Arbeitgeber gewandt und diesen gebeten, dem Versicherten eine andere Beschäftigung anzubieten, da dieser aufgrund seiner Erkrankung seine bisherige Tätigkeit nicht mehr ausüben könne. In dem Schreiben an den Arbeitgeber wurde aus dem Gutachten einer Reha-Klinik und aus dem Gutachten des Medizinischen Dienstes der Krankenversicherung (MDK) zitiert. Der Versicherte fürchtet nun um seinen Arbeitsplatz.

Als gesetzliche Grundlage für diese Datenerhebung wurden mir wiederholt die Umsetzung der gesetzlichen Ansprüche von Versicherten auf ein Versorgungsmanagement nach § 11 Absatz 4 SGB V und auf Leistungen zur Teilhabe nach § 4 SGB IX genannt. Diese Regelungen sind aber ohne weitere gesetzliche Detailregelungen aus datenschutzrechtlicher Sicht nicht tragfähig, da sie keine Befugnisse zur Erhebung und Speicherung von Sozialdaten enthalten.

Selbstauskunftsbogen

In meinem 21. TB (Nr. 13.1.3) habe ich mich dazu bereits ausführlich geäußert. Das Erheben und Verarbeiten von Sozialdaten durch Krankenkassen mittels „Selbstauskunftsbogen“ ist weder bei Versicherten noch bei deren Ärzten zulässig. Zur Erhebung der damit abgefragten Sozialdaten ist weitgehend der MDK im Rahmen seiner gesetzlichen Aufgabenerfüllung berechtigt. Die Krankenkassen dürften allenfalls um die Übermittlung dieser Daten an den MDK bitten.

Meine Rechtsauffassung wird vom Bundesversicherungsamt (BVA) und dem BMG geteilt. Dass einige Krankenkassen ungeachtet dessen an ihrer Verfahrensweise festhalten, wurde mir unverhohlen damit begründet, in meinem Tätigkeitsbericht würden datenschutzrechtliche Verstöße ohne Nennung des Namens der betroffenen Krankenkasse dargestellt, die Versicherten und die Öffentlichkeit würden also nicht erfahren, wie eine bestimmte Kasse mit den Sozialdaten ihrer Versicherten umginge. Ich möchte deshalb von dieser Praxis abweichen. Negativ aufgefallen sind mir in Sachen Selbstauskunftsbogen in letzter Zeit die folgenden Kassen: Deutsche BKK, KKH, IKK classic, SBK Siemens-Betriebskrankenkasse.

Positiv möchte ich vermerken, dass sich einige Kassen ausdrücklich von diesem Verfahren distanzieren, etwa die Audi-BKK (s. u.), BKK Mobil Oil, pronova BKK, BKK firmus, SECURVITA BKK.

Versicherte, die länger arbeitsunfähig sind und an die ggf. ein Krankengeld auszuzahlen ist, erhalten von einigen Krankenkassen ein Anschreiben mit allgemeinen Informationen und mit der Bitte um „Mithilfe“. Um Krankengeldansprüche prüfen zu können, sollen beigefügte Formulare ausgefüllt zurückgesandt werden. Es handelt sich dabei um „Selbstauskunftsbogen“ sowie um Vordrucke für Einwilligungen dazu, der Krankenkasse ausführliche medizinische Untersuchungsberichte zur Verfügung zu stellen. Gegenüber den Versicherten wird der Eindruck erweckt, dass die Angaben gemacht werden müssen, um die gesetzliche Leistung Krankengeld erhalten zu können.

Datenschutzrechtlich ist diese Vorgehensweise aus mehreren Gründen unzulässig: In den Fällen des § 275 Absatz 1 und 2 SGB V, z. B. bei Arbeitsunfähigkeit, sind die Krankenkassen verpflichtet, den MDK mit einer Begutachtung bzw. Prüfung zu beauftragen. Es besteht jedoch keine Befugnis der Kasse, zusätzliche Daten zur Arbeitssituation oder zur Gesundheit zu erheben, die mit der Prüfung der Leistungsvoraussetzungen nicht in Zusammenhang stehen. Ausschließlich der MDK ist gesetzlich befugt, weitergehende Daten zu erheben oder zu verarbeiten, sofern dies im konkreten Einzelfall erforderlich ist (§ 276 Absatz 2 Satz 1 erster Halbsatz SGB V). Dies verdeutlicht die Regelung des § 277 Absatz 1 Satz 1 SGB V, wonach der MDK der jeweiligen Krankenkasse lediglich das Ergebnis der Begutachtung mitteilen darf.

Dementsprechend sind vorformulierte Schweigepflichtentbindungserklärungen in Selbstauskunftsbogen, nach denen sämtliche ärztliche Unterlagen an die Krankenkasse herausgegeben werden dürfen, mit dem geltenden Recht nicht vereinbar. Diese Beschränkung der Krankenkassen verdeutlicht auch die Regelung des § 275 Absatz 1a Satz 4 SGB V. Danach können die Krankenkassen von einer Beauftragung des MDK nur absehen, wenn sich die medizinischen Voraussetzungen der Arbeitsunfähigkeit eindeutig aus den der jeweiligen Krankenkasse vor-

liegenden ärztlichen Unterlagen, wie z. B. Arbeitsunfähigkeitsbescheinigungen, ergeben. Zu diesen Unterlagen gehören keine Behandlungsdaten des Versicherten (Krankenhausentlassungsberichte, Arztbriefe, Befundberichte, ärztliche Gutachten etc.).

Soweit sich Krankenkassen auf ein Rundschreiben des GKV-Spitzenverbandes vom 31. Mai 2012 berufen, habe ich immer wieder darauf hingewiesen, dass derartige Rundschreiben eine gesetzliche Grundlage zur Datenerhebung nicht ersetzen und vorhandene Gesetzesbestimmungen nicht außer Kraft setzen können. Zudem lässt das zitierte Rundschreiben keine Hinweise auf eine zulässige Datenerhebung in der vorgefunden Form erkennen. Selbst die aus datenschutzrechtlicher Sicht sehr bedenkliche „Begutachtungsanleitung – Arbeitsunfähigkeit (AU)“ des GKV-Spitzenverbandes vom 12. Dezember 2011 sieht eine Datenerhebung in dem vorgefundenen Umfang nicht vor.

Meiner Aufforderung, die vorhandenen Selbstauskunftsbogen nicht mehr zu verwenden und bereits ausgefüllte zu vernichten, ist z. B. die Audi BKK gefolgt.

Um das Problem „Selbstauskunftsbogen“ grundsätzlich zu lösen, habe ich mit dem BMG und dem GKV-Spitzenverband die Bildung einer Arbeitsgruppe vereinbart, deren Ziel es ist, bis Ostern 2013 die Selbstauskunftsbogen in der jetzigen Form abzuschaffen und datenschutzgerecht sicherzustellen, dass die Krankenkassen die für die Bearbeitung von Krankengeldfällen erforderlichen Daten erhalten. Dabei ist ein modular aufgebautes System angedacht, in dem zielgerichtet nur die für den Einzelfall erforderlichen und gesetzlich zulässigen Daten erhoben werden.

Telefonische Beratung und Handakten von Mitarbeitern im Krankenfallmanagement

Die Mitarbeiter der Deutschen BKK führen mit den Versicherten bei Arbeitsunfähigkeit regelmäßig telefonische „Beratungsgespräche“, wenn zu erwarten ist, dass Krankengeld auszuzahlen sein wird. In den von mir kontrollierten Geschäftsstellen wurden Handakten über jeden arbeitsunfähigen Versicherten geführt, die, neben dem ausgefüllten Selbstauskunftsbogen, mehr oder weniger ausführliche Gesprächsvermerke mit zum Teil detaillierten Angaben zur familiären und gesundheitlichen Situation, Krankenhausentlassungsberichte, Reha-Entlassungsberichte, hausärztliche Unterlagen, Gutachten des MDK und vieles mehr enthalten. Von Petenten wird mir zudem berichtet, in den dargestellten Telefonaten würde z. T. ein erheblicher Druck durch die „Fallmanager“ der Krankenkassen aufgebaut, in dem teilweise mit Leistungskürzungen gedroht wird oder zu einem Wechsel der Krankenkasse aufgefordert werde. Die Ergebnisse der Beratungsgespräche werden von den Fallmanagern – neben handschriftlichen Vermerken in Handakten – im EDV-Programm „Krankengeld Fallmanagement“ als individuelle Gesprächsnotizen in Freitextfeldern aufgezeichnet. Die vorgefundenen Programme sahen eine maschinelle Löschung der gespeicherten Daten nicht vor.

Weder für die telefonische Datenerhebung noch für deren Speicherung gibt es eine gesetzliche Grundlage. Die kontrollierten Kassen wurden von mir gebeten, unverzüglich jegliche Datenerhebung und -speicherung durch Telefonate mit den Versicherten einzustellen sowie vorhandene Daten und gespeicherte Vermerke über die Telefongespräche zu löschen.

Einschaltung „neutraler Stellen“

In zahlreichen Fällen bieten Mitarbeiter der Deutschen BKK ihren Versicherten – z. B. bei Rückenleiden oder psychischen Erkrankungen – den Besuch bei einer „neutralen Stelle“ an. Diese „neutrale Stelle“ ist ein externer Gutachter, der die Versicherten untersucht und weitere oder alternative Maßnahmen zur schnellen Beendigung der Arbeitsunfähigkeit empfiehlt. Wenn Versicherte dieser Verfahrensweise während des Telefonates zustimmen, übermittelt die Krankenkasse die Daten der Versicherten (Name, Telefonnummer) an diese „neutrale Stelle“, damit diese anschließend Kontakt zu den Versicherten aufnimmt. Die Deutsche BKK versteht diese Vorgehensweise als „Serviceleistung“ gegenüber ihren arbeitsunfähig erkrankten Versicherten.

Bereits vor Ort haben meine Mitarbeiter der Krankenkasse vorgeschlagen, den Versicherten lediglich die Kontaktdaten der „neutralen Stelle“ (z. B. in einem Flyer zum Thema Rückenleiden) zur Verfügung zu stellen und sie zu bitten, selbst mit der „neutralen Stelle“ Kontakt aufzunehmen. Das Gegenargument, es handele sich oft um Versicherte, die aufgrund ihrer sprachlichen Fähigkeiten zu einer eigenständigen Kontaktaufnahme mit der „neutralen Stelle“ nicht in der Lage seien, kann ich nicht nachvollziehen. Es zeugt von mangelndem Respekt vor den Versicherten. Viele Institutionen – auch gesetzliche Krankenkassen – sind zudem aus Servicegründen dazu übergegangen, „Flyer“ auch in anderen Sprachen bereitzustellen.

Die dargestellte Vorgehensweise ist datenschutzrechtlich unzulässig und verletzt das Sozialgeheimnis (§ 35 Absatz 1 SGB I). Die Vermittlung von Versicherten im Krankengeldbezug an „neutrale Stellen“ gehört nicht zu den gesetzlichen Aufgaben einer Krankenkasse. Eine gesetzliche Grundlage für die Übermittlung von Sozialdaten an die „neutralen Stellen“ gibt es nicht.

Ich habe die Deutsche BKK aufgefordert, auf die rechtswidrige Einschaltung „neutraler Stellen“ zu verzichten. Die dargestellten zahlreichen Verstöße der Deutschen BKK gegen die gesetzlichen Vorgaben zum Persönlichkeitsschutz der Versicherten habe ich nach § 81 Absatz 2 SGB X i. V. m. § 25 Absatz 1 BDSG wegen Verstoßes gegen das Sozialgeheimnisses nach § 35 Absatz 1 SGB I förmlich beanstandet.

Sensible Versichertendaten in Handakten der Sachbearbeiter

Bei der Kontrolle einer Geschäftsstelle der Siemens BKK wurden in Handakten sehr umfangreiche Dokumentationen von Telefongesprächen zwischen Sachbearbeitern und Versicherten vorgefundenen. Diese enthielten Anga-

ben zu persönlichen Empfindungen der Versicherten, wie beispielsweise Suizidgedanken oder ausführliche Beschreibungen der Befindlichkeiten des Versicherten – teilweise mit subjektiven Kommentierungen der Sachbearbeiter. Weiter wurden in diesen Handakten Befund- bzw. Krankenhausentlassungsberichte von behandelnden Ärzten im Original festgestellt. Auch fanden sich Unterlagen, die ausschließlich für die Begutachtung durch den MDK zur Verfügung gestellt worden waren. Gleiches gilt für Stellungnahmen und z. T. vollständige sozialmedizinische Gutachten des MDK.

Da die vorgefundenen Handakten sehr umfangreich waren, baten meine Mitarbeiter um eine vollständige Kopie, um diese dann inhaltlich und rechtlich prüfen zu können. Wie ich bei Sichtung der Handakten feststellen musste, waren die kopierten Handakten entgegen der ausdrücklichen Zusage nicht vollständig. Prüfungsrelevante Originalunterlagen waren entnommen worden, eine ordnungsgemäße Prüfung war mir nicht mehr möglich. Die Herausgabe der vollständigen Handakten wurde nunmehr verweigert.

Gegenüber der Siemens BKK habe ich dies wegen mangelnder Unterstützung bei der Erfüllung meiner Aufgaben nach § 81 Absatz 2 i. V. m. § 25 Absatz 1 BDSG als Verstoß gegen § 24 Absatz 4 BDSG beanstandet.

11.1.9 Die Beteiligung von Gesundheitsservices bei Mutter-Kind-Kuren

Einige gesetzliche Krankenkassen kooperieren bei der Leistungsgewährung von Mutter-Kind-Kuren mit so genannten „Gesundheitsservices". Viele Mütter sahen hierin eine Verletzung datenschutzrechtlicher Grundsätze.

Im Berichtszeitraum erreichten mich zahlreiche Eingaben besorgter Mütter, deren Daten bei der Durchführung von Rehabilitationsmaßnahmen nach § 41 Absatz 1 SGB V – den so genannten Mutter-Kind-Kuren – an ein privates Unternehmen weitergegeben wurden. Diese Unternehmen haben mit einer Vielzahl von kleineren und mittleren Krankenkassen Vereinbarungen über Unterstützungsleistungen bei der Durchführung von Mutter-Kind-Kuren geschlossen, so zum Beispiel die Bereitstellung erforderlicher Kapazitäten in den Kureinrichtungen oder den Buchungsservice für die Krankenkasse und die Versicherte. Hierdurch wird eine bessere Auslastung der Einrichtungen erreicht, wofür die Krankenkasse Preisnachlässe erhält. Ferner werden die Kassen von Verwaltungsaufgaben entlastet. Nach der Bewilligung der beantragten Maßnahme beauftragt die Kasse das Unternehmen, eine bedarfsgerechte Kureinrichtung zu ermitteln. Hierzu gibt sie Angaben zu Mutter und Kind, wie Namen und Anschrift, an das Unternehmen weiter, aber auch Informationen zum Gesundheitszustand oder den vorgesehenen therapeutischen Maßnahmen. Dieses Vorgehen werte ich als Datenverarbeitung im Auftrag nach § 80 SGB X. Die Krankenkasse entscheidet selbst über die Bewilligung der Reha-Maßnahme und trägt weiterhin die datenschutzrechtliche Verantwortung für die rechtmäßige Verarbeitung der Versichertendaten. Das Unternehmen übernimmt hingegen lediglich unterstützende Tätigkeiten. Sofern in diesem Rahmen Daten der Versicherten dem Serviceunternehmen von der Krankenkasse zur Verfügung gestellt werden, ist dies datenschutzrechtlich nicht zu beanstanden.

Bedenken habe ich allerdings, ob in jedem Einzelfall die Angaben versichertenbezogen weitergegeben werden müssen. Eine Krankenkasse ist bereits dazu übergegangen, eine anonymisierte Abfrage vorzunehmen. Ich werde darauf hinwirken, dass die anderen Krankenkassen diesem Beispiel folgen.

11.1.10 Versorgung mit Heil- und Hilfsmitteln

Bei der Versorgung der Versicherten mit Heil- und Hilfsmitteln werden die datenschutzrechtlichen Regelungen nicht immer eingehalten.

Versorgung mit Heilmitteln

Bei der Versorgung von Versicherten mit Heilmitteln hat die Krankenkasse nach § 32 SGB V auf Grundlage der ihr zulässigerweise vorliegenden Unterlagen über den Leistungsanspruch zu entscheiden. Eine Befugnis, für diese Entscheidung zusätzliche Sozialdaten beim Versicherten oder gar beim Leistungserbringer zu erheben, gibt diese Regelung nicht her. Hat die Krankenkasse Zweifel, ob die geltend gemachte Leistung tatsächlich von ihr zu erbringen ist, hat sie nach § 275 Absatz 1 Nummer 1 SGB V den Medizinischen Dienst der Krankenversicherung (MDK) einzuschalten.

Die Verantwortung für die vollständige Verordnung von Heilmitteln, wie z. B. Ergotherapie, physikalische Behandlungen usw., und die damit verbundene Übermittlung von Gesundheitsdaten an die Krankenkasse trägt allerdings der verordnende Arzt, der insoweit zur Offenlegung der erforderlichen Daten befugt ist. Dieser hat nach den Vorgaben in der vom Gemeinsamen Bundesausschuss (G-BA) beschlossenen „Richtlinie über die Verordnung von Heilmitteln in der vertragsärztlichen Versorgung – Heilmittel-Richtlinie" die erforderlichen Daten zu übermitteln, damit die Krankenkasse prüfen kann, ob die beantragten Leistungen notwendig, zweckmäßig und wirtschaftlich sind. Bei unvollständigen Verordnungen ist eine Nachfrage der Krankenkasse beim verordnenden Arzt zulässig. Eine Datenerhebung beim Versicherten oder beim Leistungserbringer ist im Fünften Buch Sozialgesetzbuch weder vorgesehen noch erforderlich.

Soweit einige Krankenkassen als Grundlage für die zusätzliche Datenerhebung das Gebot der Wirtschaftlichkeit anführen, ist darauf hinzuweisen, dass die Wirtschaftlichkeitsprüfung von der gemeinsamen Prüfstelle nach § 106 Absatz 4 SGB V durchgeführt wird. Auch hier gibt es keinen Grund für eine eigene zusätzliche Datenerhebung.

Versorgung mit Hilfsmitteln

Mit dem Gesetz zur Weiterentwicklung der Organisationsstrukturen in der gesetzlichen Krankenversicherung (GKV-OrgWG) vom 15. Dezember 2008 (BGBl. I S. 2426) wurde die Hilfsmittelversorgung in der gesetzlichen Krankenversicherung neu geregelt. Seit dieser Zeit dürfen

Hilfsmittel nur noch auf der Grundlage von Verträgen nach § 127 SGB V an Versicherte abgegeben werden. Damit können die Versicherten nur noch Leistungserbringer in Anspruch nehmen, die auch Vertragspartner ihrer Krankenkasse sind. Ein Auswahlrecht unter allen zugelassenen Leistungserbringern (vgl. 21. TB Nr. 13.1.5) besteht seitdem nicht mehr. In zahlreichen Eingaben beklagen sich betroffene Versicherte darüber, ihre Sozialdaten würden von den Krankenkassen an ihre Vertragspartner weitergegeben. Dies ist aus datenschutzrechtlicher Sicht zu beanstanden, weil die Krankenkassen lediglich gesetzlich verpflichtet sind, ihre Versicherten über die zur Versorgung berechtigten Vertragspartner zu informieren (§ 127 Absatz 5 SGB V). Der Versicherte hat im Versorgungsfall selbst den Kontakt zum Leistungserbringer zu suchen und seine Verordnung sowie die zur Versorgung erforderlichen Daten an den Vertragspartner der Krankenkasse zu übermitteln.

Weiterhin datenschutzrechtlich problematisch ist der Einsatz von so genannten externen Hilfsmittelberatern im Rahmen der Hilfsmittelversorgung von Versicherten. An meiner bereits in meinem 21. TB (Nr. 13.1.5) dazu dargelegten Rechtsauffassung halte ich fest. Nach § 275 Absatz 3 Nummer 1 SGB V können die Krankenkassen in geeigneten Fällen durch den MDK vor Bewilligung prüfen lassen, ob das verordnete Hilfsmittel erforderlich ist. Der MDK hat hierbei den Versicherten zu beraten und kann dabei mit privaten Dritten – beispielsweise mit orthopädischen Beratungsstellen – zusammenarbeiten. Eine Berechtigung der gesetzlichen Krankenkassen, weitere Daten beim Versicherten zu erheben oder statt dem MDK einen Dritten, wie z. B. einen externen Hilfsmittelberater, zur Begutachtung einzuschalten, sieht das SGB V nicht vor. Wenn die gesetzliche Krankenkasse der Auffassung ist, ihr lägen nicht alle erforderlichen Daten vor, „kann“ und hat sie für die weitere Datenerhebung den MDK einzuschalten. Vor diesem Hintergrund ist zu beachten, dass die Krankenkasse in § 275 Absatz 3 Nummer 1 SGB V von einer Beauftragung des MDK absehen kann, wenn sich die medizinischen Voraussetzungen für die Hilfsmittelversorgung aus der Aktenlage der bei der Krankenkasse ohnehin vorliegenden Unterlagen ergeben und eigene Fachkräfte die Vorbereitung der Leistungsentscheidung übernehmen.

Die Einschaltung eines anderen Hilfsmittelberaters ist auch nicht nach den Regelungen über die Datenverarbeitung im Auftrag nach § 80 SGB X möglich. Die Hilfsmittelberater wurden in den mir bekannten Fällen von der Krankenkasse mit Informationen versorgt und/oder holen weitere Informationen unmittelbar beim Versicherten ein. Auf der Grundlage dieser Daten erarbeitet ein Hilfsmittelberater in gleicher Weise wie der MDK einen Entscheidungsvorschlag für die Krankenkasse. Diese Tätigkeit erfüllt die Voraussetzung einer Funktionsübertragung, was auch die staatlichen Aufsichtsbehörden des Bundes und der Länder der gesetzlichen Krankenkassen in einem gemeinsam erstellten Arbeitspapier so erläutert haben.

Ohne entsprechende gesetzliche Rahmenbedingungen ist die Beauftragung von „externen Hilfsmittelberatern“ eine Umgehung der nach den §§ 275 ff. SGB V gesetzlich dem MDK zugewiesenen Aufgaben. In Einzelfällen kann es notwendig sein, externe Gutachter heranzuziehen, wie es das o. g. Arbeitspapier vorsieht. Dies hat allerdings grundsätzlich durch den MDK zu geschehen (§ 279 Absatz 5 Satz 1 2. Halbsatz SGB V).

11.2 Rentenversicherung – Versicherungsnummern der Deutschen Rentenversicherung per Knopfdruck – das Webportal eSolution der DRV

Im Rahmen der Initiative „eGovernment 2.0“ der Bundesregierung hat die Deutsche Rentenversicherung Bund das so genannte eSolution-Portal eröffnet. Das Portal ermöglicht es, Leistungsträgern der Sozialversicherung die für ihre Aufgabenerfüllung notwendigen Daten bei der Datenstelle der Deutschen Rentenversicherung Bund zentral über das Internet abzurufen.

Die DRV Bund hat mich nach § 79 Absatz 3 SGB X über ihre Absicht unterrichtet, dieses automatische Abrufverfahren einzuführen. Auch wurde ich in den Prozess der Weiterentwicklung des Verfahrens einschließlich eines Probebetriebs bei einer gesetzlichen Krankenkasse eingebunden. Mit diesem Verfahren sollen aufwendige und zeitintensive Abfragen, die typischerweise zu erheblichen Bearbeitungszeiten führen, verkürzt sowie Verwaltungs- und Portokosten gesenkt werden. Gesetzlich ist die Übermittlung von Sozialdaten zwischen Sozialleistungsträgern nach § 79 Absatz 1 SGB X zulässig, soweit sie unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit angemessen ist. Innerhalb des Portals stehen den Nutzern verschiedene Onlinedienste zur Verfügung. Bei der weit überwiegenden Zahl der Aufrufe handelt es sich um die Ermittlung von Versicherungsnummern. Für eine solche Suchanfrage ist die Kenntnis von Vorname, Nachname, Geburtsdatum und Geschlecht des Versicherten zwingend erforderlich. Daneben kann der jeweilige Kontoführer zu einer bestimmten Versicherungsnummer abgefragt werden. Sind zuvor mehrere Versicherungsnummern an denselben Versicherten vergeben worden, kann die jeweils aktive ermittelt werden.

Zum Abruf von Sozialdaten via „eSolution“ sind derzeit die gesetzlichen Krankenkassen, die Berufsgenossenschaften sowie die Bundesagentur für Arbeit berechtigt. Ende November 2012 waren von 146 Krankenkassen und neun Berufsgenossenschaften insgesamt 101 Krankenkassen für die Benutzung des „eSolution-Portals“ registriert, acht weitere haben bereits ihr Interesse bekundet. Zudem sieht Artikel 12 Nummer 1 des am 19. Dezember 2012 vom Bundeskabinett beschlossenen Entwurfs eines Gesetzes zur Neuorganisation der bundesunmittelbaren Unfallkassen, zur Änderung des Sozialgerichtsgesetzes und zur Änderung anderer Gesetze, eine Erweiterung des Kreises der nach § 148 Absatz 3 Satz 1 SGB VI abrufbe-

rechtigten Stellen um die zugelassenen kommunalen Träger nach § 6a SGB II vor.

In technischer Hinsicht ist der Zugang nicht nur von der Eingabe einer autorisierten Nutzername/Passwort-Kombination abhängig, zugleich werden clientseitige SSL-Zertifikate zur Authentisierung verwendet. Meine Forderung nach einer verbesserten Protokollierung der Anfragen wurde umgesetzt. Hierdurch sind das Datum, die Uhrzeit, der jeweilige Nutzer und seine Transaktion ohne Schwierigkeiten nachvollziehbar. Ebenso ist die DRV Bund meinem Wunsch nach Dokumentierung der Zertifikatsvergabe an abfragende Sozialleistungsträger nachgekommen. Nach meiner datenschutzrechtlichen Bewertung hat das Bundesministerium für Arbeit und Soziales im November 2010 den Dauerbetrieb genehmigt.

Ich habe die Zusage, bei zukünftigen Änderungen und Fortentwicklungen – insbesondere im Hinblick auf spätere zusätzliche Dienste des Portals – weiterhin beteiligt zu werden.

11.3 Pflegeversicherung – Neue Wege im Pflege-Neuausrichtungs-Gesetz

Das Pflege-Neuausrichtungs-Gesetz enthält deutliche Verbesserungen bei den Leistungen für Demenzerkrankte und den Rechten Angehöriger. Erstmals wird der Kreis der Gutachter für die Feststellung der Pflegebedürftigkeit über den Medizinischen Dienst der Krankenversicherung hinaus auf andere unabhängige Gutachter erweitert. Das Gesetz normiert Wahlrechte der Betroffenen und nimmt wichtige datenschutzrechtlich relevante Änderungen vor.

Das Gesetz zur Neuausrichtung der Pflegeversicherung (Pflege-Neuausrichtungs-Gesetz (PNG) vom 23. Oktober 2012, BGBl. I S. 2246) ist in seinen wesentlichen Teilen am 30. Oktober 2012 in Kraft getreten. Mit dem Gesetz werden auch verschiedene datenschutzrechtlich relevante Änderungen in die gesetzliche Pflegeversicherung eingeführt. So werden etwa bei der Beurteilung der Pflegequalität die Pflegedokumentationen, die Inaugenscheinnahme der Pflegebedürftigen und Befragungen der Beschäftigten der Pflegeeinrichtungen sowie der Pflegebedürftigen, ihrer Angehörigen und der vertretungsberechtigten Personen berücksichtigt. Wenn diese Ergebnisse für die Erstellung eines Prüfberichts herangezogen werden sollen, ist die Einwilligung der betroffenen Pflegebedürftigen erforderlich.

Um die Leistungen der gesetzlichen Pflegeversicherung zu beschleunigen, muss nicht mehr ausschließlich der Medizinische Dienst der Krankenversicherung (MDK) mit der Beauftragung eines Gutachtens zur Feststellung der Pflegebedürftigkeit beauftragt werden. Erstmalig ist auch die Vergabe von Gutachten an einen von der Pflegekasse beauftragten Gutachter außerhalb des MDK möglich. Auf meine Initiative hin sind dabei einem Versicherten, der einen Antrag auf Anerkennung einer Pflegestufe stellt, mindestens drei unabhängige Gutachter zur Auswahl zu benennen. Hat sich der Antragsteller für einen benannten Gutachter entschieden, ist seinem Wunsch Rechnung zu tragen. Positiv bewerte ich zudem, dass ein Antragsteller grundsätzlich das Recht darauf hat, das erstattete Gutachten ausgehändigt zu bekommen. Für die Beauftragung von anderen unabhängigen Gutachtern durch die Pflegekassen im Verfahren zur Feststellung der Pflegebedürftigkeit soll der Spitzenverband Bund der Pflegekasse bis zum 31. März 2013 Richtlinien für die Zusammenarbeit erlassen, die für die Pflegekassen verbindlich sind. Im Rahmen des Genehmigungsverfahrens durch das BMG soll auch ich beteiligt werden und erneut auf die Einhaltung datenschutzrechtlicher Grundsätze und auf datenschutzfreundliche Lösungen hinwirken.

11.4 Unfallversicherung

11.4.1 Erfahrungen bei Gutachten in der Unfallversicherung – eine „never ending story“

Die Probleme bei der Umsetzung der Gutachterregelung in der gesetzlichen Unfallversicherung sind immer noch nicht gelöst. Die beabsichtigte Transparenz der Verfahren und Stärkung der Mitwirkungsrechte der Versicherten wurden nicht erreicht.

Schwerpunkt der Kontrollen bei der Berufsgenossenschaft der Bauwirtschaft (BG Bau) und der Berufsgenossenschaft Handel und Warendistribution (BGHW) war die Handhabung der seit ihrem Inkrafttreten zum 1. Juli 1997 umstrittenen Gutachterregelung des § 200 Absatz 2 SGB VII. Die Kontrollen haben – wie auch eine Vielzahl von Eingaben zu dieser Thematik – gezeigt, dass weiterhin dringender Handlungsbedarf zur Klarstellung dieser Regelung besteht. Bereits in meinem 22. Tätigkeitsbericht hatte ich über die schwerwiegenden Probleme bei der Abgrenzung eines Gutachtenauftrags nach § 200 Absatz 2 SGB VII und der Einholung einer bloßen beratungsärztlichen Stellungnahme berichtet, die auch durch die grundsätzlichen Urteile des Bundessozialgerichts vom 5. Februar 2008 – B 2 U 8/07 R und B 2 U 10/07 R – nicht gelöst wurden (vgl. 22. TB Nr. 10.3.1). Mit der Deklarierung als „beratungsärztliche Stellungnahme“ verkürzen die Berufsgenossenschaften die Rechte der Versicherten, denen bei einer Beauftragung eines Sachverständigen mit der Erstellung eines Gutachtens nach § 200 Absatz 2 SGB VII ein Auswahlrecht hinsichtlich des Gutachters sowie das Widerspruchsrecht nach § 76 Absatz 2 SGB VII zugestanden hätte.

In dem von der BGHW entwickelten „Leitfaden für die Sachbearbeitung zur Gutachterauswahl nach § 200 Absatz 2 SGB VII“ wird die Entscheidung, ob ein Gutachtenauftrag erteilt oder eine Stellungnahme eines beratenden Arztes eingeholt wird, praktisch in das Belieben des Unfallversicherungsträgers gestellt. Nach dem „Leitfaden“ wird unter Bezugnahme auf die Rechtsprechung des Bundessozialgerichts neben den inhaltlichen Abgrenzungskriterien großes Gewicht auf formale Kriterien gelegt. Anhaltspunkte für ein Gutachten sind danach, ob dieses bei der Anforderung als solches bezeichnet oder als solches erstellt oder abgerechnet wird. Diese Kriterien sind völlig ungeeignet. Die Begriffe „Gutachten“ und „beratungsärztliche Stellungnahme“ sind fast synonym gebräuchlich und beliebig austauschbar.

Aus der Feststellung des Bundessozialgerichts, der Gutachtenbegriff sei eng auszulegen, zieht die BGHW – wie auch andere Berufsgenossenschaften – den Schluss, dass immer dann eine beratungsärztliche Stellungnahme vorliegt, wenn eine Auseinandersetzung mit einem Gerichtsgutachten, Gutachten, bzw. zu einer in der Akte vorliegenden anderweitigen Beurteilung bezüglich der Schlüssigkeit, der Überzeugungskraft und der Beurteilungsgrundlage eingeholt werden soll. Auch Äußerungen zum Ursachenzusammenhang und die Erarbeitung prozessual verwertbarer Einwendungen können danach zu beratungsärztlichen Stellungnahmen zählen. Allein die Formulierung des Auftrags durch den Sachbearbeiter der Berufsgenossenschaft an den beratenden Arzt soll darüber entscheiden, ob der Versicherte die in § 200 Absatz 2 SGB VII genannten Rechte erhält und von seinem Mitwirkungsrecht Gebrauch machen kann. Dies ist nicht im Sinne des gesetzlich vorgesehenen Gutachterwahlrechts für den Betroffenen.

Sofern die Berufsgenossenschaft nach Prüfung dieser diffusen Kriterien zu dem Ergebnis gelangt, dass ein Gutachten von einem von der Berufsgenossenschaft bestimmten Sachverständigen nicht einzuholen sei, sondern ein Gutachten von einem beratenden Arzt ausreichend sei, wird die Anwendung von § 200 Absatz 2 SGB VII vor Erteilung des Gutachtenauftrags verneint. Da der beratende Arzt aufgrund der vertraglichen Bindungen wie ein Mitarbeiter des Unfallversicherungsträgers zu betrachten sei, finde keine Datenübermittlung an einen Dritten statt. Diese Handlungsanweisung findet sich nicht nur in den internen Dienstanweisungen aller Berufsgenossenschaften, sondern auch in der Muster-Dienstanweisung der Deutschen Gesetzlichen Unfallversicherung (DGUV), obwohl in den zitierten Urteilen des Bundessozialgerichts gar nicht über diesen Fall entschieden wurde.

Bereits in meinem 22. TB (Nr. 10.3.1) hatte ich eine gesetzliche Klarstellung des § 200 Absatz 2 SGB VII gefordert – leider bisher ohne Erfolg. Im Interesse der Versicherten ist diese mehr als überfällig. Die Klarstellung des gesetzgeberischen Willens gehört so schnell wie möglich auf die Agenda des Gesetzgebers. Zusätzlich zu der im 22. TB vorgeschlagenen Formulierung sollte im Gesetzestext klargestellt werden, dass es sich stets um ein Gutachten handelt, sobald der Sachverständige eine eigenständige Bewertung abgibt.

11.4.2 Kontrolle der Unfallkasse des Bundes

Themenbezogene Kontrollen können auch datenschutzrechtliche Probleme in anderen Bereichen zu Tage fördern.

Bei einem Beratungs- und Kontrollbesuch der Unfallkasse des Bundes (UK-Bund), der sich eigentlich auf den Bereich Personalwesen konzentrierte (vgl. Nr. 13.4), bin ich auch auf große Mängel beim Umgang mit Sozialdaten der Versicherten gestoßen. So war von den Arbeitsplätzen im Sachgebiet „Personal, Organisation“ generell ein automatisierter Zugriff auf Sozialdaten der Versicherten möglich. Dieser Zugang zu geschützten Sozialdaten ist für die Aufgabenerfüllung dieses Sachgebietes nicht erforderlich und verstößt gegen das in § 35 SGB I normierte Sozialgeheimnis. Nach § 35 Absatz 1 Satz 2 SGB I umfasst dessen Wahrung auch die Verpflichtung, innerhalb des Leistungsträgers die Sozialdaten nur Befugten zugänglich zu machen oder nur an diese weiterzugeben. Dies war nicht gewährleistet.

Während des Besuches fand ich zudem das Eingangsportal zum Dienstgebäude offen vor, die Pförtnerloge war unbesetzt, sodass keine Einlasskontrolle erfolgte. Hierdurch war mir ohne jegliche Kontrolle ein Zugang zu umfangreichen Versichertenakten der UK-Bund und den darin gespeicherten Sozialdaten möglich. Diese waren im Erdgeschoss in einem für jedermann erkennbar offenen Aktenlager abgelegt. Dessen Tür wurde dauerhaft offen gehalten, damit die Beschäftigten das dort befindliche Kopiergerät unproblematisch nutzen konnten. Jedermann hätte die Versichertenakten mitnehmen oder kopieren können. Ein derartiger „Datenklau“ wäre im Nachhinein für die UK-Bund nicht mehr nachvollziehbar gewesen. Dieser Umgang mit Sozialdaten der Versicherten stellt ebenfalls einen Verstoß gegen das Sozialgeheimnis dar.

Die festgestellten erheblichen Mängel im Umgang mit Sozialdaten der Versicherten habe ich nach § 81 Absatz 2 SGB X i. V. m. § 25 Absatz 1 BDSG gegenüber dem Vorstand der UK-Bund als einen Verstoß gegen § 35 Absatz 1 SGB I (Sozialgeheimnis) beanstandet.

Ich begrüße, dass die UK-Bund die von mir bereits während des Besuches empfohlenen Maßnahmen zur Wahrung des Sozialgeheimnisses inzwischen umgesetzt hat. Meine stichprobenartige Nachkontrolle zum Zugriff auf Versichertendaten (Sozialdaten) ergab keine negativen Feststellungen.

11.5 Gesundheitswesen

11.5.1 Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten

Mit dem am 29. November 2012 vom Deutschen Bundestag beschlossenen Patientenrechtegesetz sollen die Rechte der Patientinnen und Patienten gestärkt werden. Wie weit reicht die Verbesserung aus datenschutzrechtlicher Sicht?

Das „Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten“ (Bundestagsdrucksache 17/10488) soll die Verfahrensrechte der Patientinnen und Patienten im Zusammenhang mit Behandlungsfehlern verbessern. Darüber hinaus werden die Rechte der Versicherten gegenüber den gesetzlichen Krankenkassen gestärkt. Das Gesetz sieht insbesondere vor, dass

- Patientinnen und Patienten verständlich und umfassend informiert werden müssen, etwa über erforderliche Untersuchungen, Diagnosen, beabsichtigte Therapien, die mit der Behandlung verbundenen Kostenfolgen sowie unter bestimmten Voraussetzungen über einen Behandlungsfehler.
- grundsätzlich alle Patientinnen und Patienten umfassend über eine bevorstehende konkrete Behandlungsmaßnahme und über die sich daraus ergebenden Risiken aufgeklärt werden müssen.

- Patientenakten vollständig und sorgfältig zu führen sind. Behandelnde sind künftig auch verpflichtet, zum Schutz von elektronischen Dokumenten eine manipulationssichere Software einzusetzen. Fehlt die Dokumentation oder ist sie unvollständig, wird im Prozess zu Lasten des Behandelnden vermutet, dass die nicht dokumentierte Maßnahme auch nicht erfolgt ist.
- Patientinnen und Patienten ein gesetzliches Recht zur Einsichtnahme in ihre Patientenakte eingeräumt wird, das nur unter strengen Voraussetzungen und nicht ohne Begründung abgelehnt werden darf.
- die Kranken- und Pflegekassen künftig verpflichtet sind, ihre Versicherten bei der Durchsetzung von Schadensersatzansprüchen aus Behandlungsfehlern zu unterstützen.
- Sanktionen greifen, wenn Verfahrensvorschriften verletzt werden, wie beispielsweise einer nicht fristgemäßen Entscheidung bei Leistungen der gesetzlichen Krankenversicherung.
- Patientenorganisationen insbesondere bei der Bedarfsplanung stärker einbezogen und ihre Rechte im Gemeinsamen Bundesausschuss gestärkt werden.

Das Patientenrechtegesetz ist ein Schritt in die richtige Richtung, um die Rechte von Patientinnen und Patienten zu stärken. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mit ihrer Entschließung vom 23. Mai 2012 dieses Anliegen der Bundesregierung nachdrücklich begrüßt (vgl. Kasten zu Nr. 11.5.1). Allerdings hat die Datenschutzkonferenz auch auf die aus datenschutzrechtlicher Sicht unbefriedigenden Regelungen hingewiesen.

Kasten zu Nr. 11.5.1

„Patientenrechte müssen umfassend gestärkt werden“

Datenschutzkonferenz fordert die Bundesregierung zur Überarbeitung des vorgelegten Gesetzentwurfs auf!

Mit dem im Januar 2012 der Öffentlichkeit vorgestellten und nun dem Bundeskabinett zugeleiteten Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten (Patientenrechtegesetz) sollen insbesondere die bislang von den Gerichten entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts zusammengeführt und transparent für alle an einer Behandlung Beteiligten geregelt werden Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder teilt das Anliegen der Bundesregierung, die Rechte von Patientinnen und Patienten zu stärken. Die Datenschutzkonferenz hält allerdings die vorgelegten Regelungen in dem Entwurf eines Patientenrechtegesetzes für nicht ausreichend. Sie fordert die Bundesregierung nachdrücklich auf, den Gesetzentwurf zu überarbeiten und dabei die folgenden Aspekte zu berücksichtigen:

- Die vertraglichen Offenbarungsobliegenheiten der Patientinnen und Patienten gegenüber den Behandelnden dürfen nicht ausgeweitet werden. Die Patientinnen und Patienten dürfen nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden, die keinen Behandlungsbezug haben.
- Die Patientinnen und Patienten müssen in jedem Fall und nicht erst auf Nachfrage über erlittene Behandlungsfehler informiert werden.
- Der Gesetzentwurf sollte im Zusammenhang mit der Behandlungsdokumentation um verlässliche Vorgaben zur Absicherung des Auskunftsrechts der Patientinnen und Patienten sowie zur Archivierung und Löschung ergänzt werden.
- Der Zugang der Patientinnen und Patienten zu der sie betreffenden Behandlungsdokumentation darf nur in besonderen Ausnahmefällen eingeschränkt werden. Die in dem Entwurf vorgesehenen Beschränkungen sind zu weitgehend und unpräzise. Zudem sollte klargestellt werden, dass auch berechtigte eigene Interessen der Angehörigen einen Auskunftsanspruch begründen können.
- Der Gesetzentwurf ist um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) zu ergänzen.
- Regelungsbedürftig ist ferner der Umgang mit der Behandlungsdokumentation beispielsweise im Falle eines vorübergehenden Ausfalls, des Todes oder der Insolvenz des Behandelnden. Im Bereich der Heilberufe fehlt es – anders als z. B. bei den Rechtsanwälten – an einem bundesweit einheitlichen Rechtsrahmen.

11.5.2 Das kurze Leben der Ambulanten Kodierrichtlinien (AKR)

Zu Beginn des Berichtszeitraums herrschte unter den niedergelassenen Ärzten große Aufregung über die Einführung der Ambulanten Kodierrichtlinien (AKR) zum 1. Januar 2011.

Bereits seit dem Jahr 2000 waren Ärzte und Psychotherapeuten verpflichtet, bei der Abrechnung ihrer Leistungen gegenüber den Kostenträgern (gesetzliche Krankenkassen oder private Krankenversicherung) die Behandlungsdiagnosen nach ICD-10-GM (Statistical Classification of Diseases and Related Health Problems, Release 10, German modification) zu kodieren. Bei der Anwendung der ICD-10-GM bestehen aber teilweise Unklarheiten beziehungsweise Interpretationsspielräume, die mit den AKR behoben werden sollten. Denn der Gesetzgeber hat im GKV-Wettbewerbsstärkungsgesetz von 2007 die Vergütung im Gesundheitswesen stärker an die Krankheitshäufigkeiten (Morbidität) gebunden. Genaue Daten hierzu lassen sich aber nur aus den kodierten Diagnosen entnehmen.

Aus diesem Grund hatte der Gesetzgeber die Vertragspartner des Bundesmantelvertrages (Kassenärztliche Bundesvereinigung und Spitzenverband der gesetzlichen Krankenkassen) nach dem früheren § 295 Absatz 3 Satz 2 SGB V verpflichtet, „Richtlinien für die Vergabe und Dokumentation der Schlüssel … für die Abrechnung und Vergütung der vertragsärztlichen Leistungen (Kodierrichtlinien)“ zu vereinbaren. Durch einen fünfstelligen Code wurde darin verbindlich festgelegt, was alles zu einer Behandlungsdiagnose gehört und welche Leistungen der Arzt bzw. Psychotherapeut im abzurechnenden Quartal zu Lasten der gesetzlichen Krankenkassen erbringt. Die Reglungen waren deutlich spezifischer als die bereits seit dem Jahr 2001 angewandten „Deutschen Kodierrichtlinien“, die für die Abrechnung von stationären Leistungen von den beteiligten Verbänden verwendet und regelmäßig überarbeitet werden.

Obwohl die Kassenärztliche Bundesvereinigung an der Erstellung der AKR beteiligt war, wurden diese auf Druck einiger Kassenärztlichen Vereinigungen im Frühjahr 2011 wieder zurückgezogen. Gleichzeitig wurde durch das GKV-Versorgungsstrukturgesetz (vgl. hierzu Nr. 11.1.3) die gesetzliche Grundlage für die AKR gestrichen.

Ich habe diese Entwicklung begrüßt, da insbesondere im psychotherapeutischen Bereich die Vorgaben der Ambulanten Kodierrichtlinien viel zu detailliert waren. Auch im Übrigen sind Angaben in dem vorgesehenen Detaillierungsgrad bei den Krankenkassen für Abrechnungszwecke nicht erforderlich. Hierzu reicht eine Kodierung nach der bisher üblichen internationalen Klassifikation ICD-10 völlig aus.

Da die Vertragspartner des Bundesmantelvertrages in einer gemeinsamen Erklärung festgestellt haben, ohne die AKR könne eine flächendeckende Qualitätssicherung der Diagnosen weder für das Jahr 2011 noch in den Folgejahren nicht erreicht werden, gehe ich allerdings davon aus, dass dieses Thema mich in den nächsten Jahren noch einmal beschäftigen wird.

11.5.3 Das Krebsfrüherkennungs- und -registergesetz

Krebsfrüherkennungsuntersuchungen sollen künftig als organisierte Früherkennungsprogramme durchgeführt sowie flächendeckend klinische Krebsregister eingeführt werden.

Gemeinsam mit der Deutschen Krebsgesellschaft e. V., der Deutscher Krebshilfe e. V. und der Arbeitsgemeinschaft Deutscher Tumorzentren hatte das BMG am 16. Juni 2008 den Nationalen Krebsplan initiiert. Ziel der Initiative ist die Verbesserung der Krebsbekämpfung durch ein effektives, zielgerichtetes und aufeinander abgestimmtes Handeln aller Verantwortlichen im Rahmen eines langfristig ausgerichteten Koordinierungs- und Kooperationsprogramms.

Ein Schwerpunkt der Maßnahmen des Nationalen Krebsplans liegt in der Weiterentwicklung der Früherkennung von Brust-, Gebärmutterhals- und Darmkrebs durch den Gemeinsamen Bundesausschuss (G-BA). Die Bundesregierung hat hierzu einen „Entwurf eines Gesetzes zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister (Krebsfrüherkennungs- und -registergesetz – KFRG)“ (Bundestagsdrucksache 17/11267) vorgelegt.

Danach sollen organisierte Früherkennungsprogramme die Bevölkerung regelmäßig über Vorsorgeuntersuchungen (Screenings) informieren und zur Teilnahme einladen. Darüber hinaus sollen die Früherkennungsprogramme Anhaltspunkte zur Festlegung von Qualitätsstandards für das Screening liefern. Dies setzt einen Abgleich der erhobenen Gesundheitsdaten voraus. Eine datenschutzgerechte Nutzung ist möglich, wenn bei der Weitergabe von Daten zu Forschungszwecken und zur Qualitätskontrolle sowohl die vorgesehene Pseudonymisierung der Daten als auch die Widerspruchslösung für den Betroffenen – wie im Gesetzesentwurf vorgesehen – eingehalten werden.

Bei den Beratungen zum Gesetzentwurf konnte ich erreichen, dass Datenschutzbelange im Wesentlichen berücksichtigt wurden. So darf die Krankenversichertennummer nur in pseudonymisierter Form genutzt werden. Die Regelung wichtiger datenschutzrechtliche Fragen sind auf den G-BA übertragen worden, der von mir beraten wird (vgl. Nr. 11.1.4).

Ein zweiter Schwerpunkt des Nationalen Krebsplans ist die Weiterentwicklung der onkologischen Versorgungsstrukturen und deren Qualität. Priorität bei den beschlossenen Maßnahmen hat der flächendeckende Ausbau von klinischen Krebsregistern. Der KFRG-Entwurf sieht demgemäß deren flächendeckende Einführung vor. Im Gegensatz zu den epidemiologischen Krebsregistern, die lediglich Angaben zu Art und Häufigkeit der Tumorerkrankung in einer bestimmten Region wiedergeben, erfassen klinische Krebsregister den gesamten Erkrankungsverlauf von der Diagnose über die einzelnen Therapieschritte bis zum Ende der Nachsorge oder den Tod.

Durch das KFRG soll die flächendeckende klinische Krebsregistrierung eingeführt und eine möglichst vollständige Erhebung der Behandlungsdaten sowie eine jährliche Auswertung der Registerdaten erreicht werden. Die Einrichtung und konkrete Ausgestaltung der klinischen Krebsregister bleibt nach dem Entwurf jedoch den Ländern vorbehalten. Die Landesdatenschutzbeauftragten werden die Einrichtung der klinischen Krebsregister in ihren Bundesländern begleiten.

11.5.4 Nationale Kohorte

Das Großprojekt der Gesundheitsforschung bedarf intensiver datenschutzrechtlicher Begleitung.

Die sog. Nationale Kohorte ist eine bundesweite Langzeitstudie, bei der über einen Zeitraum von mindestens 20 bis 30 Jahren die Entwicklung von Volkskrankheiten wie Diabetes mellitus, Schlaganfällen, Lungenerkrankungen, Krebs, Demenz- oder Herz-Kreislauf-Krankheiten erforscht werden soll. Gemessen an der Sensibilität und Menge der Daten ist die Nationale Kohorte bisher das bedeutendste sozial-medizinische Forschungsprojekt, mit dem ich mich zu befassen hatte.

Der im September 2012 gegründete Verein „Nationale Kohorte e. V.“ koordiniert das Forschungsvorhaben. Mitglieder sind die Helmholtz-Gemeinschaft Deutscher Forschungszentren e. V., Universitäten, die Leibniz-Gemeinschaft sowie Ressortforschungseinrichtungen von Bund und Ländern. Der Verein trägt die Gesamtverantwortung für die datenschutzgerechte Handhabung der Daten und Proben. Er ist auch für die Einhaltung der datenschutzrechtlichen Vorgaben in den Studienzentren und bei den weiteren beteiligten Stellen verantwortlich. Entsprechende vertragliche Vereinbarungen wurden unter den beteiligten Institutionen vor Beginn der Feldarbeit abgeschlossen.

Das Forschungsvorhaben soll bundesweit in 18 lokalen Studienzentren durchgeführt werden. Es ist beabsichtigt, dass die Zentren die insgesamt 200 000 Studienteilnehmer – Männer und Frauen im Alter von 20 bis 69 Jahren – aus verschiedenen Regionen Deutschlands rekrutieren. Dort sollen auch die geplanten Nachbeobachtungen erfolgen. Die Studie sieht vor, die Daten direkt bei den Teilnehmern der Nationalen Kohorte auf der Grundlage einer freiwilligen, informierten Einwilligung nach § 4a Absatz 1 BDSG zu erheben. Darüber hinaus sollen für das Projekt Sekundärdaten, wie zum Beispiel Abrechnungsdaten von gesetzlichen Krankenkassen, erhoben werden. Dadurch sollen Krankheitsverläufe auch über einen langen Zeitraum vollständig erfasst werden können.

Angefangen von der Rekrutierung der Studienteilnehmer bis hin zur langfristigen Speicherung von Gesundheitsdaten sowie ihrer weiteren Verarbeitung und Nutzung stellt sich eine Reihe von datenschutzrechtlichen Fragen. Der Verein „Nationale Kohorte“ hat mir sein Datenschutzkonzept vorgelegt, das hierzu bereits zufriedenstellende Lösungen vorsieht. Weitere Fragen werden sich allerdings noch bei der Durchführung der umfangreichen Studien ergeben. Da die Studien im Wesentlichen von Universitäten und anderen Stellen durchgeführt werden, die der datenschutzrechtlichen Aufsicht der Landesbeauftragten für den Datenschutz bzw. den Datenschutzaufsichtbehörden für den nicht-öffentlichen Bereich unterliegen, werde ich in den kommenden Jahren dieses bundesweite Projekt mit den anderen betroffenen Aufsichtsbehörden intensiv begleiten.

11.5.5 Transplantationsgesetz – Organspende wird ernst genommen

Das Thema Organspende hat vor allem wegen der bekanntgewordenen Skandale die Öffentlichkeit bewegt. Einen Rückgang der Spendebereitschaft hat der Gesetzgeber durch mehrere Änderungen des Transplantationsgesetzes entgegenzuwirken versucht.

Durch das „Gesetz zur Regelung der Entscheidungslösung im Transplantationsgesetz“ vom 12. Juli 2012 (BGBl. I S. 1504) wurde die EU-Richtlinie 2010/53/EU umgesetzt, die europaweit einheitliche Qualitäts- und Sicherheitsstandards für Entnahmekrankenhäuser, Transplantationszentren und andere Bereitstellungsorganisationen festlegt. Weiter werden die Anforderungen an die Charakterisierung des Spenderorgans und das System der Rückverfolgbarkeit einschließlich der Meldung schwerwiegender Zwischenfälle und unerwünschter Reaktionen bestimmt.

Mit diesem Gesetz wurde die bisher geltende Zustimmungslösung durch die Entscheidungslösung ersetzt, mit dem Ziel, die Organspendebereitschaft zu fördern, ohne die Entscheidungsfreiheit des Einzelnen durch eine Erklärungspflicht einzuschränken. Zu diesem Zweck soll „jede Bürgerin und jeder Bürger regelmäßig im Leben in die Lage versetzt werden, sich mit der Frage seiner eigenen Spendebereitschaft ernsthaft zu befassen und aufgefordert werden, die jeweilige Erklärung auch zu dokumentieren“.

Zusätzlich wurden die allgemeinen Aufklärungspflichten ergänzt: Jede Bürgerin und jeder Bürger ist ausdrücklich aufzufordern, eine Entscheidung zur Organspende abzugeben. Die Krankenkassen und privaten Krankenversicherungsunternehmen werden ausdrücklich verpflichtet, ihren Versicherten im Zusammenhang mit der Ausgabe der elektronischen Gesundheitskarte (eGK – vgl. Nr. 4.1) geeignetes Informationsmaterial zur Organspende einschließlich eines Organspendeausweises zur Verfügung zu stellen und diese aufzufordern, eine Erklärung zur postmortalen Organ- und Gewebespende zu dokumentieren.

Um die hochsensiblen Daten zu schützen und die Akzeptanz im Hinblick auf die eGK herzustellen, wurde der Kreis der Zugriffsberechtigten auf ein absolutes Mindestmaß beschränkt: Zugriffsberechtigt ist ausschließlich der Versicherte selbst sowie die in § 291a Absatz 5a SGB V genannten Leistungserbringer in Verbindung mit einem elektronischen Heilberufeausweis, der über eine Möglichkeit zur sicheren Authentifizierung und über eine qualifizierte elektronische Signatur verfügt.

Das „Gesetz zur Änderung des Transplantationsgesetzes“ vom 21. Juli 2012 (BGBl. I S. 1601) eröffnet den Versicher-

ten die Möglichkeit, die Organspendeerklärungen selbst oder Hinweise auf das Vorhandensein und den Aufbewahrungsort von Erklärungen auf der eGK zu speichern.

Die kurz vor Verabschiedung des Gesetzes geäußerte öffentliche Kritik an der Forschungsklausel teile ich nicht. Die Regelung in § 14 Absatz 2a Satz 2 TPG sieht vor, dass Daten von Spendern und Empfängern für ein Forschungsvorhaben an Dritte übermittelt werden können, allerdings nur in anonymisierter Form. Kann aufgrund des Forschungszwecks auf eine Zuordnung der Daten nicht verzichtet werden, ist zunächst die Einwilligung des Betroffenen einzuholen. Ist dies nicht oder nur mit einem unverhältnismäßigen Aufwand möglich und kann der Forschungszweck auf andere Weise nicht erreicht werden, bedarf es einer Abwägung zwischen dem öffentlichen Interesse an der Durchführung des Forschungsvorhabens und den schutzwürdigen Interessen der Betroffenen. Dabei ist zu berücksichtigen, dass es sich um hochsensible Daten handelt – etwa Angaben über vorhandene Erkrankungen sowie Infektionen wie HIV oder Hepatitis.

Nach den bekanntgewordenen Skandalen wird darüber diskutiert, wie mit Informationen über Mediziner umzugehen ist, gegen die aufgrund von berufs- oder strafrechtlich relevantem Verhalten rechtskräftige Maßnahmen ergriffen worden sind. Hier geht es um die gegenseitige Unterrichtung der zuständigen Behörden national und innerhalb der EU sowie darum, ob derartige Fälle in einer allgemein zugänglichen Liste zu veröffentlichen sind.

Das Thema Organspende wird sicherlich auch in der nächsten Zeit in der Diskussion bleiben. Ich werde mich daran weiter aktiv beteiligen, soweit es um den Umgang mit hochsensiblen Daten geht.

11.5.6 Substitutionsregister – aber bitte datenschutzkonform!

Das Substitutionsregister soll den Landesgesundheitsbehörden verlässliche Auskünfte über Behandlungen mit Betäubungsmitteln und über die hierzu berechtigten Ärzte geben. Doch hierfür sind Daten erforderlich, die gegenwärtig nicht erhoben werden dürfen.

Die Betäubungsmittelverschreibungsverordnung (BtMVV) regelt unter anderem die Behandlung eines opiatabhängigen Patienten durch ein ärztlich verschriebenes Betäubungsmittel (Substitutionsmittel). Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) führt ein Register mit Daten über das Verschreiben von Substitutionsmitteln. Dieses Substitutionsregister muss zudem alle Ärzte ausweisen, die aktiv Substituierungen vornehmen beziehungsweise dazu berechtigt sind. Dadurch sollen insbesondere Mehrfachverschreibungen von Substitutionsmitteln durch verschiedene Ärzte für denselben Patienten so früh wie möglich verhindert werden. Ferner werden die Erfüllung der Mindestanforderungen an eine suchttherapeutische Qualifikation der substituierenden Ärzte überprüft und den Landesgesundheitsbehörden statistische Auswertungen zur Verfügung gestellt.

Nach der BtMVV sind die Ärztekammern verpflichtet, Name und Anschrift der Ärzte zu melden, die zur Substitutionsbehandlung zugelassen sind. Zusätzlich hat das BfArM Angaben zum Geburtsdatum, der Fachgruppenzugehörigkeit, dem Beginn der Qualifikation der betreffenden Ärzte und weitere Informationen wie „Wegzug ins Ausland“ angefordert.

Das BfArM sah sich zur Erhebung dieser Daten durch § 5a Absatz 1 Satz 3 BtMVV befugt, der organisatorische Festlegungen gestattet.

In meiner datenschutzrechtlichen Bewertung bin ich allerdings zu dem Schluss gekommen, dass diese Befugnis keine Ermächtigungsgrundlage für eine erweiterte Datenübermittlung sein kann. Die maßgebliche Rechtsvorschrift ist § 5a Absatz 5 Satz 1 BtMVV, der die Datenübermittlung auf den Namen und die Anschrift des Arztes beschränkt. Auch ein Rückgriff auf die Bestimmungen des Bundes- oder der Landesdatenschutzgesetze ist zur Erweiterung des Datenkatalogs nicht zulässig. Gleichwohl hat das BfArM nachvollziehbar die Erforderlichkeit des erweiterten Datensatzes für ein aktuelles und auskunftsfähiges Register dargelegt.

Zur Lösung des Problems habe ich in Gesprächen mit BfArM und dem BMG eine Erweiterung der entsprechenden Vorschrift in der BtMVV vorgeschlagen. Das BMG hat inzwischen einen Arbeitsentwurf für eine Änderungsverordnung vorgelegt, der meinen Vorschlag berücksichtigt. Ich habe die Hoffnung, dass die Änderungsverordnung in dieser Form in Kraft tritt und die für das Substitutionsregister erforderlichen Daten künftig datenschutzkonform erhoben werden.

11.6 Besserer Schutz für unsere Kinder – das neue Bundeskinderschutzgesetz

Das Bundeskinderschutzgesetz soll u. a. für den Ausschluss einschlägig Vorbestrafter von Tätigkeiten in der Kinder- und Jugendhilfe sorgen.

Das am 1. Januar 2012 in Kraft getretene Gesetz zur Stärkung eines aktiven Schutzes von Kindern und Jugendlichen (Bundeskinderschutzgesetz – BKiSchG) vom 22. Dezember 2011 (BGBl. I S. 1975) enthält Verbesserungen zum Schutz von Kindern und Jugendlichen in verschiedenen Bereichen. Wesentlicher Bestandteil des Gesetzes ist nach seinem Artikel 1 das Gesetz zur Kooperation und Information im Kinderschutz (KKG). Darin werden Leistungs- und Unterstützungsangebote für Eltern geregelt. Aus datenschutzrechtlicher Sicht war mir besonders wichtig, dass das Verfahren festlegt, welche zusätzlichen Erhebungen und Speicherungen personenbezogener Daten mit diesen Angeboten verbunden sind. Weiterhin werden Rahmenbedingungen für eine strukturelle Zusammenarbeit im Kinderschutz geschaffen, etwa bei sog. Fallberatungen. Je nach Sachverhalt können solche anonymisierten Fallberatungen auch interdisziplinär erfolgen. Dagegen bestehen keine datenschutzrechtlichen Einwände.

Die Beratungsverpflichtung der Jugendämter wird ebenso gestärkt, wie der Anspruch auf Beratung von Personen, die beruflich für den Schutz von Kindern und Jugendli-

chen verantwortlich sind. Diese Beratungsmöglichkeit begrüße ich sehr, sofern dies nicht zu einer strukturierten Ermittlung von Personen sowie der Speicherung der personenbezogenen Daten allein zum Zweck der Unterrichtung über bestehende Beratungsangebote führt. Eine solche umfassende personenbezogene Erfassung wäre im Hinblick auf den damit verbundenen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen nicht angemessen.

Nach dem neu gefassten § 72a SGB VIII dürfen die Träger der öffentlichen Jugendhilfe keine einschlägig vorbestraften Personen für Aufgaben in der Kinder- und Jugendhilfe beschäftigen. Zu diesem Zweck haben sie sich bei der Einstellung oder Vermittlung und in regelmäßigen Abständen von den Betroffenen ein erweitertes Führungszeugnis nach dem Bundeszentralregistergesetz vorlegen zu lassen. Durch Vereinbarungen mit den Trägern der freien Jugendhilfe soll zudem sichergestellt werden, dass diese Personen weder beschäftigt noch neben- oder ehrenamtlich Aufgaben der Kinder- und Jugendhilfe ausüben dürfen. Datenschutzrechtlich bedeutsam ist die Regelung, nach der die Träger der öffentlichen und freien Jugendhilfe von den eingesehenen Daten nur die Tatsache erheben dürfen, dass Einsicht in das Führungszeugnis genommen wurde, das Datum des Führungszeugnisses und die Information erheben, ob die Person einschlägig bestraft wurde. Auch hiergegen habe ich keine datenschutzrechtlichen Bedenken geltend gemacht.

12 Arbeitsverwaltung

12.1 Arbeitsverwaltung, SGB II

12.1.1 Aufsichtszuständigkeit über die Jobcenter als gemeinsame Einrichtungen

Seit dem 1. Januar 2011 liegt die Kontrollzuständigkeit für die Jobcenter als gemeinsame Einrichtungen und für die in diesen genutzten zentralen IT-Verfahren der Bundesagentur für Arbeit bei mir – eine anspruchsvolle neue Aufgabe!

Mit dem zum 1. Januar 2011 in Kraft getretenen „Gesetz zur Weiterentwicklung der Organisation der Grundsicherung für Arbeitsuchende“ (BGBl. I 2010 S. 1112) wurde mir gemäß § 50 Absatz 4 Satz 3 SGB II die Datenschutzkontrolle und die Kontrolle der Einhaltung der Vorschriften über die Informationsfreiheit bei den gemeinsamen Einrichtungen sowie für die zentralen Verfahren der Informationstechnik nach § 24 BDSG übertragen. Meine Forderungen nach personeller Ausstattung (vgl. 23. TB Nr. 11.5.1) wurden mit dem Haushaltsjahr 2012 durch Schaffung der entsprechenden Planstellen erfüllt.

Für die Datenschutzkontrolle der seit 1. Januar 2012 auf 106 erhöhten zugelassenen kommunalen Träger nach § 6b SGB II (Optionskommunen) sind weiterhin die Landesbeauftragten für den Datenschutz zuständig.

12.1.1.1 Aufsicht über die Jobcenter – Neue Aufgaben und Aktivitäten des BfDI

Es konnten zahlreiche Verbesserungen des Datenschutzes in den Jobcentern erzielt werden.

Seit mir ab 1. Januar 2011 die Zuständigkeit für die Datenschutzkontrolle bei den Jobcentern als gemeinsame Einrichtungen (§ 44b SGB II) gemäß § 50 Absatz 4 Satz 3 SGB II übertragen ist, habe ich eine Reihe von Maßnahmen ergriffen, um Geschäftsführungen und behördliche Datenschutzbeauftragte für den Sozialdatenschutz in diesen Einrichtungen zu sensibilisieren. Dazu gehören insbesondere regelmäßige Beratungs- und Kontrollbesuche vor Ort sowie die Unterstützung der Tätigkeit der behördlichen Datenschutzbeauftragten (bDSB) der Jobcenter (vgl. Nr. 12.1.1.2).

Auf meiner Website habe ich für betroffene Bürgerinnen und Bürger und Mitarbeiter der Jobcenter eine Reihe von Informationen zusammengestellt. Insbesondere verweise ich auf eine Liste mit häufig gestellten Fragen zum Arbeitslosengeld II („FAQ-Liste“) und auf das Faltblatt „Datenschutz im Jobcenter – Ihre Rechte als Antragsteller“. Das Faltblatt wurde von mir an alle Jobcenter zur Auslage in den Kundenbereichen und als Arbeitshilfe für die Mitarbeiter versandt.

Seit Anfang 2011 haben sich, teilweise auf meine Anregung hin, Netzwerke von Geschäftsführern oder bDSB in den Bundesländern oder Regionen entwickelt, die einen effektiven Erfahrungsaustausch zu datenschutzrechtlichen Fragen ermöglichen. An den Treffen haben meine Mitarbeiter auf Einladung teilgenommen und werden es auch in Zukunft gerne tun. Nicht zuletzt die Eingaben von Bürgerinnen und Bürgern geben mir die Gelegenheit, einzelne Jobcenter auf individuelle oder strukturelle Probleme im Umgang mit Sozialdaten hinzuweisen und gezielt auf die Abstellung von Mängeln hinzuwirken.

12.1.1.2 Behördliche Datenschutzbeauftragte in den Jobcentern

Die Jobcenter sind gesetzlich verpflichtet, behördliche Datenschutzbeauftragte (bDSB) zu bestellen. Diese nehmen eine wichtige und anspruchsvolle Aufgabe zur Wahrung des Datenschutzes für Kunden und Mitarbeiter wahr.

Meine Tätigkeit bei der Beratung und Kontrolle der Jobcenter (vgl. Nr. 12.1.1.1) umfasst auch die Unterstützung der bDSB. Da die gesetzliche Pflicht zur schriftlichen Bestellung eines bDSB für die Jobcenter nach § 81 Absatz 4 Satz 1 SGB X i. V. m. § 4f BDSG besteht, habe ich mir von allen Einrichtungen deren Namen mit Funktion und Umfang der Freistellung melden lassen. Wie ich dabei bisweilen feststellen musste, war die Beauftragung noch nicht erfolgt oder eine angemessene Freistellung von den sonstigen Tätigkeiten nicht eingeräumt. Teilweise hatten sich auch Geschäftsführer oder deren Vertreter – unzulässigerweise – selbst benannt oder die notwendige Fachkunde fehlte. Daraufhin forderte ich die betroffenen Jobcenter auf, die in den §§ 4f und 4g BDSG festgelegten Kriterien und Maßstäbe bei ihren bDSB zu beachten. Im Ergebnis haben die betroffenen Jobcenter zuverlässige bDSB neu bestellt, den Umfang der Freistellung entsprechend der Größe der Einrichtung angepasst oder bereits bestellte bDSB durch geeignete Maßnahmen qualifiziert.

Zu meinen Erwartungen an die bDSB gehört die uneingeschränkte Wahrnehmung ihrer internen Kontrollbefugnis. Hierunter fällt u. a. die Durchführung von Stichproben bei der Verarbeitung der elektronisch und in Akten gespeicherten Sozialdaten und die Prüfung der datenschutzgerechten Ausgestaltung in den Kundenbereichen (Eingangsbereiche und Mitarbeiterbüros). Zu ihren Aufgaben im Jobcenter zählen ebenso Schulungen, insbesondere für neue Mitarbeiter (§ 4g Absatz 1 Satz 4 Nummer 2 BDSG).

Gerade in der Anfangsphase konnte ich noch viele Unsicherheiten beim Datenschutz feststellen. So wurden zahlreiche Anfragen von bDSB zu unterschiedlichen Datenschutzsachverhalten von mir beantwortet.

12.1.1.3 Nicht nur die Kunden der Jobcenter haben Mitwirkungspflichten

Nicht alle Jobcenter unterstützten mich bei meiner Kontrolltätigkeit im Rahmen der Eingabenbearbeitung.

Jedermann, der sich mit einer Eingabe an mich wendet (§ 81 Absatz 1 Nummer 1 SGB X), darf auf eine umfassende und objektive Prüfung seiner Angelegenheit vertrauen. Dazu gehört, dem von der Beschwerde betroffenen Jobcenter die Möglichkeit zur Stellungnahme und zur Darlegung der Sach- und Rechtslage einzuräumen. Die Verpflichtung des Jobcenters, mich bei der Erfüllung meiner Aufgaben umfassend zu unterstützen, hat der Gesetzgeber in § 50 Absatz 4 Satz 3 SGB II i. V. m. § 24 Absatz 4 BDSG normiert.

Leider ist das Interesse einiger Jobcenter an der Aufklärung eines Sachverhalts merklich geringer als das der betroffenen Petenten. Wenn einzelne Jobcenter grundsätzlich erst auf meine Erinnerungsschreiben oder sogar erst nach Androhung einer Beanstandung gemäß § 25 BDSG reagiert haben, wurde der Datenschutz dort noch nicht als Grundrecht der Bürger begriffen. Aufgrund meiner Hinweise wurde der bislang mangelnden Kooperationsbereitschaft aber entweder durch Wechsel in der Person des behördlichen Datenschutzbeauftragten oder durch deren hinreichende Entlastung inzwischen abgeholfen.

Ich erwarte, dass künftig alle meiner Kontrollzuständigkeit unterliegenden Einrichtungen ihren Unterstützungspflichten mit der gebotenen Sorgfalt und in angemessener Zeit nachkommen. Diese Forderung werde ich auch weiterhin gegenüber allen Jobcentern durchsetzen.

12.1.2 Neues Leistungsgewährungsverfahren der Bundesagentur für Arbeit: „ALLEGRO“ soll „A2LL“ ablösen

*Wiederholt musste ich über datenschutzrechtliche Mängel des von der BA zentral verwalteten Erhebungs- und Leistungssystems „A2LL“ berichten (vgl. 22. TB Nr. 16.6). Inzwischen hat die BA mit der Entwicklung eines neuen IT-Verfahrens „ALLEGRO“ (**AL**g II **LE**istungsverfahren **GR**undsicherung **O**nline) begonnen.*

Die BA hat mir das neue Verfahren „ALLEGRO“ im April 2012 erstmals vorgestellt. Dabei konnte ich mich über die neuen Funktionalitäten, die Schnittstellen zu anderen zentralen Verfahren der BA, die Datenmigration und die weiteren Projektschritte bis zur geplanten Einführung in den Jobcentern (voraussichtlich Ende 2013) unterrichten. Bei dieser Gelegenheit habe ich meine datenschutzrechtlichen Erwartungen an das neue Verfahren deutlich gemacht. Dazu gehören umfassende Protokollierungsfunktionen, ein Berechtigungskonzept, das sich an den Tätigkeits- und Kompetenzprofilen für Mitarbeiter im SGB II-Bereich orientiert, individuelle Löschfunktionalitäten, die sich nach den gesetzlichen Speicherfristen bestimmen, und eine verbindliche Arbeitshilfe, die als Dienstanweisung sicherstellen muss, dass in Freitextfeldern nur die erforderlichen Daten eingetragen werden.

Ich sehe es positiv, dass keine Datenmigration aus „A2LL“ nach „ALLEGRO“ vorgesehen ist und bei jedem Neu- oder Weiterbewilligungsantrag die notwendigen Daten nur in das neue Verfahren eingegeben werden. Gleichzeitig wird der Leistungsfall im alten Verfahren „A2LL“ eingestellt und die Daten können nach einer Übergangsfrist gelöscht werden. Damit ist sichergestellt, dass keine Übernahme von – teilweise datenschutzrechtlich problematischen – Altdaten in „ALLEGRO“ erfolgt. Die BA hat zugesagt, mich fortlaufend bei der weiteren Entwicklung des IT-Verfahrens „ALLEGRO“ zu beteiligen und meine Anregungen aufzunehmen.

12.1.3 Einzelfälle

Im Berichtszeitraum haben mich zahlreiche Eingaben von Bürgerinnen und Bürgern erreicht, denen ich nachgegangen bin.

12.1.3.1 Hausbesuch mit Erfassung des Wohnungsinventars aufgrund einer anonymen Anzeige

Häufig haben sich Betroffene an mich gewandt, weil Mitarbeiter des Jobcenters im Außendienst (§ 6 Absatz 1 Satz 2, 2. Halbsatz SGB II) Hausbesuche durchgeführt haben.

In einem Einzelfall hat sich eine Leistungsberechtigte bei mir über einen unangekündigten Hausbesuch beschwert. Anlass war eine anonym beim Jobcenter eingegangene Anzeige, die Petentin würde sich nur sporadisch in ihrer Wohnung aufhalten. Während der Außendienst den von der Petentin vorgetragenen Indizien für ihre regelmäßige Nutzung der Wohnung wenig Beachtung schenkte, protokollierte er umso gewissenhafter die gesamte in der Wohnung vorhandene Einrichtung in einer Inventarliste. Im Schriftwechsel zwischen der Petentin und dem Jobcenter gab dieses später an, die Inventarliste als vorsorgliche Maßnahme bei eventuell späteren Anträgen auf finanzielle Leistungen für Einrichtungsgegenstände gefertigt zu haben.

Mit der Durchführung des unangekündigten Hausbesuchs sowie der Erhebung und Speicherung des Wohnungsinventars in einer Liste hat das Jobcenter gegen datenschutzrechtliche Bestimmungen verstoßen. Bereits der Hausbesuch stellte einen unverhältnismäßigen Eingriff in

die Persönlichkeitsrechte der Petentin dar. Dieser wurde direkt nach Eingang der anonymen Anzeige ohne Prüfung weiterer Indizien allein auf Grund des – dazu noch unsachlichen – Inhalts der Anzeige durchgeführt. Ohne weitere hinzutretende Hinweise hätte das Jobcenter die Petentin aufgrund des Ersterhebungsgrundsatzes (§ 67a Absatz 2 Satz 1 SGB X) zunächst persönlich zur anonymen Anzeige befragen müssen. Da Zweck des Hausbesuchs die Feststellung war, ob die Petentin in der Wohnung ihren gewöhnlichen Aufenthalt hat, waren weder die Fertigung der Inventarliste noch deren Speicherung in der Leistungsakte erforderlich. Hier hätte ein Prüfbericht des Inhalts genügt, die Petentin sei in der Wohnung angetroffen worden und es hätten keine Hinweise für eine regelmäßige Abwesenheit festgestellt werden können. Das Jobcenter hat eingeräumt, die Inventarliste für einen anderen, aktuell nicht anstehenden Zweck und damit auf Vorrat angefertigt zu haben.

Auf eine Beanstandung des Datenschutzverstoßes habe ich nur verzichtet, weil das Jobcenter auf meine Hinweise hin das unverhältnismäßig umfangreiche Prüfprotokoll sowie die Inventarliste aus der Akte gelöscht hat. Außerdem hat das Jobcenter seine Dienstanweisungen für die Beauftragung des Außendienstes überarbeitet und dabei meine Hinweise bei der Festlegung der Verfahrensabläufe berücksichtigt.

12.1.3.2 Beratung in Doppelbüros

Das Sozialgeheimnis muss auf jeden Fall gewahrt bleiben.

Immer wieder beschweren sich Petenten darüber, sie würden als Kunden im Jobcenter in einem Doppelbüro zur gleichen Zeit mit ihnen unbekannten Dritten beraten. Hierbei können die Betroffenen gegenseitig eine Vielzahl von persönlichen Informationen der jeweils anderen Kunden wahrnehmen. Von der Einladung von zwei Kunden zum gleichen Zeitpunkt in ein Doppelbüro konnte ich mich anlässlich meiner Kontrollbesuche vor Ort überzeugen. Die betreffenden Jobcenter begründen die Erforderlichkeit von parallelen Beratungsgesprächen in einem Raum mit den baulichen Gegebenheiten vor Ort und einem Mangel an Einzelbüros.

Alle Jobcenter haben gemäß § 78a SGB X die organisatorischen Maßnahmen zu treffen, die erforderlich sind, um den Sozialdatenschutz für ihre Kunden zu gewährleisten. Die Wahrung des Sozialgeheimnisses (§ 35 Absatz 1 SGB I) umfasst die Verpflichtung, auch innerhalb des Jobcenters sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. Somit ist die gleichzeitige Beratung mehrerer Kunden in Doppelbüros unzulässig und kann nur durch eine abwechselnde Terminvergabe vermieden werden. Ich habe die entsprechenden Jobcenter daher aufgefordert, von der Praxis der gleichzeitigen Terminierung in Doppelbüros Abstand zu nehmen. Alternativ sind Doppelbüros durch bauliche Maßnahmen wie Schall- und Sichtschutzwände so zu gestalten, dass das Sozialgeheimnis gewahrt bleibt.

12.1.3.3 Dürfen Jobcenter Daten aus sozialen Netzwerken verwenden?

Jobcenter sollten von Recherchen in Internetsuchmaschinen und sozialen Netzwerken nur ausnahmsweise Gebrauch machen.

Die von Geschäftsführern und behördlichen Datenschutzbeauftragten von Jobcentern aufgeworfene Frage, ob die Nutzung von Internetsuchmaschinen und sozialen Netzwerken im Rahmen der Sachverhaltsermittlung (§ 20 SGB X) datenschutzrechtlich zulässig ist, lässt sich nur differenziert und unter Beachtung der Grundsätze des Sozialdatenschutzes (§§ 67 ff. SGB X) beantworten.

Zunächst muss die Erforderlichkeit der Datenerhebung für die Aufgabenerfüllung in jedem Einzelfall gegeben sein (§ 67a Absatz 1 Satz 1 SGB X). Weiterhin gilt auch für die Jobcenter der Grundsatz, dass Sozialdaten zuerst beim Betroffenen zu erheben sind (§ 67a Absatz 2 Satz 1 SGB X), was dessen bewusste Mitwirkung an der Datenerhebung voraussetzt, die bei der Erhebung im Internet grundsätzlich nicht gegeben ist. Im Fall sozialer Netzwerke haben die Betroffenen zwar ihre Daten selbst eingestellt, jedoch keine Kenntnis davon, dass das Jobcenter Daten gezielt aus sozialen Netzwerken auswertet. Dazu kommt, dass die Nutzungsbedingungen dieser sozialen Netzwerke in vielen Fällen eine zweckfremde Nutzung ausschließen, soweit der Nutzer diese Daten nicht für die öffentliche Verwendung freigegeben hat. Damit haben die Betroffenen an der Datenerhebung nicht bewusst mitgewirkt. Dies gilt umso mehr, wenn die Informationen durch einen Dritten ins Internet gestellt wurden.

Ich sehe in der gezielten Abfrage von Daten aus sozialen Netzwerken eine Datenerhebung bei Dritten. Eine solche Abfrage ist nur zulässig, wenn eine gesetzliche Regelung dies ausnahmsweise erlaubt. Als Ausnahmetatbestand kommt hier § 67a Absatz 2 Satz 2 Nummer 2 lit. b) SGB X in Betracht; danach muss die Erhebung bei anderen Personen oder Stellen zur Erfüllung der Aufgaben des Jobcenters erforderlich sein, da sie nicht beim Betroffenen selbst erfolgen kann.

Im Fall einer Missbrauchskontrolle kann dies ausnahmsweise so sein, es müssen aber bereits erste konkrete Anhaltspunkte für einen Missbrauch vorliegen. Ein pauschaler Abgleich ist nicht gestattet. Die Abfrage von Daten in Suchmaschinen und sozialen Netzwerken muss aber auch eine geeignete Maßnahme sein. Hier habe ich erhebliche Zweifel, da Angaben in sozialen Netzwerken aus verschiedenen Gründen häufig nicht der Realität entsprechen. Beispielsweise kann der Nutzer sein Profil lange nicht mehr aktualisiert haben oder er möchte Änderungen seiner Lebensumstände absichtlich nicht einstellen, damit sie anderen Nutzern nicht bekannt werden. Da somit die Authentizität der eingestellten Daten nicht sichergestellt ist, ist auch die Geeignetheit der Erhebung entsprechender Daten in Frage gestellt.

Das Gesetz lässt eine Ausnahme vom Ersterhebungsgrundsatz auch dann zu, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde. Die Recherche im Internet wäre häufig ein weni-

ger aufwendiges Mittel. Das kann aber gleichwohl nicht ihren pauschalen Einsatz rechtfertigen. Es müssen Umstände vorliegen, die die Erhebung beim Betroffenen aufwendiger machen als dies gewöhnlich der Fall ist. Darüber hinaus muss auch in diesem Fall die Maßnahme geeignet sein und es dürfen keine überwiegend schutzwürdigen Interessen des Betroffenen beeinträchtigt werden. Deswegen habe ich auch hier erhebliche Zweifel den Jobcentern gegenüber geäußert. Überdies müssten in allen Fällen die Betroffenen über die entsprechende Datenerhebung bei Dritten unterrichtet werden (§ 67a Absatz 5 SGB X), sofern sie nicht bereits Kenntnis hiervon haben.

Ich habe den betroffenen Jobcentern nahegelegt, Internetsuchmaschinen und soziale Netzwerke im Rahmen der Sachverhaltsaufklärung nur in Ausnahmefällen und nach vorheriger Prüfung aller gesetzlichen Voraussetzungen zu nutzen. Dies werde ich regelmäßig im Rahmen meiner Beratungs- und Kontrollbesuche vor Ort überprüfen.

12.1.3.4 Übermittlung von Stellungnahmen der Arbeitnehmer an ehemalige Arbeitgeber

Die BA hat aufgrund meiner Hinweise ihre zentralen Vordrucke datenschutzkonform gestaltet.

Betroffene, die bei einem Jobcenter Leistungen nach dem SGB II beantragt hatten, beschwerten sich, ihre für das Jobcenter bestimmte Stellungnahme über die Beendigung des bisherigen Arbeitsverhältnisses sei von diesem an den ehemaligen Arbeitgeber übermittelt worden. Hierfür wurde häufig ein zentraler Vordruck der BA benutzt.

Erwerbsfähige Leistungsberechtigte verletzen ihre Pflichten, wenn sie sich weigern, eine zumutbare Arbeit fortzuführen (§ 31 Absatz 1 Nummer 2 SGB II). Bei Beendigung eines Arbeitsverhältnisses kann es somit für das Jobcenter erforderlich sein, eine Pflichtverletzung zu prüfen, die eine Minderung der Leistungen zur Folge hätte. Hierbei ist seitens des Jobcenters der Ersterhebungsgrundsatz zu beachten, nach dem Sozialdaten vorrangig beim Betroffenen zu erheben sind (§ 67a Absatz 2 Satz 1 SGB X). Sind die Angaben des Arbeitnehmers nicht ausreichend, hat das Jobcenter den Sachverhalt von Amts wegen zu ermitteln (§ 20 Absatz 1 SGB X). Dabei ist eine Übermittlung von Sozialdaten an den ehemaligen Arbeitgeber, um diesen nach Gründen der Beendigung eines Beschäftigungsverhältnisses zu befragen, nach §§ 67d, 68 Absatz 1 Nummer 1 SGB X i. V. m. § 31 Absatz 1 Nummer 2 SGB II zulässig, wenn dies für die Entscheidung der Pflichtverletzung erforderlich ist.

Somit müssen die Jobcenter im Einzelfall prüfen, ob die Weiterleitung der Stellungnahme des Arbeitnehmers an den Arbeitgeber überhaupt erforderlich ist. Bislang sahen die verwendeten BA-Vordrucke zur Befragung des ehemaligen Arbeitgebers keine neutrale Anfrage vor, sodass zwingend mit der Anfrage die Stellungnahme des Arbeitnehmers ganz oder in Auszügen übermittelt wurde. Das halte ich für problematisch.

Die BA hat auf meine Bitte hin den Vordruck so angepasst, dass die Stellungnahme des Arbeitnehmers zum Kündigungsgrund dem Arbeitgeber nur noch in begründeten Ausnahmefällen zur Kenntnis gegeben werden soll. Weiterhin soll der Arbeitnehmer bereits im Anhörungsschreiben einen Hinweis erhalten, dass seine Stellungnahme dem früheren Arbeitgeber ganz oder in Auszügen bekannt gegeben werden darf, wenn sich der Sachverhalt nur auf diese Weise vollständig aufklären lässt. Ich begrüße die bereits erfolgten Anpassungen der zentralen Vordrucke durch die BA und werde die künftige Umsetzung in den Jobcentern kontrollieren.

12.1.3.5 Übermittlung eines ärztlichen Gutachtens an das Sozialamt

Unter bestimmten Voraussetzungen dürfen Jobcenter ärztliche Gutachten an Sozialämter weiterleiten.

Eine Reihe von Betroffenen hat sich darüber beklagt, Jobcenter übermittelten ihre vom Ärztlichen Dienst der Bundesagentur für Arbeit (BA) erstellten Gutachten an Sozialämter, ohne ihre Einwilligung eingeholt oder ihnen zumindest einen Hinweis auf ihr Widerspruchsrecht gegeben zu haben.

Die in den ärztlichen Gutachten erhobenen Gesundheitsdaten sind sensible personenbezogene Daten besonderer Art (§ 67 Absatz 12 SGB X), die allerdings durch die Jobcenter als Stellen nach § 35 SGB I für die Prüfung der Erwerbsfähigkeit als gesetzliche Aufgabe erhoben, verarbeitet und genutzt werden dürfen (§ 67a Absatz 1 Satz 1, § 67b Absatz 1 Satz 1 SGB X i. V. m. § 8 SGB II).

Die Kenntnis der Inhalte dieser Gutachten war in den von mir geprüften Fällen für die Erfüllung einer gesetzlichen Aufgabe der Sozialämter als Leistungsträger nach § 28 SGB I erforderlich, da die Betroffenen dort Anträge auf Leistungen nach dem SGB XII gestellt hatten. Der Anspruch auf Sozialhilfe nach dem SGB XII besteht dann, wenn bei der Begutachtung eine dauerhafte oder zumindest mehr als sechsmonatige Erwerbsunfähigkeit festgestellt wurde. Die Prüfung der Anspruchsvoraussetzungen für die beantragten Leistungen konnte in den Sozialämtern nur anhand der ärztlichen Gutachten der Jobcenter (Teil B, sozialmedizinische Stellungnahme mit den Angaben zur Erwerbs- und Leistungsfähigkeit, ohne medizinische Dokumentation und Erörterung) durchgeführt werden. Dies habe ich mir von den für die Aufsicht über die Sozialämter zuständigen Landesdatenschutzbeauftragten im Einzelfall bestätigen lassen.

Der Ersterhebungsgrundsatz nach § 67a Absatz 2 Satz 1 SGB X sieht grundsätzlich eine Anforderung der Gutachten durch die Sozialämter bei den Betroffenen selbst vor. Für die Übermittlung von Gesundheitsdaten zwischen Sozialleistungsträgern lässt § 67a Absatz 2 Satz 2 Nummer 1 SGB X nur eine gesetzlich eng geregelte Ausnahme von diesem Grundsatz zu. Nach dieser durften die Sozialdaten ohne Mitwirkung der Betroffenen von den Sozialämtern nur erhoben werden, wenn die Jobcenter ihrerseits zur Übermittlung der Daten an die Sozialämter befugt waren.

Die entsprechende Befugnis leitet sich bei vorliegender Fallgestaltung aus § 76 Absatz 2 Nummer 1 i. V. m. § 69 Absatz 1 Nummer 1 SGB X ab. Danach darf ein ärztli-

ches Gutachten, das im Hinblick auf den Bezug von Sozialleistungen erstellt wurde, vom Jobcenter nur übermittelt werden, wenn es für die Erfüllung einer gesetzlichen Aufgabe des Empfängers, hier des Sozialamtes, erforderlich ist und der Betroffene der Übermittlung nicht widersprochen hat. Hierauf wurden die Betroffenen in jedem Einzelfall von den Jobcentern als verantwortliche Stelle zu Beginn des Verwaltungsverfahrens in allgemeiner Form hingewiesen.

Jeder Antragsteller auf Leistungen nach dem SGB II hat von seinem Jobcenter das „Merkblatt SGB II – Grundsicherung für Arbeitsuchende“ der BA (Stand April 2012) erhalten, wo unter der Überschrift „Datenschutz“ auf Seite 70 in einem mit blauem Hintergrund hervorgehobenen Kasten das Folgende ausgeführt ist: „Ärztliche und psychologische Gutachten sowie Befunde sind von der Übersendung ausgenommen, wenn Sie der Übermittlung ausdrücklich widersprochen haben“. Zusätzlich wird vor jeder Begutachtung durch den Ärztlichen Dienst der BA ein Gesundheitsfragebogen mit vorangestelltem „Informationsblatt zur Vorstellung im Ärztlichen Dienst“ an die Betroffenen ausgehändigt. Darin ist der im Schriftbild besonders hervorgehobene Hinweis „Medizinische Daten sind von der Übersendung ausgeschlossen, wenn Sie der Übermittlung ausdrücklich widersprochen haben“ enthalten.

Mit den schriftlichen Hinweisen auf das Widerspruchsrecht sind die Jobcenter ihrer Pflicht nach § 76 Absatz 2 Nummer 1 SGB X nachgekommen. Der Gesetzgeber hat in seiner Begründung zum 2. Gesetz zur Änderung des Sozialgesetzbuchs (2. SGBÄndG vom 18. Juni 1993) ausgeführt, der letzte Halbsatz in § 76 Absatz 2 Nummer 1 SGB X sei eingefügt worden, um klarzustellen, dass der Betroffene nur in allgemeiner Form auf sein Widerspruchsrecht hinzuweisen ist (vgl. Bundestagsdrucksache 12/5187 zu § 76 SGB X). Von diesem Widerspruchsrecht hatte keiner der Petenten Gebrauch gemacht.

Da alle gesetzlichen Voraussetzungen für eine Übermittlung der ärztlichen Gutachten an die Sozialämter erfüllt waren, konnte ich keinen Datenschutzverstoß feststellen.

12.1.3.6 Erhebung und Speicherung einer Vielzahl von Unterlagen in den Jobcentern

Zahlreiche Kunden der Jobcenter beschweren sich über die Vielzahl der angeforderten Unterlagen und deren Aufnahme in die Leistungsakten.

In Bürgereingaben wird häufig beklagt, Jobcenter forderten zu viele Unterlagen an und würden diese dann kopieren und speichern. Bei meinen Beratungs- und Kontrollbesuchen der Jobcenter habe ich in der Tat unverhältnismäßig viele Unterlagen in den Leistungsakten gefunden. Dies gilt insbesondere für Kopien des Personalausweises und der Kontoauszüge.

Bei Anträgen auf Arbeitslosengeld II müssen die dazu erforderlichen Unterlagen vorgelegt werden, um die Anspruchsvoraussetzungen nach den §§ 7 ff. SGB II feststellen zu können, was auch die Überprüfung der Identität einschließt (§ 60 Absatz 1 Nummer 3 i. V. m. § 61 SGB I). Zur Kontrolle der Personalien können die Mitarbeiter der Jobcenter auch die Vorlage eines gültigen Passes oder Personalausweises verlangen, da die Daten des Personalausweises, insbesondere die aktuelle Wohnanschrift, mit den Angaben im Antrag übereinstimmen müssen. Eine Kopie des Dokuments in der Akte ist aber zur Identifizierung und Aufgabenerfüllung nicht erforderlich. Vielmehr genügt ein dort oder auf dem Antragsformular anzubringender Vermerk, dass der aktuelle Personalausweis oder ein anderes Ausweisdokument vorgelegen hat. Dies entspricht auch der Auffassung der Bundesagentur für Arbeit (vgl. „HEGA 01/12 – 08 – Empfehlungspaket zum Aufbau und Führen einer Leistungsakte“) und der für die Jobcenter in der Rechtsform der zugelassenen kommunalen Träger (Optionskommunen) zuständigen Datenschutzbeauftragten der Länder, wie eine schriftliche Umfrage unter den Datenschutzbeauftragten des Bundes und der Länder vom 31. Januar 2012 bestätigt hat.

Die Vorlage der Kontoauszüge darf das Jobcenter bei der Beantragung von Leistungen nach dem SGB II regelmäßig für einen zurückliegenden Zeitraum von drei Monaten verlangen, gleichgültig, ob es sich um einen Erstantrag, einen Folgeantrag oder eine einmalige Leistung handelt (Urteil des BSG vom 19. Februar 2009, B 4 AS 10/08 R). Auch in Einzelfragen kann die Vorlage von Auszügen erforderlich sein, wenn der Zugang eines Einkommens auf dem Konto zu prüfen ist. Eine weitergehende Verpflichtung, Kontoauszüge für einen Zeitraum von bis zu sechs Monaten einzureichen, kann regelmäßig bei selbständigen Leistungsberechtigten bestehen, da diese die tatsächlichen Einnahmen und Ausgaben des vergangenen Bewilligungszeitraums (i. d. R. sechs Monate, vgl. § 41 Absatz 1 Satz 4 SGB II) nachweisen müssen. Schon bei der Aufforderung muss seitens des Jobcenters auf die Möglichkeit zur Schwärzung einzelner Passagen hingewiesen werden. Diese Möglichkeit besteht jedoch nur bei Ausgabebuchungen und nicht bei Einnahmen, denn Geldeingänge muss das Jobcenter daraufhin prüfen, ob diese als Einkommen (§ 11 SGB II) den Leistungsanspruch mindern. Die Schwärzungsmöglichkeit bei Ausgabebuchungen bezieht sich nicht auf das Buchungs- und Wertstellungsdatum oder den Betrag, sondern ausschließlich auf bestimmte Passagen des Empfängers und des Buchungstextes, wenn der zu Grunde liegende Geschäftsvorgang für die Prüfung durch das Jobcenter plausibel bleibt. Geschwärzt werden dürfen vor allem die in den Auszügen enthaltenen besonderen Arten personenbezogener Daten, wie Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben. Nach der Schwärzung des genauen Namens des Empfängers müssen Texte wie „Mitgliedsbeitrag“, „Zuwendung“ oder „Spende“ als grundsätzlicher Geschäftsvorgang erkennbar bleiben.

Nach der Einsicht in die Kontoauszüge muss dem Jobcenter aber regelmäßig der Vermerk in der von ihm geführten Akte genügen, diese hätten vorgelegen und keine Auswirkung auf den Leistungsanspruch gehabt. Eine Speiche-

rung einzelner Buchungen oder Auszüge (§ 67 Absatz 6 Satz 2 Nummer 1 SGB X) kommt nur dann in Betracht, wenn sich aus den Unterlagen ein weiterer Ermittlungsbedarf oder eine Änderung in der Leistungshöhe ergibt.

Ich habe die betreffenden Jobcenter zur Bereinigung ihrer Akten aufgefordert. Das Kopieren von Personalausweisen und Kontoauszügen für die Leistungsakten werde ich auch weiterhin bei meinen Kontrollen vor Ort regelmäßig ansprechen.

12.1.3.7 Übermittlung von Sozialdaten an Vermieter

Jobcenter dürfen den Sozialleistungsbezug von Antragstellern in der Regel nicht ohne deren Einwilligung an Vermieter offenbaren.

Wiederholt gingen bei mir Beschwerden ein, die sich gegen die Mitteilung des Sozialleistungsbezuges von Antragstellern an Dritte durch Jobcenter bei der Leistungsbewilligung richteten. Zum Teil wurde von Antragstellern verlangt, eine Bescheinigung vom Vermieter ausfüllen und unterzeichnen zu lassen, oder es wurden Sozialdaten ohne Einwilligung der Betroffenen unmittelbar beim Vermieter abgefragt.

Nach § 67a Absatz 2 Satz 1 SGB X sind Sozialdaten beim Betroffenen zu erheben. Das Jobcenter ist deswegen verpflichtet, die für die Prüfung von Leistungen für Unterkunft und Heizung (KdU) nach § 22 SGB II benötigten Daten beim Betroffenen selbst zu erheben. Diese Leistungen werden in Höhe der tatsächlichen Aufwendungen erbracht, soweit sie angemessen sind (§ 22 Absatz 1 Satz 1 SGB II). Für die Berechnung der KdU benötigt das Jobcenter daher Angaben zu den Wohnverhältnissen der leistungsberechtigten Person.

Die Art und Weise, wie der Betroffene die Daten zu erbringen hat, wird vom Gesetz nicht näher bestimmt. Die von Jobcentern verlangte Vermieterbescheinigung stellt insofern lediglich ein Angebot für eine erleichterte Antragstellung dar, sodass keine Verpflichtung des Betroffenen zur Vorlage der ausgefüllten Bescheinigung des Vermieters besteht. Mangels Qualität einer Beweisurkunde i. S. v. § 60 Absatz 1 Satz 1 Nummer 3 SGB I können dem Betroffenen bei Nichtvorlage auch keine Nachteile aufgrund fehlender Mitwirkung entstehen.

Als alternativer Nachweis der Mietkosten bieten sich die Vorlage des Mietvertrages und die Vorlage von Unterlagen zu Neben-, Heiz- und sonstigen Kosten an. Bei dem Mietvertrag können nicht leistungsrelevante Passagen geschwärzt werden, um etwa Daten von Mitmietern oder die des Vermieters nicht zu offenbaren. Wenn einzelne Nachweise nicht erbracht werden können oder wenn im Einzelfall der begründete Verdacht besteht, dass Angaben unrichtig oder unvollständig sind, können weitere Nachweise verlangt werden. Bei Untermietverhältnissen besteht grundsätzlich keine Verpflichtung, den Hauptmietvertrag vorzulegen. In besonders begründeten Einzelfällen kann allerdings eine Aufforderung dazu erfolgen.

Ohne eine Vermieterbescheinigung werden in der Regel Angaben wie das Alter des Hauses fehlen. Sofern der Betroffene insoweit benötigte Daten nicht vorlegt, kann das Jobcenter das Alter eines Hauses beispielsweise beim Katasteramt erfragen, ohne dass ein Bezug zum Betroffenen hergestellt werden muss.

Diese Grundsätze zur Wahrung des Sozialgeheimnisses nach § 35 SGB I gegenüber einem Vermieter durch die Jobcenter hat auch die aktuelle Entscheidung des Bundessozialgerichts (BSG) vom 25. Januar 2012 (Az. B 14 AS 65/11 R) bestätigt. Wie das BSG darin feststellt, ist der Bezug von Arbeitslosengeld II ein Sozialdatum, dessen Offenbarung durch ein Jobcenter nur zulässig ist, wenn der Leistungsbezieher eingewilligt hat oder eine gesetzliche Offenbarungsbefugnis vorliegt. An beiden Voraussetzungen fehlte es bei den von mir geprüften Eingaben, sodass ich in diesen Fällen einen Verstoß gegen das Sozialgeheimnis festgestellt habe.

12.1.3.8 Gesundheitsdaten im Jobcenter

Da der Umgang mit Gesundheitsdaten im Jobcenter mit dem bei den Agenturen für Arbeit vergleichbar ist, wird auf die dortigen Ausführungen verwiesen (vgl. Nr. 12.2.3).

12.1.3.9 Personaldatenschutz in Jobcentern – aus einer Hand

Für den behördeninternen Mitarbeiterdatenschutz in den Jobcentern sind die dortigen behördlichen Datenschutzbeauftragten zuständig – für sämtliche Mitarbeiterinnen und Mitarbeiter, unabhängig davon, ob diese Beschäftigte der Bundesagentur für Arbeit oder der Kommune sind.

Meine Kontrollbefugnis erstreckt sich dabei auch auf die Erhebung, Verarbeitung und Nutzung von Personal-/Personalaktendaten der Mitarbeiterinnen und Mitarbeiter der Jobcenter, soweit sich diese Daten im Bereich des jeweiligen Jobcenters befinden, unabhängig davon, ob es sich um Beschäftigte der Bundesagentur für Arbeit (BA) oder der Kommunen handelt.

Mich haben im Berichtszeitraum viele Anfragen aus den Jobcentern zum behördeninternen Mitarbeiterdatenschutz in den gemeinsamen Einrichtungen erreicht. Grund für die Verunsicherung sind im Wesentlichen die von der BA am 20. Juli 2012 veröffentlichten Handlungsempfehlungen/Geschäftsanweisungen (HEGA) 07/2012 – 06 „Grundsätze und Verfahren für die Beteiligung des Datenschutzbeauftragten der Bundesagentur für Arbeit“. Darin vertritt die BA die Ansicht, der Mitarbeiterdatenschutz werde mangels anders lautender gesetzlicher Regelung für die BA-Mitarbeiter vom Datenschutzbeauftragten der BA und für die kommunalen Mitarbeiter von dem kommunalen Datenschutzbeauftragten wahrgenommen. Diese Ansicht, die in den HEGA für den Rechtskreis SGB II als „Information“ des behördeninternen Mitarbeiterdatenschutzes in den gemeinsamen Einrichtungen und für den Rechtskreis SGB III als „Weisung“ charakterisiert ist, entspricht nicht der Rechtslage.

Tatsächlich besteht keine Regelungslücke bei der Zuständigkeit für den Mitarbeiterdatenschutz in den Jobcentern. Der behördeninterne Mitarbeiterdatenschutz in den gemeinsamen Einrichtungen gehört zum Zuständigkeitsbereich der nach § 81 Absatz 4 SGB X i. V. m. §§ 4g und 4f BDSG benannten behördlichen Datenschutzbeauftragten (bDSB).

Maßgeblich hierfür ist, dass die gemeinsame Einrichtung seit dem 1. Januar 2011 nach § 50 Absatz 2 SGB II selbst eine Stelle im Sinne des § 35 SGB I ist, d. h. ein dem Sozialgeheimnis verpflichteter Leistungsträger. Nach § 81 Absatz 4 Satz 1 SGB X sind auf die in § 35 SGB I genannten Stellen die §§ 4f, 4g BDSG entsprechend anwendbar. Nach § 4g Absatz 1 Satz 1 BDSG wirkt der bDSB auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hin. Dies gilt selbstverständlich auch für die Beachtung des § 32 BDSG. Diese Vorschrift regelt, neben weiteren diesen Bereich betreffenden Vorschriften, die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses.

Auch aus der Gesetzesbegründung folgt, dass die gemeinsame Einrichtung die inhaltliche Verantwortung für die durch sie vorgenommene Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten bzw. Sozialdaten trägt. Damit wird der von der gemeinsamen Einrichtung zu verantwortende Datenschutz nicht auf die Sozialdaten der Kunden beschränkt, sondern auf sämtliche durch sie vorgenommene Erhebungen, Verarbeitungen und Nutzungen von personenbezogenen Daten und somit auch von Personal-/Beschäftigtendaten erstreckt.

Schließlich spiegelt sich diese Rechtslage auch in § 44d Absatz 4 SGB II wider. Die Vorschrift überträgt dem Geschäftsführer der gemeinsamen Einrichtung die Ausübung der dienst-, personal- und arbeitsrechtlichen Befugnisse über die von den jeweiligen Trägern zugewiesenen Mitarbeiter und soll so die weitgehende Gleichbehandlung des Personals sicherstellen. Diesem gesetzgeberischen Anliegen liefe es zuwider, die Kontrolle des Mitarbeiterdatenschutzes auf unterschiedliche Stellen zu übertragen.

Die Zuständigkeit für den Personaldatenschutz verbleibt bei den entsendenden Dienststellen (BA, Kommunen) nur insoweit, als die Personalakten dort geführt werden und soweit Entscheidungen im Grundverhältnis getroffen werden.

Ich habe diese Rechtsauffassung der BA sowie dem zuständigen Bundesministerium für Arbeit und Soziales mitgeteilt und hoffe auf eine baldige Klärung, da die Verunsicherung bei den Geschäftsführungen und bDSB in den gemeinsamen Einrichtungen groß ist.

12.2 Arbeitsverwaltung, SGB III

12.2.1 E-Akte der Bundesagentur für Arbeit

Die BA stellt ihre Kundenakten von der Papierform auf elektronische Akten (E-Akte) um. Nach einer Überprüfung vor Ort bestehen gegen die Einführung der E-Akte bei der BA keine grundlegenden Bedenken.

Auch die BA stellt – wie viele andere Behörden (vgl. Nr. 3.2 f.) – ihre Akten von Papier auf elektronische Form um. Sie hat die Deutsche Post AG mit der Digitalisierung der Akten beauftragt. Die Deutsche Post AG hat ihrerseits einem ihrer Tochterunternehmen die Ausführung übertragen. Mit weiteren Firmen wurden Unterauftragsverhältnisse begründet. Dass sich die BA grundsätzlich privater Dienstleister unter den Voraussetzungen des § 80 SGB X zur Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag bedienen kann, habe ich bereits in meinem 23. TB (Nr. 11.5.3) ausgeführt.

Anders als ursprünglich geplant wurden in dem Pilotprojekt in Sachsen-Anhalt und Thüringen zunächst nur die Akten für die Arbeitslosenversicherung (Arbeitslosengeld I) digitalisiert, während die Akten für die Familienkassen zu einem späteren Zeitpunkt nachgezogen werden. Bei einem Beratungs- und Kontrollbesuch habe ich die Räumlichkeiten der Deutschen Post AG im Scanncenter DiBAS (Digitalisierung von BA-Schriftgut) in Halle/Saale besucht und mir dabei insbesondere ein Bild von der Organisation sowie der technischen und personellen Ausstattung des Scanncenters gemacht.

Dabei habe ich sämtliche Arbeitsabläufe des Digitalisierungsprozesses, beginnend mit dem Eingang der Post bis hin zur Weiterleitung der elektronischen Dokumente an die BA, überprüft. Daneben habe ich die Räumlichkeiten, die eingesetzte Technik und die eingerichteten Sicherungsmaßnahmen kontrolliert. Ich konnte mich von der datenschutzgerechten Digitalisierung des Schriftguts überzeugen. Alle Prozessschritte werden durch organisatorische und technische Maßnahmen nach dem neuesten Stand der Technik gegen Missbrauch, Manipulation, Verlust und Zerstörung geschützt.

Besonderes Augenmerk habe ich auf die Mitarbeiter im Scanncenter gerichtet. Im Scanncenter DiBAS Halle werden je nach Aufgabenfeld sowohl Mitarbeiter der beauftragten Unternehmen als auch solche der BA eingesetzt. Das Signieren des digitalisierten Schriftguts wird ausschließlich von BA-Mitarbeitern ausgeführt. Insoweit handelt es sich bei der Digitalisierung des Schriftguts nicht ausschließlich um Auftragsdatenverarbeitung, sondern teilweise auch um Verarbeitung zu eigenen Zwecken durch die BA, was die zur Verarbeitung anvertrauten Daten zusätzlich schützt.

Bei einzelnen Fragen ist die Diskussion mit der BA noch nicht beendet. Dies betrifft beispielsweise den Umfang der Stichproben, mit denen die inhaltliche und bildliche Übereinstimmung der Scannprodukte mit den Originalen sichergestellt werden sollen. Elektronische Akten müssen ebenso wie Papierakten den Anforderungen an eine ordnungsgemäße Aktenführung sowie der damit verbundenen Nachweisfunktion entsprechen. Daher ist die bildliche und inhaltliche Übereinstimmung der digitalen Repräsentationen mit den Originaldokumenten nach § 110d SGB IV mit einer qualifizierten Signatur gemäß Signaturgesetz zu bestätigen. Die BA verwendet eine sog. Stapelsignatur.

Es wird nicht jedes einzelne Dokument auf seine Übereinstimmung hin überprüft, sondern nur Stichproben. Inwieweit dies den Anforderungen einer qualifizierten Signatur nach dem Signaturgesetz Rechnung trägt, ist zweifelhaft (vgl. Nr. 13.2). Diese Diskussion wird bestimmt von der Entwicklung eines rechtssicheren ersetzenden Scannens. Hierfür erarbeitet das Bundesamt für Sicherheit in der Informationstechnik (BSI) derzeit eine technische Richtlinie (vgl. Nr. 3.2.2). In diesem Zusammenhang stellen sich dann auch weitere Fragen, beispielsweise die nach dem Umgang mit dem Schriftgut nach dem Scannen.

Das Pilotprojekt wurde inzwischen abgeschlossen und eine bundesweite Einführung beschlossen. Bei der Umsetzung werde ich das Verfahren der Digitalisierung der Akten weiter kritisch begleiten und bei Bedarf einer Überprüfung vor Ort unterziehen. Ein besonderes Augenmerk werde ich dabei auf die beabsichtigte Ausweitung auf die Grundsicherung für Arbeitsuchende (Arbeitslosengeld II) und die Familienkassen legen.

12.2.2 Forschung und Planung in der Arbeitsverwaltung

Die BA darf Sozialdaten an private Umfrage- und Meinungsforschungsinstitute ohne Einwilligung der Betroffenen weitergeben, soweit sie die gesetzlichen Vorgaben einhält.

Für die Betroffenen ist es häufig schwer nachzuvollziehen, warum die BA ihre Sozialdaten, die sie zumeist aus einer Notlage heraus für die Prüfung des Anspruchs auf Sozialleistungen in deren Obhut gegeben haben, von dieser an private Unternehmen weitergegeben werden. Sie gehen davon aus, der Schutz ihrer Sozialdaten sei durch das Sozialgeheimnis nach § 35 Absatz 1 Satz 1 SGB I gewährleistet und eine Weitergabe ihrer Daten ohne Einwilligung stelle eine Verletzung ihrer Rechte dar. Vielen ist nicht bewusst, dass der Gesetzgeber neben ihrem Recht auf informationelle Selbstbestimmung weitere Grundrechtspositionen berücksichtigen muss, wie etwa die Forschungsfreiheit nach Artikel 5 Absatz 3 Grundgesetz. Eine Verarbeitung oder Nutzung von Sozialdaten für die Zwecke der Forschung und Planung ist nach den Regelungen des Sozialgesetzbuchs auch ohne Einwilligung der Betroffenen möglich. Diese Einschränkung des Rechts auf informationelle Selbstbestimmung stellt allerdings eine Ausnahme dar, die an enge gesetzliche Voraussetzungen gebunden ist.

Um bewerten zu können, ob diese Datenweitergabe ohne Einwilligung der Betroffenen zulässig ist, müssen zunächst Forschung und Planung der BA selbst von der durch Dritte durchgeführten Forschungsvorhaben unterschieden werden. Die Differenzierung kann für die Betroffenen schwierig sein, zumal in beiden Fällen die Befragung durch externe Forschungsinstitute möglich ist. Hinzu kommt, dass bestimmte Forschungsgebiete für die BA gesetzlich vorgegeben sind und sie andere Vorhaben auf eigene Initiative durchführen kann. Bei den eigenen Vorhaben kann sich die BA eines geeigneten Dritten im Rahmen der Auftragsdatenverarbeitung nach § 80 SGB X bedienen. Dabei hat sie sicherzustellen, dass beim Auftragnehmer die gleichen datenschutzrechtlichen Anforderungen erfüllt werden, die auch sie selbst zu erfüllen hätte. Der Umfang der Datenerhebung, -verarbeitung oder -nutzung durch den Dritten ist bei der Auftragserteilung schriftlich festzuhalten. Das Institut, das den Auftrag durchführt, ist an die Vorgaben der BA gebunden. Es darf die erhaltenen Daten nicht für andere oder eigene Zwecke verwenden.

Die Weitergabe der Daten an das Forschungsinstitut stellt im Rahmen der Auftragsdatenverarbeitung nach § 80 SGB X keine Übermittlung von Sozialdaten dar, da die BA verantwortliche Stelle bleibt. Weil rechtlich keine Übermittlung erfolgt, kann auch keine Einwilligung für die Übermittlung eingeholt werden. Für die Frage der Zulässigkeit einer Telefonbefragung ist daher in diesen Fällen allein die Zulässigkeit der Datennutzung nach § 67b i. V. m. § 67c SGB X entscheidend.

Bei Forschungsvorhaben von Dritten übermittelt die BA die erforderlichen Daten auf Grundlage des § 75 SGB X. § 75 Absatz 1 SGB X sieht als Voraussetzung grundsätzlich die vorherige Zustimmung (Einwilligung) der Betroffenen in die Übermittlung vor. Hiervon darf nur unter engen Voraussetzungen abgewichen werden. Die oberste Bundesbehörde, im Fall der BA das Bundesministerium für Arbeit und Soziales (BMAS), muss zudem der Übermittlung nach § 75 Absatz 2 SGB X immer zustimmen.

Weil im Rahmen telefonischer Anfragen in der Vergangenheit Missbrauchsfälle vorgekommenen sind, unterrichten die Forschungsinstitute nun in der Regel die Betroffenen durch ein Ankündigungsschreiben von der erfolgten Datenübermittlung und der geplanten Befragung. In einigen Fällen werden diese Informationen auch zu Beginn des Telefongesprächs mitgeteilt. Zudem äußern sich die Mitarbeiter von seriösen Forschungsinstituten bei einer telefonischen Befragung zu ihrem Auftraggeber, zum Zweck der Befragung und zur Dauer der Datenspeicherung und rufen mit sichtbarer Rufnummer an, durch die ein Rückruf und der Erhalt weiterer Informationen ermöglicht werden.

Ich habe mehrere Eingaben zu Forschungsvorhaben des BMAS erhalten, bei denen Kontaktdaten (Name, Anschrift und Telefonnummer) von der BA an ein privates Forschungsinstitut übermittelt wurden. Meine Prüfung hat ergeben, dass in diesen Fällen auf eine Einwilligung der Betroffenen verzichtet werden konnte und die Weitergabe der Sozialdaten nach § 75 SGB X zulässig war.

12.2.3 Gesundheitsdaten bei den Agenturen für Arbeit

Bei den nötigen Feststellungen zu ihrer Gesundheit haben die Betroffenen mitzuwirken, die Einstellung der Leistungen kann aber nur das letzte Mittel sein. Nicht alle Streitfragen konnten mit der BA geklärt werden.

Die Fachkräfte der Agenturen für Arbeit haben neben den beruflichen Kenntnissen und Fähigkeiten auch gesundheitliche Einschränkungen ihrer Kunden zu berücksichtigen, die sich auf deren berufliche Eingliederung aus-

wirken. Bei Angaben zur Gesundheit handelt es sich um sensible persönliche Daten i. S. d. § 67 Absatz 12 SGB X. Deshalb wundert es mich nicht, wenn sich viele Bürgerinnen und Bürger mit Fragen zum Umgang mit Gesundheitsdaten an mich wenden.

Muss ich meine Ärzte von der Schweigepflicht entbinden?

Bei der Erhebung von Gesundheitsdaten können Mitwirkungspflichten der arbeitslos gemeldeten Personen bestehen. Schwierig bleibt die Unterscheidung, wo die freiwillige Angabe durch die Betroffenen endet und wo die – sanktionierbare – Mitwirkungspflicht beginnt.

Zu Fragen der Erhebung von und des weiteren Umgangs mit Gesundheitsdaten befinde ich mich daher im ständigen Dialog mit der BA. Neben Verbesserungen, die ich beispielsweise bei der Gestaltung der Schweigepflichtsentbindungen (23. TB Nr. 11.5.4, dritter Spiegelstrich) erreichen konnte, bestehen nach wie vor unterschiedliche Auffassungen darüber, bis zu welchem Grad hierbei Betroffene mitwirken müssen und welche Folgen eine fehlende Mitwirkung auslöst. Zu meinen Ausführungen zur unrechtmäßigen Anforderung einer Schweigepflichtsentbindung (20. TB Nr. 16.7.3) teilte mir die BA mit, die Abgabe einer Schweigepflichtsentbindung falle unter die Mitwirkungspflichten der §§ 60 ff. SGB I. Käme ein Betroffener dieser Pflicht nicht nach, könnten die Leistungen versagt oder entzogen werden (§ 66 Absatz 1 SGB I).

Ich stimme mit der BA darin überein, dass ihre Mitarbeiter im erforderlichen Umfang Kenntnis über gesundheitliche Einschränkungen der Betroffenen haben müssen. Wenn diese Auswirkungen auf die Vermittlung haben können, ist es Aufgabe der Agenturen für Arbeit festzustellen, worin die konkreten Einschränkungen bestehen und wie sich diese auf die Leistungsfähigkeit auswirken. Die Betroffenen sind dazu verpflichtet, bei der Aufklärung des Sachverhaltes mitzuwirken (§§ 60 bis 62 SGB I).

Allerdings teile ich nicht die Auffassung der BA, bereits die fehlende Erteilung einer Schweigepflichtsentbindung berechtige sie dazu, die Leistungen einzustellen. Die Entbindung der Ärzte von der Schweigepflicht ist nicht der einzige Weg, um den Sachverhalt aufzuklären. Die BA kann den vom Betroffenen ausgefüllten Gesundheitsfragebogen und eingereichte Befundunterlagen durch den eigenen Ärztlichen Dienst auswerten lassen oder eine persönliche Meldung des Betroffenen zu einer Untersuchung beim Ärztlichen Dienst anordnen. Bevor die Agentur die Leistungen versagt oder entzieht, sind daher die weiteren Ermittlungsmöglichkeiten auszuschöpfen. Eine Entziehung oder Versagung der Leistungen allein aufgrund einer nichterteilten Schweigepflichtsentbindung würde einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen, wenn der Betroffene bereit ist, auf andere Weise mitzuwirken.

Meine Rechtsauffassung habe ich der BA mitgeteilt. Ihre Antwort auf mein letztes Schreiben lag bei Redaktionsschluss noch nicht vor. Ich erwarte aber, dass die BA meine Rechtsauffassung bei ihren Entscheidungen über die Entziehungen von Leistungen nach § 66 SGB I künftig berücksichtigt, und werde dies gegebenenfalls vor Ort kontrollieren.

Darf mein Arbeitsvermittler die Unterlagen für den Ärztlichen Dienst lesen?

Der „Praxisleitfaden zur Einschaltung des Ärztlichen Dienstes im Bereich des SGB II und SGB III“ der BA regelt, dass Gesundheitsunterlagen im verschlossenen Umschlag einzureichen sind. Gleichwohl erreichen mich immer wieder Beschwerden, verschlossen übergebene Unterlagen würden von den Fachkräften ohne Einwilligung der Betroffenen geöffnet und eingesehen.

Die in den Agenturen für Arbeit tätigen Fachkräfte sind nicht dafür ausgebildet, medizinische Unterlagen auszuwerten. Dies ist Aufgabe des Fachpersonals des Ärztlichen Dienstes. Die BA hat in diesen Fällen einen Verstoß eingeräumt. Ich hoffe, die Mitarbeiter der BA werden aufgrund der Bürgereingaben weiter dahingehend sensibilisiert, dass für den Ärztlichen Dienst eingereichte Unterlagen sensible Daten enthalten, die nicht in die Hände der Arbeitsvermittler gehören.

12.2.4 Einzelfälle

– *Die BA verlangt für die Zulassung als Maßnahmeträger die Übermittlung personenbezogener Daten der Lehrkräfte.*

Ein Mitarbeiter eines Unternehmens, das Maßnahmen zur Arbeitsförderung im Sinne des SGB III anbietet, machte mich auf die Praxis der BA aufmerksam, im Rahmen des Zulassungsverfahrens personenbezogene Daten der Lehrkräfte abzufragen. Nachdem die BA bisher 13 Angaben zu den Lehrkräften angefordert hatte, werden – nach BA-interner Überprüfung des Datenkatalogs – nunmehr nur noch sieben Punkte abgefragt (Name und Vorname, Geburtsdatum, Einsatz als …, Qualifikation für den vorgesehenen Einsatz, Zeitstunden in der Maßnahme, Anstellungsverhältnis, Einsatz in weiteren Maßnahmen). Diese Reduzierung begrüße ich.

Die BA darf diese Daten nach §§ 176 ff. SGB III i. V. m. der Akkreditierungs- und Zulassungsverordnung Arbeitsförderung erheben. Die Kenntnis dieser Daten ist erforderlich, um eine ordnungsgemäße Maßnahmedurchführung durch entsprechend geeignetes und qualifiziertes Personal zu gewährleisten. Bezüglich der Speicher- und Löschfristen stehe ich in Kontakt mit der BA.

– *Inkassostelle einer Regionaldirektion der BA versendet Ratenzahlungsvereinbarung und Mahnung an unbeteiligten Dritten.*

Ein Petent hatte von der Inkassostelle einer Regionaldirektion der BA eine Ratenzahlungsvereinbarung und eine Mahnung über eine Forderung erhalten, die gegen eine andere Person gerichtet war. Diese hatte zwar den gleichen Vornamen, Nachnamen und Geburtstag, jedoch einen anderen Geburtsort. Aufgrund der Verwechslung erhielt der Petent neben eigenen Sozialdaten unzulässigerweise auch Daten zu einer anderen Person.

Die BA, die als übermittelnde Stelle die Verantwortung für die Zulässigkeit der Übermittlung von Sozialdaten trägt (§ 67d Absatz 2 SGB X), räumte die Personenverwechslung ein. Um solche Fälle zu vermeiden, erfolge die Anschriftenermittlung grundsätzlich über die Kunden- bzw. Rentenversicherungsnummer sowie durch Abgleich des gespeicherten Geburtsorts. Dies sei im konkreten Einzelfall nicht geschehen. Bei der Aufenthaltsermittlung sei es für unwahrscheinlich gehalten worden, dass es mehr als eine Person mit dem nicht alltäglichen Nachnamen des Petenten gebe, die auch noch den gleichen Vornamen und Geburtstag habe. Die Inkassostelle habe den Petenten aufgefordert, die irrtümlich erhaltenen Schreiben als gegenstandslos zu betrachten. Ich habe ihm zusätzlich empfohlen, diese entweder zu vernichten oder an die Inkassostelle zurückzusenden.

Wie die BA mir mitteilte, aktualisiere sich seit Einführung der Finanzanwendung ERP (Software „Enterprise-Resource-Planning“ der Firma SAP) im Januar 2011 die Kundenanschrift bei seitdem angelegten Neufällen automatisiert. Im vorliegenden Fall habe es sich aber um einen Altfall gehandelt, der eine manuelle Bearbeitung der Anschriftenaktualisierung erfordert habe. Ich beabsichtige, die automatisierte Aktualisierung von Kundenanschriften über die neu eingeführte Finanzanwendung ERP im Rahmen einer Kontrolle bei der BA zu prüfen.

– *Die Zentrale Auslands- und Fachvermittlung (ZAV) der BA hatte eine vollständig ausgefüllte und unterschriebene Datenschutzerklärung als zwingende Voraussetzung einer Künstlervermittlung angefordert, ohne auf die Freiwilligkeit und den Verwendungszweck von zum Teil sensiblen Angaben hinzuweisen.*

Die BA begründete ihr Vorgehen damit, die Datenschutzerklärung beruhe auf den Vorgaben der §§ 67 ff. SGB X und eine Weitergabe von Sozialdaten bedürfe der Einwilligung des Betroffenen (§ 67c Absatz 2 Satz 1 Nummer 2 SGB X). Neben Merkmalen wie Augenfarbe, Haarfarbe oder Körpergröße würde im Falle der Einwilligung auch die Angabe „ethnische Zugehörigkeit“ der Künstler als besonders sensibles Datum i. S. d. § 67 Absatz 12 i. V. m. § 67a Absatz 1 SGB X erhoben, falls dessen Kenntnis im Einzelfall für die Vermittlungsarbeit erforderlich sei (Sparten Schauspiel, Film, Oper). Zudem seien diese Daten in der Vermittlungsdatenbank VerBIS der BA nur für die Mitarbeiter der ZAV-Künstlervermittlung einsehbar.

Die Datenschutzerklärung wurde aufgrund meiner Nachfrage datenschutzfreundlich umformuliert. Durch die Neufassung wird für die Betroffenen klar, dass die Angabe der Daten freiwillig ist, bei fehlenden Daten die Vermittlung in den gewünschten künstlerischen Beruf aber erschwert sein kann.

13 Beschäftigtendatenschutz

13.1 Beschäftigtendatenschutzgesetz – eine Hängepartie

Noch immer fehlt die seit langem überfällige gesetzliche Ausgestaltung des Beschäftigtendatenschutzes. Auf europäischer Ebene bringt der Kommissionsentwurf einer Datenschutz-Grundverordnung Bewegung in die Thematik.

Die Bundesregierung hat bereits im Sommer 2010 den Entwurf eines Beschäftigtendatenschutzgesetzes vorgelegt (vgl. 23. TB Nr. 12.1). Die vorgeschlagenen Regelungen sollten den aufgrund von Datenschutzskandalen 2009 eingeführten § 32 BDSG ersetzen, der den Umgang mit Beschäftigtendaten nur lückenhaft regelt. Der Regierungsentwurf war sicher weit davon entfernt, das Recht der Beschäftigten auf informationelle Selbstbestimmung im Beschäftigtenverhältnis zu stärken. Andererseits ist auch der derzeitige Rechtszustand alles andere als optimal. § 32 BDSG bleibt als Grundsatzregelung recht unbestimmt. Seine Konkretisierung, etwa im Hinblick auf die Zulässigkeit der heimlichen oder offenen Videoüberwachung oder des zulässigen Umfangs von Screeningmaßnahmen, ist sehr wünschenswert.

Trotz vieler Kritikpunkte an dem Gesetzentwurf hatte ich die Hoffnung, dass in konstruktiver Diskussion die notwendigen Verbesserungen in den Entwurf Eingang finden und das Gesetzgebungsverfahren zu einem für den Beschäftigtendatenschutz positiven Abschluss kommen würde. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mit ihrer Entschließung vom 16./17. März 2011 die Notwendigkeit bekräftigt, „durch umfassende allgemeingültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen“ (vgl. Kasten a zu Nr. 13.1).

Diese Hoffnungen wurden aber weitgehend enttäuscht. Die letzte offizielle Befassung des Innenausschusses des Deutschen Bundestages durch eine Sachverständigenanhörung liegt lange zurück – sie fand am 23. Mai 2011 statt. Die von den Regierungsfraktionen Anfang Januar 2013 schließlich dem Innenausschuss vorgelegten Änderungsvorschläge waren enttäuschend. Nicht nur die Datenschutzkonferenz setzte sich damit in ihrer Entschließung vom 25. Januar 2013 kritisch auseinander (vgl. Kasten b zu Nr. 13.1). Nachdem auch Gewerkschaften und Arbeitgeberverbände zum Teil sehr heftig dagegen protestierten, nahmen die Koalitionsfraktionen das Beschäftigtendatenschutzgesetz wieder von der Agenda des Innenausschusses. Mittlerweile haben die Koalitionsfraktionen entschieden, den Gesetzentwurf in dieser Legislaturperiode überhaupt nicht mehr zu beraten, so dass dieser endgültig gescheitert ist. Ich hoffe sehr, dass sich der Gesetzgeber in der nächsten Legislaturperiode wieder und diesmal erfolgreich mit einem Beschäftigtendatenschutzgesetz befasst, das seinen Namen zu Recht trägt.

Wichtige Impulse für den Beschäftigtendatenschutz könnten eigentlich von dem diskutierten Entwurf einer Datenschutz-Grundverordnung (vgl. Nr. 2.1.1) ausgehen. Das dabei verfolgte Ziel eines hohen gemeinsamen Datenschutzniveaus in der gesamten Europäischen Union ist an und für sich erfreulich. Der Beschäftigtendatenschutz findet aber in dem Kommissionsentwurf nur wenig Platz, so dass auch hier weitreichender Verbesserungsbedarf besteht.

Es bleibt also dabei, dass es in Sachen Beschäftigtendatenschutz zwar viele Fragen, aber nur wenige befriedigende Antworten gibt.

Kasten a zu Nr. 13.1

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011

Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt die Notwendigkeit, durch umfassende allgemein gültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordert klare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Die Bundesregierung und die Bundestagsfraktionen der SPD und von BÜNDNIS 90/DIE GRÜNEN haben hierzu Gesetzentwürfe vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende notwendige Anforderungen sicherzustellen:

- Im Bewerbungsverfahren und im Beschäftigungsverhältnis
  - ist die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme zu dokumentieren,
  - sind Datenerhebungen nur zulässig, wenn und soweit diese Daten wegen der Art und der Ausübung der Tätigkeit oder der Bedingung ihrer Ausübung unabdingbar sind und entscheidende berufliche Anforderungen oder Hindernisse darstellen,
  - sind Eignungstests ausschließlich zulässig, wenn sie auf einer wissenschaftlichen Methode beruhen.
- Arbeitgeber müssen verpflichtet werden, Bewerber so früh wie möglich umfassend über die Datenerhebung aus allgemein zugänglichen Quellen (z. B. im Internet) und bei Dritten zu unterrichten.
- Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürfen Beschäftigtendaten nur oberhalb normenklarer und verhältnismäßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeber dürfen dabei – insbesondere verdeckte – Überwachungsmaßnahmen nur ergreifen, wenn zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen ist die Grenze zwischen eigenverantwortlichen Recherchen des Arbeitgebers und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig zu bestimmen. Aus präventiven Gründen ist eine verdeckte Datenerhebung unzulässig.
- Insbesondere bezüglich der Durchführung von Screening-Verfahren sind klare materielle Kriterien – z. B. Prüfung der Verhältnismäßigkeit, Vorliegen von tatsächlichen Hinweisen auf Unregelmäßigkeiten – erforderlich. Zudem sollten Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.
- Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltens- und Leistungskontrolle sind nach wie vor zu weitgehend. Der Gesetzgeber muss hier strenge Voraussetzungen vorgeben. Die Konferenz weist auf die gefestigte verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck hin.
- Die Konferenz der Datenschutzbeauftragten fordert, die offene Videoüberwachung stärker zu begrenzen und insbesondere
  - zu verbieten, die z. B. bei der Qualitätskontrolle anfallenden Daten zur Verhaltens- und Leistungskontrolle zu nutzen.
  - für Bereiche zu untersagen, die nicht nur „überwiegend“, sondern auch der privaten Nutzung dienen.
- Das Petitionsrecht darf nicht beschränkt werden. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemaßregelt zu werden.
- In gesetzliche Regelungen zum Beschäftigtendatenschutz sind darüber hinaus Bestimmungen aufzunehmen
  - zur Personalaktenführung – einschließlich der automatisierten Personalaktenführung,
  - zur privaten Nutzung von Telekommunikationsdiensten,
  - zum Thema Whistleblowing,
  - zum Bereich der Videoüberwachung im öffentlich zugänglichen Bereich, bei denen Beschäftigtendaten mit anfallen,
  - zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung,
  - zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs.

Kasten b zu Nr. 13.1

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25. Januar 2013

Beschäftigtendatenschutz nicht abbauen, sondern stärken!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert an ihre Entschließung vom 16./17. März 2011 und ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz. Bei einer Gesamtbetrachtung ist die Konferenz enttäuscht von dem jetzt veröffentlichten Änderungsentwurf der Koalitionsfraktionen.

Bereits der ursprünglich von der Bundesregierung vorgelegte Entwurf enthielt aus Datenschutzsicht erhebliche Mängel. Der nun vorgelegte Änderungsentwurf nimmt zwar einzelne Forderungen – etwa zum Konzerndatenschutz – auf und stärkt das informationelle Selbstbestimmungsrecht auch gegenüber Tarifverträgen und Betriebsvereinbarungen. Das Datenschutzniveau für die Beschäftigten soll jedoch in einigen wesentlichen Bereichen sogar noch weiter abgesenkt werden.

Besonders bedenklich sind die folgenden Regelungsvorschläge:

- Die Möglichkeiten der offenen Videoüberwachung am Arbeitsplatz sollen noch über das bisher Geplante hinaus ausgeweitet werden. Überdies ist die Beschreibung der zuzulassenden Überwachungszwecke unverständlich und würde deshalb nicht zur Rechtssicherheit beitragen.
- Beschäftigte in Call-Centern sollen noch stärker überwacht werden können, als dies der Regierungsentwurf ohnehin schon vorsah. Die Beschäftigten müssen sich nunmehr auf eine jederzeit mögliche, unbemerkte Überwachung einstellen. Hierdurch kann ein unzumutbarer Überwachungsdruck entstehen.
- Die Datenerhebungsbefugnisse im Bewerbungsverfahren sollen erweitert werden. Der noch im Regierungsentwurf vorgesehene Ausschluss von Arbeitgeberrecherchen über Bewerberinnen und Bewerber in sozialen Netzwerken außerhalb spezieller Bewerbungsportale wurde gestrichen. Damit wird der Grundsatz der Direkterhebung bei den Betroffenen weiter unterlaufen.
- Dem Arbeitgeber soll es gestattet sein, auch nicht allgemein zugängliche Beschäftigtendaten bei Dritten zu erheben, wenn die Beschäftigten eingewilligt haben. Die tatsächliche Freiwilligkeit einer solchen Einwilligung ist fraglich.
- Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, soll wieder entfallen.

Die Konferenz appelliert an den Bundestag, bei seinen Beratungen zum Gesetz den Forderungen der Datenschutzbeauftragten Rechnung zu tragen.

13.2 Automatisierte Personaldatenverarbeitung: Beratungen und Entwicklungen in der Bundesverwaltung

Die Bundesverwaltung setzt weiterhin verstärkt auf automatisierte Verfahren der Personaldatenverarbeitung. Bei deren Projektierung ist eine frühestmögliche Berücksichtigung von Datenschutzaspekten unverzichtbar.

In vielen Bereichen des Personalwesens ist eine weitere Ablösung des manuellen Umgangs mit Beschäftigtendaten durch den Einsatz automatisierter Verfahren erkennbar. Zahlreiche Bundesministerien und -behörden wollen neue Verfahren der automatisierten Personaldatenverarbeitung einführen oder bereits bestehende Systeme durch dem aktuellen Stand der Technik entsprechende neue Verfahren ersetzen. Dies betrifft Großverfahren wie Personalinformations- und Personalverwaltungssysteme, sonstige automatisierte/technikunterstützte Abläufe in vielen Bereichen des Personalwesens (z. B. Bewerbungs- oder Beihilfeverfahren), aber auch die Einführung elektronischer Personalakten (vgl. Nr. 13.3, 3.2.1).

Wegen der bestehenden Risiken für die Persönlichkeitsrechte der Beschäftigten müssen die datenschutzrechtlichen Vorgaben zum automatisierten Umgang mit Beschäftigtendaten schon bei der Planung und Entwicklung solcher Verfahren frühzeitig berücksichtigt werden. Alle Datenschutzaspekte sollten von vorneherein in die Gesamtkonzeption eines solchen Projektes einfließen. Nur so lassen sich später ein datenschutzkonformer Praxisbetrieb gewährleisten und zeit- und kostenaufwendige Umplanungen vermeiden.

Im Berichtszeitraum habe ich zahlreiche öffentliche Stellen des Bundes, aber auch deren Personalvertretungen, bei solchen Planungen beraten, wobei meine Beteiligung in vielen Fällen noch andauert (vgl. Kasten zu Nr. 13.2). Hierbei zeigten sich ausnahmslos alle Bundesbehörden den Belangen des Datenschutzes beim automatisierten Umgang mit Beschäftigtendaten gegenüber sehr aufgeschlossen.

Immer wieder auftretende Fragestellungen/Themen sind hierbei z. B.:

- die Abgrenzung, ob es sich um eine Datenverarbeitung im Auftrag nach § 11 BDSG oder um eine Funktionsübertragung handelt,
- die Reichweite von Zugriffsrechten und Auswertungsmöglichkeiten,
- die Umsetzung der Grundsätze der Datenvermeidung und Datensparsamkeit,
- die Sicherstellung der Auskunfts- und Einsichtsrechte der Betroffenen,
- der Inhalt von Freitextfeldern,
- die nach § 9 BDSG und dessen Anlage zu treffenden erforderlichen technischen und organisatorischen Maßnahmen zum Schutze der Beschäftigtendaten,
- die Regelungen von Dienstvereinbarungen,
- der Umfang der Kontrollrechte und Handlungsmöglichkeiten des internen Beauftragten für den Datenschutz,
- insbesondere jedoch die (technische/physikalische) Umsetzung der gesetzlichen Aufbewahrungs-/Löschungsvorschriften von Beschäftigtendaten (z. B. nach den §§ 106 ff. BBG) im Praxisbetrieb.

Wie ich bei Kontrollen (vgl. Nr. 13.4) feststellte, ist es wichtig, dass alle erforderlichen datenschutzrechtlich relevanten Maßnahmen nicht nur bei zentralen Personalinformations- und Personalverwaltungsverfahren umgesetzt werden, sondern auch bei solchen Verfahren, die aus Sicht der Behörde geringere Bedeutung haben, insbesondere bei der dezentralen Verarbeitung von Personaldaten.

Bei meinen Beratungen nimmt die datenschutzkonforme Einführung und Führung von elektronischen Personalakten zunehmenden Raum ein. Diese Entwicklung steht zwar erst am Anfang. Ich gehe aber davon aus, dass die öffentlichen Stellen (nicht nur) des Bundes von der gesetzlichen Möglichkeit, Personalakten vollständig oder in Teilen automatisiert („elektronisch“) zu führen, in absehbarer Zukunft verstärkt Gebrauch machen werden.

Im Rahmen meiner Beratungen weise ich die Bundesbehörden u. a. auf die nach wie vor aktuellen Handlungsempfehlungen hin, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung erarbeitet hat und die ich im Kern in meinem 21. TB dargestellt habe (vgl. 21. TB Kasten zu Nr. 14.3).

Wie wichtig eine frühzeitige datenschutzrechtliche Beratung im Zusammenhang mit der automatisierten Personaldatenverarbeitung ist, zeigen einmal mehr die großen datenschutzrechtlichen Mängel und Rechtsverstöße im Umgang mit Beschäftigtendaten, die ich im Berichtszeitraum bei meinen stichprobenartigen Beratungs- und Kontrollbesuchen bei Bundesbehörden feststellen und auch förmlich beanstanden musste (vgl. Nr. 13.4). Ich werde die Entwicklung weiter beobachten und die öffentlichen Stellen des Bundes hierbei im Rahmen meiner Beratungsaufgabe auch zukünftig unterstützen.

Kasten zu Nr. 13.2

Automatisierte Personaldatenverarbeitung: Beratungen

Im Berichtszeitraum hat mich das BMF beratend in seine Planungen zur Einführung des „Einheitlichen Personalverwaltungssystems in der Bundesfinanzverwaltung (PVS)“ eingebunden. Gleiches gilt für das AA zum dortigen „Integrierten Personalverwaltungs- und Organisationsmanagementsystem IPOS“ (PVS-AA). Das BMI habe ich weiterhin bei seinen Planungen zum Auf- und Ausbau von Dienstleistungszentren zum Umgang mit Beschäftigtendaten beraten (vgl. 23. TB Nr. 12.5), aber auch bei Erstellung und Abschluss einer neuen Rahmendienstvereinbarung mit seinem Hauptpersonalrat (HPR) über die automatisierte Verarbeitung personenbezogener Daten mit dem elektronischen Personal-, Organisations- und Stellenmanagement-System „EPOS 2.0“. Ferner unterstütze ich derzeit die DTAG sowohl bei den elektronischen Personalakten als auch bei der Umsetzung ihres Projektes „Datenschutzkonformes Löschen“ personenbezogener Daten ihrer beamteten Beschäftigten im Personalverwaltungssystem. Schließlich berate ich das BMVBS im neuen Projekt eines „Elektronischen Bewerbungsverfahrens“, ebenso das BMF und das BADV bei den aktuellen Planungen zum Projekt „elektronische Beihilfe – eBiV“.

13.3 Entwicklungen bei der elektronischen Personalakte

Einführung elektronischer Personalakten – zwei Fallbeispiele. Was bei der Telekom geht, muss auch bei der DRV Bund möglich sein.

Mit dem Dienstrechtsneuordnungsgesetz vom 5. Februar 2009 (BGBl. I S. 160 – vgl. 21. TB Nr. 14.2 sowie 22. TB Nr. 16.15) wurde die Möglichkeit geschaffen, Personalakten der Bundesbeamtinnen und -beamten in Teilen oder vollständig automatisiert („elektronisch“) zu führen (§ 106 Absatz 1 Satz 3 Bundesbeamtengesetz – BBG). Bei der datenschutzgerechten Führung von elektronischen Personalakten in der Bundesverwaltung müssen die Authentizität und die Integrität der darin eingescannten Dokumente durch vollständige Sichtprüfung und eine qualifizierte digitale Signatur nach dem Signaturgesetz (SigG) gewährleistet werden (vgl. 23. TB Nr. 12.3, 5.5).

Die DRV Bund hat mich über die Bedingungen eines Pilotverfahrens zur Einführung einer elektronischen Personalakte informiert. Hierbei war u. a. vorgesehen, die in Papierform vorliegenden Personalaktendaten der Beschäftigten einer Abteilung einzuscannen und vor dem Anbringen einer Signatur stichprobenartig die (nach Zufallsauswahl durch das System) bis zum Erreichen der 2-Prozent-Quote notwendige Anzahl an Dokumenten per Sicht zu prüfen. Anschließend sollen aber – sofern die wenigen digitalisierten Dokumente, deren Sichtprüfung erzwungen wurde, als lesbar und beanstandungsfrei bestätigt werden –

alle Dokumente des Stapels eine qualifizierte elektronische Signatur erhalten. Zur Qualitätssicherung/-kontrolle will die DRV Bund in diesem Testverfahren anschließend nochmals alle Papierdokumente mit ihren digitalen Abbildern vergleichen, dies dokumentieren und auf dieser Basis (Abgleich von Stichproben- und vollständiger Sichtprüfung) die Frage der hinreichenden Sicherheit des Verfahrens bewerten.

Um eine hinreichend sichere und vollständige Digitalisierung der Personalakten zu gewährleisten, reicht aus meiner Sicht eine lediglich 2-Prozent-Sichtprüfung der eingescannten Dokumente nicht aus, um anschließend eine qualifizierte elektronische Signatur nach dem Signaturgesetz für alle Dokumente anzubringen. Mit dieser technischen Begrenzung kann z. B. ein Mitarbeiter nicht mehr selbständig bestimmen, ob er mehr oder gar alle Dokumente vergleicht. Er wird im Zweifel zur Unterschrift/qualifizierten Signatur verpflichtet.

Im Dezember 2012 hat mich die DRV Bund informiert, sie habe mit ausdrücklicher Zustimmung des BMAS testweise mit der Einführung elektronischer Personalakten begonnen. Die derzeit nach dem Scannen durchgeführte 100prozentige-Sichtprüfung diene der Ermittlung der Fehlerquote. Damit ist zumindest in diesem Pilotverfahren eine 100prozentige-Sichtprüfung und damit eine sichere und vollständige Digitalisierung der ausgewählten Personalakten gewährleistet. Die DRV Bund hat zugesagt, mich nach Beendigung des Testverfahrens erneut zu beteiligen. Hierbei werde ich auch auf die nachfolgend dargestellten positiven Ergebnisse meiner entsprechenden Beratung der Deutschen Telekom AG (DTAG) hinweisen.

Bei der DTAG werden die Personalakten aller Beschäftigten bereits seit einigen Jahren elektronisch (bisher jedoch ohne eine Signatur der Dokumente) geführt, die der Beamtinnen und Beamten bisher ausnahmsweise zusätzlich parallel noch in Papierform. Im Berichtszeitraum habe ich die DTAG im Zusammenhang mit den elektronischen Personalakten der dort beschäftigten Beamtinnen und Beamten bei der vollständigen Umsetzung der gesetzlichen Vorgaben des Dienstrechtsneuordnungsgesetzes zur Führung elektronischer Personalakten beraten. Dabei habe ich der DTAG insbesondere empfohlen, alle in den automatisiert geführten Teilen der Personalakten gespeicherten Dokumente mit einer qualifizierten Signatur nach dem SigG zu versehen. Meine früheren Vorschläge (vgl. 23. TB Nr. 12.3, 5.5, Zusammenfassungen aller Empfehlungen) hat die DTAG bereits zum größten Teil umgesetzt. Sie hat mir ferner ausdrücklich zugesichert, nach Prüfung ausnahmslos aller Dokumente der elektronischen Personalakten ihrer beamteten Beschäftigten diese nach einem mit mir abgestimmten Konzept mit einer qualifizierten elektronischen Signatur nach dem SigG zu versehen und im Anschluss die entsprechenden Papierunterlagen datenschutzkonform zu vernichten. Ich begrüße ausdrücklich, dass die DTAG bei allen Dokumenten, sowohl den bereits in den elektronischen Personalakten eingescannten/gespeicherten ca. 22 Millionen Dokumente, als auch zukünftig bei neuen Personalaktendaten, eine vollständige Sichtprüfung durchgeführt hat bzw. durchführen und anschließend die Dokumente qualifiziert signieren wird.

Meine datenschutzrechtlichen Hinweise sind auch in die am 1. Dezember 2011 in Kraft getretene Personalaktenrichtlinie für die bei der DTAG beschäftigten Beamtinnen und Beamte eingeflossen, die der neuen Rechtslage nach dem Dienstrechtsneuordnungsgesetz angepasst worden ist. Danach werden die Personalakten der Beamtinnen und Beamten als Hybridakten – die Grundakte automatisiert sowie bestimmte Teilakten weiterhin in Schriftform – geführt. Das Recht auf Einsicht in die vollständige Personalakte nach § 110 Absatz 1 BBG ist sichergestellt, die Aufbewahrungs-/Löschungsfristen in der elektronischen Personalakte der beamteten Beschäftigten entsprechen den Vorgaben des Bundesbeamtengesetzes. Die Löschung von elektronischen Dokumenten wird derzeit durch die Aufhebung von Verknüpfungen zum Archiv realisiert. Das von der DTAG erstellte, von mir empfohlene Konzept zur physikalischen Löschung der Dokumente im Archiv wird die DTAG im 2. Quartal 2013 umsetzen.

Bezüglich der elektronischen Personalakten ihrer Tarifbeschäftigten steht die DTAG auf meine Anregung hin in Kontakt mit dem hierfür zuständigen Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

13.4 Kontrollen im Personalwesen

Bei datenschutzrechtlichen Kontrollbesuchen festgestellte Mängel musste ich in zahlreichen Fällen beanstanden.

Im Berichtszeitraum habe ich die Unfallkasse des Bundes, das Wasser- und Schifffahrtsamt Dresden sowie das Jobcenter Wittenberg im Umgang mit Beschäftigtendaten in den Personalabteilungen und bei Fachvorgesetzten – insbesondere im Hinblick auf die automatisierte Personaldatenverarbeitung – beraten und kontrolliert. Zu meinem Bedauern musste ich zahlreiche Verstöße, insbesondere gegen die §§ 106 ff. BBG, feststellen und in mehreren Fällen förmlichen Beanstandungen aussprechen.

Kontrollen bei der Unfallkasse des Bundes

Die Unfallkasse des Bundes (UK-Bund) habe ich im Berichtszeitraum zweimal kontrolliert. Dabei zeigten sich erhebliche Datenschutzverstöße beim automatisierten Umgang mit personenbezogenen Daten der Beschäftigten. So habe ich unzulässige Verfahren der automatisierten Personaldatenverarbeitung und sonstige Dokumente mit Personal-/Personalaktendaten vorgefunden, die neben dem für Zwecke der Personalverwaltung, Organisation und Stellenbewirtschaftung eingesetzten Verfahren EPOS betrieben wurden. In diesen Verfahren waren ohne Rechtsgrundlage Personal-/Personalaktendaten von Beschäftigten, u. a. mit Angaben über ihre Gesundheit, zu bereits lange abgeschlossenen Personalvorgängen – teilweise als „Muster“ für zukünftige Vergleichsfälle – gespeichert.

Datenschutzrechtliche Mängel ergaben sich auch beim Betrieb des sog. elektronischen Zeitwirtschaftssystems. Mit diesem System werden auch die Urlaubs- und Erkrankungsdaten verwaltet. Allerdings wurden die gesetzlichen Aufbewahrungsfristen (§ 113 Absatz 2 Satz 1 BBG) für diese Personalaktendaten nicht eingehalten. Sowohl automatisiert als auch in Papierform waren diese Daten unzulässig zu früh gelöscht worden, was die Persönlichkeitsrechte der Betroffenen verletzt.

Am Arbeitsplatz des Leiters einer Fachabteilung der UK-Bund wurden unzulässig Personal-/Personalaktendaten (hierunter auch Angaben über Gesundheit) automatisiert gespeichert, dabei auch solche von Beschäftigten anderer Abteilungen. Unter welchen engen Voraussetzungen Vorgesetzte im Rahmen der täglichen Aufgabenerledigung berechtigt sind, personenbezogene Daten der Mitarbeiterinnen und Mitarbeiter ihrer Organisationseinheit zu verwenden, habe ich ausführlich in meinem 21. TB (Nr. 14.1) dargestellt. Diese Voraussetzungen waren vorliegend nicht gegeben.

Die Datenschutzverstöße habe ich nach § 25 Absatz 1 BDSG gegenüber dem Vorstand der UK-Bund beanstandet. Der Besuch zeigte auch Datenschutzverstöße im Umgang der UK-Bund mit Sozialdaten der bei ihr Versicherten auf, die ebenfalls zu einer förmlichen Beanstandung führten (vgl. hierzu Nr. 11.4.2).

Bei einer unangekündigten Nachkontrolle musste ich erneut feststellen, dass entgegen der mir zuvor gegebenen Bestätigung, dass die schon beanstandeten Mängel im Umgang mit Personal-/Personalaktendaten der Beschäftigten und mit Sozialdaten abgestellt worden seien, nach wie vor eine sehr große Anzahl an Dateien mit Personal-/Personalaktendaten der Beschäftigten ohne Rechtsgrundlage und damit weiterhin unzulässig gespeichert waren. Ich habe dies gegenüber dem Vorstand der UK-Bund erneut als einen Verstoß gegen die Regelungen der §§ 106 ff. BBG beanstandet.

Nach § 24 Absatz 4 BDSG sind die öffentlichen Stellen des Bundes verpflichtet, mich und meine Mitarbeiterinnen und Mitarbeiter bei der Erfüllung meiner Aufgaben zu unterstützen. Die unzutreffende Bestätigung der Löschung von unzulässig gespeicherten Personal-/Personalaktendaten durch den Geschäftsführer – nach der ich von einem nunmehr datenschutzkonformen Umgang mit Beschäftigtendaten ausgehen konnte – habe ich deshalb nach § 25 Absatz 1 BDSG gegenüber dem Vorstand der UK-Bund als einen Verstoß gegen das in § 24 Absatz 4 BDSG normierte Unterstützungsgebot beanstandet.

Auch in Freitextfeldern in EPOS und im Zeitwirtschaftssystem der UK-Bund habe ich unzulässige, für die Aufgabenerfüllung nicht erforderliche Einträge mit Beschäftigtendaten festgestellt. Noch während des Besuches hat die UK-Bund die von mir empfohlenen notwendigen Maßnahmen für einen datenschutzgerechten Umgang mit Beschäftigtendaten in den Freitextfeldern beider Systeme eingeleitet und mir die Löschung aller unzulässigen Beschäftigtendaten erneut zugesichert. Unter Berücksichtigung dieser Maßnahmen habe ich insoweit von einer Beanstandung abgesehen.

Kontrolle im Wasser- und Schifffahrtsamt (WSA) Dresden

Im Zusammenhang mit meinen beiden im Jahr 2009 durchgeführten Beratungs- und Kontrollbesuchen im Geschäftsbereich des BMVBS (vgl. 23. TB Nr. 12.4) habe ich im WSA Dresden überprüft, ob die vom BMVBS zugesagten/bestätigten Maßnahmen und Veranlassungen für einen datenschutzgerechten Umgang mit Beschäftigtendaten im Geschäftsbereich im Praxisbetrieb umgesetzt wurden. Insbesondere galt mein Augenmerk möglichen weiteren unzulässigen Verfahren der automatisierten Personaldatenverarbeitung neben dem im Geschäftsbereich eingesetzten einheitlichen Personalverwaltungssystem PVS BMVBS (PVS).

Die Prüfung im WSA Dresden des dort seit Oktober 2007 eingesetzten PVS führte erfreulicherweise im Ergebnis zu keinen datenschutzrechtlichen Beanstandungen bei der Nutzung des eigentlichen Systems. Allerdings habe ich dort im Sachbereich Personal erneut in großer Anzahl weitere unzulässige Verfahren der automatisierten Personaldatenverarbeitung für Zwecke der Personalverwaltung/Personalwirtschaft vorgefunden. In der Regel waren dort Personal-/Personalaktendaten der Beschäftigten gespeichert, die nach den gesetzlichen Aufbewahrungs-/Löschungsregelungen längst hätten gelöscht sein müssen. Ich habe deutlich gemacht, dass das in PVS grundsätzlich gewährleistete gesetzmäßige Löschen von Beschäftigtendaten nicht durch einen Umgang mit Beschäftigtendaten außerhalb von PVS „unterlaufen“ werden darf.

Nach meinen Kontroll- und Beratungsbesuchen im Jahr 2009 hatte das BMVBS seinen Geschäftsbereich u. a. darauf hingewiesen, dass auch bei Papierunterlagen die gesetzlichen Löschungsfristen zu beachten sind. Dennoch habe ich im WSA Dresden in sehr großem Umfang unzulässig gespeicherte Personal-/Personalaktendaten in Papierform – auch besondere Arten personenbezogener Daten (Angaben über politische Meinungen, Gesundheit) – festgestellt. So waren z. B. in drei Karteikästen Hunderte alter Karteikarten (Personalkarten) zu ausgeschiedenen, in überwiegender Zahl bereits verstorbenen Beschäftigten des WSA Dresden bzw. der Vorgängerbehörden und zu deren Angehörigen abgelegt. Die Geburtsdaten der Betroffenen datierten ab dem Jahr 1885!

Die unzulässige Speicherung von Personal-/Personalaktendaten in automatisierter und in manueller Form habe ich gegenüber dem BMVBS als Verstoß gegen die Regelungen der §§ 106 ff. BBG bzw. gegen § 12 Absatz 4 i. V. m. § 32 Absatz 1 BDSG beanstandet.

Geprüft habe ich auch das automatisierte Gleitzeitverfahren. Wie ich dabei feststellen musste, waren dort alle Zeitbuchungen der Beschäftigten rückwirkend noch bis zum 1. Januar 2010 gespeichert, was mit den entsprechenden Regelungen der Verordnung über die Arbeitszeit der Beamtinnen und Beamten des Bundes (Arbeitszeitverordnung – AZV) vom 23. Februar 2006 nicht in Ein-

klang steht. Welche personenbezogenen Daten der Beschäftigten den unmittelbaren Vorgesetzten im Rahmen der automatisierten Gleitzeit mitgeteilt werden dürfen, hatte ich u. a. in meinem 21. TB (Nr. 14.1) dargestellt. Dass die unmittelbaren Vorgesetzten an ihren Rechnern einen permanenten automatisierten und unkontrollierten Zugang zu den Gleitzeitkonten der Beschäftigten ihrer Organisationseinheit hatten und somit jederzeit die Möglichkeit bestand, unzulässigerweise Gleitzeitdaten (Einzelbuchungen) zur Kenntnis zu nehmen und das Verhalten der einzelnen Beschäftigten zu überprüfen, verstößt gegen § 7 Absatz 8 AZV. Auch die maßgebliche Regelung zu diesem Datenzugriff – der der Personalrat zugestimmt hatte – entsprach nicht der Rechtslage. In der Gleitzeitstelle habe ich ferner unzulässig gespeicherte alte Gleitzeitlisten und Monatsjournale von ausgeschiedenen Beschäftigten festgestellt. Unzulässig war auch die im WSA geübte Praxis, täglich eine automatisierte Abwesenheitsliste mit Zugriffsmöglichkeit für alle Beschäftigten des Amtes zu erstellen.

Die festgestellten Mängel im Umgang mit Beschäftigtendaten bei der Durchführung der gleitenden Arbeitszeit habe ich gegenüber dem BMVBS nach § 25 Absatz 1 BDSG als Verstoß gegen die Regelungen des § 12 Absatz 4 i. V. m. § 32 Absatz 1 BDSG und § 7 Absatz 7 und 8 AZV beanstandet.

Im Ergebnis habe ich dem BMVBS mitgeteilt, dass ich hinsichtlich zahlreicher Kontrollfeststellungen grundsätzlichen Handlungsbedarf für den gesamten Geschäftsbereich sehe.

Kontrolle im Jobcenter Landkreis Wittenberg

Der Beratungs- und Kontrollbesuch im Jobcenter Landkreis Wittenberg diente dazu, den Umgang mit personenbezogenen Daten aller zugewiesenen Beschäftigten im Rahmen der dem Geschäftsführer des Jobcenters zustehenden dienst-, personal- und arbeitsrechtlichen Befugnisse zu überprüfen (vgl. Nr. 12.1.3.9). Konkrete datenschutzrechtliche Anweisungen/Vorgaben oder Verfügungen zum zulässigen Umgang mit Beschäftigtendaten gab es zum Zeitpunkt meines Besuches im Jobcenter leider nicht.

Am Arbeitsplatz einer Bereichsleiterin habe ich u. a. festgestellt, dass auf die tagesaktuell erstellte automatisierte Liste „Abwesenheit von Beschäftigten“ neben der Geschäftsführung alle Teamleiter des Jobcenters Zugriff hatten und zwar nicht beschränkt auf die ihnen zugewiesenen Mitarbeiter. Dies war für deren Aufgabenerfüllung nicht erforderlich und somit ebenso unzulässig, wie die Speicherung der detaillierten Abwesenheitsgründe. Ferner waren dort noch einige automatisierte Listen (automatisierte Verfahren) und Dokumente mit Personal-/Personalaktendaten der Beschäftigten gespeichert, die bereits gelöscht hätten sein müssen, da sie zur Aufgabenerfüllung der Vorgesetzten nicht mehr erforderlich waren. Ich habe darauf hingewiesen, dass es sich bei solchen automatisierten Listen des Jobcenters als verantwortliche Stelle um Verfahren der automatisierten Personaldatenverarbeitung handelt. Sie sind u. a. in das Verfahrensverzeichnis des Jobcenters aufzunehmen und unterliegen der Mitbestimmung. Ferner sind rechtzeitig der Beauftragte für den Datenschutz der verantwortlichen Stelle und in allgemeiner Form die betroffenen Beschäftigten zu unterrichten. Diese Voraussetzungen waren im Jobcenter noch nicht umgesetzt.

Am Arbeitsplatz eines Teamleiters wurden die einzelnen Urlaubskarten der Beschäftigten des Teams aufbewahrt. Nach seiner Aussage erfolgte dies mit freiwilliger Zustimmung der Betroffenen. Entsprechende schriftliche Einwilligungen nach § 4a BDSG konnten allerdings nicht vorgelegt werden. Die Urlaubskarte stellt eine Unterlage mit Personalaktendaten dar und gehört materiell-rechtlich zur Personlakte des jeweiligen Beschäftigten. Eine Aufbewahrung der Urlaubskarten bei einem Vorgesetzten verstößt gegen das Personalaktengeheimnis. Nach § 107 BBG dürfen Vorgesetzte keinen Zugang zur Personalakte eines Beschäftigten haben und auch keine Personalakten – auch nicht als Teilakte – führen. Festgestellt habe ich auch, dass im elektronischen Zeiterfassungssystem des Jobcenters noch Einzelzeitbuchungen gespeichert waren, die nach der AZV bereits hätten vernichtet sein müssen.

Da das Jobcenter Landkreis Wittenberg noch während des Besuches notwendige Maßnahmen eingeleitet hat, habe ich nach § 25 Absatz 2 BDSG davon abgesehen, die festgestellten Datenschutzverstöße zu beanstanden.

13.5 Arzneimittelrabatte auf der Grundlage von Beihilfeabrechnungen

Das Gesetz über Rabatte für Arzneimittel verändert auch die Beihilfebearbeitung – mit Auswirkungen auf den Datenschutz.

Zum 1. Januar 2011 wurden viele Beihilfeberechtigte davon überrascht, dass die Beihilfestelle ihnen nicht mehr die eingereichten Rezepte nach Abrechnung ihrer Anträge zurücksandte. Weil auch nach dem Bundesbeamtengesetz Unterlagen, aus denen die Art einer Erkrankung ersichtlich ist, unverzüglich zurückzugeben sind, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden, haben sich zahlreiche Beamte an mich gewandt.

Das Anfang 2011 in Kraft getretene Gesetz über Rabatte für Arzneimittel hat sich auch auf das Beihilfeverfahren des Bundes ausgewirkt. In seiner Umsetzung haben die Beihilfestellen durch entsprechende Hinweiszettel mitgeteilt, Rezeptbelege würden ab Kaufdatum 1. Januar 2011 nicht mehr zurückgesandt. Denn bei der Beihilfesachbearbeitung werden alle Arzneimittel, zu denen ein Beihilfeanspruch geltend gemacht wurde, auf Rabattfähigkeit geprüft. Handelt es sich um ein rabattfähiges Arzneimittel, so hat die Festsetzungsstelle über die zentrale Stelle den Rabatt geltend zu machen. Weil die meisten Beihilfeanträge auch Arzneimittel betreffen, müssen die Prüfung auf Rabattfähigkeit und die Geltendmachung der Rabatte organisatorisch in das Verfahren der Beihilfesachbearbeitung eingegliedert werden. Die Geltendmachung erfolgt grundsätzlich in anonymisierter Form, erfordert also nicht die Nutzung oder Übermittlung

personenbezogener Daten an die zentrale Stelle oder das rabattverpflichtete Unternehmen. Allerdings erlaubt das Gesetz über Rabatte für Arzneimittel dem rabattverpflichteten pharmazeutischen Unternehmer, „in begründeten Fällen sowie in Stichproben“ die Prüfung der Rabattabrechnung durch einen Treuhänder. Gegen diese Praxis und das einzuführende Treuhänderverfahren in der Beihilfe hatte ich gegenüber dem BMI datenschutzrechtliche Bedenken geäußert, die insbesondere die Vereinbarkeit mit den Regelungen des § 108 Absatz 1 Satz 5 und § 113 Absatz 2 Satz 3 BBG betrafen.

Die fehlenden beamtenrechtlichen Vorgaben wurden zwischenzeitlich ergänzt. Durch den entsprechenden Zusatz in § 113 Absatz 2 BBG sind Verfahren, mit denen Rabatte oder Erstattungen geltend gemacht werden, nunmehr berücksichtigt.

14 Verteidigung und Bundesfreiwilligendienst

14.1 Feldpost aus Afghanistan

Ein böser Verdacht hat sich nicht bestätigt.

Im Januar 2011 schreckten mich Presseberichte auf, Postsendungen deutscher Soldaten aus Afghanistan an ihre Angehörigen in Deutschland seien geöffnet und zum Teil ohne Inhalt angekommen. Die Vermutungen beruhten auf Beschwerden an den Wehrbeauftragten des Deutschen Bundestags. Ich bat das Bundesministerium der Verteidigung (BMVg) um Auskunft, woraufhin der Beauftragte für den Datenschutz in der Bundeswehr (BfDBw) umgehend die ihm vorliegenden Informationen übersandte und mitteilte, dass er bereits mit der datenschutzrechtlichen Prüfung der Vorfälle begonnen habe. Daneben hätten auch das Einsatzführungskommando der Bundeswehr sowie das Streitkräfteunterstützungskommando Ermittlungen aufgenommen. Auch die zuständige Staatsanwaltschaft hatte im Februar 2011 ein Ermittlungsverfahren gegen Unbekannt eingeleitet. Es bestand der Verdacht, die Postsendungen seien in Deutschland unerlaubt geöffnet worden. Schließlich führte auch die Deutsche Post AG in ihrem Zuständigkeitsbereich Untersuchungen durch.

Alle Stellen fanden nach Abschluss ihrer Ermittlungen keine Anhaltspunkte dafür, dass Postsendungen systematisch geöffnet und Gegenstände entwendet worden waren. Verletzungen des Postgeheimnisses (Artikel 10 GG) konnten nicht festgestellt werden. Auffällig viele Verdachtsfälle betrafen Speichermedien, wie beispielsweise Micro-SD-Karten, die in DIN-A5-Briefumschlägen verschickt worden waren. Die Briefe wiesen alle an der gleichen Stelle eine Öffnung vor. Wie die staatsanwaltschaftlichen Ermittlungen ergaben, waren die Beschädigungen aller Wahrscheinlichkeit nach durch eine Sortiermaschine verursacht worden. Erkennen die Postmitarbeiter nicht, dass sich im Umschlag ein Gegenstand befindet, wird der Brief in eine Sortiermaschine eingelegt. Die Speichermedien werden dann durch die Maschine herausgedrückt. Wird dies anschließend erkannt, werden die Briefe verschlossen und der Adressat wird durch ein mitgesendetes Anschreiben auf den Grund der Beschädigung hingewiesen. Die herausgedrückten Gegenstände werden täglich eingesammelt, können bei ca. 40 000 Briefen aber nicht mehr zugeordnet werden. Die gesammelten Gegenstände werden für ein Jahr aufbewahrt, Speichermedien anschließend vernichtet.

In zahlreichen Verdachtsfällen konnte somit eine wahrscheinliche Ursache für die Beschädigungen und den Verlust der Speichermedien identifiziert werden. Weitere Fälle konnten durch die Staatsanwaltschaft aufgeklärt werden (Paket wurde verspätet zugestellt oder rechtmäßig durch den Zoll geöffnet, zusätzlich angebrachte Verklebungen zum Schutz vor Witterungseinflüssen). Lediglich in einem Fall bestand der Verdacht eines Diebstahls, der aber nicht mehr aufgeklärt werden konnte.

Das BMVg und der BfDBw haben mir in dieser Angelegenheit alle erforderlichen Informationen zeitnah zur Verfügung gestellt und damit ein Beispiel für gute Zusammenarbeit gegeben.

14.2 Wehrrechtsänderungsgesetz 2011 – das Ende der Wehrpflicht?

Die Aussetzung der Wehrpflicht hat zahlreiche Auswirkungen – auch für den Datenschutz.

Der Gesetzgeber hat mit dem Gesetz zur Änderung wehrrechtlicher Vorschriften vom 28. April 2011 (Wehrrechtsänderungsgesetz 2011 – WehrRÄndG) die Aussetzung des allgemeinen Grundwehrdienstes zum 1. Juli 2011 beschlossen.

Was geschieht mit den personenbezogenen Daten der ausscheidenden Soldaten und Mitarbeiter? Wie lange dürfen Akten mit Personaldaten aufbewahrt werden und welche Rechtsgrundlagen gelten hierfür? Werden die neuen Dienste (freiwilliger Wehrdienst und Bundesfreiwilligendienst) datenschutzkonform durchgeführt? Diesen Fragen war im Rahmen von Beratungs- und Kontrollbesuchen sowie den inhaltlich damit im Zusammenhang stehenden Bürgereingaben nachzugehen.

14.2.1 Aussetzung des Zivildienstes

Als Folge der Aussetzung des Wehrdienstes wurde auch der Zivildienst für anerkannte Kriegsdienstverweigerer zum 1. Juli 2011 ausgesetzt.

Die Änderung des Zivildienstgesetzes (ZDG) erfolgte in Artikel 3 des Gesetzes zur Einführung eines Bundesfreiwilligendienstes vom 28. April 2011. Nach § 1a ZDG wird der Zivildienst nur noch im Spannungs- oder Verteidigungsfall abgeleistet werden. Infolge der Aussetzung haben sich die Aufgaben im Bundesamt für Familie und zivilgesellschaftliche Aufgaben (BAFzA, ehemals Bundesamt für Zivildienst) erheblich verändert. Eine Vielzahl der bisherigen Aufgaben ist entfallen.

Ob die Verfahren bei der Abwicklung des Zivildienstes den datenschutzrechtlichen Grundsätzen entsprechen, habe ich bei einem Beratungs- und Kontrollbesuch im BAFzA überprüft. Bei der Kontrolle habe ich insoweit keine datenschutzrechtlichen Mängel festgestellt und konnte mich von einem kompetenten und datenschutzgerechten Umgang der Mitarbeiter mit den Akten und Daten

der ehemaligen Zivildienstleistenden überzeugen. Durch die seit 2006 erfolgte Umstellung der Papierakten auf elektronische Akten (vgl. auch 21. TB Nr. 4.7) gelten die für dieses Verfahren festgelegten Sicherungsmaßnahmen sowie die Lösch- und Vernichtungsregelungen weiter. Speicherung und Aufbewahrung der Akten im elektronischen Verfahren sind systemgesteuert und werden nach den hierfür festgelegten Routinen behandelt. Dies gilt ebenso für die Datenlöschung. Die Ausführung wird von der behördlichen Datenschutzbeauftragten regelmäßig kontrolliert.

14.2.2 Einführung des Bundesfreiwilligendienstes

Mit dem Gesetz zur Einführung des Bundesfreiwilligendienstes (BFDG) vom 28. April 2011 wurde ein neuer Dienst auf Basis freiwilliger Teilnahme eingerichtet. Prüfungen vor Ort ergaben nur Hinweise auf kleinere Mängel.

Im Bundesfreiwilligendienst engagieren sich Frauen und Männer für das Allgemeinwohl, insbesondere im sozialen, ökologischen und kulturellen Bereich sowie im Bereich des Sports, der Integration sowie des Zivil- und Katastrophenschutzes. Das Freiwilligendienstverhältnis kommt durch Abschluss einer Vereinbarung nach § 8 BFDG zwischen der Bundesrepublik Deutschland (vertreten durch das BAFzA) und dem Freiwilligen zustande. Die Inhalte der Vereinbarung, zu denen insbesondere die Dauer des zu leistenden Dienstes sowie Art und Umfang der an den Freiwilligen zu entrichtenden Leistungen zählen, werden vorab mit der Einsatzstelle und dem Freiwilligen abgestimmt. Der Bundesfreiwilligendienst wird in der Regel für eine Dauer von zwölf zusammenhängenden Monaten geleistet. Er dauert mindestens sechs und höchstens 18 Monate (§ 3 Absatz 2 Satz 1 und 2 BFDG). Die Zuständigkeit für den Bundesfreiwilligendienst wurde auf das Bundesamt für Familie und zivilgesellschaftliche Aufgaben übertragen.

Mit den vertraglichen Vereinbarungen werden personenbezogene Daten erhoben und gespeichert. Anlässlich meines Beratungs- und Kontrollbesuchs beim BAFzA habe ich ein ausgeprägtes Bewusstsein für einen sorgfältigen Umgang mit personenbezogenen Daten wahrgenommen. Vor Ort wurden nur geringe datenschutzrechtliche Mängel festgestellt, die größtenteils bereits während meines Besuchs beseitigt wurden. Für die Bearbeitung steht nicht die aus dem Zivildienst bekannte „E-Akte“ als Verfahrens- und Bearbeitungsinstrument zur Verfügung. Zwar werden die Bearbeitungstexte mit einem Textverarbeitungsprogramm erstellt, jedoch erfolgt die Aktenführung noch in Papier. Zu Einzelfragen der entsprechenden Datenschutzorganisation befinde ich mich noch im Dialog mit dem BAFzA.

14.2.3 Personalgewinnung durch Karrierecenter der Bundeswehr

Die Bundeswehr verarbeitet vielfältige personenbezogene Bewerberdaten. Bei Prüfungen festgestellte kleinere Datenschutzmängel konnten im Wesentlichen abgestellt werden.

Die Bundeswehr kann für ihren Personalbedarf nicht mehr auf die Unterstützung durch Wehrpflichtige zurückgreifen. Um Zeit- und Berufssoldaten sowie Zivilpersonal zu gewinnen, hat sich die Bundeswehr für eine Lösung „aus einer Hand“ entschieden und ihr Personalgewinnungsverfahren mit der Einrichtung von sog. Karrierecentern neu gestaltet.

Das Zentrum für Nachwuchsgewinnung Nord (ZNwG NORD) in Hannover wurde beauftragt, im Rahmen eines Pilotprojekts unter einem Dach Nachwuchs für alle Bereiche der Bundeswehr – militärische und zivile – zu gewinnen. Dabei wird eine Vielzahl von Daten erhoben, die neben den persönlichen Angaben auch medizinische und psychologische Erkenntnisse enthalten.

Bei einem Beratungs- und Kontrollbesuch habe ich nur geringe datenschutzrechtliche Mängel festgestellt. Meine entsprechenden Empfehlungen wurden bereits beim Abschlussgespräch angenommen. Die Stellungnahme zu meinem Kontrollbericht lag bei Redaktionsschluss noch nicht vor.

In den Räumlichkeiten des ZNwG NORD konnte ich mich von einem datenschutzbewussten Umgang mit Bewerberakten durch die Bundeswehrmitarbeiter überzeugen. Der Datenschutz wird bei der Arbeits- und Terminplanung ebenso berücksichtigt wie auf den Fluren und in den Aufenthaltsbereichen, in denen sich die Bewerber während des Auswahlverfahrens aufhalten.

Der Umgang mit den Bewerbern in den Bereichen des psychologischen und medizinischen Dienstes vollzieht sich individuell, diskret und datenschutzgerecht. Die hierfür benötigten Akten werden von Hand zu Hand weitergegeben, nachdem sie zuvor entsprechend der Terminierung bereitgestellt wurden. Die Aufbewahrung bzw. Bereithaltung richtet sich nach den geplanten Terminen und erfolgt zentral in den dafür vorgesehenen Aktenräumen.

Bei der medizinischen Untersuchung werden auch Patientenakten angelegt, um die medizinische Tauglichkeit des Bewerbers oder Verwendungsausschlüsse ermitteln zu können. Die erreichte Tauglichkeitsstufe sowie die aus der Untersuchung resultierenden Verwendungsmöglichkeiten werden in die Bewerberakte übernommen, nicht jedoch die medizinischen Befunde. Diese werden in verschlossenen Umschlägen mit den Akten aufbewahrt und verschlossen weitergeleitet. Sie dürfen nur von besonders dazu befugten Personen, z. B. Ärzten oder besonders beauftragten Mitarbeitern des medizinischen Dienstes geöffnet werden.

Insgesamt sind etwa 16 Karrierecenter der Bundeswehr geplant. Bei der Einrichtung der weiteren Karrierecenter erwarte ich ein ebenso hohes Maß an Datenschutzbewusstsein und einen verantwortungsvollen Umgang mit den Daten, wie ich sie bei meiner Kontrolle vorgefunden habe.

14.2.4 Aufbewahrungsdauer von Akten Wehrpflichtiger bei der Bundeswehr

Für Musterungsakten gelten differenzierte Aufbewahrungsfristen. Nach deren Ablauf sind die Akten zu vernichten.

Mit der Aussetzung des Wehrdienstes haben ehemalige Wehrpflichtige um Aufklärung über die Aufbewahrungsdauer ihrer Musterungsakten gebeten. Für die Aufbewahrung der Musterungsakten gelten unterschiedliche Regelungen je nach Zeitpunkt der Musterung.

Für Wehrpflichtige, die vor dem 30. Juni 2011 gemustert wurden, richten sich die Aufbewahrungsfristen nach der Personalaktenverordnung Wehrpflichtige (WPersAV) vom 15. Oktober 1998. Diese Verordnung regelt Einzelheiten zum Personalaktenrecht der ungedienten Wehrpflichtigen. Sie gilt fort, weil der Wehrdienst zwar ausgesetzt, die Wehrpflicht aber nicht abgeschafft wurde. Folglich gilt weiterhin eine Wehrpflicht (§ 1 WPflG), die aber in Friedenszeiten keine praktischen Folgen mehr hat. Daher handelt es sich bei den Musterungsakten weiterhin um die Akten von Wehrpflichtigen, für deren Aufbewahrung die WPersAV gilt.

Nach § 4 WPersAV gelten folgende Fristen: Die Personalakte des (ungemusterten und gemusterten) Wehrpflichtigen ist so lange aufzubewahren, wie dies zur Erfüllung der Wehrpflicht erforderlich ist, längstens bis zum Ablauf des Jahres, in dem der Wehrpflichtige das 45. Lebensjahr vollendet. Im Falle der Wehrdienstunfähigkeit ist die Personalakte längstens bis zum Ablauf von fünf Jahren nach Eintritt der Wehrdienstausnahme aufzubewahren, § 4 Absatz 1 Satz 2 WPersAV. Abweichend hiervon sind die Gesundheitsunterlagen längstens bis zum Ablauf des Jahres aufzubewahren, in dem der Wehrpflichtige das 45. Lebensjahr vollendet, sofern nicht nach anderen Vorschriften eine längere Aufbewahrungsfrist vorgesehen ist. In Fällen der Wehrdienstunfähigkeit sind also spätestens mit Ablauf des Jahres, in dem das 45. Lebensjahr vollendet wurde, die Musterungsakten gemäß § 4 Absatz 3 Satz 3 WPersAV zu vernichten.

Für Personen (wehrpflichtige Männer und nicht wehrpflichtige Frauen), die nach dem 30. Juni 2011 für den Freiwilligen Wehrdienst untersucht wurden, finden die §§ 58, 59 WPflG Anwendung. Die erhobenen Daten sind zu löschen, wenn die Betroffenen dies verlangen, spätestens jedoch nach Ablauf eines Jahres nach ihrer erstmaligen Speicherung beim Bundesamt für Wehrverwaltung. Bei Nichttauglichkeit sind die bei der Untersuchung erhobenen Daten nach Ablauf eines Jahres nach der Untersuchung zu löschen. Im Fall der Tauglichkeit gelten für Wehrpflichtige bei Nichtantritt des Freiwilligen Wehrdienstes wiederum die Fristen der WPersAV.

14.2.5 Stärkung des Beauftragten für den Datenschutz in der Bundeswehr

Die Unabhängigkeit des Beauftragten für den Datenschutz in der Bundeswehr wurde endlich gestärkt.

Mit der Neuausrichtung der Bundeswehr ist auch eine Neustrukturierung des Bundesministeriums der Verteidigung verbunden, in deren Rahmen meine Empfehlungen zur unabhängigen Stellung des Beauftragten für den Datenschutz in der Bundeswehr (BfDBW) umgesetzt wurden. War der BfDBW vor der Reform in Zugleichfunktion Leiter des administrativen Datenschutzes, so gehört der administrative Datenschutz nach der Neustrukturierung nicht länger zum Aufgabenbereich des BfDBW, sondern bildet einen eigenen, in die ministerielle Hierarchie eingebundenen Fachstrang.

Der BfDBW kann sich nunmehr ohne die Gefahr von Interessenkonflikten völlig auf seine eigentlichen, originären Aufgaben als behördlicher Datenschutzbeauftragter (bDSB) konzentrieren. Damit ist er neutraler Ansprechpartner für Soldaten und Zivilbeschäftigte der Bundeswehr und in seiner Funktion als bDSB unmittelbar dem Minister unterstellt.

14.3 Versendung von Werbematerial an Jugendliche durch die Bundeswehr

Die Meldeämter übersenden dem Bundesamt für Wehrverwaltung jährlich Meldedaten zur Werbung Freiwilliger. Die Bundeswehr nutzt diese Meldedaten, um Informationsmaterial an junge Menschen zu versenden.

Mit dem Wehrrechtsänderungsgesetz 2011 (WehrRÄndG) wurde die allgemeine Wehrpflicht (vgl. Nr. 14.2) ausgesetzt. Die bis dahin geltende Regelung des § 58 des Wehrpflichtgesetzes (WPflG) verpflichtete die Meldeämter, die Namen und Adressen aller 17-jährigen Männer dem Kreiswehrersatzamt zu übermitteln, damit diese zur Musterung einbestellt werden konnten. Diese Musterungspflicht ist außerhalb des Spannungs- und Verteidigungsfalles entfallen. Nun wird die Ableistung eines freiwilligen Wehrdienstes mit einer Dauer von bis zu 23 Monaten für Männer und Frauen angeboten.

Die neue Fassung des § 58 Absatz 1 WPflG verpflichtet die Meldebehörden, dem Bundesamt für Wehrverwaltung jährlich Familienname, Vorname und Anschrift von deutschen Staatsangehörigen zu übermitteln, die im nächsten Jahr volljährig werden. Damit wird diesem die Möglichkeit eingeräumt, einem ausgewählten Empfängerkreis Informationsmaterial zuzusenden. Die Datenübermittlung unterbleibt, wenn die Betroffenen nach § 18 Absatz 7 des Melderechtsrahmengesetzes widersprochen haben.

Erstmalig erfolgte diese Meldung der Einwohnermeldeämter im Oktober 2011. Im Anschluss daran versandte die Bundeswehr ihre Informationsschreiben „Freiwilliger Wehrdienst oder Soldat auf Zeit“. In einigen Fällen führten diese Schreiben zu Unverständnis bei den Betroffen oder ihren Eltern, wie in Eingaben an meine Behörde zum Ausdruck kam. Die Ursachen hierfür waren unterschiedlicher Natur. Aufgrund der kurzfristigen Änderung der Rechtsgrundlage war vielen Bürgerinnen und Bürgern ihre Widerspruchsmöglichkeit nicht bekannt. In Einzelfällen handelte es sich auch um schlichte Übermittlungsfehler der Meldebehörden, die auch Daten von Kleinkindern ohne Angabe der Geburtsdaten übermittelten, sodass auch diesen von der Bundeswehr Informationsmaterial zugesandt wurde.

Die Bundeswehr darf zur Erfüllung ihres verfassungsmäßigen Auftrags die erhaltenen Meldedaten auf der Grundlage des § 58 WPflG nutzen, um Informationsmaterial zum Zwecke der Personalwerbung zu versenden. Die erhobenen Daten dürfen allerdings nur zu diesem Zweck verwendet werden. Sie sind zu löschen, wenn die Betroffenen dies verlangen, spätestens jedoch nach Ablauf eines Jahres nach der erstmaligen Speicherung der Daten beim Bundesamt für Wehrverwaltung.

Jugendlichen, die diese Werbung der Bundeswehr nicht erhalten möchten, empfehle ich daher, das ihnen eingeräumte Widerspruchsrecht gegenüber der Meldebehörde zu nutzen.

15 Aus meiner Dienststelle

15.1 Erfahrungsaustausch mit Datenschutzbeauftragten der Obersten Bundesbehörden

Ein regelmäßiger Erfahrungsaustausch ist ein unverzichtbares Element der Zusammenarbeit mit den behördlichen Datenschutzbeauftragten der Obersten Bundesbehörden.

Die bei den Dienststellen des Bundes bestellten Beauftragten für den Datenschutz haben eine wichtige Funktion bei der Verwirklichung des Datenschutzes. Sie sind quasi der Motor der datenschutzrechtlichen Entwicklung in ihrer Behörde. Zu ihren Aufgaben gehört neben der Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften die Beratung der Dienststellenleitung, die Schulung und Sensibilisierung der mit der Verarbeitung personenbezogener Daten betrauten Mitarbeiterinnen und Mitarbeiter sowie die Unterstützung von Betroffenen bei der Wahrnehmung ihrer Datenschutzrechte. Im Hinblick auf diese verantwortungsvolle Tätigkeit habe ich die behördlichen Datenschutzbeauftragten im Berichtszeitraum nicht nur in zahlreichen Einzelfällen beratend unterstützt, sondern ihnen im Rahmen des regelmäßig stattfindenden Erfahrungsaustausches mit den Datenschutzbeauftragten der Obersten Bundesbehörden auch wieder Gelegenheit gegeben, in der Praxis auftretende Datenschutzprobleme gemeinsam zu erörtern und Rechtsfragen vertieft zu diskutieren.

Beim Erfahrungsaustausch im Juli 2011 habe ich die Teilnehmer über aktuelle Entwicklungen im Datenschutz informiert, insbesondere über den Entwurf zur Regelung des Beschäftigtendatenschutzes und den Stand der Planungen zur Errichtung einer Stiftung Datenschutz. Einen breiten Raum nahm die gemeinsame Erörterung datenschutzrechtlicher Fragen aus dem Bereich des Personaldatenschutzes ein, die sich in der täglichen Praxis ergeben hatten. Weitere Themen waren die Auftragsdatenverarbeitung und die sich aus der Änderung des § 11 BDSG ergebenden praktischen Konsequenzen sowie die datenschutzgerechte Gestaltung von Internetangeboten. Hinweise und Empfehlungen zur IT-Sicherheit, u. a. zur Löschung von Daten bzw. Datenträgern standen ebenso auf der Tagesordnung wie eine Darstellung der rechtlichen Problematik der Schnittstelle zwischen dem Recht auf Informationszugang nach dem Informationsfreiheitsgesetz des Bundes und dem Schutz personenbezogener Daten.

Die Veranstaltung im Juli 2012 gab mir Gelegenheit, über den aktuellen Stand der Planungen zur Reform des europäischen Datenschutzrechtsrahmens und das vorgesehene Datenschutzpaket zu berichten. Die Tagesordnung sah auch einen Austausch der Erfahrungen der Datenschutzbeauftragten mit ihrer organisatorischen Stellung in den jeweiligen Dienststellen und ihren praktischen Arbeitsmöglichkeiten vor. Weitere Themen waren datenschutzrechtliche Fragen im Zusammenhang mit telefonischen oder schriftlichen Eingaben von Bürgerinnen und Bürgern, der Einsatz von Datenverarbeitungsprogrammen in Personalangelegenheiten oder bei der Beihilfebearbeitung, Datenschutz im Rahmen von Telearbeit sowie einzelne Probleme aus dem IT-Bereich. Auch Fragen zum Internetauftritt (Einbindung des Facebook-Like-Buttons, Einsatz von Webanalyseprogrammen) wurden behandelt. Schließlich habe ich die Teilnehmer auch über das Ergebnis der durchgeführten Umfrage zum Einsatz von Videoüberwachungstechnik in Bundesbehörden (vgl. Nr. 3.3.1) informiert.

15.2 Teilnahme an Datenschutzgremien

Mit meinen Kolleginnen und Kollegen arbeite ich auf nationaler, europäischer und internationaler Ebene eng zusammen.

In folgenden Datenschutzgremien war ich im Berichtszeitraum regelmäßig vertreten:

Nationale Ebene

Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit

- Arbeitskreis Grundsatzfragen
  - Unterarbeitsgruppe Auftragsdatenverarbeitung/ Outsourcing
  - Unterarbeitsgruppe Geodaten
- Arbeitskreis Verwaltungsmodernisierung
- Arbeitskreis Steuerverwaltung
- Arbeitskreis Personalwesen
- Arbeitskreis Gesundheit und Soziales
  - Unterarbeitsgruppe „Elektronische Gesundheitskarte“
- Arbeitskreis Wissenschaft
- Arbeitskreis Statistik
- Ad-hoc Arbeitsgruppe Zensus 2011
- Arbeitskreis Verkehr
- Arbeitskreis Datenschutz und Bildung
- Arbeitskreis Justiz
- Arbeitskreis Sicherheit
  - Unterarbeitsgruppe INPOL
  - Unterarbeitsgruppe Europa
- Arbeitskreis Technik

– Arbeitskreis Medien
– Arbeitskreis Europa
– Ad-hoc Arbeitsgruppe Smart Meter

Düsseldorfer Kreis mit

– Arbeitsgruppe Auskunfteien
– Arbeitsgruppe Kreditwirtschaft
– Arbeitsgruppe Versicherungswirtschaft
– Arbeitsgruppe Internationaler Datenverkehr
– ad-hoc-Arbeitsgruppe Werbung und Adresshandel
– Workshop der Aufsichtsbehörden

Neu eingerichtet wurde gegen Ende des Berichtszeitraums noch die ad-hoc-Arbeitsgruppe Videoüberwachung, an der ich auch teilnehmen werde.

Weitere Gremien

Beirat bei der Arbeitsgemeinschaft für Datentransparenz nach § 303b SGB V

NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA) mit

– NA 043-01-27-05 AK Arbeitskreis Identitätsmanagement und Datenschutz-Technologien
– NA 043-01-37 AA Arbeitsausschuss Biometrie
– NA 043-01-17 AA Arbeitsausschuss Karten und persönliche Identifikation
– NA 043-01-51 AA Arbeitsausschuss Vernichten von Datenträgern

Arbeitskreis Identitätsmanagement und Datenschutz-Technologien beim DIN

Koordinierungsstelle IT-Sicherheit (KITS) Fachbeirat beim DIN

Teletrust Arbeitsgruppe 3 Biometrie

(CAST) Competence Center for Applied Security Technology e. V.

Beirat der gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH)

IT-Sicherheitsmanagement im Geschäftsbereich des Bundesministeriums des Innern

IT-Rat der Bundesregierung mit

– IT-Sicherheitsmanagement der Ressorts (Unterarbeitsgruppe IT-Rat)
– Netz des Bundes (Unterarbeitsgruppe IT-Rat)

Arbeitsgruppe 4 des IT-Gipfels: Vertrauen, Datenschutz und Sicherheit im Internet mit

– Unterarbeitsgruppe 1 IT-Gipfel: Cloud Computing
– Unterarbeitsgruppe 2 IT-Gipfel: Anforderungen an Sichere Identitäten
– Unterarbeitsgruppe 4 IT-Gipfel: Mobile Sicherheit

IT-Planungsrat

Jour Fixe Telekommunikation

VIS-Anwendergruppe

Projektpartner Virtuelles Datenschutzbüro

Treffen der Presseverantwortlichen der Dienststellen des Bundes- und der Landesbeauftragten bzw. der Aufsichtsbehörden für den Datenschutz

Europäische Ebene

Europäische Datenschutzkonferenz

Artikel-29-Datenschutzgruppe mit

– Subgroup Financial Matters
– Subgroup Biometrics & eGovernment
– Health Data Subgroup
– BTLE Subgroup
– Technology Subgroup
– Future of Privacy Subgroup
– Key Provisions Subgroup
– Working Group International Transfers
– WADA-Subgroup

Weitere Gremien

Gemeinsame Kontrollinstanz Europol

Gemeinsame Kontrollinstanz Schengen

Gemeinsame Kontrollinstanz Zoll

Kontroll- und Koordinierungsgruppe des Zollinformationssystems (ZIS)

Case Handling Workshop

Europarat (sog. T-PD-Gruppe)

Eurodac-Koordinierungsgruppe

VIS-Koordinierungsgruppe

Internationale Ebene

Internationale Datenschutzkonferenz mit

– International Working Group Enforcement Coordination
– International Working Group on Data Protection in Telecommunications (IWGDPT bzw. „Berlin Group")

Weitere Gremien

OECD Working Party on Information Security and Privacy – WPISP

Global Privacy Enforcement Network (GPEN)

Accountability Project

15.3 Neues Design für meine Öffentlichkeitsarbeit

Im Berichtzeitraum habe ich die Öffentlichkeitsarbeit weiter intensiviert. Das Design der Faltblätter und Broschüren wurde überarbeitet und der Relaunch meines Internetauftritts eingeleitet.

Inzwischen habe ich zahlreiche Broschüren und Faltblätter publiziert. Die „Info-Reihe“ richtet sich hauptsächlich an Fachleute und solche Personen, die sich vertieft in die Materie einarbeiten wollen oder die Informationen als Nachschlagewerk und Ergänzung zu den gesetzlichen Vorschriften nutzen. Anhand der Bestellzahlen gehe ich davon aus, dass die „Infos“ u. a. auf vielen Schreibtischen behördlicher und betrieblicher Datenschutzbeauftragter liegen. Meine Publikationen richten sich aber nicht nur an ein Fachpublikum. Gerade für Bürgerinnen und Bürger aller Altersschichten ist es wichtig, kurze und klare Handreichungen zum Datenschutz zu erhalten. An sie richten sich insbesondere meine Faltblätter. Das Spektrum reicht von Grundlagen des Datenschutzes und der Informationsfreiheit über Tipps für den sicheren Umgang mit elektronischen Medien bis hin zu wertvollen Informationen zu Adresshandel und unerwünschter Werbung. Das Informationsangebot werde ich auch in den kommenden Jahren aktualisieren und weiter ausbauen.

Neben den Inhalten kommt es auch auf die Darstellung in der Öffentlichkeit an. Deshalb wurden die Faltblätter und Broschüren graphisch ansprechender gestaltet. Inzwischen sind alle meine Publikationen im einheitlichen (neuen) Design. Um den Wiedererkennungswert zu steigern, wird ein eigenes Logo verwendet (vgl. Kasten zu Nr. 15.3), das nun neben dem Corporate Design der Bundesregierung auf meinen Druckwerken angebracht ist.

Eine gute Möglichkeit, Informationsmaterial der Öffentlichkeit zur Verfügung zu stellen und über meine Aufgaben zu informieren, ist die Teilnahme an öffentlichen Veranstaltungen. So habe ich an den jährlich stattfindenden Tagen der offenen Tür der Bundesregierung in Berlin teilgenommen und die Möglichkeit genutzt, mit einem Informationsstand an den Feierlichkeiten zum Tag der Deutschen Einheit und NRW-Tag in Bonn für Datenschutz und Informationsfreiheit zu werben. An den jeweils zweitägigen Veranstaltungen haben sich viele Bürgerinnen und Bürger bei meinen Mitarbeiterinnen und Mitarbeitern ausführlich informiert, diskutiert und ihr Datenschutzwissen in einem Quiz getestet.

Ebenfalls etabliert haben sich die Informationsveranstaltungen für politisch Interessierte aus den Wahlkreisen der Abgeordneten des Deutschen Bundestags. Rund vierzig Gruppen mit jeweils 50 Teilnehmern haben sich in diesem Berichtszeitraum für Datenschutzthemen interessiert. Auch Schüler, Studenten und kirchliche oder gewerkschaftliche Einrichtungen fragen vermehrt nach, wie sie sich bei mir über die neuesten Entwicklungen im Datenschutz und der Informationsfreiheit informieren können. Gerne stehen meine Mitarbeiterinnen und Mitarbeiter im Rahmen der Möglichkeiten nach vorheriger Anmeldung für diese Diskussionsrunden zur Verfügung.

Die Öffentlichkeitsarbeit wird durch eine aktive Pressearbeit ergänzt. Die Vertreterinnen und Vertreter der Medien sollen zügig mit adressatengerechten und qualitativ hochwertigen Informationen versorgt werden. Dazu dienen Pressemitteilungen, Pressekonferenzen und Interviews. Prägnante Pressethemen im Berichtszeitraum waren die Reform des Melderechts und der Einsatz des so genannten Staatstrojaners.

Ein weiterer wesentlicher Bestandteil der Öffentlichkeitsarbeit ist mein Internetauftritt. Auch in diesem Berichtzeitraum war ein erfreulich hoher Abruf der Inhalte meiner Website zu verzeichnen. Über zehneinhalbmillionen Mal wurde der Internetauftritt aufgerufen. Neben den Pressemitteilungen interessieren sich die Nutzerinnen und Nutzer am meisten für die Informationsmaterialien sowie die Reden und Interviews. Thematisch informieren sich die Besucherinnen und Besucher meiner Website am häufigsten über die grundlegenden Dinge des Datenschutzes sowie den Datenschutz bei der Arbeit und der Telekommunikation. Seit dreieinhalb Jahren diskutieren viele Fachleute und interessierte Bürgerinnen und Bürger in dem von mir bereitgestellten interaktiven Datenschutzforum intensiv Themen rund um den Datenschutz und die Informationsfreiheit. Hier sind ebenfalls steigende Nutzerzahlen festzustellen. So ist die Zahl der Beiträge im Berichtszeitraum um mehr als vierzehntausend angestiegen. Ferner sind fast zweitausend Neuregistrierungen zu verzeichnen gewesen, so dass das Forum nun mehr als viertausend registrierte Nutzerinnen und Nutzer zählt. Um mein Internetangebot noch besser nutzbar zu gestalten, habe ich eine Projektgruppe eingerichtet, die den Internetauftritt überarbeitet. Der Relaunch wird voraussichtlich zum Ende des 1. Halbjahrs 2013 abgeschlossen sein.

Kasten zu Nr. 15.3

Logo

15.4 Besuche ausländischer Delegationen

Verschiedene Datenschutzexperten, insbesondere aus Asien und Osteuropa, haben meine Dienststelle besucht, um aktuelle Fragen des Datenschutzes zu diskutieren und Erfahrungen auszutauschen.

Im Berichtszeitraum habe ich mehrere ausländische Delegationen in meiner Dienststelle empfangen. Bereits seit einigen Jahren existiert ein regelmäßiger Erfahrungsaustausch mit Datenschutzexperten aus Japan. So informierten sich Experten des Nomura-Research-Instituts und Professoren verschiedener japanischer Universitäten über das Konzept des Datenschutzes in Deutschland und die nationalen Erfahrungen mit dem Europäischen Recht. Mit einer Delegation des Justizministeriums der Republik China (Taiwan) wurden praxisrelevante Fragen besprochen, etwa zur Wahrnehmung der Datenschutzaufsicht in Deutschland oder zur Einwilligungserklärung der Betroffenen in die Datenverarbeitung im Internet.

Zur Unterstützung von Datenschutzbehörden in den Kandidatenländern der EU sowie im Rahmen der Europäischen Nachbarschaftspolitik (ENPI) haben Mitarbeiter meiner Dienststelle an Veranstaltungen mitgewirkt, die als Teil des Informationsaustausches und der technischen Verwaltungshilfe – dem sog. TAIEX-Programm – von der Europäischen Kommission organisiert wurden. Auf Anfrage der Europäischen Kommission habe ich zudem Delegationen der Datenschutzbehörden aus Kroatien, der Republik Moldau sowie der Republik Mazedonien (FYROM – Former Yugoslav Republic of Macedonia) sowohl in meiner Dienststelle in Bonn als auch in meinem Verbindungsbüro in Berlin empfangen, um diese nicht nur über den Datenschutz in Deutschland zu unterrichten, sondern auch um mit ihnen beiderseits aktuelle datenschutzrechtliche Fragen zu diskutieren. Dem Erfahrungsaustausch diente auch der einwöchige Besuch einer Gruppe von Angehörigen der bulgarischen Datenschutzbehörde im Rahmen des Leonardo-da-Vinci-Programmes der EU.

Es bleibt mir ein wichtiges Anliegen, den Aufbau neuer Datenschutzbehörden im Ausland mit den in Deutschland gewonnenen Erfahrungen zu unterstützen und dabei im Dialog mit den ausländischen Partnern auch selbst neue Einsichten zu gewinnen.

15.5 Personal

In den vergangenen Jahren bewegte sich der Aufgaben- und Arbeitsanfall auf einem hohen Niveau. Pro Monat haben sich im Berichtszeitraum durchschnittlich 408 Bürgerinnen und Bürger mit Ihren Beschwerden und Fragen rund um den Datenschutz an mich gewandt – gegenüber der Vorperiode bedeutet dies ein Rückgang von 5 Prozent.

Nachdem ich im Haushaltsjahr 2010 bereits über neue Stellen verfügen konnte, erhielt meine Dienststelle in 2012 zehn weitere Stellen, ganz überwiegend für das neue Aufgabengebiet SGB II. Dadurch konnte das Personalsoll von 77,5 Stellen im Jahr 2010 auf 86,5 Stellen in 2012 erhöht werden.

Durch das zusätzliche Personal kann meine Dienststelle ihre gesetzlichen Aufgaben besser bewältigen und neue Aufgaben in Angriff nehmen. Der Stellenzuwachs machte es zudem möglich, die Organisation meiner Dienststelle endlich an aktuelle Entwicklungen anzupassen und mir zugewiesene neue Aufgabengebiete besser abzudecken. Gleichwohl ist die Arbeitsbelastung immer noch extrem hoch, insbesondere auch durch notwendige Mitarbeit bei der Rechtsetzung im nationalen und europäischen Rahmen und durch gestiegene Anforderungen bei der Beratung der öffentlichen Stellen des Bundes.

15.6 Meine Präsenz in Berlin

Das 2008 in der Friedrichstraße 50 in Berlin-Mitte eingerichtete Verbindungsbüro koordiniert die Termine in Berlin, insbesondere an den Ausschusssitzungen des Deutschen Bundestages und Besprechungen der Bundesressorts in Berlin nehmen häufig Mitarbeiter des Verbindungsbüros teil. Es ist mit 15 Mitarbeiterinnen bzw. Mitarbeitern besetzt, wobei jedes Referat meiner Dienststelle mit mindestens einem Mitarbeiter vertreten ist.

Das Verbindungsbüro hat sich hervorragend bewährt. Seit Inbetriebnahme konnten vermehrt die Termine in Berlin von Mitarbeitern des Verbindungsbüros wahrgenommen werden, wodurch eine wirkungsvollere und direktere Teilnahme am politischen Geschehen in der Bundeshauptstadt erreicht wurde. Der Dienstreiseaufwand meiner Bonner Dienststelle konnte so deutlich verringert werden.

15.7 Forschung braucht Datenschutz, Datenschutz braucht Forschung!

Forschungsaufträge für den Datenschutz und die Informationsfreiheit führten zu wertvollen neuen Erkenntnissen.

In den Jahren 2011 und 2012 standen mir jeweils 90 000 Euro für Forschungszwecke zur Verfügung. Hiervon konnten folgende Gutachten und Forschungsaufträge finanziert werden:

– **Informationsfreiheitsgesetz und der Schutz der Betriebs- und Geschäftsgeheimnisse**

  Bereits 2010 wurde das Forschungsprojekt mit dem Ziel, Zweck und Reichweite des Schutzes von Betriebs- und Geschäftsgeheimnissen in den verschiedenen Rechtsgebieten zu erarbeiten und einen praktischen Ansatz zur Lösung von Konflikten mit dem Anspruch auf Informationsfreiheit in Auftrag gegeben. 2011 erfolgte eine Erweiterung des Forschungsauftrages. Das Forschungsprojekt konnte 2012 erfolgreich abgeschlossen werden. Das Gutachten ist auf meiner Internetseite unter www.informationsfreiheit.bund.de abrufbar.

– **Automatisierte Auswertung von Protokolldaten**

  Bei diesem Forschungsprojekt sollte ein System entwickelt werden, mit dem automatisiert unautorisierte Zugriffe auf Datenbanken erkannt werden können.

Dabei sollten die Ausgangslage erfasst und die Anforderungen an ein solches System definiert werden. Zu Beginn wurde nach bestehenden Tools recherchiert, die diesen Anforderungen genügen. Das Forschungsprojekt konnte 2012 abgeschlossen werden. Zwar gibt es derzeit entsprechende Tools auf dem Markt, von denen erfüllt aber keins die Anforderungen vollständig.

– **Anpassung des Tools zur automatisierten Auswertung von Protokolldaten**

  Dieses Forschungsprojekt setzt auf das vorausgegangene auf. Wurden dort Anforderungen an ein Tool zur automatisierten Auswertung von Protokolldaten definiert, so geht es jetzt um bedarfsgerechte Weiterentwicklung. Ein auf dem Markt existierendes Produkt erfüllt die gestellten Analyse- und Auswerteanforderungen zum großen Teil und erlaubt es auch, bedarfsorientierte Anpassungen und Erweiterungen vornehmen zu können.

  Die Implementierung von Plugins, um zusätzlichen Protokolldatenformate analysieren zu können, sowie die Erweiterung und Anpassung der Analysefunktionen und Implementierung dieser neuen Plugins in die ausgewählte Software wird im nun vergebenen Auftrag vorgenommen. Ebenfalls werden Schulungsunterlagen für die Software erstellt, um späteren Nutzern eine Einarbeitung zu erleichtern.

Die in 2010 angestoßenen Forschungsprojekte zur „Erstellung eines Leitfadens zur Evaluation von Gesetzen“ und „PRIVIDOR – PRIvacy Violation DetectOR“ konnten erfolgreich abgeschlossen werden (vgl. 23. TB Nr. 14.6).

15.8 BfDI als Ausbildungsbehörde

Referendare, Praktikanten und Anwärter zeigen Interesse am Datenschutz.

Das Interesse an Praktikumsaufenthalten in meiner Dienststelle ist auch 2011 und 2012 groß geblieben. Insbesondere Studierenden der Rechtswissenschaften und Rechtsreferendaren, die sich für Fragen des Datenschutzes und der Informationsfreiheit interessierten und praktische Kenntnisse erwerben wollten, habe ich einen Einblick in die Aufgaben und Arbeitsweise einer Datenschutzbehörde gewährt.

Insgesamt haben im Berichtszeitraum 18 Studierende und Referendare Teile ihrer Ausbildung in meinem Hause absolviert. Darüber hinaus konnte ich vier Anwärtern des gehobenen Verwaltungsdienstes die Möglichkeit bieten, ihr Pflichtpraktikum in meiner Dienststelle abzuleisten.

15.9 Gesund im Job – der BfDI als Pilotbehörde

Die Ergebnisse der Untersuchung sollen in ein betriebliches Gesundheitsmanagement einfließen.

Der Gesundheitsbericht der Bundesregierung 2012 zeigte beim Gesundheitsmanagement im öffentlichen Dienst Handlungsbedarf. Dies nahm ich in Zusammenarbeit mit dem Bundesministerium des Inneren zum Anlass, in meiner Dienststelle zu untersuchen, welche Verbesserungsmöglichkeiten es zur Gesunderhaltung meiner Mitarbeiterinnen und Mitarbeiter gibt. Die sich daraus ergebenden Lösungsvorschläge sollen anschließend in ein betriebliches Gesundheitsmanagement einfließen. Damit geht meine Dienststelle als Pilotbehörde mit gutem Beispiel voran.

Beginnend im April 2012 wurden daher in verschiedenen Arbeitsgruppen Ideen und Lösungsvorschläge für ein verbessertes Gesundheitsmanagement erarbeitet. Ergebnisse gab es in unterschiedlichsten Bereichen, wie z. B. bei der Ergonomie, Arbeitssicherheit und IT-Ausstattung. Einige Ergebnisse, wie Headsets für Mitarbeiter, die viel telefonieren müssen, konnten sofort umgesetzt werden. Andere werden als regelmäßige Angebote in den nächsten Jahren in den Arbeitsalltag einfließen.

16 Wichtiges aus zurückliegenden Tätigkeitsberichten

1. 23. TB Nr. 2.3 **Sie haben Post – Ablauf der Altregelung zur Nutzung personenbezogener Daten zu Werbezwecken**

   Mit dem Inkrafttreten der Neuregelungen für den werblichen Umgang mit personenbezogenen Daten am 1. September 2009 wurde – jedenfalls dem Grundsatz nach – festgelegt, dass personenbezogene Daten nur mit Einwilligung des Betroffenen zu Zwecken der Werbung und des Adresshandels verarbeitet und weitergegeben werden dürfen. Leider gibt es viele Ausnahmen. Jedoch gestaltet sich die Datenverarbeitung im Bereich des so genannten Listenprivilegs, das für die Nutzung bestimmter Daten wie Name, Anschrift und Geburtsjahr nach wie vor nur ein Widerspruchsrecht vorsieht, mittlerweile transparenter. Der Betroffene muss nun bei der werblichen Ansprache darüber informiert werden, welche Stelle bei der Werbung für fremde Angebote für die Nutzung der Daten verantwortlich ist bzw. wer die Daten im Fall einer Weitergabe erstmals erhoben hat.

   Für die Umstellung auf die neue Rechtslage hatte der Gesetzgeber der Werbewirtschaft eine Übergangsfrist von drei Jahren eingeräumt. Für Daten, die vor dem 1. September 2009 erhoben wurden, galt daher die alte Rechtslage zunächst fort. Seit dem 31. August 2012 unterliegen nun auch diese Altdaten der neuen Regelung.

   Den Neuregelungen merkt man an, dass das Gesetz in der letzten Legislaturperiode im Eilverfahren verabschiedet und bis zuletzt immer wieder geändert und ergänzt wurde. Sie sind für den Bürger schwer verständlich und in der Praxis mit zahlreichen Auslegungsschwierigkeiten verbunden.

   Die Aufsichtsbehörden haben deshalb in der Ad-hoc-Arbeitsgruppe „Werbung und Adresshandel“ des Düsseldorfer Kreises unter Leitung des Bayerischen Landesamts für Datenschutzaufsicht praktische Anwendungshinweise erarbeitet, die den Unternehmen

und den Verbraucherinnen und Verbrauchern in wichtigen Auslegungsfragen Rechtssicherheit beim Umgang mit personenbezogenen Daten vermitteln. Die Anwendungshinweise sind im Internet abrufbar unter www.lda.bayern.de.

2. 23. TB Nr. 3.6 **Kein Überflieger: ELSTER-Online**

   Über das ELSTER-Online-Portal kann der Steuerpflichtige elektronisch Dokumente wie beispielsweise seine Steuererklärung an die Finanzverwaltung übermitteln. Dabei handelt es sich um besonders sensible Daten, die dem Steuergeheimnis nach § 30 Abgabenordnung (AO) unterliegen. Die Möglichkeiten der elektronischen Kommunikation bestimmen sich nach § 87a AO. Neben der qualifizierten elektronischen Signatur ist nunmehr auch ein anderes sicheres Verfahren zugelassen, das ursprünglich bis zum 31. Dezember 2012 befristet war. Die Befristung und auch die Verpflichtung zur Evaluierung für das andere sichere Verfahren (ELSTER-Online-Verfahren) wurden nach Abschluss der Evaluierung des ELSTER-Online-Verfahrens aufgehoben, da es sich als sicher und zuverlässig erwiesen habe (vgl. Bundestagsdrucksache 17/5125 S. 49). Gesetzlich wurde klargestellt, dass das andere sichere Verfahren den Datenübermittler zu authentifizieren hat und die Integrität des elektronisch übermittelten Datensatzes gewährleisten muss (§ 87a Absatz 6 Satz 1 AO).

   Ich halte dies für unbefriedigend, denn die Gleichstellung des „anderen sicheren Verfahrens“ mit der qualifizierten elektronischen Signatur berücksichtigt nicht die unterschiedlichen Sicherheitsstandards der Verfahren und führt letztlich zu einer Absenkung des Datenschutzniveaus. Die Hinnahme einer möglichen unsicheren elektronischen Kommunikation ist angesichts des hohen Schutzanspruches des Steuergeheimnisses nach § 30 AO nicht akzeptabel. Ich werde darauf drängen, dass diesem Schutzanspruch entsprechend Rechnung getragen wird.

3. 23. TB Nr. 11.5.2 **Reform von „Hartz IV“ – Bildungsgutscheine und Datenschutz**

   Mit dem Urteil des Bundesverfassungsgerichts vom 9. Februar 2010 zu den Hartz IV-Regelsätzen (1 BvL 1/09, 1 BvL 3/09, 1 BvL 4/09) war dem Gesetzgeber aufgegeben worden, für den Bedarf von Kindern und Jugendlichen künftig besondere Leistungen vorzusehen. Das entsprechende Gesetzgebungsverfahren war seinerzeit noch nicht abgeschlossen. Inzwischen ist das Gesetz vom 24. März 2011 (BGBl. I S. 453) rückwirkend zum 1. Januar 2011 in Kraft getreten.

   Im Gesetzgebungsverfahren wurde § 29 SGB II gegenüber dem Referentenentwurf, auf den sich meine Ausführungen im 23. TB bezogen hatten, noch einmal modifiziert und die Leistungserbringung für Bildung und Teilhabe wurde nach § 28 SGB II vollständig auf den kommunalen Träger übertragen. Insbesondere wurden personalisierte Gutscheine, bis dahin eine Unterform der Sachleistungen, als neue Leistungsform in das SGB II und das SGB XII eingeführt. Meine Forderung, als Alternative zu personalisierten Gutscheinen dem Leistungsberechtigten auch die Möglichkeit zur direkten Zahlung an den Anbieter einzuräumen, wurde zwar dem Grundsatz nach berücksichtigt. Jedoch bestimmt der kommunale Träger und nicht der Leistungsberechtigte die Form der Leistungserbringung. Damit wird in bestimmten Fallkonstellationen eine Bekanntgabe von Sozialdaten gegenüber Dritten in Kauf genommen. Ich bedauere, dass die Gutscheinlösung nicht durchgängig neutral gestaltet wurde.

4. 23. TB Nr. 11.5.4 **Übermittlung von Sozialdaten an potentielle Arbeitgeber**

   Ich hatte darüber berichtet, dass Bewerber trotz einer anonymen Veröffentlichung ihres Stellengesuchs in der JOBBÖRSE der BA Anrufe von potentiellen Arbeitgebern (Zeitarbeitsfirmen) erhalten hatten. Wie sich herausstellte, konnten die Firmen, die über einen Arbeitgeber-Account in der JOBBÖRSE verfügen, bei einem Vermittlungsvorschlag auch die bei der BA freiwillig angegebenen Kontaktdaten wie E-Mail-Adresse und Telefonnummer der Bewerber einsehen. Die BA hat mir daraufhin zugesichert, das System so zu ändern, dass die Kontaktdaten nur noch bei einer entsprechenden Einwilligung des Bewerbers für die Arbeitgeber sichtbar sind.

   Ich begrüße die im April 2012 erfolgte Umsetzung durch eine technische Änderung. Seit diesem Zeitpunkt sind die freiwillig angegebenen Kontaktdaten von Bewerbern nun auch im Vermittlungsprozess für potentielle Arbeitgeber mit eigenem Arbeitgeber-Account nicht mehr ohne Einwilligung einsehbar. Bei einer Kontrolle vor Ort in einer Agentur für Arbeit konnte ich mich davon überzeugen, dass die Erfassung der Kontaktdaten für eine externe Kommunikation tatsächlich nur nach vorheriger ausdrücklicher Einwilligung des Bewerbers erfolgt.

5. 21. TB Nr. 6.7 **Novellierung der Prozesskostenhilfe**

   In meinem 21. TB hatte ich über einen Bundesratsentwurf zur Novellierung der Prozesskostenhilfe berichtet. Da das Gesetzgebungsverfahren in der 16. Legislaturperiode nicht abgeschlossen werden konnte, brachte der Bundesrat den Entwurf Anfang 2010 erneut ein. Zentrales Anliegen war die Reduzierung der Ausgaben für die Prozesskostenhilfe. Der Entwurf sah umfangreiche Auskunftsrechte des Gerichts über den Antragsteller (z. B. bei Finanzämtern, Arbeitgebern und Sozialleistungsträgern) vor. Voraussetzung sollte zwar eine Einwilligung des Antragstellers sein, der Antrag sollte jedoch allein aufgrund einer fehlenden Einwilligung abgelehnt werden können. Dies sah ich nach wie vor kritisch, da der Antragsteller mangels Freiwilligkeit i. S. v. § 4a BDSG faktisch zur Einwilligung genötigt worden wäre (vgl. 21. TB Nr. 6.7). Auch die Bundesregierung griff diese Bedenken in ihrer Stellungnahme zum 21. TB teilweise auf.

Auf meinen Vorschlag hin wurden in dem vom Bundesjustizministerium im März 2012 vorgelegten Gesetzentwurf nicht nur der Ablehnungsgrund, sondern auch die pauschale Abfrage der Einwilligung bei Antragstellung ersatzlos gestrichen. Das Gericht muss im Einzelfall prüfen, ob die Auskunft eines Dritten zur Prüfung der wirtschaftlichen Verhältnisse des Antragstellers erforderlich ist und dann ggf. die Einwilligung beim Antragsteller anfordern. Wird diese nicht erteilt, darf das Gericht die Prozesskostenhilfe nicht pauschal ablehnen, sondern muss die Umstände des Einzelfalles berücksichtigen. In der Begründung wird zudem klargestellt, dass die Anforderung von Belegen beim Antragsteller Vorrang vor der Auskunftseinholung bei Dritten hat. Auf diese Weise wird dem Grundsatz der Direkterhebung Rechnung getragen. Das Gesetzgebungsverfahren war bei Redaktionsschluss noch nicht abgeschlossen.

6. 23. TB Nr. 9.3 **Einführung der elektronischen Lohnsteuerkarte**

Die Einführung der elektronischen Lohnsteuerkarte verläuft alles andere als reibungslos. Bereits der Starttermin hat sich aufgrund technischer Probleme um ein Jahr verzögert, erst zum 1. Januar 2013 ist es zur beabsichtigten Umstellung von der Papierlohnsteuerkarte auf das elektronische Verfahren gekommen.

Zu technischen Problemen kam es bei der Übermittlung nach § 39e Absatz 2 Satz 2 Einkommensteuergesetz (EStG) von bislang bei den Meldebehörden als örtlichen Landesfinanzbehörden gespeicherten steuerlich relevanten Daten an das BZSt, die dieses zum Aufbau der ELStAM-Datenbank benötigt. So wurden personenbezogene Daten von Steuerpflichtigen (Angaben zu Familienangehörigen und zur Religionszugehörigkeit) nicht richtig zusammengeführt, da u. a. Daten aus dem Jahre 2010 zugrunde gelegt wurden, die in zahlreichen Fällen nicht mehr aktuell waren. Deswegen habe ich das Bundesministerium der Finanzen (BMF) um Aufklärung sowie Behebung der aufgetretenen Fehler gebeten. Es ist sicherzustellen, dass die übermittelten personenbezogenen Daten richtig zugeordnet und die elektronischen Lohnsteuerabzugsmerkmale korrekt gebildet werden. Das BMF hat mir Maßnahmen zur Verbesserung der Datenqualität zugesagt. Insbesondere soll dabei das BZSt mit der jeweils zuständigen Meldebehörde Kontakt aufnehmen, um eine Korrektur der konkret betroffenen Daten zu gewährleisten.

Die vom BMF zugesicherte Ausarbeitung eines IT-verfahrensspezifischen Sicherheitskonzepts, die ich bereits im 23. TB (Nr. 9.3) angemahnt hatte, steht immer noch aus. Ich erwarte jetzt eine zügige Umsetzung dieses Vorhabens und werde das Verfahren weiterhin kritisch begleiten, um einen besseren Schutz der in der zentralen Steuerdatenbank gespeicherten sensiblen Lohnsteuerdaten durchzusetzen.

7. 23. TB Nr. 9.4 **Verankerung des Auskunftsrechts in der Abgabenordnung**

Die von den Datenschutzbeauftragten des Bundes und der Länder bereits seit Jahrzehnten erhobene Forderung auch gegenüber der Steuerverwaltung in der Abgabenordnung (AO) ein datenschutzrechtliches Auskunftsrecht des Betroffenen festzuschreiben, blieb auch im Berichtszeitraum unerfüllt. Damit verweigert sich die Finanzverwaltung hartnäckig der Notwendigkeit, die Rechtsprechung des Bundesverfassungsgerichts umsetzt (BVerfG, Beschluss vom 10. März 2008, 1 BvR 2388/03) für ihren Bereich umzusetzen. Dabei hatte der Deutsche Bundestag bereits vor Jahren, in seinen Entschließungen zu meinem 20. und 21. Tätigkeitsbericht (Bundestagsdrucksache 16/12271, Nr. 5; Bundestagsdrucksache 16/4882, Nr. 10) die Bundesregierung aufgefordert, die AO um einen entsprechenden Anspruch zu erweitern. Das BMF hatte in dieser Legislaturperiode zwar einen entsprechenden Entwurf eingebracht, doch dieser ist liegen geblieben und wird – soweit ersichtlich – auch nicht mehr aktiv verfolgt. Eine Umsetzung des Auskunftsrechts in der AO würde auch die Entwicklung im Bereich des Informationsfreiheitsrechts des Bundes und der Länder nachvollziehen (vgl. Bundesverwaltungsgericht, Beschluss vom 14. Mai 2012, 7 B 53.11). Es besteht also nach wie vor erheblicher gesetzgeberischer Handlungsbedarf.

8. 22. TB Nr. 10.2.4 und 23. TB Nr. 15.7 **Verstöße von Krankenkassen bei der Vermittlung privater Zusatzversicherungen**

Aufgrund der außergewöhnlich schweren datenschutzrechtlichen Verstöße zweier gesetzlicher Krankenkassen bei der Kooperation mit jeweils einer privaten Krankenversicherung bei der Vermittlung privater Zusatzversicherungen 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 einer mit ihnen verbundenen privaten Krankenversicherung Zugang zu zum Teil sehr sensiblen Daten ihrer Versicherten verschafft. In beiden Fällen haben die Staatsanwaltschaften die Verfahren nach teilweise mehr als fünfjähriger Verfahrendauer trotz meiner Einsprüche eingestellt. Die Begründungen der Staatsanwaltschaften waren zum Teil abenteuerlich.

9. 23. TB Nr. 11.1.8 **Anbindung medizinischer Subsysteme an ein Klinikinformationssystem**

Im Rahmen meiner datenschutzrechtlichen Beratung der DRV Bund bei der geplanten Anbindung medizinisch-technischer Subsysteme an das eigene Klinikinformationssystem KLInet habe ich mich bei einem weiteren Beratungsbesuch in einem Reha-Zentrum der DRV Bund von den zwischenzeitlich getroffenen

Datenschutz- und Datensicherheitsmaßnahmen überzeugt. Dabei habe ich weiteren Handlungsbedarf aufgezeigt und erneut konkrete datenschutzrechtliche Verbesserungshinweise und Empfehlungen gegeben. Diese betrafen sowohl den aktuellen Umgang mit personenbezogenen Daten und die Nutzung der verschiedenen medizinisch-technischen Geräte im besuchten Reha-Zentrum als auch grundsätzlich den künftigen Einsatz solcher medizinischer Subsysteme und deren Vernetzung mit KLInet. Meine weitere beratende Beteiligung ist sichergestellt.

10. 23. TB Nr. 11.1.5 **Verfahren zur Erhebung von Zusatzbeiträgen und Datenerhebung zum Sozialausgleich – das GKV-Finanzierungsgesetz**

    Ich hatte über die mit dem GKV-Finanzierungsgesetz den Krankenkassen neu auferlegte Aufgabe berichtet, den Sozialausgleich durchzuführen. Meine Kritik zielte darauf, dass hierdurch der Arbeitgeber Kenntnis davon erlangt, wenn ein Beschäftigter über weitere beitragspflichtige Einnahmen verfügt, obwohl dieser unter Umständen ein Interesse an der Geheimhaltung dieser Information hat. Meine Bedenken haben sich in der Praxis bestätigt. So haben mich einige Beschwerden von betroffenen Arbeitnehmern erreicht. Diese berichteten mir u. a., die Rückmeldungen der Krankenkassen an die Arbeitgeber enthielten zu einem hohen Prozentsatz Daten von Arbeitnehmern, die nicht bei diesem Arbeitgeber beschäftigt seien.

11. 22. TB Nr. 6.1.2 und 23. TB Nr. 15.6 **„Statuskennzeichen auf der Krankenversichertenkarte“**

    Ich hatte 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. Obwohl mir versichert worden war, der GKV-Spitzenverband werde einen Verzicht auf die Statuskennzeichen prüfen, hat mir das BMG mittlerweile mitgeteilt, dass eine derartige Prüfung nicht stattgefunden hat. In demselben Schreiben hat mir das BMG allerdings auch mitgeteilt, mit der Ablösung der Krankenversichertenkarte durch die elektronische Gesundheitskarte (eGK) werde sich das datenschutzrechtliche Problem in dieser Weise nicht mehr stellen (vgl. Nr. 4.1). Bei der eGK wird das Merkmal „Sozialhilfeempfänger“ nicht mehr sichtbar auf dem Kartenkörper aufgedruckt. Mit dem weiteren Aufbau der Telematikinfrastruktur werde es darüber hinaus im zugriffsgeschützten Teil der Versichertenstammdaten nach § 291 Absatz 2 Satz 1 SGB V gespeichert werden können.

12. 23. TB Nr. 5.8 **Elektronischer Fahrzeugdatenspeicher**

    Eine Vielzahl elektronischer Fahrerassistenzsysteme speichert temporär oder permanent technische Daten. Diese sollen hauptsächlich den störungsfreien und sicheren Betrieb des Fahrzeugs im Straßenverkehr gewährleisten. Daneben erleichtern sie der Werkstatt im Reparatur- oder Wartungsfall, Fehler zu erkennen und zu beseitigen. Mit einem universellen Diagnosegerät lassen sich die Daten über die On-Board-Diagnoseschnittstelle auslesen. Werden sie mit weiteren Daten (z. B. Kundendaten) verknüpft, lässt sich ein Personenbezug herstellen und die neu gewonnenen Informationen könnten für andere Zwecke verwendet werden. In der Regel hat der Fahrzeugnutzer jedoch keine Kenntnis, dass und welche Daten in seinem Fahrzeug erhoben, verarbeitet und gespeichert werden.

    Zur Verbesserung der Transparenz für Fahrer und Halter hat der Düsseldorfer Kreis die Arbeitsgruppe „Fahrzeugdatenspeicher“ eingerichtet. Die Datenschutzaufsichtsbehörden von Bund und Ländern unter der Leitung des Bayerischen Landesamts für Datenschutzaufsicht haben zusammen mit dem Verband der Automobilindustrie eine Musterinformation über Datenspeicherung in Kraftfahrzeugen entwickelt, die künftig in die Betriebsanleitung von neuen Fahrzeugen aufgenommen wird. Durch diese zusätzliche Information werden Halter und Fahrer besser darüber informiert, welche personenbezogenen Daten in ihren Fahrzeugen gespeichert sind.

    Wer über diese Information hinaus detailliert wissen möchte, welche Daten zu welchem Zweck aus seinem Fahrzeug ausgelesen werden können, muss sich an seine Kfz-Werkstatt oder den Fahrzeughersteller wenden.

13. 23. TB Nr. 16 zu **Datenschutz am Pranger – werden Forschungsergebnisse zensiert?**

    Das Bundesinstitut für Sportwissenschaft (BISp) hatte ein Forschungsprojekt mit dem Thema Doping unter historisch-soziologischen und ethischen Aspekten ausgeschrieben, das von der Humboldt-Universität in Berlin (HU) und der Westfälischen Wilhelms-Universität in Münster durchgeführt wird. Das Vorhaben konnte bislang nicht abgeschlossen werden, weil die HU aus verschiedenen Gründen ihren Teilbeitrag nicht vollständig erbracht hat. In diesem Zusammenhang ist dem BISp vorgeworfen worden, es verbiete den Forschern die Nennung von Personen, die nach deren Überzeugung entweder als Sportler oder Ärzte aktiv Doping betrieben oder als Sportfunktionäre oder Politiker Doping gefördert oder zumindest toleriert haben sollen. Der Datenschutz werde als Instrument benutzt, um unliebsame Ergebnisse zu verhindern.

    Das BISp hatte der HU allerdings nicht verboten, Namen zu nennen, sondern nur auf die geltende Rechtslage aufmerksam gemacht. Nach § 40 Absatz 3 BDSG dürfen Forscher personenbezogene Daten nur veröffentlichen, wenn entweder der Betroffene eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist. Meines Wissens liegen keine Einwilligungen vor. Die notwendige Bewertung der Uner-

lässlichkeit im Einzelfall hat die HU bislang nicht vorgenommen. Von einer Zensur kann daher keine Rede sein. Vielmehr führt § 40 Absatz 3 BDSG zu einem verhältnismäßigen Ausgleich zwischen den Persönlichkeitsrechten der Betroffenen auf der einen Seite und der Forschungsfreiheit sowie dem legitimen öffentlichen Interesse an Aufklärung über Geschehnisse der Zeitgeschichte auf der anderen Seite.

Die technisch-organisatorischen Prozesse zur Datensicherheit, die anlässlich des Forschungsprojektes initiiert wurden, gestalteten sich allerdings schwierig. So war hinsichtlich des IT-Sicherheitskonzeptes lange nicht klar, dass das BISp aufgrund seiner infrastrukturellen Anbindung an das Statistische Bundesamt von diesem abhängig ist. Aufgrund dortiger, noch andauernder Umstrukturierungen fehlt bislang ein aktuelles IT-Sicherheitskonzept. Auch das vorgelegte Datenschutzkonzept war verbesserungswürdig, weil nur unzureichende technisch-organisatorische Maßnahmen nach der Anlage zu § 9 BDSG getroffen oder beschrieben worden waren. Das Bewusstsein für die datenschutzrechtliche Verantwortlichkeit des Auftraggebers eines Forschungsprojektes ist durch die Zusammenarbeit in diesem Projekt gestärkt worden.

14. 23. TB Nr. 8.5.3 **Änderung des Stasi-Unterlagen-Gesetzes**

Ich hatte darüber berichtet, dass die im Stasi-Unterlagen-Gesetz (StUG) vorgesehene Möglichkeit, Stasi-Unterlagen zur Überprüfung bestimmter Personen auf eine frühere Stasi-Tätigkeit zu verwenden, bis Ende 2019 verlängert werden sollte. Die entsprechende Gesetzesänderung, mit der zugleich auch der überprüfbare Personenkreis im öffentlichen Dienst wieder erweitert wurde, ist inzwischen in Kraft getreten (8. StUÄndG vom 22. Dezember 2011, BGBl. I S. 3106).

Leider wurde meine Empfehlung, dieses Gesetzgebungsverfahren auch dazu zu nutzen, im StUG vorhandene Regelungslücken zur Auftragsdatenverarbeitung zu schließen, nicht umgesetzt. Im Rahmen meiner Beratungstätigkeit beim BStU hatte ich Rechtsunsicherheit bei Fragen der Auftragsdatenverarbeitung festgestellt, da § 41 Absatz 3 StUG hierfür keine hinreichenden Verfahrensregelungen enthält. Erforderlich wäre eine Bestimmung, die die umfassenden verfahrensmäßigen Absicherungen des § 11 Absatz 1 und 2 BDSG für analog anwendbar erklärt. Für eine entsprechende Ergänzung des StUG werde ich mich auch weiterhin einsetzen.

Ich bedauere außerdem, dass im Zuge des Gesetzgebungsverfahrens die zuvor im StUG enthaltenen Regelungen zum Kopierschutz und anderen technisch-organisatorischen Sicherungsmaßnahmen bei personenbezogenen Internetveröffentlichungen des BStU ersatzlos gestrichen wurden. Diese Bestimmungen waren – trotz eines in der Praxis des BStU teilweise eher geringen Anwendungsbereiches – angesichts der besonderen Eingriffsqualität einer Internetveröffentlichung in das Persönlichkeitsrecht datenschutzrechtlich von wesentlicher Bedeutung.

15. 23. TB Nr. 8.2.1 **Änderung des Gesetzes über das Ausländerzentralregister**

In meinem letzten Tätigkeitsbericht hatte ich über den Beginn des Gesetzgebungsverfahrens zur Umsetzung des EuGH-Urteils „Huber“ (Urteil vom 16. Dezember 2008, C-524/06) berichtet. Der Europäische Gerichtshof hatte die Speicherung von Daten zu Unionsbürgern in einem zentralen Register wie dem Ausländerzentralregister (AZR) sowie deren Übermittlung an andere Behörden nur unter engen Voraussetzungen für zulässig erklärt. Der vom BMI zunächst vorgelegte Referentenentwurf zur Änderung des Gesetzes über das Ausländerzentralregister (AZRG) setzte diese Vorgaben nur unzureichend um.

Im Zuge der Ressortabstimmung, an welcher ich intensiv beteiligt war, hat der Entwurf deutliche Verbesserungen erfahren. Der Umfang der zu Unionsbürgern im AZR gespeicherten Daten wurde reduziert (z. B. wurde auf die Speicherung des Lichtbildes verzichtet) und die Möglichkeit der Übermittlung dieser Daten ausdrücklich auf ausländer- oder asylrechtliche Zwecke und an mit solchen Aufgaben betraute Behörden beschränkt. Außerdem dürfen Gruppenauskünfte über Unionsbürger nicht erteilt werden. Das Gesetz wurde inzwischen von Bundestag und Bundesrat beschlossen (Bundestagsdrucksache 17/11051, 17/11364) und soll neun Monate nach seiner Verkündung in Kraft treten. Ich werde mich für eine zeitnahe technische Umsetzung der Änderungen im AZR einsetzen.

Erfreulicherweise wurde dieses Gesetzgebungsverfahren auch dazu genutzt, eine Forschungsklausel für das Bundesamt für Migration und Flüchtlinge (BAMF) in das AZRG aufzunehmen und damit einer langjährigen datenschutzrechtlichen Forderung Rechnung zu tragen (vgl. 21. TB Nr. 7.1.3). Damit wird die Nutzung von AZR-Daten für die wissenschaftliche Begleitforschung des BAMF auf eine eindeutige bereichsspezifische Rechtsgrundlage gestellt.

16. 23. TB Nr. 8.2.2 **Elektronischer Aufenthaltstitel**

Der elektronische Aufenthaltstitel (eAT) im Scheckkartenformat, der die bislang als Klebeetikett im Reisedokument eingefügten Aufenthaltstitel ersetzt, wird seit dem 1. September 2011 von den Ausländerbehörden ausgegeben. Entsprechend den europäischen Vorgaben (Verordnung (EG) Nr. 380/2008 vom 18. April 2008) und vergleichbar dem neuen elektronischen Personalausweis (nPA) enthält der eAT einen Chip, auf dem ein digitales Lichtbild und zwei Fingerabdrücke des Inhabers als biometrische Merkmale gespeichert werden. Anders als beim nPA ist die Aufnahme der Fingerabdrücke beim eAT allerdings obligatorisch. Als freiwillige Zusatzfunktion verfügt der eAT – wie der nPA – über die Möglichkeit des elektronischen Identitätsnachweises (eID), mit dem der

Inhaber sich im Internet oder z. B. auch an Verkaufsautomaten ausweisen kann (vgl. Nr. 2.3.4, 8.5 und 23. TB Nr. 3.2).

Wie bereits im letzten Tätigkeitsbericht dargelegt, habe ich mich mit Blick auf die gespeicherten biometrischen Merkmale und die eID-Funktion für ein hohes Datenschutz- und Datensicherheitsniveau beim eAT eingesetzt. Ich begrüße, dass das Gesetz zur Anpassung des deutschen Rechts an o. g. EG-Verordnung (Gesetz vom 12. April 2011, BGBl. I S. 610) sowie die entsprechende Rechtsverordnung (Verordnung vom 22. Juli 2011, BGBl. I S. 1530) dies jetzt u. a. durch Verweise auf die bereits für den nPA geltenden datenschutzrechtlichen Bestimmungen sicherstellen.

17. 23. TB Nr. 6.11 **Mail Sampling Unit, Sendungsfotografien**

Bereits im 23. Tätigkeitsbericht hatte ich über die Abrechnungsverfahren im internationalen Postverkehr und die von der Deutschen Post AG durchgeführten Stichprobenerhebungen mittels Sendungsfotografien berichtet. Damals stand noch eine Antwort der Deutschen Post AG aus, so dass keine abschließende Bewertung möglich war. Hieran hat sich nichts geändert, auch wenn mir inzwischen weitere Erkenntnisse vorliegen.

Der internationale Postverkehr hat sich auf ein (quasi-standardisiertes) Verfahren zum Ausräumen von etwaigen Unstimmigkeiten in der Abrechnung geeinigt. Dieses Verfahren basiert zum größten Teil auf einem Parameter, der die Menge von bestimmten Sendungen pro Kilogramm („Items per Kilo“) angibt. Kommt es nun im Postaustausch zu Unstimmigkeiten, wird genau dieser Wert angezweifelt und die Postunternehmen versuchen, ihre Angaben zu belegen. An dieser Stelle haben sich die Sendungsfotografien im internationalen Umfeld etabliert, um pro Raumeinheit Größe, Beschaffenheit und Anzahl der einzelnen Sendungen zu dokumentieren. Die Speicherung der Aufnahmen erfolgt in den anderen Ländern in der Regel für ungefähr zwei Jahre, da die Abrechnungsläufe sehr langwierig sind.

Meiner Aufforderung an die Deutsche Post AG zu prüfen, ob eine Beschränkung der Bildaufnahmen auf die relevanten Daten (Bestimmungsland, -ort und Postleitzahl) möglich ist, kam diese zwar nach, jedoch gibt es keine erfolgversprechenden Ergebnisse. Dies zeigte auch ein Besuch der Sortieranlage in Frankfurt. Ich habe deshalb erneut auf den Maßstab der Erforderlichkeit aufmerksam gemacht, der es verbietet, Namen von Absender und Adressat auf einer Fotografie zu erfassen. Die Deutsche Post AG kündigte an, künftig die nicht benötigten Bildbereiche der Fotografien zu verpixeln (unkenntlich zu machen), um gleichwohl ein angemessenes Maß der Beweissicherung für die Abrechung im internationalen Postverkehr zu erreichen; ob es zur Umsetzung kommt, werde ich weiterhin beobachten.

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	2.1.1, 2.4.4, 4.4
Innenausschuss	2.1, 2.1.1, 2.1.2, 2.2.1, 2.4.1.1, 2.3.4, 2.5.1, 2.5.2.1, 2.5.2.2, 2.5.3, 2.5.3.3, 3.1, 3.2.1, 3.2.3, 3.2.4, 3.3.1, 3.3.3, 3.3.3.2, 3.4, 3.5, 3.5.1, 3.5.2, 3.5.3, 3.6, 4.3 bis 4.9, 5.1.2, 5.2, 5.3, 6.1 bis 6.11, 7.1, 7.2, 7.3, 7.4.1, 7.4.4, 7.4.7, 7.6.2, 7.7.1, 7.7.2, 7.7.3, 7.7.4, 7.7.5, 7.7.6, 8.1.1, 8.2, 8.4, 8.5, 8.6, 8.7, 8.9, 8.10, 8.12, 8.13, 10.2, 10.3, 10.4, 13.1 bis 13. 5, 16.1, 16.5, 16.15
Sportausschuss	
Rechtsausschuss	2.1.1, 2.2.1, 2.5.2.1, 2.5.2.2, 3.3.3, 3.3.3.2, 3.5.3, 3.6, 6.1 bis 6.11, 7.1, 7.4.1, 7.4.7, 7.7.3, 7.7.4,
Finanzausschuss	2.5.5, 4.3, 7.5.1, 7.10, 9.1 bis 9.7, 16.2, 16.6, 16.7
Ausschuss für Wirtschaft und Technologie	2.1.1, 2.3.1, 3.4, 3.5.1, 3.5.3, 3.6, 4.3, 4.5, 4.6, 4.9, 5.3, 5.4 bis 5.10, 6.1 bis 6.13, 10.1, 10.2, 10.3, 10.4, 10.5, 16.1
Ausschuss für Ernährung, Landwirtschaft und Verbraucherschutz	2.1.1, 3.5.1, 4.3 bis 4.6, 4.9, 5.3, 5.4 bis 5.7, 5.8.2, 5.8.3, 5.9, 5.10, 6.12, 6.13, 10.2, 10.3, 10.4, 16.1
Ausschuss für Arbeit und Soziales	2.3.3, 4.2.1, 4.2.2, 4.2.3, 11.2, 11.4.1 bis 11.4.1, 12.1.1 bis 12.2.4, 13.1 bis 13.5, 16.3, 16.4
Verteidigungsausschuss	3.3.3.3, 14.1, 14.2, 14.2.3 bis 14.2.5, 14.3
Ausschuss für Familie, Senioren, Frauen und Jugend	11.6, 14.2.1, 14.2.2
Ausschuss für Gesundheit	2.3.2, 3.5.1, 4.1, 11.1 bis 11.1.10, 11.5.5, 11.5.6
Ausschuss für Verkehr, Bau und Stadtentwicklung	10.7, 10.8, 10.11, 13.4
Ausschuss für Menschenrechte und Humanitäre Hilfe	
Ausschuss für Bildung, Forschung und Technikfolgenabschätzung	2.1.1, 3.5.1, 4.3 bis 4.5, 4.7, 4.9, 5.3
Ausschuss für Tourismus	
Ausschuss für die Angelegenheiten der Europäischen Union	2.1, 2.1.1, 2.1.2, 2.2.1, 2.4.1.3, 2.4.4, 2.5.1, 2.5.2.2, 2.5.3.3, 4.4, 7.6.2
Ausschuss für Kultur und Medien	5.4 bis 5.7, 5.8.2, 5.8.3, 5.9, 5.10, 8.8, 16.14
Ausschuss für Kultur und Medien – Unterausschuss „Neue Medien“ –	2.1.1, 2.4.1.3, 2.4.4, 4.5, 4.9, 5.3, 5.4 bis 5.7, 5.8.2, 5.8.3, 5.9, 5.10

Anlage 2

Übersicht über die durchgeführten Kontrollen, Beratungen und Informationsbesuche

Auswärtiges Amt

- Zentrale
- Botschaft

Bundeskanzleramt

- Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU)
- Bundesarchiv
- Bundesnachrichtendienst

Deutscher Bundestag

- Verwaltung
- Besucherdienst

Bundesministerium des Innern

- Ministerium
- Bundesdruckerei
- Bundesverwaltungsamt
- Statistisches Bundesamt
- Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS)
- Bundespolizeipräsidium
- Bundespolizeidirektion Sankt Augustin
- Bundespolizeidirektion Flughafen Frankfurt/Main
- Bundespolizeiinspektion Flughafen München
- Bundesanstalt Technisches Hilfswerk
- Bundeskriminalamt (Wiesbaden, Meckenheim und Berlin)
- Bundesamt für Verfassungsschutz
- Bundesamt für Migration und Flüchtlinge
- Bundesamt für die Sicherheit in der Informationstechnik
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
- Bundeszentrale für politische Bildung

Bundesministerium der Finanzen

- Ministerium
- Bundeszentralamt für Steuern
- Zentrum für Informationsverarbeitung und Infromationstechnik
- ein Hauptzollamt
- ein Zollamt
- Zollkriminalamt (Köln-Dellbrück)
- Bundesamt für zentrale Dienste und offene Vermögensfragen

Bundesministerium für Arbeit und Soziales

- Bundesagentur für Arbeit (Pilotprojekt eAkte; Halle)
- zwei Agenturen für Arbeit
- 19 Jobcenter (Stadt Koblenz, Kreis Euskirchen, Rhein-Erft, Mönchengladbach, Berlin Tempelhof-Schöneberg, Heidelberg, Erfurt, Bremen, StädteRegion Aachen, Oberhausen, Neuwied, team.arbeit.hamburg, Limburg-Weilburg, Landkreis Wittenberg, Osnabrück, Potsdam, Stadt Aschaffenburg, Saarbrücken, Kreis Pinneberg)
- eine Familienkasse der Bundesagentur für Arbeit
- Deutsche Rentenversicherung Bund

Bundesministerium der Verteidigung

- Zentrum für Nachwuchsgewinnung NORD
- Militärischer Abschirmdienst

Bundesministerium für Familie, Senioren, Frauen und Jugend

- Bundesamt für Familie und zivilgesellschaftliche Aufgaben

Bundesministerium für Gesundheit

- Ministerium
- GKV Spitzenverband
- Bundesversicherungsamt
- Gemeinsamer Bundesausschuss
- Paul-Ehrlich-Institut (PEI)
- Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM)

Bundesministerium für Verkehr, Bau und Stadtentwicklung

- Ministerium
- Bundesamt für Bauwesen und Raumordnung
- Bundesamt für Güterverkehr
- Bundesanstalt für Straßenwesen
- Eisenbahn-Bundesamt

noch Anlage 2

- Kraftfahrt-Bundesamt
- Luftfahrt-Bundesamt
- Bundesanstalt für Gewässerkunde
- Deutscher Wetterdienst
- Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT)
- Wasser- und Schifffahrtsamt

Bundesministerium für Wirtschaft und Technologie

- Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz

- Ministerium

Postdienstunternehmen

- CITIPOST GmbH
- Deutsche Post AG
  - Zentrale
  - Briefverteilzentrum
  - Packstation
  - Zustellstützpunkt
- Leipziger Volkszeitung
- TNT Express GmbH

Telekommunikationsunternehmen

- Congstar GmbH
- Deutsche Telekom AG
- disquom funktechnik GmbH
- E-Plus Mobilflunk GmbH & Co. KG
- Hansa Funktaxi eG
- Kabel BW GmbH
- mr. net group GmbH & Co. KG
- NetCologne Gesellschaft für Telekommunikation mbH
- Tchibo GmbH
- Telefónica Germany GmbH & Co. OHG
- United Internet AG (1&1, web.de, GMX)
- Vodafone D2 GmbH

Sonstige

- Deutsche Angestellten Krankenkasse (DAK)
- Techniker Krankenkasse
- City BKK
- Hanseatische Ersatzkasse
- Deutsche Betriebskrankenkasse
- Audi Betriebskrankenkasse
- Siemens Betriebskrankenkasse
- Unfallkasse des Bundes
- Berufsgenossenschaft Handel und Warendistribution (BGHW)

Anlage 3

Übersicht über Beanstandungen nach § 25 BDSG

Bundesministerium des Innern

- Verstoß des BfV gegen § 15 Abs. 1 und 2 BVerfSchG und die Vorgaben des Bundesverfassungsgerichts in Bezug auf die Auskunftserteilung .
- Verstoß beim Bundesamt für Sicherheit in der Informationstechnik gegen § 9 Satz 1 BDSG einschließlich Anlagen (fehlendes Berechtigungskonzept beim Schadprogramm-Erkennungssystem; vgl. Nr. 4.7).
- Verstoß des Bundesamtes für Verfassungsschutz (BfV) gegen § 14 Abs. 1 BVerfSchG (fehlende Dateianordnung für eine Datei mit personenbezogenen Daten, die durch den verdeckten Einsatz technischer Mittel erhoben worden sind – vgl. 21. TB Nr. 5.5.2).
- Verstoß des BKA gegen § 20 Buchstabe l Abs. 2 Satz 2 BKAG i. V. m. § 20 Buchstabe k Abs. 3 BKAG i. V. m. § 9 Satz 1 BDSG i. V. m. Satz 1, Satz 2 Nr. 2 bis 5 sowie Satz 3 der Anlage zu § 9 Satz 1 BDSG (unzureichende technische und organisatorische Beschränkung der zum Zweck der Quellen-TKÜ eingesetzten Software; vgl. Nr. 7.2.1).

Bundesministerium der Finanzen

- Verstoß des ZKA gegen § 20 Abs. 1 Zollfahndungsdienstgesetz (ZFdG) i. V. m. § 9 Satz 1 BDSG i. V. m. Satz 1, Satz 2 Nr. 2 bis 5 sowie Satz 3 der Anlage zu § 9 Satz 1 BDSG (unzureichende technische und organisatorische Beschränkung der zum Zweck der Quellen-TKÜ eingesetzten Software; vgl. Nr. 7.2.1).
- Verstoß eines Hauptzollamtes gegen Nr. 253 der Dienstanweisung „Zugelassener Wirtschaftsbeteiligter – AEO“ vom 22. Juni 2010 mit der die Überprüfung auf Beschäftigte in sicherheitsrelevanten Bereichen begrenzt wird (vgl. Nr. 7.3.1).
- Verstoß einer Familienkasse der Bundesagentur für Arbeit gegen § 24 Absatz 1 i. V. m. Absatz 4 BDSG wegen Verletzung meiner Kontroll- und Prüfbefugnisse, da wiederholt Aktenübersendung an mich abgelehnt wurde (vgl. Nr. 9.4).

Bundesministerium für Verkehr, Bau und Stadtentwicklung

Zwei Beanstandungen (vgl. Nr. 13.4)

- Verstoß gegen die Regelungen der §§ 106 ff. BBG bzw. gegen § 12 Abs. 4 i. V. m. § 32 BDSG,
- Verstoß gegen die Regelungen des § 12 Abs. 4 i. V. m. § 32 Abs. 1 BDSG und § 7 Abs. 7 und 8 AZV.

Telekommunikationsunternehmen

Vodafone D2 GmbH

Verstoß gegen § 113 TKG wegen Übermittlung von Bestandsdaten an Sicherheitsbehörden ohne Rechtsgrundlage (vgl. Nr. 7.4.6)

Unfallkasse des Bundes

Vier Beanstandungen (vgl. Nr. 13.4 und Nr. 11.4.2)

- zwei Verstöße gegen die Regelungen der §§ 106 ff. BBG,
- Verstoß gegen das in § 24 Abs. 4 BDSG normierte Unterstützungsgebot,
- Verstoß gegen § 35 Abs. 1 SGB I (Sozialgeheimnis).

Gesetzliche Krankenkassen

Siemens BKK

Beanstandung nach § 81 Abs. 4 SGB X i. V. m. § 25 Abs. 1 BDSG wegen zahlreicher Verstöße gegen das Sozialgeheimnis nach § 35 Abs. 1 SGB I (vgl. Nr. 11.1.8).

Anlage 4

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, des technologischen Datenschutzes und des Datenschutzes im Internet. Der Umgang mit Geodaten eröffnet dabei eine neue Dimension von Datenschutzfragen.

B. Lösung

Einstimmige Annahme einer Entschließung und Kenntnisnahme der Unterrichtung

C. Alternativen

Keine

D. Kosten

Keine

noch Anlage 4

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.	**Noch nicht in allen Punkten erledigt** – geeignete Ansätze sind z. B. de-Mail (vgl. 23. TB Nr. 3.3 [22. TB Nr. 6.6]), ePersonalausweis (vgl. 23. TB Nr. 3.2 [22. TB Nr. 6.3.2]) oder Privacy impact assessments bei RFID (vgl. 23. TB Nr. 5.9 [22. TB Nr. 6.7]) – die neue EU-Datenschutz-Verordnung ist für die Entwicklung eines präventiven technologischen Datenschutzes entscheidend
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.	**Nicht erledigt** vgl. auch 23. TB Nr. 1.1, 1.2, 4.1 und 4.2
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.	**Nicht erledigt** vgl. 23. TB Nr. 4.1.3, 4.2 sowie 24. TB Nr. 3.4

noch Anlage 4

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.	**Teilweise erledigt** vgl. Nr. 3.6
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.	**Nicht erledigt**
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.	**Nicht erledigt**
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.	**Überwiegend noch nicht erledigt** die neue EU-Datenschutz-Verordnung enthält (bisher m. E.) keine ausreichenden Regelungen für ein einheitliches Datenschutzaudit vgl. Nr. 3.6

noch Anlage 4

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.	**Nicht erledigt** vgl. 23. TB Nr. 2.1 sowie 24. TB Nr. 3.1, 6.9
9.	Der Deutsche Bundestag fordert die Bundesregierung dazu auf, sich in den bevorstehenden Verhandlungen zur Novellierung der EU-Datenschutzrichtlinie 95/46 vom 23. November 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.	**Hat sich weitgehend erledigt** vgl. Nr. 2.1
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.	**Noch nicht erledigt** vgl. 23. TB Nr. 13.8 Die Verhandlungen zwischen den Vertretern der Europäischen Union und den Vereinigten Staaten von Amerika sind ohne nennenswerte Fortschritte ins Stocken geraten.
11.	Der Deutsche Bundestag hat bereits in seiner Entschließung zum 20. Tätigkeitsbericht des BfDI zur Übermittlung von Fluggastdaten in die USA Stellung genommen Bundestagsdrucksache 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.	**Noch nicht erledigt** vgl. 24. TB Nr. 2.5.2.1 Im Berichtszeitraum standen die Verhandlungen mit den Vereinigten Staaten von Amerika, Australien und Kanada im Blickpunkt. Über das weitere Vorgehen hat die Europäische Kommission noch nicht entschieden.
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.	**Nicht erledigt** vgl. 24. TB Nr. 9.5

noch Anlage 4

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	**Noch nicht erledigt** vgl. Nr. 8.1.1
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.	**Teilweise erledigt** vgl. Nr. 8.2
15.	Der Deutsche Bundestag bedauert, dass seine Aufforderung aus den Entschließungen zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Bundestagsdrucksache 16/4882, Nr. 10) und zum 21. Tätigkeitsbericht (Bundestagsdrucksache 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	**Noch nicht erledigt** Das Bundesministerium der Finanzen hatte in dieser Legislaturperiode einen Diskussionsentwurf eingebracht. Dieser ist jedoch liegen geblieben und wird – soweit ersichtlich – auch nicht mehr verfolgt. vgl. 24. TB Nr. 16.9
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	**Noch nicht erledigt** vgl. Nr. 10.1

In der Plenarsitzung des Deutschen Bundestages vom 18. Dezember 2010 einstimmig angenommen.

Anlage 5

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht
Frau Dagmar Hartge
Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes
und der Länder 2012

Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Datenschutz-Grundverordnung KOM (2012) 11 endg. vom 25. Januar 2012

11. Juni 2012

Angesichts des rasanten technologischen Fortschritts, zunehmender Vernetzung und Globalisierung ist der grundrechtsorientierte Ansatz des europäischen Datenschutzrechts mit vielfältigen Herausforderungen konfrontiert. Das durch Art. 8 der Europäischen Grundrechtecharta garantierte Grundrecht auf den Schutz personenbezogener Daten ist seit dem Inkrafttreten des Vertrags von Lissabon unmittelbar anwendbares Recht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Konferenz) begrüßt deshalb das von der Kommission verfolgte Ziel eines hohen gemeinsamen Datenschutzniveaus in der gesamten Europäischen Union.

Mit der Datenschutz-Grundverordnung (Verordnung) strebt die Kommission eine Harmonisierung des Datenschutzrechts an. Die Konferenz hält es für sinnvoll und erforderlich, einen effektiven Datenschutz für alle Bürgerinnen und Bürger in Europa zu gewährleisten. Ungeachtet der Frage, ob sich die Kompetenz der EU zum Erlass einer Verordnung auf Basis von Art. 16 Abs. 2 Satz 1 AEUV im Hinblick auf das Prinzip der begrenzten Einzelermächtigung und das Subsidiaritätsprinzip auch auf rein innerstaatliche Datenverarbeitungen im öffentlichen Bereich erstreckt, ist die Konferenz der Auffassung, dass auch insoweit ein möglichst hoher Mindeststandard gewährleistet werden muss. Es darf insgesamt zu keiner Absenkung des in den Mitgliedsstaaten bereits erreichten Schutzniveaus kommen. Die Mitgliedsstaaten sollten daher auch in Zukunft – vor allem bei besonders sensiblen Datenverarbeitungen – gesetzliche Regelungen mit einem möglichst hohen Schutzniveau erlassen dürfen. Die Verordnung muss in jedem Fall den Verfassungs- und Rechtstraditionen der Mitgliedsstaaten Rechnung tragen.

Der Entwurf ermächtigt die Kommission in einer Vielzahl von Vorschriften zu einer näheren Regelung durch delegierte Rechtsakte. Die Konferenz appelliert an das Europäische Parlament und den Rat, die Notwendigkeit jeder einzelnen Delegationsermächtigung kritisch zu überprüfen. Im Hinblick auf den Wesentlichkeitsgrundsatz müssen entsprechend Art. 290 AEUV die entscheidenden Regelungen in der Verordnung selbst getroffen oder aber im Hinblick auf fachspezifische Regelungen dem nationalen Gesetzgeber überlassen werden. Auch wenn das Parlament bei einer Ausübung der Delegationsrechte durch die Kommission auf den Erlass dieser Rechtsakte einwirken kann, ist deren demokratische Legitimation deutlich geringer, als bei einer Regelung der wesentlichen Punkte in der Verordnung selbst. Die Konferenz lehnt daher insbesondere solche delegierten Rechtsakte ab, bei denen grundlegende materiell- und verfahrensrechtliche Regelungen (wie z. B. in Art. 6 bei der Rechtmäßigkeit der Verarbeitung) konkret ausgestaltet werden sollen.

Die Konferenz weist auch darauf hin, dass der Entwurf in zahlreichen Regelungen unbestimmte Rechtsbegriffe sowie Interessenabwägungen enthält, deren hoher Abstraktionsgrad einen großen Spielraum bei der Auslegung und Anwendung zulässt. Sie empfiehlt dringend, die notwendigen Klarstellungen in den Regelungen selbst vorzunehmen.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf vorgesehene Kohärenzverfahren, welches in der gegenwärtigen Ausgestaltung die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb stark vereinfacht und praktikabler gestaltet werden. Die durch Art. 8 der Grundrechtecharta und Art. 16 AEUV gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Die Konferenz hält es für erforderlich, die in den Art. 8 (3), 12 (6), 14 (7) und 22 (4) vorgesehenen Ausnahmen für die Datenverarbeitung kleiner und mittlerer Unternehmen (KMU) zu überprüfen. Ausnahmen sollten sich generell weniger an der Größe eines Unternehmens, sondern vielmehr an den Gefahren und Risiken für die Rechte und

Freiheiten des Einzelnen orientieren. Auch von sehr kleinen Unternehmen können erhebliche Gefährdungen für den Datenschutz ausgehen.

Der Entwurf der Verordnung führt in erheblichem Umfang zu Abgrenzungsschwierigkeiten mit der RL 2002/58/EG. Art. 89 (1) ist insoweit zu abstrakt und unklar formuliert. Welche besonderen Pflichten gibt es konkret, die in der Richtlinie 2002/58/EG festgelegt sind? Weder Art. 89 noch die einschlägige Erwägung 135 geben hierüber Aufschluss.

Die Konferenz schlägt vor, eine Regelung „Erziehung und Bildung" aufzunehmen. Der Datenschutz dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

„Art. Xx – Erziehung und Bildung

Um sich in der Informationsgesellschaft behaupten zu können, ist den Bürgerinnen und Bürgern durch geeignete Maßnahmen Datenschutzkompetenz zu vermitteln. Sie ist Teil der übergreifenden Medienkompetenz; ihre Vermittlung ist eine gesamtgesellschaftliche Aufgabe in den Mitgliedstaaten, die hierbei von der Union unterstützt werden."

Zu den einzelnen Regelungen nimmt die Konferenz wie folgt Stellung:

Kapitel I – Allgemeine Bestimmungen

Zu Art. 2:

Die Konferenz spricht sich dafür aus, dass auch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union entweder in den Geltungsbereich der Verordnung einbezogen werden (Art. 2 (2) lit. b)) oder die Verordnung 45/2001 zeitgleich angepasst wird. Es wäre nicht vertretbar, wenn sich die EU selbst von der angestrebten Modernisierung des Datenschutzrechts ausnehmen würde. Zudem spricht auch das Ziel der Harmonisierung für eine Einbeziehung der Organe der Union, da zunehmend auch zwischen diesen und den Mitgliedstaaten ein Austausch personenbezogener Daten stattfindet.

Die Beibehaltung der Ausnahme der Datenverarbeitung durch natürliche Personen zu ausschließlichen persönlichen oder familiären Zwecken in Art. 2 (2) lit. d) wird grundsätzlich begrüßt. Allerdings wäre eine Klarstellung wünschenswert, die in einer differenzierten Regelung die datenschutzrechtlichen Pflichten von natürlichen Personen angemessen ausgestaltet. Dies könnte beispielsweise in einer eigenständigen Regelung zur Veröffentlichung personenbezogener Daten an einen unbestimmten Personenkreis geschehen.

Zu Art. 3:

Die Konferenz begrüßt die Einführung des Marktortprinzips in der Verordnung.

Zum räumlichen Anwendungsbereich für Verarbeitungen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen weist sie darauf hin, dass Ermittlungs- und Rechtsdurchsetzungsbefugnisse im EU-Ausland nur nach Maßgabe bislang nicht existierender zwischenstaatlicher Verträge bestehen. In Vorentwürfen der Verordnung war deshalb bereits vorgesehen, dass der innerhalb der EU zu bestellende Vertreter (Art. 25) umfassend in die Rechtsstellung des Verantwortlichen und dessen Pflichten eintreten solle. Dessen zusätzliche Einbeziehung in die Rechte und Pflichten wäre aus Sicht der Konferenz zu begrüßen.

Der Begriff der „Beobachtung" sollte konkretisiert werden (Art. 3 (2) lit. b)), weil nicht hinreichend klar ist, welche Anwendungsfälle hierdurch erfasst werden sollen.

Zu Art. 4:

Die Definition der „betroffenen Person" sollte ohne die Formulierung „nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde", die damit eine subjektive Komponente impliziert, wie folgt gefasst werden: „eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt von der für die Verarbeitung verantwortlichen oder jeder sonstigen natürlichen oder juristischen Person bestimmt werden kann" (Art. 4 (1)).

Es sollte auch klargestellt werden, dass Kennnummern, Standortdaten usw. zu den personenbezogenen Daten zählen (siehe Erwägungsgrund 23 der bekannt gewordenen Entwurfsfassung 56; Art. 4 (1) und (2)).

Es sollte definiert werden, was „automatisiert" bedeutet (Art. 4 (3)).

In der Definition der „Datei" sollte klargestellt werden, dass die Zugänglichkeit nach mindestens einem bestimmten Kriterium ausreicht (Art. 4 (4)).

Die Definition der „biometrischen Daten" sollte nicht nur auf die eindeutige Identifizierbarkeit abstellen, sondern auch das harmonisierte biometrische Vokabular verwenden: „Daten zu den physischen, physiologischen oder verhaltenstypischen Charakteristika eines Menschen wie Gesichtsbilder oder daktyloskopische Daten" (Art. 4 (11)).

Für Betroffene und Aufsichtsbehörden fehlt es an Transparenz und Verlässlichkeit, wenn die Hauptniederlassung über unternehmensinterne Regelungen („Ort (...), an dem die Grundsatzentscheidungen (...) getroffen werden") bzw. über den Schwerpunkt der Verarbeitung („Ort, an dem die Verarbeitungstätigkeiten (...) hauptsächlich stattfinden") definiert wird. Eine Präzisierung wird dringend für erforderlich gehalten, insbesondere im Hinblick auf

die Regelungen des „One-Stop-Shops“ in Art. 51 (2) sowie die Regelungen des gerichtlichen Rechtschutzes in Kapitel VIII.

Die Definition des „Dritten“ sollte in Art. 4 aufgenommen werden, um insbesondere die Figur des Auftragsdatenverarbeiters entsprechend Art. 2 lit. f)) der RL 95/46/EG klarer zu fassen.

Die Begriffe „Anonymisierung“ und „Pseudonymisierung“ sollten ebenfalls definiert werden, da beiden Vorgängen materiell-rechtlich eine größere Bedeutung eingeräumt wird und aus Sicht der Konferenz auch eingeräumt werden sollte.

Kapitel II – Grundsätze

Zu Art. 5:

Als weiterer Grundsatz sollte in Art. 5 die Verpflichtung aufgenommen werden, dass bei der Verarbeitung personenbezogener Daten die technischen und organisatorischen Maßnahmen zum Datenschutz einzuhalten sind, um die hohe Bedeutung des technologischen Datenschutzes zu unterstreichen.

Die Zweckbindung ist bei der Verarbeitung personenbezogener Daten eines der wichtigsten Grundprinzipien zur Gewährleistung des Datenschutzes. Im Hinblick auf Art. 5 lit. b) sollte die Zweckbindung deshalb strikter gefasst werden. Zumindest erwartet die Konferenz die Klarstellung, dass der in der Verordnung gewählte Begriff der Zweckvereinbarkeit der Zweckbindung im Sinne des deutschen Datenschutzrechts entspricht.

In Art. 5 lit. e) sollte zusätzlich die anonyme und pseudonyme Nutzung der Daten als Gestaltungsauftrag mit aufgenommen werden. Dies sollte im Weiteren mit Regelungen zu einer Privilegierung der pseudonymen Datenverarbeitung flankiert werden.

Zu Art. 6:

Die Abwägungsklausel des Art. 6 (1) lit. f) wird in der Praxis eine herausragende Bedeutung erlangen. Die Vorgaben und Maßstäbe, anhand derer die Interessenabwägung innerhalb dieser Auffangregelung vorzunehmen ist, müssen daher hinreichend klar sein. In Art. 6 (1) lit. f) sollte eine Regelungsstruktur gefunden werden, die branchen- und situationsspezifischen Konkretisierungen Rechnung trägt. Die Verordnung sollte dabei beispielsweise auf die spezifischen Datenschutzaspekte der Auskunfteien und des Scorings eingehen. Im Hinblick auf die Verarbeitung von personenbezogenen Daten zu Direktmarketingzwecken sollte – wie in der bekannt gewordenen Entwurfsfassung 56 – grundsätzlich ein Einwilligungserfordernis (opt-in) vorgesehen werden.

Zudem erscheint es – wie Art. 20 des Vorschlags zeigt – auch denkbar, abschließende Fallgruppen zu definieren, die einer Interessenabwägung aufgrund des hohen Gefährdungspotentials der Datenverarbeitung von vornherein nicht zugänglich sind.

Vor dem Hintergrund des in Art. 290 AEUV niedergelegten Wesentlichkeitsgrundsatzes sollten die hier geforderten Konkretisierungen in der Verordnung selbst formuliert werden, da es sich um wesentliche Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten handelt. Art. 6 (5) wäre daher zu streichen.

Ausgehend von Art. 6 (3) lit. b) ist sicherzustellen, dass durch den Verweis auf das mitgliedstaatliche Recht im öffentlichen Bereich ein über die Anforderungen der Verordnung hinausgehendes Datenschutzrecht erhalten bleiben kann, wie dies in verschiedenen bundes- und landesrechtlichen Regelungen bereits jetzt verwirklicht ist. Es muss auch weiterhin ohne Zweifel gewährleistet sein, dass in einem ausdifferenzierten bereichsspezifischen Datenschutzrecht dem erhöhten Schutzbedarf staatlicher Datenverarbeitung auch in Zukunft Rechnung getragen wird. Dies muss sich eindeutig und ausdrücklich aus dem Wortlaut von Art. 6 (3) lit. b) ergeben. Anderenfalls wäre der derzeit bestehende besondere Schutz, beispielsweise der in der Bundesrepublik Deutschland bestehende Schutz von Sozialdaten, durch die Verordnung gefährdet.

Zu Art. 7:

Die Konferenz unterstützt die Absicht der Kommission, in Art 7 (4) die Freiwilligkeit von Einwilligungen zu konkretisieren. Sie weist allerdings darauf hin, dass ein erhebliches Ungleichgewicht nur ein Indiz für Unfreiwilligkeit sein kann.

Zu Art. 8:

Der besondere Schutz von Kindern und Jugendlichen bei der Verarbeitung der auf sie bezogenen Daten ist der Konferenz ein besonderes Anliegen. Insofern begrüßt sie, dass sich der Verordnungsentwurf dieser Thematik annimmt und sie in einer spezifischen Regelung verankern will. Die Vorschrift sollte sich jedoch stärker an den konkreten, für diese Altersgruppe spezifischen Gefährdungen orientieren. Aus diesem Grunde sollte bei Einwilligungen auch stärker auf die Einsichtsfähigkeit des Kindes und weniger auf starre Altersgrenzen abgestellt werden.

In Art. 8 (1) sollte das Regelungsziel der Norm präzisiert werden. Es ist zu klären, ob eine Beschränkung auf Dienste der Informationsgesellschaft ausreichend ist, da es sich gemäß der Begriffsbestimmung aus der Richtlinie 98/34/EG hierbei in der Regel um gegen Entgelt erbrachte Dienste handelt, obwohl offensichtlich auch entgeltfreie Dienste erfasst werden sollen. Einer Klarstellung bedarf auch, wann einem Kind solche Dienste „direkt“ angeboten werden. Es ist ebenfalls zu klären, ob sich Art. 8 (1) ausschließlich auf solche Datenverarbeitungen bezieht, bei denen die Rechtmäßigkeit nach Art. 6 (1) lit. a) auf die Einwilligung gestützt wird oder ob bei jeder Datenverarbeitung der Einwilligungsvorbehalt der Eltern bzw. gesetzlichen Vertreter gelten soll.

Zudem ist das Verhältnis zwischen den Absätzen 1 und 2 des Art. 8 klärungsbedürftig.

Die Profilbildung (Art. 20) sollte bei Minderjährigen generell verboten sein.

Zu Art. 9:

Art. 9 soll den bedeutsamen Bereich der Zulässigkeit der Verarbeitung von besonderen Kategorien personenbezogener Daten regeln. Die Konferenz sieht hier den aus Art. 8 der RL 95/46/EG übernommenen Ansatz eines abschließenden Katalogs sensitiver Daten kritisch. Vorzugswürdig wäre es, auf den tatsächlichen Verarbeitungskontext abzustellen und den Katalog der sensitiven Daten als Regelbeispiele auszugestalten.

Die Vorgaben sind im Sinne des Wesentlichkeitsgrundsatzes in der Verordnung selbst zu treffen, die entsprechend zu ergänzen ist. Die in Art. 9 (3) enthaltene Delegationsermächtigung wird deshalb abgelehnt.

Zu Art. 10:

Das von der Verordnung hier offenbar verfolgte Regelungsziel wird in Erwägungsgrund 45 deutlich. Dort wird ausführt, dass der für die Verarbeitung Verantwortliche nicht verpflichtet sein sollte, zusätzliche Daten einzuholen, um eine betroffene Person zu bestimmen. Er sollte das Recht haben, bei der betroffenen Person, falls diese von ihrem Auskunftsrecht Gebrauch macht, weitere Informationen einzuholen, um die zu dieser Person gesuchten personenbezogenen Daten zu lokalisieren. Dies spiegelt sich im Wortlaut des Art. 10 jedoch nicht wider. Dieser sollte deshalb so gefasst werden, dass sich der Erwägungsgrund 45 im Regelungstext selbst niederschlägt.

Kapitel III – Rechte der betroffenen Person

Zu Art. 11:

Der Vorschlag wird grundsätzlich begrüßt. Es sollte jedoch in Abs. 1 klargestellt werden, was der für die Verarbeitung Verantwortliche (konkret) leisten muss.

Zu Art. 12:

Aus Gründen der Bestimmtheit und wegen der Erheblichkeit der hier zu treffenden Konkretisierungen sollte unmittelbar in der Verordnung selbst dargelegt werden, unter welchen Voraussetzungen ein Antrag offenkundig unverhältnismäßig ist, insbesondere auch, wann eine missbräuchliche Häufung von Betroffenenrechten vorliegt (vgl. Art. 12 (4)). Die Befugnis der Kommission zu delegierten Rechtsakten in Art. 12 (5) sollte daher entfallen.

Die Konferenz spricht sich gegen eine Missbrauchsgebühr aus. Aus ihrer Sicht reicht es aus, dass in Missbrauchsfällen das jeweilige Betroffenenrecht nicht in Anspruch genommen werden kann. Sofern an der Missbrauchsgebühr festgehalten wird, muss vermieden werden, dass sich Betroffene völlig unerwartet Gebührenforderungen gegenübersehen. Deshalb sollte der für die Verarbeitung Verantwortliche die betroffene Person im konkreten Einzelfall darüber informieren müssen, wenn er die Ausübung der Betroffenenrechte für offenkundig unverhältnismäßig erachtet und aus diesem Grund ein Entgelt verlangen will. Die Höhe des Entgelts muss verhältnismäßig sein und sich an dem tatsächlichen Aufwand bemessen.

Art. 12 sollte um das Erfordernis sicherer Übertragungswege für personenbezogene Daten nach dem Stand der Technik ergänzt werden.

Zu Art. 13:

Die Regelung wird grundsätzlich begrüßt. Die Nachberichtspflicht gemäß Art. 13 sollte sich jedoch auch auf Widersprüche nach Art. 19 erstrecken.

Zu Art. 14:

In der Verordnung ist unter Art. 14 (4) lit. b) klarzustellen, was unter einer „angemessenen“ Frist zu verstehen ist. Ferner ist zu prüfen, ob anstatt dieser nicht ein „unverzügliches Handeln“ geboten ist. Benachrichtigungen erst bei Datenübermittlungen dürfen nur bei Datenverarbeitern möglich sein, die geschäftsmäßig Daten zur Übermittlung vorhalten (u. a. Auskunfteien, Adresshandel, Detekteien).

Zu Art. 15:

In Art. 15 (1) lit. g) sollte die Einschränkung auf die (lediglich) „verfügbaren“ Herkunftsdaten gestrichen werden, da eine Angabe über die Herkunft personenbezogener Daten stets geboten ist und diese nicht verschleiert werden darf.

Die Aufklärungspflicht nach Art. 15 (1) lit. h) sollte auf die „Bedeutung und Tragweite“ der Verarbeitung erstreckt werden. Ein (ausdrücklicher) Hinweis auf besondere Risiken bei der Profilbildung, Auskunfteien oder dem Scoring ist aufzunehmen.

Es muss zudem sichergestellt werden, dass für eine Mitteilung in elektronischer Form gemäß Art. 15 (2) nur sichere Übertragungswege nach dem Stand der Technik in Betracht kommen.

Zu Art. 16:

Es ist klarzustellen, ob unter einem Korrigendum eine Richtigstellung zu verstehen ist. Zudem regelt die Vorschrift nicht, wie zu verfahren ist, wenn sich die Unrichtigkeit oder Richtigkeit der Daten nicht beweisen lässt, bzw. wer die Beweislast trägt. Dieser Punkt sollte ergänzt werden. Denkbar wäre z. B. eine Verpflichtung, diese Daten im Sinne von Art. 17 (4) zu beschränken.

Zu Art. 17:

In Art. 17 (2) sollte eine Pflicht der Dritten zur Löschung der Daten analog Art. 17 (1) geregelt werden. Insbesondere sollte klargestellt werden, ob die Regelung auf den Bereich des Internets beschränkt ist und ob sie nach Maßgabe des Lindqvist-Urteils auch für Privatpersonen gilt.

Das Verhältnis der „umgehenden“ Löschungspflicht in Art. 17 (3) zu der in Art. 12 (2) geregelten Monatsfrist ist klärungsbedürftig. Es erscheint jedenfalls nicht sinnvoll,

wenn der für die Verarbeitung Verantwortliche zwar einerseits die personenbezogenen Daten umgehend löschen müsste, andererseits aber für die Benachrichtigung des Betroffenen über die Löschung einen Monat Zeit hätte.

Die Formulierung in Art. 17 (2) „alle vertretbaren Schritte“ bedarf insbesondere aus technischer Sicht der Präzisierung.

Die Beschränkung nach Art. 17 (4) sollte verpflichtend vorgegeben werden.

Zu Art. 18:

Die Konferenz unterstützt die Einführung eines Rechts auf Datenportabilität in Art. 18 (1). Dieses Recht sollte aber nicht davon abhängen, ob der für die Verarbeitung Verantwortliche seine Verarbeitungen in einem gängigen Format tätigt. Vielmehr sollte durch die Streichung des Wortes „gängige“ eine allgemeine Konvertierungspflicht geregelt werden. Es ist klärungsbedürftig, ob Art. 18 (1) auch den öffentlichen Bereich erfasst.

Die in Art. 18 (2) verwandten Begriffe des Zur-Verfügung-Stellens und des Entziehens von Daten sollten in der Verordnung definiert werden, falls auf diese Begriffe nicht in Gänze verzichtet werden kann.

Zu Art. 19:

In Art. 19 (1) sollte der Begriff „schutzwürdige Gründe“ durch „berechtigte Interessen“ ersetzt werden. Es sollte zudem geprüft werden, ab wann und wie der Nachweis für das überwiegende Verarbeitungsinteresse des für die Verarbeitung Verantwortlichen als erbracht gelten soll.

Kommerzielle Werbung sollte, wie bereits zu Art. 6 angemerkt, grundsätzlich nur mit Einwilligung des Betroffenen gestattet sein. Art. 19 (2) sollte deshalb entsprechend angepasst werden. Die Konferenz empfiehlt zudem, den Begriff „unentgeltlich“ in Art. 19 (2) zu streichen, da sich die Unentgeltlichkeit bereits aus Art. 12 (4) Satz 1 ergibt. Andernfalls wäre im Einzelnen darzulegen, weshalb welche Maßnahmen nach Kapitel III jeweils entgeltfrei sein sollen oder nicht.

Unter Hinweis zu den Anmerkungen zu Art. 13 sollte auch Art. 19 entsprechend angepasst werden.

Zu Art. 20:

Die Konferenz unterstützt grundsätzlich die Aufnahme einer speziellen Regelung zur Profilbildung. Allerdings hält sie den Vorschlag für stark ergänzungsbedürftig.

Schon die Profilbildung selbst (z. B. in sozialen Netzwerken, beim Scoring und bei Auskunfteien) greift in erheblicher Weise in das Grundrecht auf Datenschutz ein und ist deshalb regelungsbedürftig.

Art. 20 (1) sollte zudem auf jede – auch nur teilweise automatisierte – systematische Verarbeitung zur Profilbildung Anwendung finden und daher das Wort „rein“ gestrichen werden.

Bei Minderjährigen (Art. 8) sollte die Profilbildung generell verboten sein.

Die Verarbeitung besonderer Kategorien personenbezogener Daten wird wegen ihrer besonderen Sensitivität äußerst kritisch gesehen. Dort, wo sensitive Daten für eine Prognose unerlässlich sind, wie z.B. bei der Risikobeurteilung im Krankenversicherungsbereich, müssen enge, branchenspezifische Ausnahmetatbestände eingeführt werden, die an dem Grundsatz der Erforderlichkeit auszurichten sind. In Art. 20 (3) ist zudem klarzustellen, ob die Voraussetzungen des Art. 9 kumulativ gelten sollen. Dies würde sicherstellen, dass die Verwendung besonderer Kategorien personenbezogener Daten materiellrechtlichen Beschränkungen unterliegt und sie nicht beliebig in Profilbildungen einfließen können.

Im Hinblick auf die besonderen Risiken der Bildung von Profilen, die auf einzelne Personen bezogen werden können, ist die Wiederherstellung eines Personenbezugs bei unter Pseudonym oder einem technischen Identifikationsmerkmal geführten Profilen grundsätzlich zu untersagen.

Wegen der Erheblichkeit der in Art. 20 (5) zu treffenden Konkretisierungen und aus Gründen der Bestimmtheit sollte eine entsprechende Reglung in die Verordnung aufgenommen und die Befugnis der Kommission zu delegierten Rechtsakten gestrichen werden.

Zu Art. 21:

Statt einer Öffnungsklausel für den nationalen Gesetzgeber nur zur Beschränkung der Rechte Betroffener (Art. 21) sollten weiter reichende Betroffenenrechte gewährt werden dürfen. Dies gilt ungeachtet der bereits zu Art. 6 geforderten generellen Öffnungsklausel für den öffentlichen Bereich.

Art. 21 (1) lit. c) sollte gestrichen werden. Es ist nicht nachvollziehbar, weshalb die bisher in der RL 95/46/EG nicht vorgesehene Beschränkung in Bezug auf den Schutz sonstiger öffentlicher Interessen geboten sein soll. Zumindest sollten die Anforderungen an die Beschränkung strikter formuliert werden, damit die Betroffenenrechte nicht leerlaufen.

Kapitel IV – Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter

Ein zukunftsfähiger Datenschutz umfasst technische und organisatorische Maßnahmen, die Datenschutz und Datensicherheit angemessen berücksichtigen. Um dies zu gewährleisten, sind die elementaren Datenschutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit als Zielvorgaben für technische und organisatorische Maßnahmen in die Bestimmungen der Art. 23 ff. aufzunehmen.

Zu Art. 22:

Um sicherzustellen, dass eine Verarbeitung personenbezogener Daten erst dann erfolgt, wenn die geeigneten Strategien und Maßnahmen auch umgesetzt sind, sollte Art. 22 (1) wie folgt formuliert werden: „Der für die Ver-

arbeitung Verantwortliche stellt durch *die Umsetzung* geeigneter Strategien und Maßnahmen sicher, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden und er den Nachweis dafür erbringen kann."

Art. 22 (3) sollte dahingehend ergänzt werden, dass die Entscheidung über Konsequenzen aus der Überprüfung der in den Absätzen 1 und 2 genannten Maßnahmen nicht dem Prüfer, sondern weiterhin dem für die Verarbeitung Verantwortlichen obliegt.

Zu Art. 23:

In Art. 23 (1) könnte die ausdrückliche Bezugnahme auf die Berücksichtigung der Implementierungskosten zu einem Einfallstor für das Unterlassen von Maßnahmen zur datenschutzfreundlichen Technikgestaltung werden. Zumindest müssen – wie in Art. 30 (1) – die Implementierungskosten technisch-organisatorischer Maßnahmen in ein angemessenes Verhältnis zum konkreten Gefahrenpotential der Datenverarbeitung gesetzt werden, um eine Relation zwischen Kosten und Eingriffstiefe in das Recht auf informationelle Selbstbestimmung herzustellen.

Art. 23 (2) sollte präzisiert und um Kriterien und Anforderungen in Bezug auf die zu treffenden Maßnahmen und Verfahren ergänzt werden. Hierbei sind insbesondere Anonymisierung und Pseudonymisierung nach dem Stand der Technik zu fordern, sofern dies nicht bereits in Art. 5 geregelt wird.

Es sollte klargestellt werden, dass Datenschutz durch Technik auch die Auswahl und Gestaltung von Datenverarbeitungssystemen betrifft.

Die Grundeinstellungen von Produkten und Diensten sind so zu gestalten, dass so wenig personenbezogene Daten wie möglich erhoben oder verarbeitet werden und bereits ohne Zutun der Nutzer eine datenschutzfreundliche Nutzung sichergestellt wird.

Die Regelung sollte ausdrücklich auch für Verhaltensbeobachtungen („Tracking") im Internet durch den für die Verarbeitung Verantwortlichen oder durch Dritte gelten.

Satz 2 des Art. 23 (2) sollte wie folgt lauten: „Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich *nur den von der betroffenen Person zu bestimmenden Personen* zugänglich gemacht werden." Damit soll erreicht werden, dass die betroffene Person den Personenkreis selbst bestimmt, dem ihre personenbezogenen Daten zugänglich gemacht werden dürfen, und der für die Verarbeitung Verantwortliche hierfür die entsprechenden Vorkehrungen zu treffen hat.

Zu Art. 24:

In Art. 24 sollte im Text ausdrücklich ergänzt werden, dass sich die betroffene Person zur Wahrnehmung ihrer Rechte an jeden der für die gemeinsame Verarbeitung Verantwortlichen wenden kann.

Zu Art. 25:

Die Konferenz schlägt vor, auch in den Fällen des Art. 25 (2) lit. a) einen Vertreter zu bestellen. Art. 25 (2) lit. a) sollte daher gestrichen werden.

Der in Art. 25 (2) lit. b) geplante Verzicht bei Unternehmen mit weniger als 250 Mitarbeitern auf die Benennung eines Vertreters, der umfassend in die Rechtsstellung des Verantwortlichen und dessen Pflichten eintreten sollte, stellt eine Ausnahme dar, die nicht nachvollziehbar ist. Die Konferenz schlägt daher vor, diese Ausnahmeregelung ebenfalls zu streichen. Diese Klausel eröffnet weitgehende Umgehungsmöglichkeiten, da nicht geprüft werden kann, wie viele Beschäftigte bei einem nicht in der Union niedergelassenen Unternehmen tatsächlich tätig sind.

Zu Art. 26:

Der in Art. 26 (2) geregelte Mindestinhalt eines Vertrages oder Rechtsaktes zur Auftragsdatenverarbeitung sollte die wesentlichen Aspekte enthalten und daher um die Angabe von Gegenstand und Dauer des Auftrags sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung, der Art der Daten und den Kreis der Betroffenen ergänzt werden. In lit. a) sollte durch Streichung des 2. Halbsatzes sichergestellt werden, dass der Auftragsverarbeiter in jedem Fall ausschließlich auf Weisung des für die Verarbeitung Verantwortlichen tätig wird und nicht nur in besonderen Fällen, in denen die Übermittlung der Daten nicht zulässig ist.

Der Schutz der betroffenen Person erfordert die Klarstellung, dass sie sich bei gemeinsam für die Verarbeitung Verantwortlichen gemäß Art. 24 sowohl an den für die Verarbeitung Verantwortlichen als auch an den Auftragsverarbeiter wenden kann.

Eine wirksame Kontrolle des Auftragsverarbeiters kann nur umfassend erfolgen, wenn dem für die Verarbeitung Verantwortlichen in Art. 26 (2) auch ein Kontrollrecht, beispielsweise durch einen Treuhänder, eingeräumt wird und den Auftragsverarbeiter entsprechende Mitwirkungspflichten treffen. Dies gilt auch für etwaige Unterauftragsverhältnisse.

Die Kriterien und Anforderungen für die Verantwortlichkeiten, Pflichten und Aufgaben des Auftragsverarbeiters sind wesentliche Fragen, die letztlich auch die Zulässigkeit der Auftragsdatenverarbeitung insgesamt berühren. Insbesondere wäre etwa die Einführung und nähere Ausgestaltung eines Konzernprivilegs eine wesentliche Frage, die im Sinne von Art. 290 AEUV – soweit in den Absätzen 1 bis 4 nicht ohnehin bereits geschehen – in der Verordnung selbst geregelt werden sollte. Die Konferenz sieht daher die in Art. 26 (5) vorgesehene Ermächtigung zu delegierten Rechtsakten kritisch.

Zu Art. 28:

In Art. 28 sollte geregelt werden, dass die Dokumentation grundsätzlich vor Aufnahme der Verarbeitung personenbezogener Daten zu erstellen ist. Zudem sollte der für die

Verarbeitung Verantwortliche verpflichtet werden, die Dokumentation dem Datenschutzbeauftragten (soweit vorhanden) zur Verfügung zu stellen.

Die zeitliche Befristung einer Verarbeitung personenbezogener Daten ist im Sinne des Erforderlichkeitsprinzips ein wesentlicher Grundsatz. Art. 28 (2) lit. g) sollte daher in „eine *konkrete* Angabe der Fristen für die Löschung der verschiedenen Datenkategorien“ geändert werden.

Zu Art. 30 bis 32 allgemein:

Verfahren mit Personenbezug müssen durch technische und organisatorische Maßnahmen, ausgerichtet an den Datenschutzzielen, geschützt werden. Dieser Grundsatz ist in der Verordnung selbst zu verankern. Die Konferenz verweist in diesem Zusammenhang auf Vorbemerkungen zu Kapitel IV. Im Übrigen sollten Aufzählungen technischer und organisatorischer Maßnahmen durch entsprechende Verweise ersetzt werden.

Zu Art. 30:

Die in Art. 30 (1) geforderten angemessenen technischen und organisatorischen Maßnahmen können nur durch eine vorab und kontinuierlich durchgeführte Risikobewertung bzw. Risikoanalyse gewährleistet werden. IT-Sicherheit erfordert in diesem Sinne ein konzeptionelles Herangehen sowie die Etablierung von IT-Sicherheits- und Datenschutzmanagementsystemen. Art. 30 (1) sollte daher durch die Forderung nach einem Sicherheitskonzept ergänzt werden, welches Teil der Verfahrensdokumentation gemäß Art. 28 (2) lit. h) werden muss.

Wie in Art. 23 (1) sollte auch in Art. 30 (1) die Bezugnahme auf Implementierungskosten gestrichen werden.

Zu Art. 32:

Die in Art. 32 (3) geforderte Verschlüsselung personenbezogener Daten muss dahingehend präzisiert werden, dass sie durch Verfahren nach dem Stand der Technik erfolgen muss.

Zu Art. 33:

Eine Regelung der Datenschutz-Folgenabschätzung (Art. 33), die nachhaltig dem Schutz personenbezogener Daten dienen soll, muss die elementaren Datenschutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit umsetzen, um vollumfänglich Risiken und dafür angemessene Maßnahmen identifizieren zu können. Die Ergebnisse sind in einem regelmäßigen Monitoring zu überprüfen.

Die Begriffe der Datenschutz-Folgenabschätzung und der Vorab-Genehmigung bzw. -Zurateziehung sollten voneinander abgegrenzt werden, da sich diese wechselseitig nicht ersetzen können.

Da jede der in Art. 33 (2) lit. a) genannten Auswertungen bereits erhebliche Risiken mit sich bringt, sollten die Worte „systematische und umfassende“ entfallen.

Die Konferenz schlägt vor, in Art. 33 (2) lit. c) das Wort „weiträumig“ zu streichen, da der Begriff zu unbestimmt ist und aus Sicht der betroffenen Person kein Unterschied besteht, ob die Überwachung weiträumig oder kleinräumig stattfindet.

In Art. 33 (2) lit. d) sollte die Durchführung einer Datenschutz-Folgenabschätzung für die Verarbeitung personenbezogener Daten aus Dateien, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten, nicht vom Umfang der Datei abhängen, sondern in jedem Fall erfolgen. Das Wort „umfangreich“ sollte daher gestrichen werden.

Für die Datenschutz-Folgenabschätzung muss auch zwingend in Art. 33 (3) eine Dokumentationspflicht aufgenommen werden.

Schließlich sollte Art. 33 um einen zusätzlichen Absatz ergänzt werden, der das Verbot der Datenverarbeitung bei unangemessen hohen Eingriffen in die Rechte der Betroffenen fordert. Grundsätzlich sollten Verfahren ausgewählt werden, die den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung mit sich bringen.

Zu Art. 34:

Die Konferenz hält den Vorschlag, dass der interne Datenschutzbeauftragte die Beantragung einer vorherigen Genehmigung bzw. Zurateziehung nach Art. 37 (1) lit. f) nur überwachen soll, für nicht ausreichend. Zur Entlastung der Aufsichtsbehörden und zur Stärkung des betrieblichen Datenschutzes sollte ihm diese Aufgabe komplett übertragen werden können. Deutschland hat mit der Durchführung der Vorabkontrolle durch die internen Datenschutzbeauftragten gute Erfahrungen gemacht.

Zu Art. 35:

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv.

Es sollte eine Frist geregelt werden, innerhalb derer der Datenschutzbeauftragte nach Aufnahme der Daten verarbeitenden Tätigkeit zu bestellen ist. Die Konferenz schlägt hierfür eine Frist von einem Monat vor.

Die Konferenz bedauert, dass in Art. 35 (1) lit. b) eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten vorgesehen ist. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Art. 35 (1) lit. c) sollte dahingehend geändert werden, dass bei jeder risikobehafteten Datenverarbeitung (z. B. Auskunfteien, Detekteien, Callcenter, Lettershops etc.) unabhängig von der Mitarbeiterzahl eine Bestellungspflicht für einen Datenschutzbeauftragten besteht. Das Gleiche gilt für Unternehmen, bei denen eine Datenschutzfolgenabschätzung erforderlich ist. Die Anknüp-

fung an die „regelmäßige und systematische Beobachtung von betroffenen Personen“ ist insoweit nicht ausreichend.

Durch die in Art. 35 (7) geregelte Möglichkeit der Befristung der Amtszeit des Datenschutzbeauftragten kann die Unabhängigkeit beeinträchtigt werden. Die Amtszeit des internen Datenschutzbeauftragten sollte daher nicht befristet werden und das dem Amt zugrunde liegende Arbeitsverhältnis nur aus wichtigem Grund kündbar sein. Die Amtszeit von externen Datenschutzbeauftragten sollte mindestens vier Jahre betragen.

Art. 35 (11) ist zu streichen. Die Fälle, in denen unabhängig von der Mitarbeiterzahl ein Datenschutzbeauftragter zu bestellen ist, betreffen eine wesentliche Frage und sind deshalb in der Verordnung selbst zu regeln.

Zu Art. 36:

Der Datenschutzbeauftragte sollte nicht nur ein unmittelbares Vorspracherecht gegenüber der Leitung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters haben, sondern dieser – als Ausdruck seiner Unabhängigkeit – unmittelbar unterstellt sein. Außerdem sollte für interne Datenschutzbeauftragte ein wirksamer arbeitsrechtlicher Kündigungsschutz sowie die Aufnahme eines Benachteiligungsverbots vorgesehen werden, um seine Unabhängigkeit besser zu sichern.

In Art. 36 (3) ist das Recht des Datenschutzbeauftragten auf Fort- und Weiterbildung sowie die Kostenübernahme hierfür zu normieren. Zudem sind Regelungen zur Verschwiegenheit des Datenschutzbeauftragten sowie zum Zeugnisverweigerungsrecht aufzunehmen.

Zu Art. 37:

Die Aufgaben des Datenschutzbeauftragten sind in der deutschen Sprachfassung missverständlich formuliert. So wird sprachlich nicht hinreichend deutlich, ob der Datenschutzbeauftragte beispielsweise selbst die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 31 vornehmen muss oder diese Meldung nur zu überwachen hat (Art. 37 (1) lit. e).

In diesem Zusammenhang sollte auch klargestellt werden, dass die Aufgaben des Datenschutzbeauftragten den für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter nicht von seinen Pflichten entbinden bzw., dass keine Möglichkeit zur Exkulpation bei Nicht- oder Schlechterfüllung seitens des Datenschutzbeauftragten besteht.

Zu Art. 38 und Art. 39:

In Art. 39 (2) sollten die wesentlichen Regelungstatbestände einer Zertifizierung und der Vergabe eines Siegels und Zeichens direkt aufgenommen und nicht an die Kommission delegiert werden. Die Zertifizierungs- und Vergabekriterien sind insbesondere an den Grundsätzen der Verarbeitung personenbezogener Daten in Art. 5, der Rechtmäßigkeit der Datenverarbeitung gemäß Art. 6, der Betroffenenrechte und an den Datenschutzzielen in Art. 30 nach Maßgabe der Verordnung auszurichten.

Zertifizierungs-, Vergabe- und Widerrufsverfahren müssen den Anforderungen des Grundsatzes der Transparenz hinsichtlich der Kriterien, des Verfahrens und der wesentlichen Evaluierungsergebnisse genügen. Die Unabhängigkeit und Fachkunde der Zertifizierungs- und Vergabestellen und der Evaluatoren sind zu gewährleisten.

Eine datenschutzspezifische Zertifizierung gemäß Art. 39 (1) beinhaltet stets auch eine Bewertung der IT-Sicherheit. Diese sollte sich an europäischen und internationalen Standards orientieren und die Datenschutzziele Nichtverkettbarkeit, Transparenz und Intervenierbarkeit aus Betroffenensicht einbeziehen. Ein entsprechender Zusatz – unter Einbeziehung des Ergänzungsvorschlags der Konferenz zu Kapitel IV (elementare Datenschutzziele) – ist daher vorzusehen.

Zertifizierungen sind zeitlich zu befristen. Eine Rücknahme eines Zertifikates bei gravierenden Mängeln muss auch vor Fristablauf möglich sein.

Bei der Ausgestaltung der Verhaltensregeln und Zertifizierungsverfahren ist der Europäische Datenschutzausschuss zu beteiligen.

Kapitel V – Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen

Zu Art. 41:

Die Kommission sollte bei der Angemessenheitsprüfung nach Art. 41 (2) stets auch die Stellungnahme des Europäischen Datenschutzausschusses einholen und berücksichtigen müssen. Im Zusammenhang mit Art. 41 (6) muss klargestellt werden, dass in den Fällen, in denen die Kommission durch Beschluss feststellt, dass kein angemessenes Datenschutz-Niveau gegeben ist, die Datenübermittlung automatisch verboten ist, so dass es keines weiteren Umsetzungsaktes durch die Aufsichtsbehörde bedarf.

Ferner muss klargestellt werden, ob die Formulierung „unbeschadet der Art. 42 - 44“ bedeutet, dass bei einem Negativ-Beschluss gleichwohl Datenübermittlungen nach allen diesen Vorschriften vorgenommen werden können. Insbesondere die Vorschriften des Art. 41 (6) und des Art. 42 (1) erscheinen in dieser Frage widersprüchlich.

Zu Art. 42:

Da die Genehmigungsfähigkeit der Datenflüsse von vornherein fraglich ist, wenn keine geeigneten Garantien vorliegen, ist der Anwendungsbereich der Regelung des Art. 42 (5) unklar (Auffangtatbestand?). Deshalb sollte der Absatz 5 (bis auf den letzten Satz) entweder gestrichen oder um die genehmigungspflichtigen Fälle präzisiert werden.

Zu Art. 43:

In Art. 43 (1) sollte die Rechtsfolge der Genehmigung der BCR durch die Aufsichtsbehörde explizit aufgenommen

werden, z. B. durch folgenden Satz 2: „In diesem Fall gilt die Genehmigung in der gesamten EU."

Die in Art. 43 (3) genannten Kriterien und Anforderungen an BCR sollten nicht von der Kommission, sondern ausschließlich von dem Europäischen Datenschutzausschuss festgelegt werden.

Zu Art. 44:

Es sollte eine Klausel zum Umgang mit Aufforderungen zur Datenübermittlung durch Gerichte oder Behörden aus Drittstaaten eingefügt werden. Eine (interne) Vorversion des Vorschlags der Kommission beinhaltete eine solche explizite Klausel. Derartige Aufforderungen sollten hiernach grundsätzlich unbeachtlich sein und unter Genehmigungsvorbehalt durch zuständige nationale Behörden stehen. Die Konferenz fordert, dass Datentransfers grundsätzlich nur auf der Basis gegenseitiger Rechtshilfeabkommen (Mutual Legal Assistance Treaties, MLATs) zulässig sind.

In Art. 44 (1) müssen bei sensitiven Daten zusätzlich zur informierten Einwilligung geeignete Garantien vorgesehen werden, weil sonst zwar die Datenübermittlung nach Art. 44 (1) lit. a) legitimiert ist, die Datenverarbeitung im Drittland aber keinen besonderen Anforderungen unterliegt. Das Wort „zugestimmt" sollte durch „eingewilligt" (entsprechend Art. 7) ersetzt werden.

Art. 44 (1) lit. d) darf nicht für den Datenaustausch „zwischen für die Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten zuständigen Behörden" gelten, wie Erwägungsgrund 87 es vorsieht. Dies würde im Widerspruch zum sachlichen Anwendungsbereich der Verordnung nach Art. 2 (2) lit. e) stehen. Deshalb sollten diese Fälle in Erwägungsgrund 87 gestrichen werden.

Der Anwendungsbereich des Art. 44 (1) lit. h) ist unklar. Insbesondere ist fraglich, ob es sich um einen Auffangtatbestand handeln soll. Die Regelung muss konkretisiert werden. In jedem Fall muss eine Abwägung der berechtigten Interessen des für die Verarbeitung Verantwortlichen mit den schutzwürdigen Interessen der betroffenen Person vorgesehen werden.

Die Anwendungsbereiche der Art. 44 (3), (4), (6) und (7) sind unklar und müssen konkretisiert werden.

Zu Art. 45:

Art. 45 (2) sollte dahingehend ergänzt werden, dass neben der Kommission auch die Aufsichtsbehörden die Förderung der Beziehungen zu Drittländern betreiben können, und zwar auch – und gerade – zu Drittländern ohne angemessenen Datenschutz.

Kapitel VI – Unabhängige Aufsichtsbehörden

Zu Art. 47 und 48:

Die Regelung zur völligen Unabhängigkeit der Aufsichtsbehörden in Art. 47 (1) ist grundsätzlich positiv zu werten. Es sollte allerdings überdacht werden, wie die Unabhängigkeit der Aufsichtsbehörden auch bei der Zusammenarbeit mit den anderen Aufsichtsbehörden, insbesondere im Rahmen des Kohärenzverfahrens, garantiert werden kann (Art. 46 (1) Satz 2).

Zu Art. 51:

Die Regelung des „One-Stop-Shops" gemäß Art. 51 (2) ist nur praktikabel, wenn sie nicht im Sinne einer ausschließlichen Zuständigkeit, sondern im Sinne einer „Federführung" der Aufsichtsbehörde des Mitgliedstaates der Hauptniederlassung zu verstehen ist, falls der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter über mehrere Niederlassungen innerhalb der EU verfügt.

Der One-Stop-Shop-Grundsatz sollte dann nicht gelten, wenn es sich um einen Sachverhalt handelt, der im Schwerpunkt die Anwendung nationalen Datenschutzrechts eines Mitgliedstaats im Sinne des Kapitels IX betrifft, so dass es hier bei der allgemeinen Zuständigkeit nach Art. 51 (1) bleiben sollte.

Mangels eines einheitlichen Verwaltungsverfahrens-, -prozess- und -vollstreckungsrechts kann die Aufsichtsbehörde in anderen Mitgliedsstaaten grundsätzlich nicht selbst tätig werden. Derartige hoheitliche Maßnahmen sollten daher nur im Wege der Amtshilfe möglich sein. Diese Klarstellung ist auch im Hinblick auf Art. 55 (1) und (2) sowie Art. 63 notwendig.

Es sollte überprüft werden, ob die sich aus Erwägungsgrund 19 ergebende Einbeziehung rechtlich selbständiger Tochtergesellschaften in die One-Stop-Shop-Regelung tatsächlich erforderlich ist. Diese könnten aufgrund ihrer rechtlich selbständigen Handlungsfähigkeit auch getrennt betrachtet werden. Sofern eine Einbeziehung für erforderlich gehalten wird, sollte dies einschließlich einer Definition des Begriffs Tochtergesellschaft unmittelbar im Verordnungstext und nicht nur in einem Erwägungsgrund geregelt werden.

Zu Art. 52:

Ausgehend von dem Vorschlag, eine Regelung zu „Erziehung und Bildung" aufzunehmen (s.o.), sollten auch die Aufgaben der Aufsichtsbehörden entsprechend erweitert werden. Die Konferenz schlägt für Art. 52 (2) daher folgenden Wortlaut vor:

„Jede Aufsichtsbehörde fördert die Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten und über geeignete Maßnahmen zum eigenen Schutz. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder."

Die in Art. 52 (6) vorgesehene Missbrauchsgebühr sollte gestrichen werden, da nach den Erfahrungen der deutschen Aufsichtsbehörden derartige Beschwerden äußerst selten vorkommen, so dass – auch im Hinblick auf den Verwaltungsaufwand – eine Erhebung von Gebühren unverhältnismäßig wäre.

Zu Art. 53:

Die Konferenz weist darauf hin, dass auch die EU-rechtlich gebotene Unabhängigkeit der Aufsichtsbehörden nur im Rahmen der jeweiligen verfassungsrechtlichen Staatsstrukturprinzipien bestehen kann (Art. 4 Abs.2 EUV). Dies gilt insbesondere für deren Sanktionsbefugnisse und Sanktionspflichten.

Art. 53 (2) sollte auch den anlasslosen Zugang zu Geschäfts- und Diensträumen umfassen. Unklar ist, was in Art. 53 (3) mit der Formulierung, dass Verstöße gegen die Verordnung den Justizbehörden zur Kenntnis zu bringen sind, gemeint ist.

Zu Art. 54:

Art. 54 sollte gestrichen werden. Hilfsweise wird angeregt, die Aufsichtsbehörden lediglich zur Erstellung eines regelmäßigen Jahresberichts zu verpflichten, der der Öffentlichkeit (und damit automatisch dem nationalen Parlament, der Kommission, dem Europäischem Datenschutzausschuss u.a.) zugänglich gemacht werden muss.

Kapitel VII – Zusammenarbeit und Kohärenz

Zu Art. 55 und Art. 56:

In dem in Art. 55, 56 geregelten Verfahren der Amtshilfe und der Zusammenarbeit sollten die betroffenen Behörden grundsätzlich sowohl im Hinblick auf die rechtliche Bewertung eines Sachverhalts als auch hinsichtlich erforderlicher aufsichtsbehördlicher Maßnahmen einvernehmlich zusammenwirken. Dies gilt insbesondere dann, wenn es sich um eine Maßnahme der federführenden Behörde i.S.d. Art. 51 (2) handelt, die von der Aufsichtsbehörde eines anderen Mitgliedstaates durchzuführen ist. Bei Divergenzen im Hinblick auf die Bewertung eines Sachverhalts oder die Vornahme aufsichtsbehördlicher Maßnahmen sollte der Europäische Datenschutzausschuss von den beteiligten Behörden angerufen werden können.

Die Gründe, aus denen Amtshilfeersuchen nach Art. 55 (4) abgelehnt werden können, sind zu eng. Sie sollten auch zwingende Hinderungsgründe nach nationalem Recht (z. B. im Falle des Sozialgeheimnisses) umfassen.

In Fällen, in denen der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter zwar über mehrere Niederlassungen innerhalb der EU verfügt, es sich aber um einen rein nationalen Sachverhalt handelt, sollte es aus Gründen der Verfahrensökonomie ebenfalls bei der allgemeine Zuständigkeitsregelung des Art. 51 (1) bleiben. Anderenfalls würde die Abstimmung mit der Hauptniederlassungsbehörde einen unverhältnismäßigen Verfahrensaufwand bedeuten. In diesen Fällen sind die Voraussetzungen der Art. 55, 56 (Betroffenheit von Personen in mehreren Mitgliedstaaten) nicht erfüllt.

Unbestimmt ist, was unter „Vorkehrungen für eine wirksame Zusammenarbeit“ in Art. 55 (1) und „praktische Aspekte spezifischer Kooperationsmaßnahmen“ in Art. 56 (4) zu verstehen ist. Die verfahrenstechnischen Aspekte der Amtshilfe und der Zusammenarbeit sollten in Art. 55, 56 klar formuliert werden.

Es muss sichergestellt sein, dass hinreichende Mittel bereitstehen, um die praktische Arbeit im Rahmen der Amtshilfeleistungen zu erleichtern (insbesondere im Hinblick auf Übersetzungsleistungen, ggfs. durch das Sekretariat des Datenschutzausschusses).

Die Ermächtigung der Kommission zum Erlass von Durchführungsrechtsakten betreffend „Form und Verfahren der Amtshilfe (...)“ in Art. 55 (10) sollte präzisiert und beschränkt werden. Das Verfahren der Amtshilfe sollte in der Verordnung, die Form der Amtshilfe und die Ausgestaltung des elektronischen Informationsaustausches im Sinne einer Standardisierung hingegen in einem Durchführungsrechtsakt geregelt werden.

Zu Art. 58:

Im Hinblick auf Art. 58 (2) lit. a) sollte klargestellt werden, ob hiervon ausschließlich der Fall des Art. 3 (2) lit. a), b) umfasst ist, oder ob auch Fälle ohne Drittlandbezug dem Kohärenzverfahren unterfallen sollen. Ansonsten würden unübersehbar viele Fälle der Kohärenz unterfallen (z. B. Versandhandel innerhalb der EU).

Zu Art. 59 – Art. 63:

Die Kompetenzen der Kommission im Verhältnis zum unabhängigen Datenschutzausschuss sowie in Bezug auf das Kohärenzverfahren (Art. 59 – 63) sind abzulehnen. Dies gilt insbesondere im Hinblick auf die umfassenden Informationspflichten des Ausschusses gegenüber der Kommission und die Befugnis der Kommission zur Aufforderung der Aussetzung aufsichtsbehördlicher Maßnahmen. Gleiches gilt hinsichtlich der Ermächtigung der Kommission zum Erlass von Durchführungsrechtsakten über die „ordnungsgemäße Anwendung“ der Verordnung aus Anlass eines aufsichtsbehördlichen Einzelfalles und von „sofort geltenden Durchführungsrechtsakten“ in Fällen „äußerster Dringlichkeit“. Diese Kompetenzen der Kommission sind mit Art. 8 (3) Grundrechtecharta und 16 (2) Satz 2 AEUV nicht vereinbar, weil die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. Auf der Ebene der Mitgliedstaaten soll die Datenschutzkontrolle völlig unabhängig von jeglichem Einfluss erfolgen. Daher ist es widersprüchlich, wenn für die Kommission mit ihren unterschiedlichsten Aufgaben, auch solchen, die in einem Spannungsverhältnis zum Datenschutz stehen, jene Maßstäbe keine Geltung haben sollen.

Über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, sollte als Folge der Unabhängigkeit der Aufsichtsbehörden – statt der Kommission – ausschließlich der Datenschutzausschuss entscheiden. Im Hinblick auf den personellen, sächlichen und zeitlichen mit dem Kohärenzverfahren verbundenen Aufwand sollte dessen Anwendungsbereich beschränkt werden. Es wird wesentlich im Interesse der Funktionsfähigkeit des Kohärenzverfahrens und eines europaweit wirksamen Datenschutzes darauf ankommen, entsprechende Fallgruppen

zu definieren. Nicht alle datenschutzrechtlichen Fragen, die auch in anderen Mitgliedstaaten der EU auftauchen können, bedürfen einer Behandlung im Kohärenzverfahren. Für dieses eignen sich insbesondere:

– Fragen des Drittstaatentransfers
– BCR mit mitgliedstaatenübergreifendem Bezug
– Konstellationen, in denen unterschiedliche Auffassungen zwischen einer nach dem One-Stop-Shop-Prinzip zuständigen Aufsichtsbehörde und einer anderen Aufsichtsbehörde nicht zu einem einvernehmlichen Ergebnis führen
– Fälle von grundsätzlicher Bedeutung für den Datenschutz in der EU, insbesondere bei einer Datenverarbeitung außerhalb der EU, falls alle Mitgliedstaaten betroffen sind und es nicht allein einer unternehmens- oder konzerninternen Verteilung von Verantwortlichkeiten überlassen bleiben kann, die verantwortliche Behörde in Europa festzulegen.

Es sollte darüber hinaus den Aufsichtsbehörden möglich sein, Fragen von sich aus an den Europäischen Datenschutzausschuss heranzutragen. Es ist zu erwägen, ob der Ausschuss in Fällen, in denen eine Aufsichtsbehörde von der Stellungnahme des Ausschusses abzuweichen beabsichtigt, eine verbindliche Stellungnahme annehmen kann, für die ein höheres Abstimmungsquorum als die einfache Mehrheit der Mitglieder zu fordern wäre.

Die Vollstreckbarkeit von Entscheidungen anderer Aufsichtsbehörden nach Art. 63 sollte unter dem Vorbehalt stehen, dass es sich hierbei um rechtmäßige Entscheidungen der nach Art. 51 zuständigen Aufsichtsbehörde handelt, die unter Beachtung der Vorschriften des Kapitel VII (Amtshilfe, Zusammenarbeit, Kohärenz) getroffen wurden.

Zu Art. 64:

Die umfassende Informationspflicht über alle Tätigkeiten des unabhängigen Ausschusses gegenüber der Kommission nach Art. 64 (4) ist unangemessen.

Zu Art. 66:

Die Streichung der in Art. 30 (1) lit. d) RL 95/46 ausdrücklich enthaltenen Befugnis zur Abgabe von Stellungnahmen zu Verhaltensregeln auf EU-Ebene wird abgelehnt. Der Ausschuss sollte ebenfalls bei der Entwicklung von Zertifizierungsverfahren mitwirken und auch, entsprechend dem jetzigen Art. 30 (1) lit. b) RL 95/46, Stellung nehmen können zum Schutzniveau in der EU und in Drittstaaten.

Es ist abzulehnen, dass die bisherige Kompetenz der Art. 29-Gruppe gemäß Art. 30 (3) RL 95/46, „von sich aus Empfehlungen zu allen Fragen“ abzugeben, „die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen“, nach Art. 66 (1) lit. a) unter der einschränkenden Zweckbestimmung der Beratung der Kommission stehen soll.

Über die in Art. 66 genannten Kompetenzen hinaus sollte dem Ausschuss ein Stellungnahmerecht insbesondere zu Entwürfen der Kommission für delegierte Rechtsakte zukommen. Auf diesem Wege könnten die Expertise und die Kompetenz der Datenschutzbehörden in diesen Bereich eingebracht und gewahrt werden. Zudem würde hierdurch die Transparenz des Delegations- und Komitologieverfahrens erhöht.

Zu Art. 69:

Art. 69 (1) Satz 2 sollte gestrichen werden. Vorsitz- und Stellvertreterposten des Ausschusses sollten ausschließlich durch eine Wahl besetzt werden. Weshalb dem Europäischen Datenschutzbeauftragten zumindest die Funktion eines Stellvertreters zustehen soll, erscheint nicht nachvollziehbar, zumal die Verordnung in der derzeitigen Entwurfsfassung nicht für Organe und Ämter der EU gilt.
Kapitel VIII – Rechtsbehelfe, Haftung und Sanktionen

Zu Art. 73 bis Art. 79:

Es ist sicherzustellen, dass durch den neuen Rechtsrahmen auch ein EU-weit wirksamer Rechtsschutz für die Betroffenen gewährleistet wird. Die in Kapitel VIII vorgesehenen Regelungen sind unklar gefasst und erfüllen diese Voraussetzungen nicht.

Länderübergreifende Klagen durch Aufsichtsbehörden im Namen Betroffener nach Art. 74 (4) gegen Aufsichtsbehörden anderer Mitgliedsstaaten können zu gegenseitigen Kontrollen der Aufsichtsbehörden führen, die im Gegensatz zum sonst geregelten Zusammenarbeitsgebot stehen würden. Es wären Klagen möglich, die der eigenen Rechtsauffassung der Aufsichtsbehörden zuwiderliefen.

Kapitel IX – Vorschriften für besondere Datenverarbeitungssituationen

Zu Art. 80 bis Art. 85:

Die Art. 81, 82 und 84 eröffnen den Mitgliedsstaaten die Befugnis, eigene Regelungen „in den Grenzen dieser Verordnung“ zu treffen. Entscheidend ist, dass damit nicht nur Konkretisierungen auf der Ebene des durch die Verordnung geregelten Datenschutzniveaus möglich sind, sondern dass durch nationalstaatliche Regelungen im Interesse des Datenschutzes weitergehende Anforderungen normiert werden können. Es sollte eine ausdrückliche Klarstellung im Verordnungstext in diesem Sinne erfolgen. Eine solche Regelung müsste mit den unter Art. 6 und Art. 21 vorgeschlagenen Öffnungsklauseln für mitgliedsstaatliches Recht abgestimmt werden.

Soweit in den Art. 81 (3) und 82 (3) auf die Möglichkeit für die Kommission verwiesen wird, delegierte Rechtsakte zu erlassen, ist deren Geltung auf die Mitgliedstaaten zu beschränken, die keinen Gebrauch von der Möglichkeit gemacht haben, die betreffenden Sachbereiche selbst zu regeln. Anderenfalls würde sich der Rechtsakt selbst in Widerspruch setzen. Wenn die Mitgliedstaaten die Ermächtigung bekommen, diese Bereiche selbst zu regeln, ist nicht nachvollziehbar, warum der Kommission den-

noch weitreichende Regelungskompetenzen zur Konkretisierung eingeräumt werden sollen. Diese Konkretisierungen sollten dann konsequenterweise unmittelbar von den Mitgliedstaaten selbst vorgenommen werden können.

Gesundheitsdaten dürfen nach Art. 81 (2) unter den gleichen Voraussetzungen zu historischen oder statistischen Zwecken sowie zu wissenschaftlichen Zwecken verarbeitet werden wie sonstige personenbezogene Daten. Gesundheitsdaten sollten aber auch in diesem Zusammenhang stärker geschützt werden.

Anders als die Art. 80 bis 82 sieht der Art. 83 keine Ermächtigung für die Mitgliedsstaaten vor. Die Vorschrift würde also unmittelbar geltendes Recht werden. Die Konferenz erwartet hier – ebenso wie bereits bei Art. 6 (3) ausgeführt – dass das ausdifferenzierte nationale Statistikrecht und dessen vielfach strengere Vorgaben (im Vergleich zum allgemeinen Datenschutzrecht) weiterhin bestehen bleiben können. Dies sollte in Art. 83 klargestellt werden.

In Art. 85 sollte klargestellt werden, dass sich der Vorbehalt zugunsten kirchlicher Regelungen auf die Bereiche beschränkt, die von Art. 17 AEUV erfasst werden (vgl. Erwägungsgrund 128).

Kapitel X – Delegierte Rechtsakte und Durchführungsrechtsakte

Zu Art. 86 und Art. 87:

Im Hinblick auf die Rechtssicherheit sollten die Delegationsermächtigungen nach Art. 86 auf ein Mindestmaß reduziert werden. Nach Auffassung der Konferenz sind, wie bereits ausgeführt, alle wesentlichen materiellen Fragen in der Verordnung selbst bzw. durch Gesetze der Mitgliedstaaten zu regeln.

Hinsichtlich der verbleibenden Delegationsermächtigungen sollte in die Verordnung eine Verpflichtung der Kommission zur Konsultation des Europäischen Datenschutzausschusses vor dem Erlass delegierter Rechtsakte aufgenommen werden.

Anhang: Fehler und Übersetzungsfehler

In Art. 6 (1) lit. c) sollte in der deutschen Übersetzung das Wort „gesetzlichen“ durch das Wort „rechtlichen“ ersetzt werden, um auch – wie bisher in Art. 7 lit. c)) der RL 95/46/EG – untergesetzliche Normen mit einzubeziehen. Der englische Wortlaut („legal obligation“) ist in beiden Vorschriften identisch.

In Art. 26 (1) sollte „… dass die betreffenden technischen und organisatorischen Maßnahmen … “ durch „… dass geeignete technische und organisatorische Maßnahmen …“ ersetzt werden.

In Art. 26 (2) lit. f) sollte „… den Auftragsverarbeiter …“ durch „… den für die Verarbeitung Verantwortlichen …“ ersetzt werden.

In Art. 30 (3) muss es im letzten Satz anstatt „Art. 4“ „Abs. 4“ heißen.

In den Art 11 (1), Art 22 (1), Art 37 (1) lit. b) und Art 79 (6) lit. e) sollte anstatt „Strategie“ eine zutreffendere Übersetzung für „policy“ gefunden werden.

noch Anlage 5

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht
Frau Dagmar Hartge
Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2012

Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

zur

Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

KOM(2012) 10 endg. vom 25.01.2012

11. Juni 2012

Ungeachtet der Frage, ob sich die Kompetenz der EU zum Erlass einer Richtlinie auf Basis von Art. 16 Abs. 2 Satz 1 AEUV im Hinblick auf das Prinzip der begrenzten Einzelermächtigung und das Subsidiaritätsprinzip auch auf rein innerstaatliche Datenverarbeitungsvorgänge im Bereich der Gefahrenabwehr, der Strafverfolgung und des Strafvollzugs erstreckt, bewertet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Konferenz) den Richtlinienentwurf wie folgt:

Zielsetzung der Richtlinie

Die Richtlinie sollte durch Mindeststandards für die Mitgliedstaaten ein möglichst hohes Datenschutzniveau festschreiben. Den Mitgliedstaaten sollte die Möglichkeit verbleiben, in ihrem nationalen Recht über die Richtlinie hinausgehende datenschutzfreundlichere Regelungen zu treffen. Diese grundsätzliche Weichenstellung sollte in der Richtlinie selbst vorgenommen werden.

Eine solche Klarstellung würde nicht nur die durch die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) entwickelten Datenschutzgrundsätze wahren (z. B. Rechtsprechung zum Kernbereich der privaten Lebensgestaltung), sondern es darüber hinaus den nationalen Verfassungsgerichten ermöglichen, den Grundrechtsschutz in Zusammenarbeit mit dem Europäischen Gerichtshof weiterzuentwickeln.

Ohne entsprechende Festlegungen in der Richtlinie bestünde die Gefahr, dass grundrechtswahrende nationale Regelungen angesichts der Vorgaben der Richtlinie (die Gewährleistung des Datenschutzes und Sicherstellung des Datenaustauschs zwischen den Mitgliedstaaten gemäß Art. 1 (2) lit. b)) im Sinne einer Vollharmonisierung als richtlinienwidrig ausgelegt werden. Eine entsprechende Auslegung wäre vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofs für den Bereich der geltenden Datenschutzrichtlinie 95/46/EG keineswegs ausgeschlossen und hätte unvertretbare Konsequenzen, etwa im Hinblick auf die im Strafprozess- und im Polizeirecht enthaltenen Schutzvorkehrungen für die Rechte der Betroffenen.

Zu den einzelnen Bestimmungen wird folgendermaßen Stellung genommen:

Kapitel I – Allgemeine Bestimmungen

Anwendungsbereich (Art. 1-2)

Die Richtlinie ist gemäß Art. 2 (1) sachlich nur anwendbar, wenn eine „zuständige Behörde“ zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung personenbezogene Daten verarbeitet. Nicht erfasst sind damit Aufgaben im Bereich der Abwehr von Gefahren, die nicht der Abwehr von Straftaten dient (Beispiel: Fahndung nach Vermissten ohne Bezug auf das Vorliegen einer Straftat oder nach Strafunmündigen). Inwieweit andere Aufgaben im Bereich der Grenzkontrolle, des Zolls oder des Aufenthaltsrechts, die je nach der Tradition des Mitgliedstaates als eine polizeiliche Aufgabe verstanden werden, ebenfalls in den Anwendungsbereich der Richtlinie fallen, dürfte innerhalb der Mitgliedstaaten der EU durchaus unterschiedlich beurteilt werden. Nach Auffassung der Konferenz sollte vermieden werden, dass dieselbe polizeiliche Tätigkeit in einem Mitgliedstaat der Verordnung und in einem anderen Mitgliedstaat der Richtlinie unterfällt. Für die deutschen Polizeibehörden dürfte aus der

vorgesehenen Bestimmung der Anwendungsbereiche von Datenschutz-Grundverordnung und Richtlinie folgen, dass sie in ihrem heutigen Aufgabenbereich sowohl die Datenschutz-Grundverordnung als auch die Richtlinie anzuwenden hätte. Zwar sind Abgrenzungsprobleme für Behörden mit polizeilichen Aufgaben nicht neu, wie etwa im Bereich von Zollverwaltung und Zollfahndung schon heute deutlich wird. Dennoch sollte der daraus folgenden Schwierigkeit der Abgrenzung nach Auffassung der Konferenz in erster Linie dadurch abgeholfen werden, weitest gehende Konsistenz zwischen der Datenschutz-Grundverordnung und der Richtlinie herzustellen.

Soweit der vorgeschlagene Rechtsakt Mindestanforderungen auch für die innerstaatliche Datenverarbeitung bei Polizei- und Strafverfolgungsbehörden umfasst, entspricht dies der schon vor einigen Jahren geäußerten Forderung der Konferenz. Angesichts der zunehmenden Verwirklichung des sog. Grundsatzes der Verfügbarkeit (Schwedische Initiative, Prümer Vertrag etc), wonach ein in einem Mitgliedstaat erhobenes und verarbeitetes Datum auch den Polizei- und Strafverfolgungsbehörden eines anderen Mitgliedstaats zur Verfügung stehen soll, ist die Gewährleistung eines hohen Datenschutzniveaus in allen Mitgliedsstaaten erforderlich.

In Art. 2 (2) wird der Anwendungsbereich im Hinblick auf die Umstände der Verarbeitung bestimmt (automatisiert/nicht-automatisiert). Die Konferenz weist insofern darauf hin, dass der Wortlaut insbesondere auf der Grundlage der deutschen Fassung im Unklaren lässt, ob auch Akten von dem Anwendungsbereich umfasst sind. Im Ergebnis sollte die Richtlinie auf die Erhebung und die Verarbeitung personenbezogener Daten unabhängig von dem Verarbeitungsmedium Anwendung finden. Eine Unterscheidung zwischen automatisierter bzw. nicht-automatisierter Verarbeitung einerseits und Verarbeitung in Akten anderseits ist nicht sachgerecht. Dies sollte klargestellt werden.

Nach Art. 2 (3) lit. a) soll die Richtlinie keine Anwendung finden, sofern personen-bezogene Daten im Rahmen einer Tätigkeit verarbeitet werden, die nicht in den Anwendungsbereich des Unionsrechts fällt, etwa im Bereich der „nationalen Sicherheit“. Die Konferenz hält es für erforderlich, den Begriff der „nationalen Sicherheit“ zu präzisieren.

Der Richtlinienvorschlag nimmt auch die Organe und Einrichtungen der EU (u. a. Europol) vom Anwendungsbereich aus. Ungeachtet der Frage, durch welches Rechtsinstrument die Einrichtungen der EU erfasst werden sollten, wäre es aus Sicht der Konferenz nicht sachgerecht, sie von den Reformbemühungen um ein erhöhtes Datenschutzniveau auszunehmen. Wenn das Ziel der Datenschutzreform ist, einen umfassenden Rechtsrahmen auf einem hohen Datenschutzniveau in Europa zu schaffen, sollte dieser auch für die Einrichtungen der EU gelten. Zwar ist nachvollziehbar, dass die komplexen Regelungen der ehemaligen 3. Säule nur schwer in einem einzigen Gesetzespaket überarbeitet werden können. Es muss jedoch vermieden werden, dass für die Einrichtungen der EU andere Maßstäbe gelten als für die Polizei- und Justizbehörden der Mitgliedstaaten. Die Konferenz regt daher eine zügigere als in Art. 60 vorgesehene Anpassung der bestehenden Vorschriften an. Es ist zumindest zu prüfen, ob das mit der Richtlinie zu setzende Mindestniveau für alle Mitgliedstaaten auch für alle bestehenden Einrichtungen der EU zum Mindestniveau erklärt werden könnte.

Begriffsbestimmungen (Art. 3)

Zu den Begriffsbestimmungen ist im Rahmen der Richtlinie auf folgende Besonderheiten hinzuweisen:

Die Definition eines Kindes in Art. 3 (13) sollte gestrichen werden, da hieran im Entwurf einer Richtlinie keine spezifischen Verarbeitungsregeln bzw. Schutzgarantien geknüpft sind.

Im Hinblick auf die Regelung in Art. 7 lit. d) sollte eine Definition für den Begriff der „Gefahr für die öffentliche Sicherheit“ aufgenommen werden.

Im Hinblick auf die Regelung in Art. 16 (3) sollte die Definition der „Einschränkung der Verarbeitung“ in Art. 3 (4) überarbeitet werden.

Kapitel II – Grundsätze

Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten (Art. 4)

Wesentliche Grundlagen für den effektiven Schutz personenbezogener Daten sind u. a. enge Vorgaben für die Anforderungen an die Erforderlichkeit, die Zweckbindung und die Datensparsamkeit. Die Prinzipien der Datenverarbeitung gemäß Art. 4 bedürfen nach Auffassung der Konferenz insgesamt der Ergänzung und Präzisierung. Sie sollten grundsätzlich mehr Konsistenz zu den Prinzipien aufweisen, die in Art. 5 für die Datenschutz-Grundverordnung vorgeschlagen sind.

Die Regelung zur Zweckbindung in Art. 4 lit. b) enthält eine sehr offene Formulierung zur zweckändernden Weiterverarbeitung („nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise“). Sie sollte nach Auffassung der Konferenz strikter gefasst werden, insbesondere vor dem Hintergrund der unklaren und offenen Regelung des Art. 7 zur Rechtmäßigkeit der Verarbeitung. Es sollte klargestellt werden, dass Art. 4 und 7 im Zusammenwirken nicht so verstanden werden dürfen, dass ein einmal im Anwendungsbereich der Richtlinie für einen bestimmten Zweck erhobenes Datum ohne weitere gesetzliche Voraussetzungen für jeden anderen von der Richtlinie erfassten Zweck weiterverarbeitet werden darf.

Es sollte zudem eine engere Bestimmung des Grundsatzes der Erforderlichkeit in Art. 4 lit. c) formuliert werden. Die Bestimmungen „angemessen, sachlich relevant und nicht exzessiv“ stellen nach Auffassung der Konferenz nur eine schwache Begrenzung für die Zulässigkeit der Datenverarbeitung dar. Dies gilt insbesondere deshalb, weil eine Beschränkung auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß, wie sie in Art. 5 lit. c) der Datenschutz-Grundverordnung vorgesehen ist, in dem Entwurf für die Richtlinie fehlt. Zudem

wird die Datensparsamkeit nicht als Grundsatz aufgeführt. Es entsteht vielmehr der Eindruck, dass der Grundsatz der Erforderlichkeit kaum mehr beinhaltet als das Verbot exzessiver Datenverarbeitung.

Als weiterer Grundsatz sollte die Verpflichtung aufgenommen werden, dass bei der Verarbeitung personenbezogener Daten immer die technischen und organisatorischen Maßnahmen zum Datenschutz einzuhalten sind.

In sprachlicher Hinsicht sollte es in Art. 4 lit. a) auch in der deutschen Fassung „Fairness“ bzw. „faires Verfahren“ anstelle von „nach Treu und Glauben“ heißen.

Unterscheidungen nach Kategorien von Betroffenen, Richtigkeit und Betroffenheit (Art. 5 und Art. 6)

Der Entwurf sieht vor, dass die Mitgliedstaaten bei der Verarbeitung personenbezogener Daten sowohl im Hinblick auf verschiedene Personenkategorien (Verdächtige, verurteilte Straftäter, Zeugen, Opfer etc., Art. 5) als auch im Hinblick auf die Richtigkeit und Zuverlässigkeit der Daten (Art. 6) – so weit wie möglich – Unterscheidungen vorzunehmen haben. Unterscheidungen nach anderen Kriterien, die für das deutsche Recht maßgeblich sind, sieht der Entwurf nicht vor. Dabei geht es beispielsweise um die Frage, ob der Eingriff den Kernbereich der persönlichen Lebensgestaltung berührt oder die Daten aus besonders einschneidenden Grundrechtseingriffen (Telekommunikationsgeheimnis, Unverletzlichkeit der Wohnung) herrühren. Damit das erreichte und nach deutschem Verfassungsrecht unabdingbare Schutzniveau erhalten bleiben kann, sollte die Richtlinie Mindeststandards und keine Obergrenzen für mitgliedstaatliche Regelungen regeln.

Sowohl in Art. 5 als auch in Art. 6 bleibt offen, was aus den vorzunehmenden Unterscheidungen bzw. was aus dem Unterlassen der Unterscheidung folgen soll. Die Konferenz befürwortet insbesondere engere Grenzen für die Verarbeitung von Daten zu bestimmten Personengruppen (z. B. Opfer oder Zeugen von Straftaten).

Rechtmäßigkeit der Verarbeitung (Art. 7)

Artikel 7 enthält die zentrale Vorschrift zur Bestimmung der Rechtmäßigkeit von Datenverarbeitungen. Dabei bedarf die in Art. 7 getroffene Unterscheidung zwischen lit. a), b), c) und d) nach Auffassung der Konferenz der weiteren Erläuterung.

Ebenfalls erläuterungsbedürftig ist das Zusammenwirken dieser Vorschrift mit den in Art. 4 aufgeführten Prinzipien der Datenverarbeitung, insbesondere im Hinblick auf den Grundsatz der Zweckbindung.

Die Konferenz begrüßt, dass eine Einwilligung als Legitimation für die Datenverarbeitung im Bereich der Richtlinie ausgeschlossen ist. Ihre Anwendung ist von der Konferenz wiederholt infrage gestellt worden, insbesondere dann, wenn dadurch die Grenzen der gesetzlichen Befugnisse erweitert werden sollen.

Kapitel III – Rechte der betroffenen Personen

Rechte der Betroffenen (Art. 10 – 17)

Umfangreiche Rechte der Betroffenen sind wesentlich für ein hohes Datenschutzniveau. Um den Richtlinienentwurf zu einer geeigneten Grundlage für die Erweiterung der Betroffenenrechte in den Mitgliedstaaten zu machen, bedarf es einzelner Klarstellungen und Änderungen.

Besonderer Klärungsbedarf besteht im Hinblick auf Art. 17 i. V. m. Erwägungsgrund 82. Der Konferenz ist weder klar, in welchen Fällen Art. 17 anwendbar ist, noch, welche Folgen die Anwendbarkeit von Art. 17 hat. Die Auslegung wird zudem dadurch erschwert, dass die deutsche und die englische Fassung („Gerichtsbeschluss“ oder „Gerichtsdokument“/„judicial decision or record“) unterschiedliche Interpretationen nahe legen. Eine Klarstellung ist in dieser Frage von besonderer Bedeutung, weil davon letztlich abhängt, ob und inwieweit die Betroffenenrechte während des gesamten staatsanwaltlichen Ermittlungsverfahrens gelten.

Nach Auffassung der Konferenz sollten die in den Art. 11 – 16 gewährten Rechte grundsätzlich auch im Bereich des staatsanwaltlichen Ermittlungsverfahrens Anwendung finden. Mindeststandards bezüglich der Ausgestaltung der Betroffenenrechte zählen zu den zentralen Elementen eines hohen Datenschutzniveaus und müssen auch bei der Verarbeitung personenbezogener Daten durch Staatsanwaltschaften gelten.

Darüber hinaus sind die Möglichkeiten der Mitgliedstaaten, die Betroffenenrechte einzuschränken, zu weitgehend. Als nicht vertretbar sieht die Konferenz die Regelungen in Art. 11 (5) und Art. 13 (2) der Richtlinie an. Sie eröffnen dem Gesetzgeber die Möglichkeit, bei bestimmten Datenkategorien die Information bzw. die Auskunftserteilung an den Betroffenen per se auszuschließen, ohne dass eine Abwägung im Einzelfall erfolgen muss. Es sollte vielmehr in Art. 11 und 13 klargestellt werden, dass Einschränkungen stets nur nach Prüfung des Einzelfalls zulässig sind.

Es ist nachvollziehbar, dass die Information des Betroffenen bzw. sein Auskunftsrecht in bestimmten Fällen (zunächst) beschränkt werden muss. Die Beschränkungen müssen allerdings in der Richtlinie hinreichend konkret bestimmt werden. Insofern werfen die Art. 11 (4) und Art. 13 (1) erneut Fragen auf. Sie eröffnen einen zu weiten Spielraum für den nationalen Gesetzgeber, die Rechte der Betroffenen einzuschränken.

Die Information der betroffenen Person über die Erhebung personenbezogener Daten sollte zudem unverzüglich (d. h. ohne schuldhaftes Zögern) erfolgen. Die Angabe „innerhalb einer angemessenen Frist“ in Art. 11 (3) lit. b ist insoweit zu unbestimmt.

In Art. 15 sollte klargestellt werden, ob unter einem „Korrigendum“ eine Richtigstellung zu verstehen ist.

Zudem sollte der Richtlinienentwurf dahingehend ergänzt werden, dass den Betroffenen in geeigneten Fällen neben dem Auskunftsrecht auch ein Akteneinsichtsrecht zu gewähren ist.

Kapitel IV – Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter

Vorschriften über die Verarbeitung Verantwortlicher und Auftragsverarbeiter (Art. 18 – 32)

Die Konferenz bedauert, dass die Vorschrift zu „Datenschutz durch Technik“ („privacy by design“) in Art. 19 keine konkreten Vorgaben macht und so zu einem reinen Programmsatz ohne praktische Auswirkungen werden könnte. Zudem könnte die ausdrückliche Bezugnahme auf die Berücksichtigung der entstehenden Kosten in der vorliegenden Formulierung zu einem Einfallstor für das Unterlassen von Maßnahmen zur datenschutzfreundlichen Technikgestaltung werden.

Bei verschiedenen Vorschriften des Kapitels IV sieht die Konferenz einen weiteren Klarstellungsbedarf. Dazu gehört das Verhältnis der „unabhängigen internen oder externen Prüfer“ zum Datenschutzbeauftragten und zu den Aufsichtsbehörden nach Art. 18 (3). Dazu gehören ebenso die Regelungsgehalte der Art. 20 und 22 (z. B. hinsichtlich der Kontrollpflichten des Auftragnehmers) und das Verhältnis der Art. 20 und 21 zueinander.

Die in Art. 23 (2) formulierten Dokumentationspflichten sollten ergänzt werden durch eine Beschreibung der betroffenen Personengruppen, der diesbezüglichen Daten oder Datenkategorien und durch eine Festlegung von Regelfristen zur Datenlöschung.

Die Vorschriften über die Datensicherheit (Art. 27 – 29) sollten um Datenschutzzielbestimmungen ergänzt werden.

Die nach Art. 27 (2) erforderliche Risikobewertung ist nur als angemessene Sicherheitsmaßnahme zu bewerten, wenn eine kontinuierlich durchgeführte Risikobewertung bzw. Risikoanalyse gewährleistet ist. IT-Sicherheit erfordert in diesem Sinne ein konzeptionelles Herangehen sowie die Etablierung von IT-Sicherheits- und Datenschutzmanagementsystemen. Artikel 27 sollte daher durch die Forderung nach einem Sicherheitskonzept, welches Teil der Verfahrens-dokumentation gemäß Art. 23 (2) werden muss, ergänzt werden.

Die in Art. 28 (5) enthaltene Delegation an die Kommission bedarf der Überprüfung. Die Kriterien und Anforderungen für die Feststellung einer Verletzung des Schutzes personenbezogener Daten sind so wesentlich, dass sie im Rechtsakt selbst bestimmt werden sollten.

Die in Art. 29 (3) geregelte Pflicht zur Benachrichtigung der betroffenen Person von einer Verletzung des Schutzes personenbezogener Daten sollte nicht davon abhängig gemacht werden, ob die verantwortliche Stelle ausreichende technische Schutzmaßnahmen getroffen hat.

Bei den Pflichten des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters sollten in der Richtlinie entsprechend den Vorgaben der Datenschutz-Grundverordnung nicht nur die „vorherige Zurateziehung“ („prior consultation“) der Datenschutzbehörden, sondern auch eine Folgenabschätzung („privacy impact assessment“) durch die jeweilige Stelle vorgesehen werden.

Bei den Anforderungen an den Datenschutzbeauftragten ist der Begriff der „Zuverlässigkeit“ aufzunehmen (Art. 30 (2). Darüber hinaus sollte eine Verschwiegenheitspflicht des Datenschutzbeauftragten festgelegt werden sowie die Aufnahme eines Benachteiligungsverbots, eines Kündigungsschutzes und die Möglichkeit der Teilnahme an Fort- und Weiterbildungsveranstaltungen.

In Art. 32 der Richtlinie sollte zudem klargestellt werden, dass die Aufgaben des Datenschutzbeauftragten die verantwortliche Stelle nicht von ihren eigenen Pflichten entbindet, d. h., dass sie sich nicht unter Verweis auf die Nicht- oder Schlechterfüllung durch den Datenschutzbeauftragten exkulpieren kann. Insbesondere Art. 32 lit. a), lit. d) und lit. h) sind insoweit missverständlich.

Kapitel V – Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen

Die Vorschriften zu den Übermittlungen von personenbezogenen Daten in Drittstaaten sind in einem wichtigen Punkt widersprüchlich und sind insgesamt zu weit gefasst.

Im Hinblick auf die Übermittlung von personenbezogenen Daten an internationale Organisation sollte in Art. 33 klargestellt werden, dass nur solche internationale Organisationen gemeint sind, die einen Bezug zu Fragen der inneren Sicherheit aufweisen. Dies gilt ebenso für die sog. Weiterübermittlungen („onward transfers“), die in einer spezifischen Vorschrift geregelt werden sollten.

Es fehlt eine Klarstellung, dass bestehende Angemessenheitsbeschlüsse, die auf der Grundlage der RL 95/46/EG ergangen sind, für den JI-Bereich nicht gelten.

Entsprechend den bisherigen Regelungen in der Richtlinie 95/46/EG enthält der Vorschlag die Einführung von Angemessenheitsbeschlüssen zum Datenschutzniveau von Drittstaaten. Sofern die Kommission einen solchen Beschluss gefasst hat, ist die Angemessenheit des Datenschutzniveaus verbindlich festgestellt. Es bedarf allerdings der Klarstellung, dass bei Negativbeschlüssen der Kommission nach Art. 34 (5) Datenübermittlungen nur auf der Grundlage der Ausnahmen nach Art. 36, nicht aber auf der Grundlage des Art. 35 (1) vorgenommen werden dürfen. Die Vorschriften des Art. 34 (5) und Art. 35 (1) sind in dieser Frage widersprüchlich.

Die Möglichkeit der Mitgliedstaaten, personenbezogene Daten auf der Grundlage einer eigenen Einschätzung in Drittstaaten zu übermitteln, ist im Hinblick auf Art. 35 (1) lit. b) zu unbestimmt gefasst. Jedenfalls ist eine Bezugnahme auf Art. 34 (2) lit. a) vorzunehmen, der die bei der Angemessenheitsentscheidung zu berücksichtigenden Faktoren aufführt. Darüber hinaus sollte die Einbeziehung des Auftragsverarbeiters in Art. 35 gestrichen werden.

Die Konferenz hält die Ausnahmevorschrift des Art. 36 für zu weit gefasst. Dies gilt insbesondere für lit. d) und lit. e), nach denen kaum noch eine Übermittlung denkbar ist, die nicht auf eine der Ausnahmeklauseln gestützt werden könnte. Die Konferenz regt daher im Hinblick auf die in den lit. a) bis e) enthaltenen Ausnahmevorschriften die Streichung der lit. d) und e) an. Zudem sollte in Art. 36 eine Dokumentationspflicht entsprechend des Art. 35 (2) aufgenommen werden.

Artikel 37 bezieht sich auf die Übermittlung von Daten in Drittstaaten, für die auf nationaler Ebene besondere Verwendungsbeschränkungen gelten. Insofern seien alle „vertretbaren Vorkehrungen“ zu treffen, um diese Beschränkungen einzuhalten. Dies ist nach Auffassung der Konferenz zu unbestimmt und sollte daher, insbesondere auch bezüglich der zu ergreifenden technischen und organisatorischen Maßnahmen, konkretisiert werden. Die Vorschrift sollte zudem um die Verpflichtung ergänzt werden, den Empfänger der übermittelten Daten über Berichtigungs- und Löschungsansprüche zu informieren.

Artikel 37 ist nicht auf Übermittlungen zwischen den Mitgliedstaaten anwendbar. Daher muss die Richtlinie an geeigneter Stelle klarstellen, dass die in den nationalen Vorschriften der Mitgliedstaaten enthaltenen Verwendungsbeschränkungen und Mitteilungspflichten auch für Datentransfers innerhalb der Europäischen Union gelten. Die Richtlinie sollte die Daten empfangenden Mitgliedstaaten verpflichten, die Verwendungsbeschränkungen des übermittelnden Mitgliedstaates umzusetzen.

Schließlich sollte die Regelung des Art. 38 dahingehend ergänzt werden, dass neben der Kommission auch die Aufsichtsbehörden die Förderung der Beziehungen zu Drittländern betreiben können, und zwar auch – und gerade – zu Drittländern ohne angemessenen Schutz.

Kapitel VI und VII – Unabhängige Aufsichtsbehörden und Zusammenarbeit

Die Regelungen zur Unabhängigkeit sind grundsätzlich positiv zu werten. In Art. 39 (1) Satz 2 sollte allerdings klargestellt werden, dass die Unabhängigkeit der Aufsichtsbehörden auch bei der Zusammenarbeit mit der Kommission sowie den anderen Aufsichtsbehörden garantiert sein muss.

Eine im Bereich von Polizei und Justiz zentrale Frage betrifft die Zuständigkeit von Datenschutzbehörden bei der Datenverarbeitung durch Gerichte im Rahmen ihrer gerichtlichen Tätigkeiten. Im Text von Art. 44 (2) sollte unmissverständlich klargestellt werden, dass der Ausschluss der Zuständigkeit der Aufsichtsbehörden sich nicht auf Akte der Exekutive bezieht, die nach nationalem Recht unter Beteiligung eines Richters zustande gekommen sind (in Deutschland etwa im Hinblick auf Maßnahmen der Strafverfolgungsbehörden, die einem Richtervorbehalt unterlegen haben).

In Art. 45 (4) sollte verdeutlicht werden, dass die Nutzung eines Formulars für Beschwerden nicht verbindlich ist und technische Schutzvorkehrungen im Sinne des Art. 27 zu treffen sind.

Die Konferenz begrüßt, dass Art. 46, insbesondere lit. b), die bisherige Ausgestaltung der aufsichtsbehördlichen Befugnisse im deutschen Recht auch weiterhin zulässt, ohne Änderungen für die Zukunft auszuschließen, wie die Verleihung von Anordnungskompetenzen. Die Frage der Ausgestaltung der Befugnisse für die Aufsichtsbehörden ist von besonderer Bedeutung und steht in engem Zusammenhang mit der Möglichkeit der gerichtlichen Auseinandersetzung zwischen der Aufsichtsbehörde und der beaufsichtigten Stelle und/oder dem Betroffenen (vgl. Art. 51).

Zur Vermeidung jeden Zweifels, der aus dem Vergleich mit der Datenschutz-Grundverordung resultieren könnte, sollte gleichfalls in der Richtlinie ausdrücklich klargestellt werden, dass Art. 46 auch den anlasslosen Zugang zu Diensträumen umfasst.

Zuletzt muss sichergestellt sein, dass hinreichende Mittel bereitstehen, um die praktische Arbeit im Rahmen der Amtshilfeleistungen zu erleichtern (insbesondere im Hinblick auf Übersetzungsleistungen, ggf. durch das Sekretariat des Datenschutzausschusses). Die Amtshilfeverpflichtung nach Art. 48 sollte durch Ausnahmevorschriften, etwa zum Schutz von Geheimhaltungsvorschriften, ergänzt werden.

Kapitel VIII – Rechtsbehelfe, Haftung und Sanktionen

Die Erweiterung der Vertretungsbefugnis für Einrichtungen, Organisationen und Verbände gemäß Art. 50 (2) ist grundsätzlich zu begrüßen.

In Art. 51 (1) sollte klargestellt werden, dass gerichtliche Rechtsbehelfe nur gegen Entscheidungen der Aufsichtsbehörde mit Regelungswirkung gegenüber Bürgern und anderen Behörden möglich sind.

In Art. 51 (2) sollte klargestellt werden, dass die vorgesehene Klagemöglichkeit gegen die Aufsichtsbehörde auf die Untätigkeit der Aufsichtsbehörde begrenzt ist. Die unklare Formulierung „wenn keine zum Schutz ihrer Rechte notwendige Entscheidung ergangen ist“ sollte gestrichen werden.

Die Regelung über gemeinsame Vorschriften zum Gerichtsverfahren (Art. 53) sieht in Absatz 2 vor, dass jede Aufsichtsbehörde das Recht hat (im Englischen: „shall have the right“), Klage zur Durchsetzung der in der Richtlinie enthaltenen Rechte zu erheben. Die Konferenz spricht sich dafür aus, Art. 53 (2) so zu ändern, dass die Mitgliedstaaten eine entsprechende Berechtigung der Aufsichtsbehörden vorsehen können, jedoch nicht hierzu verpflichtet sind.

Die in Art. 54 (2) der Richtlinie vorgesehene Einführung einer gesamtschuldnerischen Haftung aller an der Verarbeitung beteiligten Stellen wird von der Konferenz als sinnvoll angesehen und daher begrüßt.

Kapitel IX und X – Delegierte Rechtsakte und Durchführungsbestimmungen, Schlussbestimmungen

Die Konferenz begrüßt, dass internationale Übereinkommen, die von den Mitgliedstaaten vor Inkrafttreten der Richtlinie geschlossen worden sind, innerhalb von fünf Jahren überarbeitet werden sollen, um sie in Übereinstimmung mit den Vorgaben der Richtlinie zu bringen (Art. 60). Es sollte klargestellt werden, dass die Richtlinie insofern nur als ein Mindestniveau anzusehen ist und in keinem Fall eine Herabstufung bestehender höherer Standards zu erfolgen hat. Die bisher fehlende Anwendbarkeit der Richtlinie auf die Einrichtungen der EU darf nicht dazu führen, dass die zwischen der EU und Drittstaaten vereinbarten Abkommen (wie etwa das TFTP-Abkommen oder das PNR-Abkommen) von dieser Regelung ausgenommen sind.

Entsprechend der allgemeinen Forderung der Konferenz sollte eine substanziellere Vorschrift für die Evaluierung der Richtlinie aufgenommen werden, als dies gegenwärtig in Art. 61 (3) vorgesehen ist. Die Evaluierungsklausel sollte auch die Hinzuziehung von externem Sachverstand enthalten.

Anlage 6

Bonn, 18. Januar 2013

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand von De-Mail

Die Handreichung soll die Nutzer von De-Mail für die datenschutzrechtlichen Aspekte bei der Versendung besonders schützenswerter Daten mittels De-Mail sensibilisieren. Sie soll Hinweise für einen datenschutzgerechten Versand dieser Daten mittels De-Mail unter Berücksichtigung der Möglichkeit einer Ende-zu-Ende-Verschlüsselung geben, um damit zu einer rechtssicheren und weiten Verbreitung von De-Mail-Diensten beizutragen.

Am 3. Mai 2011 ist das De-Mail-Gesetz in Kraft getreten. Auf Grundlage dieses Gesetzes können sich Unternehmen akkreditieren lassen, um De-Mail-Dienste anzubieten. De-Mail-Dienste sind nach § 1 Abs. 1 De-Mail-Gesetz Telekommunikationsdienste auf einer elektronischen Plattform, die eine sichere, vertrauliche und nachweisbare Kommunikation für jedermann im Internet gewährleisten sollen. Die De-Mail ist letztlich eine besondere Form der E-Mail. Sie soll ohne zusätzliche Hard- und Software genauso einfach bedienbar sein, aber die Nachteile der E-Mail ausgleichen. Eine E-Mail kann nämlich mit geringem technischem Aufwand abgefangen, mitgelesen und verändert werden.

Das De-Mail-Gesetz stellt einerseits Anforderungen an Datenschutz und Datensicherheit beim De-Mail-Dienstеanbieter (DMDA) und regelt andererseits, wie De-Mail für die rechtssichere elektronische Kommunikation eingesetzt werden kann. Dies bedingt einige Besonderheiten im Vergleich zur Nutzung von E-Mail-Diensten, so z. B. eine eindeutige Identifizierung vor der erstmaligen Nutzung von De-Mail. De-Mail bietet die Gewähr dafür, dass der Absender einer De-Mail zweifelsfrei ermittelt werden kann. Absende- und Eingangsbestätigungen, die mit einer qualifizierten elektronischen Signatur des DMDA versehen werden, bieten den sicheren Nachweis, dass die De-Mail versendet wurde und eingegangen ist. Schließlich wird die Nachricht durch den Anbieter transport- und inhaltsverschlüsselt.

Das De-Mail-Gesetz fordert:

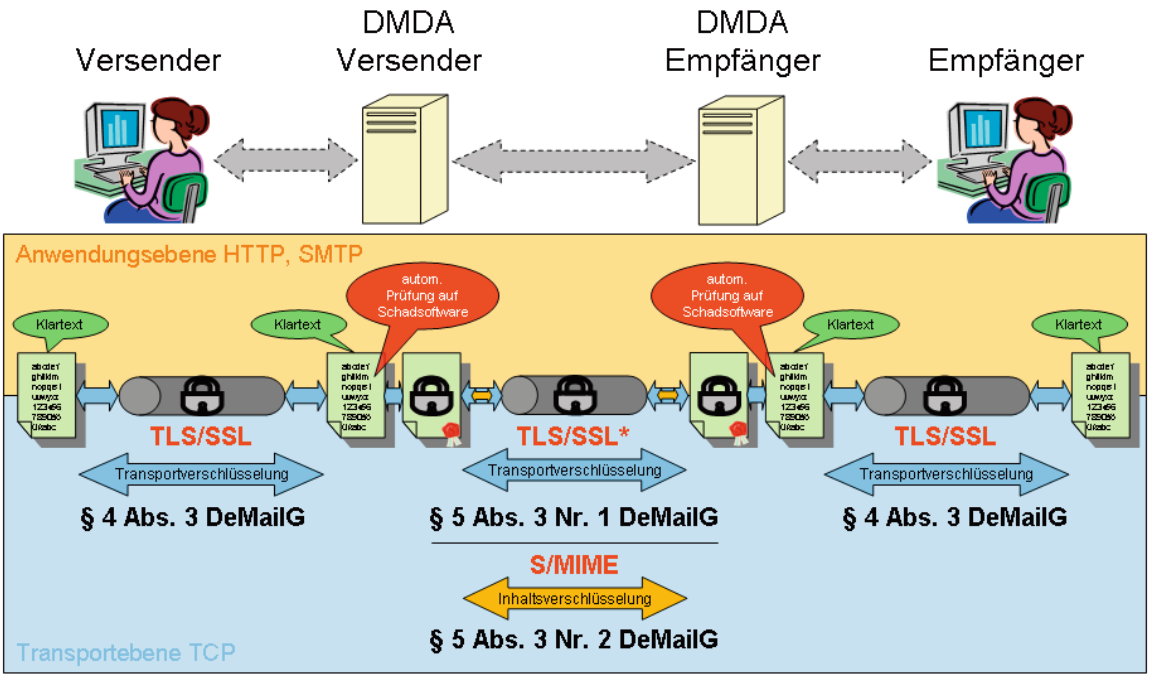
- Der akkreditierte DMDA hat sicherzustellen, dass die Kommunikationsverbindung zwischen dem Nutzer und seinem De-Mail-Konto verschlüsselt erfolgt.
- Der Versand von einem DMDA zu jedem anderen DMDA muss über einen verschlüsselten gegenseitig authentisierten Kanal erfolgen.
- Der Inhalt einer De-Mail-Nachricht muss vom DMDA des Versenders zum DMDA des Empfängers verschlüsselt übertragen werden.

Die technischen Details lassen sich wie folgt zusammenfassen:

- Die Nachricht vom Versender an seinen DMDA und weiter vom DMDA des Empfängers an den Empfänger ist auf der Transportebene jeweils einfach durch Transportverschlüsselung gesichert (TCP + SSL/TLS). Die Authentisierung des Clients erfolgt automatisch mittels SSL-Handshake. Eine zertifikatsbasierte Clientauthentifizierung wird optional unterstützt.
- Die Nachricht ist zwischen dem DMDA des Versenders und dem DMDA des Empfängers doppelt gesichert: auf Anwendungsebene durch Inhaltsverschlüsselung und Signatur der Nachricht (S/MIME) sowie auf Transportebene durch Transportverschlüsselung (TCP + implizites1 SSL/TLS). Eine gegenseitige Clientauthentisierung muss zwingend zertifikatsbasiert erfolgen.
- Die Transportverschlüsselung (TLS) ist eine Punkt-zu-Punkt-Verschlüsselung (SSL-Handshake), weshalb die Nachricht nach dem Versand wieder unverschlüsselt vorliegt. Auf Transportebene liegt die Nachricht also in einem zufälligen Bitmuster vor, jedoch wäre sie auf Anwendungsebene ohne weiteres im Klartext zu lesen.
- Die Inhaltsverschlüsselung (S/MIME) ist eine Ende-zu-Ende-Verschlüsselung, wird aber gemäß TR De-Mail nur zwischen zwei DMDA gefordert.

§ 3 Abs. 4 Nr. 4 De-Mail-G sieht vor, dass der DMDA die De-Mail auf Befall mit Schadsoftware überprüfen muss. Vor dem Versand der Nachricht an den DMDA des Empfängers liegt diese beim DMDA des Versenders unverschlüsselt vor, so dass er sie zu diesem Zeitpunkt auf Schadsoftwarebefall hin prüfen kann. Anschließend leitet er die Nachricht zusätzlich zur Transportverschlüsselung inhaltsverschlüsselt an den DMDA des Empfängers weiter. Ist die Nachricht beim DMDA des Empfängers eingegangen, wird die Inhaltsverschlüsselung aufgehoben und die Nachricht wiederum auf Schadsoftwarebefall hin geprüft. Abschließend wird die Nachricht verschlüsselt im Postfach des Empfängers abgelegt. Nach jeder Prüfung wird die Nachricht in den Metadaten mit einem Hinweis

Abbildung 1



versehen, ob die Überprüfung zu einem Befund geführt hat. Dieser Prüfprozess erfolgt zwar automatisiert auf Servern in einem Rechenzentrum des DMDA, das den Vorgaben des BSI entspricht. Zudem gibt es weitere technische und organisatorische Maßnahmen, die einen Zugriff durch einen Innen- wie auch einen Außentäter verhindern sollen. Gleichwohl besteht ein Restrisiko, dass insbesondere Administratoren des Anbieters vom Nachrichteninhalt Kenntnis nehmen.

Im Gegensatz dazu stellt die Ende-zu-Ende-Verschlüsselung eine durchgängige Verschlüsselung zwischen Versender und Empfänger dar und bietet sich daher für eine Versendung besonders schutzbedürftiger Daten an. Dies wird vom De-Mail-Gesetz jedoch nicht gefordert. Für den DMDA ergeben sich dementsprechend keine Pflichten. Er darf den Versand Ende-zu-Ende-verschlüsselter Nachrichten lediglich nicht verhindern. Faktisch bedeutet dies, dass sich die Nutzer selbst um die Installation und Nutzung einer Verschlüsselungssoftware kümmern müssen. Eine Prüfung auf Schadsoftware kann der DMDA dann allerdings nicht durchführen. Problematisch ist zudem, dass Nachrichten nur dann verschlüsselt versendet werden können, wenn auch der Empfänger eine entsprechende Kryptografiesoftware einsetzt. Dies führt zu Verunsicherungen und Erschwernissen, die sich hätten vermeiden lassen, wenn die Ende-zu-Ende-Verschlüsselung zu den mit De-Mail bereitgestellten Standardmaßnahmen gehören würde.

Da die bisher akkreditierten DMDA für den Privatanwender bislang nur den Zugang per Web-Client ermöglichen, ist eine Ende-zu-Ende-Verschlüsselung für diesen derzeit kaum praktikabel. Der Versender muss die zu übermittelnde Nachricht auf seinem lokalen Rechner erstellen und mit einer Kryptografiesoftware verschlüsseln. Danach meldet er sich über den Web-Client an seinem De-Mail Konto an, erzeugt eine leere „Pseudo“-De-Mail und hängt dieser per Upload die verschlüsselte Datei an. Wirtschaftsunternehmen und die öffentliche Verwaltung haben es hier einfacher, da die Anbindung an De-Mail über ein Gateway erfolgt, d. h. im Firmen- bzw. Behördennetzwerk können normale E-Mail-Clients wie Outlook oder Lotus Notes genutzt werden, die von Hause aus eine Verschlüsselung unterstützen, so dass diese weitestgehend automatisiert erfolgen kann.

Es ist ein Grundsatz des Datenschutzes, dass bei der elektronischen Übertragung personenbezogener Daten die Integrität, Authentizität und Vertraulichkeit der Daten sichergestellt sein muss. Je schützenswerter ein Datum ist, desto strenger sind die technisch-organisatorischen Maßnahmen, die die verantwortliche Stelle einhalten muss. Bei bestimmten personenbezogenen Daten wie zum Beispiel Gesundheitsdaten, spielt besonders die Vertraulichkeit eine große Rolle. Unbefugte sollen in keinen Fall Kenntnis von diesen Daten erhalten. Bei der elektronischen Kommunikation wird die Vertraulichkeit dadurch gewährleistet, dass die Nachricht und ihre Anhänge mit einer geeigneten Software verschlüsselt werden. Betroffen sind hiervon alle besonders schutzbedürftigen personenbezogenen Daten, also solche, die potentiell eine besondere Sensibilität aufweisen. Dies gilt etwa für personenbezogene Daten an deren Verarbeitung und Nutzung besondere gesetzliche Anforderungen gestellt werden, wie z. B. die so genannten besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG oder die dem Sozialdatenschutz unterfallenden personenbezogenen Daten. Welche Schutzmaßnahmen für diese Daten angemessen sind, ergibt sich allerdings nicht automatisch, sondern

bedarf einer Prüfung im Einzelfall, die im Folgenden weiter ausgeführt wird.

Mangels entsprechender gesetzlicher Vorgaben im De-Mail-Gesetz sind nicht die DMDA, sondern die Versender von De-Mails für die Beachtung datenschutzrechtlich angemessener Verfahren verantwortlich. Um ein angemessenes Schutzniveau bei der Versendung besonders schutzbedürftiger personenbezogener Daten (z. B. Sozialdaten oder Daten die Rückschlüsse auf den Gesundheitszustand einzelner Betroffener zulassen) mittels De-Mail zu gewährleisten, ist aus datenschutzrechtlicher Sicht eine Ende-zu-Ende-Verschlüsselung grundsätzlich erforderlich. Die Vorgaben des De-Mail-Gesetzes, die Technische Richtlinie des BSI nach § 18 Abs. 2 De-Mail-Gesetz und der Kriterienkatalog des BfDI gemäß § 18 Abs. 3 Nr. 4 De-Mail-Gesetz machen zwar deutlich, dass bei De-Mail das Datenschutz- und Datensicherheitsniveau im Vergleich zum E-Mail-Versand erheblich höher ist. Trotzdem müssen über diesen Mindeststandard hinaus beim Versand besonders schutzbedürftiger Daten grundsätzlich zusätzliche Schutzvorkehrungen getroffen werden.

Ob eine Ende-zu-Ende-Verschlüsselung im Einzelfall die datenschutzrechtlich angemessene Sicherungsmaßnahme darstellt, orientiert sich an dem konkreten Schutzbedarf der Daten. Dieser ist zunächst anhand der Grundschutzmethodik des BSI von der datenverarbeitenden Stelle festzustellen:

- Bei einer Schutzbedarfsfeststellung ist grundsätzlich danach zu fragen, welcher Schaden entstehen kann, wenn die Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit verletzt werden. Es muss also gefragt werden, welcher Schaden eintritt, wenn vertrauliche Informationen unberechtigt zur Kenntnis genommen oder weitergegeben werden (Verletzung der Vertraulichkeit), die Korrektheit der Informationen und die Funktionsweise von Systemen nicht mehr gegeben ist (Verletzung der Integrität) oder autorisierte Benutzer am Zugriff auf Informationen und Systeme behindert werden (Verletzung der Verfügbarkeit). Dabei wird zwischen den Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ unterschieden. Der Schaden, der von einer Verletzung der Grundwerte ausgehen kann, kann sich auf verschiedene Schadensszenarien beziehen:
  - Verstöße gegen Gesetze, Vorschriften oder Verträge,
  - Beeinträchtigungen des informationellen Selbstbestimmungsrechts,
  - Beeinträchtigungen der persönlichen Unversehrtheit,
  - Beeinträchtigungen der Aufgabenerfüllung,
  - negative Außenwirkung oder
  - finanzielle Auswirkungen.
- Beim Schutzbedarf „normal“ sind die Schadensauswirkungen begrenzt und überschaubar. Beim Versand von Daten mit dem Schutzbedarf „normal“ ist eine Ende-zu-Ende-Verschlüsselung dann nicht notwendig.
- Beim Schutzbedarf „hoch“ können die Schadensauswirkungen beträchtlich sein. Beim Versand von Daten mit dem Schutzbedarf „hoch“ ist eine Ende-zu-Ende-Verschlüsselung grundsätzlich erforderlich. Auf sie kann jedoch dann verzichtet werden, wenn die datenverarbeitende Stelle anhand einer Risikoanalyse zu dem Ergebnis kommt, dass sie aufgrund der getroffenen technischen und organisatorischen Sicherheitsmaßnahmen das Restrisiko im Bereich des Versenders als vertretbar bewertet. Versender und Empfänger müssen sich aber auf jeden Fall an ihrem Konto im Sinne des § 4 Abs. 1 Satz 2 De-Mail-Gesetz sicher anmelden.
- Beim Schutzbedarf „sehr hoch“ können die Schadensauswirkungen bei unberechtigtem Zugriff ein existentiell bedrohliches Ausmaß erreichen. Beim Versand von Daten mit dem Schutzbedarf „sehr hoch“ ist eine Ende-zu-Ende-Verschlüsselung zwingend notwendig.
- Bei der Schutzbedarfsanalyse ist Folgendes zu beachten:
  - Die Einstufung des jeweiligen personenbezogenen Datums kann je nach Kontext, in dem das Datum verwendet wird, unterschiedlich sein. So ist beispielsweise der Schutzbedarf einer Adresse im Regelfall behördlicher Anwendungen normal oder hoch. Befindet sich die betroffene Person aber in einem Zeugenschutzprogramm, ist der Schutzbedarf sehr hoch und die Daten dürften nur mit Ende-zu-Ende-Verschlüsselung übertragen werden.
  - Sozial- und Steuergeheimnisdaten sind zwar nach dem Gesetz insofern als besonders schützenswert eingestuft, als ihre Verarbeitung zum Teil besonderen Restriktionen unterliegt. Allerdings bedeutet dies nicht, dass sämtliche Sozial- und Steuergeheimnisdaten Ende-zu-Ende-verschlüsselt werden müssen. Die Tatsache, dass eine Person beispielsweise bei einer bestimmten gesetzlichen Krankenkasse versichert ist, ist im Regelfall kein besonders schützenswertes Datum.
  - Gesundheitsdaten unterliegen dagegen in aller Regel dem Schutzbedarf „sehr hoch“. Dies gilt wiederum auch unabhängig vom Kontext als Sozialdatum. Auch die Angabe von besonderen Belastungen bei Krankheitsaufwendungen im Zusammenhang mit einer Einkommenssteuererklärung sind besonders schutzbedürftig, auch wenn Steuergeheimnisdaten nicht automatisch Ende-zu-Ende-verschlüsselt werden müssen.

Neben der Schutzbedarfsanalyse muss für eine Einschätzung der notwendigen Sicherheitsmaßnahmen beim Versand besonders schutzbedürftiger Daten auch berücksichtigt werden, wer Versender und Empfänger der De-Mail ist:

- Versenden Behörden oder andere Institutionen besonders schutzbedürftige personenbezogene Daten unmit-

telbar an den Betroffenen, richtet sich die Verpflichtung zur Ende-zu-Ende-Verschlüsselung grundsätzlich nach dem im Wege der Schutzbedarfsanalyse ermittelten Schutzbedarf der Daten. Daneben muss der Versender vor dem Versand das Einverständnis des potentiellen Empfängers einholen[1]. Dies sollte mindestens einmalig für alle diesen Transportweg betreffenden Kommunikationsvorgänge erfolgen. Zusätzlich muss für den Versand besonders schutzbedürftiger Daten mittels De-Mail an den Betroffenen eine individuelle Zugangseröffnung vorliegen[2]. Dies gilt insbesondere für eine differenzierte Betrachtung bei der Zugangseröffnung gegenüber Behörden. Der Bürger sollte die Möglichkeit haben, den Zugang differenziert nach einzelnen Behörden zu gestalten.

– Versenden Behörden oder andere Institutionen wie etwa gesetzliche Krankenkassen, die mit besonders schutzbedürftigen personenbezogenen Daten Dritter umgehen, solche Daten untereinander, muss die Nachricht im Ergebnis auch ohne ein Schutzbedarfsanalyse Ende-zu-Ende verschlüsselt werden. Betrachtet man den Versand einzelner Nachrichten, würde eine Schutzbedarfsanalyse an sich zu dem Ergebnis kommen, dass in bestimmten Fällen (z. B. beim Schutzbedarf „normal“) eine Ende-zu-Ende-Verschlüsselung nicht erforderlich ist. Hier muss aber berücksichtigt werden, dass im Falle eines unberechtigten Zugriffs beim DMDA durch die Vielzahl der versandten bzw. empfangenen Daten ein erhöhtes Angriffsrisiko und Schadenspotential vorliegt (Kumulationseffekt). Außerdem kann der Betroffene nicht entscheiden, auf welche Weise seine Daten versandt werden. Die Tatsache, dass der Betroffene in diesen Fällen keinen Einfluss auf die Ausgestaltung der De-Mail-Nutzung nehmen kann, darf nicht zu einer Absenkung des Datenschutzniveaus bei der Versendung besonders schutzbedürftiger Daten mittels De-Mail führen. Schließlich kann man davon ausgehen, dass solche Einrichtungen den De-Mail-Dienst über ein Gateway nutzen können und daher eine Ende-zu-Ende-Verschlüsselung in diesen Fällen mit vertretbarem technischen Aufwand möglich ist. Die Verpflichtung gilt unabhängig von der Größe der Einrichtung und unabhängig davon, ob eine gesetzliche Pflicht zur Datenverarbeitung besteht. Letztlich führt die einheitliche Behandlung alle Nachrichteninhalte in diesem Kommunikationsverhältnis auch zur einer handhabbaren Anwendung für Versender und Empfänger.

Der Entwicklungsstand der Technik und die tatsächliche Verfahrensweise im Umgang mit De-Mail muss beobachtet werden. Daraus können sich in Zukunft neue oder andere Anforderungen des Datenschutzes an die Verwendung von De-Mail und die Verschlüsselung ergeben. Die DMDA werden aufgefordert, leicht handhabbare Verschlüsselungsoptionen für die Nutzer zu entwickeln. Dies kann auch Datenschutzverstöße aufgrund einer fehlerhaften Schutzbedarfsfeststellung der verantwortlichen Stelle verhindern.

Schließlich müssen auch die internen Verfahrensabläufe bei der versendenden sowie bei der empfangenden Stelle betrachtet werden, also z. B. die Verknüpfung des Fachverfahrens mit dem De-Mail-Postfach und interne Zugriffsberechtigungen in den Unternehmen und Behörden. Auch diese müssen datenschutzkonform ausgestaltet sein und die Sicherheit der Daten gewährleisten.

[1] Dies gilt generell für den Versand personenbezogener Daten, also auch für solche, die als nicht besonders schutzbedürftig eingestuft werden.

[2] Vgl. Fußnote 1.

Anlage 7

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

BfDI

Datenschutzrechtliche Grundlagen der Videoüberwachung in der öffentlichen Verwaltung des Bundes

Stand: Februar 2013

Nach einer Erhebung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) im Jahr 2011 werden in der Bundesverwaltung über 17.500 Videokameras im Innen- und Außenbereich eingesetzt.

Werden personenbezogene Daten (§ 3 Abs. 1 Bundesdatenschutzgesetz [BDSG]) durch Videoüberwachungstechnik erhoben und/oder verarbeitet, stellt dies einen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen - Passanten, Besucher, Anwohner, Mitarbeiter der Dienststelle - dar. Dies gilt unabhängig davon, ob die erhobenen Bilddaten dauerhaft aufgezeichnet oder lediglich auf einen Monitor übertragen werden. Der Eingriff in das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung (Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 des Grundgesetzes) bedarf stets einer besonderen Rechtfertigung.

Bei der datenschutzrechtlichen Beurteilung der Zulässigkeit der Videoüberwachung spielt die Unterscheidung zwischen öffentlich zugänglichen und nicht öffentlich zugänglichen Räumen eine wichtige Rolle:

Liegenschaften von Behörden des Bundes sind in der Regel nicht dazu bestimmt, von einem unbestimmten Personenkreis betreten und genutzt zu werden (nicht öffentlich zugängliche Räume). Etwas anderes gilt beispielsweise bei den ebenfalls der Kontrolle des BfDI unterliegenden Jobcentern, die über Amtsbereiche mit Publikumsverkehr verfügen. Aber auch dort, wo eine Nutzungsmöglichkeit durch die Allgemeinheit nicht gegeben ist, kann die Videoüberwachung öffentlich zugängliche Bereiche erfassen, zum Beispiel Gehwege im öffentlichen Straßenraum. Die Videoüberwachung dieser allgemein zugänglichen Bereiche kann notwendig sein, um auf der Grundstücksgrenze verlaufende Häuserfassaden vor Schäden durch Vandalismus zu schützen oder ein unbefugtes Übertreten der Grundstücksgrenzen zu verhindern bzw. zu dokumentieren (Objektsicherung, Zugangskontrolle). Da die Videoüberwachung im öffentlich zugänglichen Bereich viele Personen trifft, die keinen Anlass für die Überwachung gegeben haben, müssen deren schutzwürdige Belange angemessen berücksichtigt werden.

Auch dort, wo in nicht öffentlich zugänglichen Räumen Beschäftigte oder andere Personen mittels Videoüberwachung erfasst werden, müssen datenschutzrechtliche Vorgaben beachtet werden. Dies gilt auch für Bereiche, die nur mit individueller Erlaubnis oder nach einer Zugangskontrolle betreten werden können. Für die Beschäftigten ist der mit der Überwachung des Dienstgebäudes (Eingangsbereiche, Büroflure, Parkplatz, Sicherheitsbereiche) verbundene Eingriff in das Recht auf informationelle Selbstbestimmung von besonderer Intensität, weil sie regelmäßig keine Möglichkeit haben, sich der Videoüberwachung zu entziehen.
Werden öffentlich zugängliche Räume zum Zweck der Eigensicherung der verantwortlichen Stelle überwacht, richtet sich dies nach § 6b BDSG (Abschnitt 1). Die Videoüberwachung von Beschäftigten in nicht öffentlich zugänglichen Räumen bestimmt sich hingegen nach § 32 i.V.m. § 12 Absatz 4 BDSG (Abschnitt 2). Im Anschluss wird die Videoüberwachung durch die Bundespolizei nach § 27 Bundespolizeigesetz als eine bereichsspezifische Regelung zur Videoüberwachung (auch) öffentlich zugänglicher Räume dargestellt (Abschnitt 3). Solche bereichsspezifische Regelungen gehen § 6b BDSG vor (vgl. § 1 Abs. 3 BDSG).

I. Videoüberwachung öffentlich zugänglicher Räume, § 6b BDSG

1. Rechtsgrundlage

Die datenschutzrechtliche Zulässigkeit der Videoüberwachung öffentlich zugänglicher Räume richtet sich nach § 6b BDSG. Eine Einwilligung der Betroffenen kommt hier als Legitimationsgrundlage aus praktischen Gründen nicht in Betracht. Allein das Betreten eines videoüberwachten Bereichs in Kenntnis der Videoüberwachung stellt keine Einwilligung dar.

Für die Anwendbarkeit des § 6b BDSG ist ohne Belang, ob lediglich eine reine Beobachtung erfolgt oder die erfassten Bilder dauerhaft aufgezeichnet (gespeichert) werden (Gesetzesbegründung, BT-Drs. 14/4329, S. 38). Bereits die Beobachtung (Kamera-Monitor-Prinzip) öffentlich zugänglicher Räume ohne Aufzeichnungsfunktion stellt wegen ihrer potentiell verhaltenslenkenden Wirkung einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar und muss sich an § 6b BDSG messen lassen.

2. Öffentlich zugänglicher Raum

Öffentlich zugängliche Räume sind alle Bereiche, die dazu bestimmt sind, von einem unbestimmten Personenkreis betreten und genutzt zu werden. Es kommt nicht darauf an, ob die Bereiche umschlossen oder überdacht sind. Öffentlich zugängliche Räume können somit innerhalb und außerhalb von Gebäuden liegen.

3. Erfassung personenbezogener Daten

Voraussetzung für die Anwendbarkeit des BDSG ist, dass personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Personenbezogene Daten sind Einzelangaben über persönli-

che oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG).

Abstrakte Kriterien, ab wann ein Personenbezug zu bejahen ist, bestehen nicht. Insbesondere hat sich eine technische Definition (z.B. anhand der Pixelzahl) als nicht praktikabel erwiesen. Maßgeblich ist somit stets der Einzelfall, der anhand der Bildqualität (Entfernung, Auflösung) zu beurteilen ist. Kein Personenbezug besteht bei solchen Übersichtsaufnahmen, bei denen einzelne Personen aufgrund der Bildauflösung auch durch nachträgliche Vergrößerung oder sonstige Bearbeitungsschritte nicht individualisiert werden können.

Der Personenbezug ist bei dem Einsatz von Videoüberwachungstechnik regelmäßig zu bejahen. Es ist schließlich Ziel der Videoüberwachung, potentielle Störer zu erkennen und zu überführen. Es reicht aus, dass einzelne Personen aufgrund der Bildaufnahmen erkennbar und somit individualisierbar sind. Es kommt nicht darauf an, dass die von der Videoüberwachung erfasste Person der verantwortlichen Stelle namentlich bekannt ist oder von ihr identifiziert werden kann.

4. Zweck der Videoüberwachung

§ 6b BDSG knüpft die Zulässigkeit der Videoüberwachung öffentlich zugänglicher Räume an konkrete Überwachungszwecke. Öffentliche Stellen dürfen Videoüberwachung entweder **zur Aufgabenerfüllung** (§ 6b Abs.1 Nr. 1) oder **zur Wahrnehmung ihres Hausrechts** (§ 6b Abs. 1 Nr. 2) einsetzen. Auf die in § 6b Abs. 1 Nr. 3 BDSG ebenfalls vorgesehene „Wahrnehmung berechtigter Interessen“ können sich öffentliche Stellen nicht berufen (Beschlussempfehlung und Bericht des Innenausschusses, BT-Drs. 14/5793, S. 61). Zu beachten ist außerdem, dass die Videoüberwachung gegenüber Beschäftigten allein aufgrund des Hausrechts nicht gerechtfertigt ist. Da die Beschäftigten sich der Überwachung nicht durch Verlassen der Räumlichkeiten entziehen können, unterliegt das Hausrecht insoweit Einschränkungen (BAG, Beschluss vom 14. Dezember 2004, 1 ABR 34/03, NJOZ 2005, 2708, 2714).

Die Zwecke der Videoüberwachung müssen bereits vor Inbetriebnahme der Anlage konkret festgelegt und im Verfahrensverzeichnis dokumentiert werden. Eine Videoüberwachung für unbestimmte Zwecke ist unzulässig.

Der Einsatz von Videoanlagen in der Bundesverwaltung dient in aller Regel der Eigensicherung der jeweiligen Liegenschaften. Dadurch sollen Schäden an dem überwachten Gebäude und der sich darin aufhaltenden Personen (Objektsicherung) oder das Betreten durch unbefugte Personen (Zugangskontrolle) verhindert bzw. zur Beweissicherung dokumentiert werden. Videoüberwachung kann sowohl präventive (Abwehr von drohenden Gefahren) als auch repressive Ziele (Dokumentation von Verstößen) verfolgen.

Bei dem Einsatz von Videoüberwachungstechnik zu präventiven Zwecken (Gefahrenabwehr) genügt die bloße Behauptung oder Vermutung einer Gefährdungslage grundsätzlich nicht. Andererseits muss es in der Vergangenheit nicht bereits zu konkreten Vorfällen gekommen sein, um eine Videoüberwachung zu begründen. Erforderlich, aber auch ausreichend ist das Vorliegen konkreter Anhaltspunkte, die das Bestehen einer Gefährdungslage nach der allgemeinen Lebenserfahrung wahrscheinlich erscheinen lässt (abstrakte Gefahr). Bei der Gefahrenprognose ist einerseits die Höhe der möglichen Schäden, andererseits die Wahrscheinlichkeit eines Vorfalls zu berücksichtigen.

Erfolgt die Überwachung zur Beobachtung von Besuchern, ist sicherzustellen, dass zweckentfremdende Leistungskontrollen der miterfassten Beschäftigten ausgeschlossen sind. Eine solche Kontrolle wäre mit der Zweckbestimmung der Datenerhebung und -speicherung unvereinbar.

5. Erforderlichkeit

Der Einsatz von Videoüberwachungstechnik darf nur erfolgen, wenn kein milderes, gleich geeignetes Mittel zur Verfügung steht, mit dem sich die verfolgten Zwecke erreichen lassen.

Bei der Beschränkung auf das erforderliche Maß spielen technisch-organisatorische Maßnahmen (§ 9 BDSG) eine wichtige Rolle. Schon vor der Inbetriebnahme einer Videoüberwachungsanlage sollten folgende Fragen berücksichtigt werden:

- Muss eine permanente Videoüberwachung erfolgen oder kann sie zeitlich begrenzt werden (z.B. Videoüberwachung nur innerhalb oder außerhalb der Dienstzeiten, anlassbezogene Aktivierung)?

- Bedarf es einer Aufzeichnung oder genügt eine Übertragung auf einen Monitor (z.B. beim Einsatz eines Wachdienstes, ggf. mit anlassbezogener Aktivierung der Aufzeichnung)?

- Kann der verfolgte Zweck auch auf andere Weise erreicht werden (z.B. Schutz vor unbefugtem Betreten durch Zugangskontrollsysteme, Umzäunungen; Schutz vor Vandalismus durch bessere Beleuchtung, häufigere Kontrollen durch den Sicherheitsdienst)?

- Muss zwingend ein großflächiger Bereich überwacht werden oder kann die Videoüberwachung räumlich beschränkt werden? Können nicht überwachungsbedürftige Zonen (digital) ausgeblendet werden?

- Die Aufnahmen und Aufzeichnungen sind vor unberechtigter Nutzung angemessen zu schützen, z.B. durch Aufstellung der Server in verschließbaren Räumen, Passwort-

schutz, Festplattenverschlüsselung, Vergabe von Zugriffsberechtigungen, revisionssichere Protokollierung des Zugriffs. Zudem sind die Monitore so aufzustellen, dass Unbefugte keinen Einblick nehmen können. Für eine fristgerechte datenschutzrechtliche Löschung der Daten ist zu sorgen.

- Die technisch-organisatorischen Mindestanforderungen an digitale Videoüberwachungsanlagen werden in dem gemeinsam von BfDI und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelten Schutzprofil für Videoüberwachungsanlagen[1] beschrieben. Das Video-Schutzprofil enthält technische Anforderungen, die von digitalen Videosystemen erfüllt sein müssen, damit sie gemäß den Bestimmungen der Datenschutzgesetze des Bundes und der Länder eingesetzt werden können. Das Schutzprofil definiert einen Mindestsatz an Sicherheitsfunktionalität, der bei der Beschaffung, der Installation und dem Betrieb von Videoüberwachungsanlagen zu beachten ist. Es legt besonderen Wert darauf, dass die Funktionen für einen sicheren Zugriffsschutz, eine datenschutzrechtliche Löschung der Daten sowie eine revisionssichere Protokollierung vorhanden sind.

Bei der Überwachung der Liegenschaft ist zudem darauf zu achten, dass die Kontrollbefugnis der verantwortlichen Stelle an der Grundstücksgrenze endet. Sollen an der Grundstücksgrenze verlaufende Hausfassaden oder Umzäunungen kontrolliert werden, muss sich die Videobeobachtung des öffentlichen Straßenraums auf das unbedingt erforderliche Maß beschränken. Allenfalls ein Toleranzbereich von einem Meter ab der Grundstücksgrenze ist als noch zulässig anzusehen, sofern schutzwürdige Interessen dem nicht entgegenstehen (vgl. AG Berlin-Mitte, Urteil vom 18. 12. 2003 - 16 C 427/02, NJW-RR 2004, 531-534).

Die Videoüberwachung des öffentlichen Straßenraums, öffentlicher Grünflächen oder von Nachbargrundstücken ist unzulässig.

6. Verhältnismäßigkeit

Für den datenschutzkonformen Einsatz von Videoüberwachungstechnik unabdingbar ist eine konkrete Interessenabwägung mit den schutzwürdigen Belangen der Betroffenen. Bestehen Anhaltspunkte, dass die schutzwürdigen Belange der durch die Videoüberwachung betroffenen Personen gegenüber den von der verantwortlichen Stelle verfolgten Zwecken überwiegen, hat die Videoüberwachung zu unterbleiben.

Im Rahmen der Interessenabwägung ist zu berücksichtigen, dass die Aufzeichnung der Bilddaten gegenüber der speicherlosen Übertragung einen wesentlich tieferen Eingriff in die Rechte der Betroffenen darstellt, da die Daten mit der Speicherung für eine dauerhafte Auswertung und Verknüpfung zur Verfügung stehen.

[1] Common Criteria Protection Profile - Software zur Verarbeitung von personenbezogenen Bilddaten, Stand: Januar 2007, BSI-PP-0023

Es muss zudem zwischen analogen und digitalen Überwachungsanlagen unterschieden werden. Während die Auswertbarkeit von analogen Überwachungen sehr beschränkt ist und in der Regel sich nur auf die Speicherung von Videosequenzen beschränkt, kann bei digitalen Anlagen eine vollautomatisierte Auswertung vorgenommen werden, die auch biometrische und andere Techniken (Datenabgleiche) umfassen kann. Heute werden in der Regel digitale Anlagen eingesetzt.

Die Prüfung der Verhältnismäßigkeit hat für jeden Schritt der Verarbeitung und Nutzung der Daten separat zu erfolgen. Sollen personenbezogene Daten daher nicht nur erhoben und gespeichert, sondern darüber hinaus noch weiter verarbeitet werden, ist eine gesonderte Bewertung der Zulässigkeit geboten (Beschlussempfehlung und Bericht des Innenausschusses, BT-Drs. 14/5793, S. 62), vgl. auch § 6b Abs. 3 BDSG.

Je stärker in die schutzwürdigen Belange der Betroffenen eingegriffen wird, desto höher sind die Anforderungen an die Rechtfertigung der Videoüberwachung. Je leistungsfähiger die eingesetzte Technik ist und je größer die Möglichkeiten der automatisierten Auswertung, desto stärker sind die schutzwürdigen Belange der Betroffenen in der Abwägung zu berücksichtigen.

In folgenden Fällen sind schutzwürdige Belange der Betroffenen besonders stark betroffen:

- Permanente und lückenlose Überwachung, der sich die Betroffenen nicht entziehen können

- Möglichkeit der automatisierten Auswertung der Bilddateien (z.B. zum Bildabgleich; zum Zweck biometrischer Gesichtserkennung; Vergrößern und Selektion einzelner Personen; Bildung von Bewegungsprofilen)

- Erfassung einer Vielzahl von Personen, die ohne konkreten Anlass überwacht werden

- Erfassung von Bereichen, die der ungezwungenen und freien Entfaltung der Persönlichkeit dienen (Kantinen, Raucherecken, Wartebereiche).

Die Erfassung von Nachbargrundstücken und -wohnungen durch Videokameras ist datenschutzrechtlich unzulässig. Sie kann zudem strafrechtliche Relevanz haben (§ 201a Strafgesetzbuch). Nach Ansicht des LG Bonn (Urteil v. 16.11.2004, Az. 8 S 139/04) verletzt dabei auch das Aufstellen von täuschend echt aussehenden Attrappen das allgemeine Persönlichkeitsrecht der Nachbarn, da für sie nicht erkennbar ist, ob sie tatsächlich gefilmt werden oder nicht.

Unzulässig ist zudem die Erfassung höchstpersönlicher Bereiche (z.B. Waschräume).

Werden auch Beschäftigte von der Überwachung erfasst, so ist bei der Verhältnismäßigkeitsprüfung deren allgemeines Persönlichkeitsrecht (Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 GG) von besonderer Bedeutung. Die im zweiten Abschnitt dargestellten Abwägungskriterien sind daher bei der Überwachung in öffentlich zugänglichen Bereichen gleichermaßen zu beachten (vgl. dazu unten Seite 10f.).

7. Hinweispflicht, § 6b Abs. 2 BDSG

Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen (§ 6b Abs. 2 BDSG). Die Betroffenen sollen durch die Hinweispflicht eine Vorstellung davon bekommen, welcher Bereich erfasst wird und an wen sie sich zur Ausübung ihrer Betroffenenrechte wenden können. Erst hierdurch werden sie in die Lage versetzt, der Videoüberwachung auszuweichen oder sich zumindest auf diese einzustellen. Zur Erfüllung der Hinweispflicht kommen Hinweisschilder oder Piktogramme in Betracht. Diese müssen deutlich sichtbar platziert sein, so dass die Betroffenen eine zumutbare Möglichkeit der Kenntnisnahme haben.

Zur Erfüllung der Hinweispflicht sollte das Info-Zeichen nach DIN 33450 in Verbindung mit dem Hinweis auf die verantwortliche Stelle („Dieser Bereich wird von/vom ...videoüberwacht“) genutzt werden:

Die Hinweispflicht gilt ausnahmslos. Heimliche Videoüberwachungen sind im Bereich des § 6b BDSG ausgeschlossen. Eine andere Auffassung vertritt das Bundesarbeitsgericht zur heimlichen Überwachung von Mitarbeitern in öffentlich zugänglichen Räumen in seinem Urteil vom 21. Juni 2012 (2 AZR, 153/11, NZA 2012, 1025 ff.). Dieses Urteil knüpft an die „Wahrnehmung berechtigter Interessen“ nach § 6b Absatz 1 Nummer 3 BDSG an. So soll eine verdeckte Videoüberwachung auch in öffentlich zugänglichen Räumen nach § 6b Absatz 1 Nummer 3 BDSG zulässig sein, falls sie das einzige Mittel zur Überführung von Beschäftigten ist, die der Begehung von Straftaten konkret verdächtig sind. § 6b Absatz 1 Nummer 3 BDSG ist für öffentliche Stellen aber nicht anwendbar (vgl. oben Seite 3). Bezogen auf die Zwecke „Aufgabenerfüllung öffentlicher Stellen“ sowie „Wahrnehmung des Hausrechts“

wird es bereits an der Erforderlichkeit der heimlichen Mitarbeiterüberwachung fehlen, so dass diese unzulässig ist.

8. Benachrichtigung der Betroffenen, § 6b Absatz 4 BDSG

Auch wenn eine Identifizierung der erfassten Personen für die Anwendung des § 6b BDSG nicht entscheidend ist (dazu bereits oben unter 3.), muss die verantwortliche Stelle die Betroffenen nach Maßgabe des § 19a BDSG benachrichtigen (§ 6b Abs. 4 BDSG), wenn sie diesen die durch Videoüberwachung erhobenen Daten zuordnet. Die Benachrichtigungspflicht greift allerdings nur, wenn die Daten einer bestimmten, identifizierten Person tatsächlich zugeordnet werden. Das ist typischerweise erst der Fall, wenn einzelne Videosequenzen zum Nachweis bspw. eines strafbaren Verhaltens selektiert und ausgewertet werden. Andererseits löst allein das Durchschreiten eines videoüberwachten Bereichs durch eine bekannte Person (z.B. einen Mitarbeiter der Dienststelle) nicht die Benachrichtigungspflicht aus. Durch die Benachrichtigungspflicht soll gewährleistet werden, dass die Person von der Überwachung und der anschließenden Speicherung/Auswertung Kenntnis erhält und selbst für die Wahrung ihrer Recht eintreten kann.

9. Löschung der Daten

Die durch Videoüberwachung aufgezeichneten personenbezogenen Daten sind **unverzüglich** zu löschen, wenn sie zur Erreichung des verfolgten Zwecks **nicht mehr erforderlich sind** oder **schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegen stehen** (§ 6b Abs. 5 BDSG). Nicht mehr erforderlich und daher zu löschen sind alle Aufzeichnungen, die nicht mehr für die Gefahrenabwehr (präventive Zwecke) oder zur Rechtsverfolgung (repressive Zwecke) benötigt werden. Die zweite Alternative (schutzwürdige Interessen der Betroffenen stehen einer weiteren Speicherung entgegen) wird relevant, wenn die verantwortliche Stelle festgestellten Vorkommnissen nicht in angemessener Zeit nachgeht.

Um der Löschungspflicht nachzukommen, hat die verantwortliche Stelle zunächst festzustellen, ob das angefallene Videomaterial überhaupt aufklärungsbedürftige Vorkommnisse enthält. Diese Bedarfsklärung hat unverzüglich zu erfolgen (BT-Drs. 14/5793, S. 63).

Der Begriff „unverzüglich“ ist als Handeln ohne schuldhaftes Zögern (§ 121 Bürgerliches Gesetzbuch) zu verstehen. Die Bedarfsklärung und die sich unmittelbar daran anschließende Entscheidung, ob die weitere Sicherung der Aufzeichnungen notwendig ist, kann regelmäßig innerhalb von ein bis zwei Arbeitstagen erfolgen (Beschlussempfehlung und Bericht des Innenausschusses, BT-Drs. 14/5793, S. 63). Nicht erforderliche Daten sind daher im Regelfall **spätestens** nach Ablauf **einer Woche** zu löschen. Empfehlenswert ist hierbei, die Regellöschfristen durch ein automatisches Überschreiben der zurückliegenden Aufnahmen zu gewährleisten.

10. Verfahrensverzeichnis und Vorabkontrolle

Stellt die Videoüberwachung ein Verfahren automatisierter Datenverarbeitung dar, ist sie in das Verfahrensverzeichnis der verantwortlichen Stelle aufzunehmen (§ 4g Abs. 2 i. V. m. §§ 4e Abs. 1, 18 Abs. 2 BDSG).

Entscheidend für das Vorliegen einer automatisierten Verarbeitung ist die **erleichterte Zugänglichkeit und Auswertbarkeit** der Daten in einem Datenbestand. Ein Verfahren automatisierter Verarbeitung ermöglicht es also, verschiedene personenbezogene Daten programmgesteuert nach ihrem Informationsgehalt zu selektieren, wie dies z.B. bei der Unterscheidung nach dem Zeitpunkt der Aufnahme oder nach bestimmten Identifikations- und Sachmerkmalen wie biometrischen Daten der Fall ist.

Erfolgt bereits die **Erfassung** der Bilder programmgesteuert und selektiv oder ist dies technisch möglich – z.B. Videosystem mit integrierter Gesichts- und Stimmerkennung, selektive Erfassung anhand von Name, Zeit oder Ort des Aufenthalts – ist die Kameratechnik wegen der bestehenden Auswertungsmöglichkeiten der erfassten Bilder schon bereits bei reinen Übertragungen verzeichnispflichtig. Hier handelt es sich häufig um digitale, „intelligente" Kameras bzw. „*thinking cameras*". Gleiches gilt wenn die **Aufzeichnung** programmgesteuert nach bestimmten Merkmalen auswertbar ist. Ist dies nicht möglich, stellt die Aufzeichnung der Bilddaten kein automatisiertes Verfahren dar.

Die Übertragung von Bildaufzeichnungen auf einen Monitor (Kamera-Monitor-Prinzip) ist nicht verzeichnispflichtig, wenn das übertragene Monitorbild lediglich als „verlängertes Auge" die Wirklichkeit abbildet, ohne dass eine inhaltsbezogene Datenverarbeitung automatisiert stattfindet. Dies betrifft insb. die Verwendung analoger Videotechnik.

Die als automatisierte Verarbeitung erfolgende Videoüberwachung unterliegt zudem regelmäßig der **Vorabkontrolle** durch den behördlichen Datenschutzbeauftragten (vgl. § 4d Abs. 5 BDSG), weil der Einsatz der Videotechnik besondere Risiken für die Rechte und Freiheiten der betroffenen Personen aufweist. Anhaltspunkte für das Vorliegen besonderer Risiken sind u.a.:

- Anlasslose Überwachung einer Vielzahl von Betroffenen
- Großflächigkeit und Intensität der Überwachung,
- eingesetzte Technik (hohe Auflösung, Schwenkbarkeit) und damit verbundene Auswertbarkeit, insb. zu Bewegungsprofilen.

Ausnahmen von der Vorabkontrolle sind im Einzelfall denkbar, wenn die Videoüberwachung lediglich punktuell, ohne hohe Auflösung und ohne Möglichkeit des Herausfilterns einzelner Personen eingesetzt wird.

II. Videoüberwachung von Beschäftigten in nicht öffentlich zugänglichen Räumen

1. Rechtsgrundlage

Seit Inkrafttreten des § 32 BDSG zum 1. September 2009 richtet sich die datenschutzrechtliche Rechtmäßigkeit der Videoüberwachung von Beschäftigten in nicht öffentlich zugänglichen Räumen nach § 32 Absatz 1 Satz 1 und 2 i.V.m. § 12 Absatz 4 BDSG. § 32 BDSG soll jedoch, so der Gesetzgeber, die bis dahin von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen (BT-Drs. 16/13657, S. 20).

Für die Beurteilung der Rechtmäßigkeit der Videoüberwachung ist wesentlich, ob es sich um eine offene oder um eine verdeckte Maßnahme handelt.

2. Offene Videoüberwachung

§ 32 Absatz 1 Satz 1, 2. Variante BDSG sieht vor, dass personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden dürfen, wenn dies nach der Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Nach dem Willen des Gesetzgebers soll diese Regelung den von der Rechtsprechung entwickelten Grundsätzen des Datenschutzrechts im Beschäftigungsverhältnis entsprechen (BT-Drs. 16/13657, S. 21); diese Grundsätze finden folglich weiterhin Anwendung.

Daher ist es nicht allein ausreichend, dass die Maßnahme – wie der Wortlaut des § 32 Absatz 1 Satz 1 BDSG vermuten ließe – nützlich ist. Vielmehr muss die Videoüberwachung einer umfassenden Verhältnismäßigkeitsprüfung standhalten. Ausgangspunkt der Verhältnismäßigkeitsprüfung ist der mit der Maßnahme verfolgte Zweck.

Eine rein präventive Videoüberwachung ohne konkreten Anlass stellt einen besonders schwerwiegenden Eingriff in die Persönlichkeitsrechte der Beschäftigten dar und muss daher im Regelfall unterbleiben. Auch zur dauerhaften Überprüfung, ob die Beschäftigten ihren Arbeitspflichten nachkommen, darf Videoüberwachung nicht eingesetzt werden.

Eine präventive Videoüberwachung kann jedoch zur Durchsetzung besonderer Sicherheitsbedürfnisse zulässig sein. In Betracht kommen sowohl Sicherheitsinteressen der verantwortlichen Stelle als auch des Beschäftigten selbst. Es müssen jedoch bereits konkrete Verdachtsmomente oder Anhaltspunkte vorliegen, die das schutzwürdige Interesse der verantwortlichen Stelle belegen.

Wegen der besonderen Intensität des Eingriffs in die Persönlichkeitsrechte des Betroffenen ist die Rechtfertigungsschwelle für die Videoüberwachung allerdings hoch. Denn bei der Videoüberwachung am nicht öffentlich zugänglichen Arbeitsplatz ist der Personenkreis überschaubar und dem Dienstherrn bekannt. Der Überwachungs- und Anpassungsdruck ist für die beo-

bachteten Personen sehr hoch, weil die Überwachung regelmäßig über mehrere Stunden andauert und sich die Beschäftigten der Überwachung nicht entziehen können (BAG, Beschluss vom 29. Juni 2004, 1 ABR 21/03, NZA 2004, 1278, 1282). Der Überwachungsdruck, den bereits die Möglichkeit der jederzeitigen Überwachung auf den Beschäftigten erzeugt, kann nur durch **überwiegende schutzwürdige Belange der verantwortlichen Stelle** gerechtfertigt sein, wobei hier eine Abwägung im Einzelfall zu erfolgen hat (BAG, Beschluss vom 14. Dezember 2004, 1 ABR 34/03, NJOZ 2005, 2708, Ls. 2 und 3).

Bei der Abwägung ist die Eingriffsintensität von Bedeutung, also die Frage, wie viele Personen wie intensiven Beeinträchtigungen ausgesetzt sind, ohne dass sie hierfür einen Anlass gegeben hätten. Die Intensität der Beeinträchtigung hängt dabei maßgeblich von der Dauer und Art der Überwachungsmaßnahme ab (BAG aaO S. 2711 f.). Die Eingriffstiefe verringert sich nicht allein dadurch, dass die Kameras nur zeitweise in Betrieb sind, wenn die Beschäftigten nicht erkennen können, ob und wann eine Videoüberwachung tatsächlich erfolgt. Die Beschäftigten unterliegen in diesem Fall während der gesamten Dauer ihrer Tätigkeit einem erheblichen Überwachungsdruck (BAG, Beschluss vom 14. Dezember 2004, 1 ABR 34/03, NJOZ 2005, 2708, 2712).

Ein schutzwürdiges Interesse der verantwortlichen Stelle kann bei der Aufklärung von Straftaten eines Beschäftigten in Betracht kommen. Die Zulässigkeit beurteilt sich nach § 32 Absatz 1 Satz 2 BDSG. § 32 Absatz 1 Satz 2 BDSG setzt voraus, dass zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten zur Aufklärung erforderlich ist und das schutzwürdige Interesse des Beschäftigten nicht überwiegt, insbesondere Art und Ausmaß der Erhebung, Verarbeitung oder Nutzung im Hinblick auf den Anlass nicht unverhältnismäßig sind. In diesem Fall ist also eine strenge einzelfallbezogene Verhältnismäßigkeitsprüfung notwendig.

3. Verdeckte Videoüberwachung

Eine verdeckte Videoüberwachung kommt allenfalls als *ultima ratio* in Betracht. Das Bundesarbeitsgericht hat vor Inkrafttreten des § 32 BDSG die Auffassung vertreten, dass die verdeckte Videoüberwachung dann zulässig ist, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist (BAG, Urteil vom 27. März 2003, 2 AZR 51/02, NZA 2003, 1193). Der Arbeitgeber hat zu dokumentieren, dass diese Voraussetzungen gegeben sind und er muss die Betroffenen im Nachhinein frühest möglich von der Tatsache und den Ergebnissen der Überwachung informieren. Im Hinblick auf die enorme Eingriffstiefe einer heimlichen Überwachung wird empfohlen, auf derartige Maßnahmen unbeschadet der älteren Rechtsprechung und in Anbetracht der durch den Gesetzgeber mit der Schaffung des § 32 BDSG unterstrichenen Bedeutung des Beschäftigtendatenschutzes zu verzichten.

4. Löschung der Daten

Die Löschung der Daten richtet sich, sofern Beschäftigtendaten nach § 32 BDSG betroffen sind, nach § 35 Absatz 2 BDSG. Die im Rahmen einer Videoüberwachung für eigene Zwecke gespeicherten personenbezogenen Daten sind nach § 35 Absatz 2 Satz 2 Nummer 3 BDSG zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Die Löschung ist zu dokumentieren.

5. Mitbestimmung des Personalrats

Nach § 75 Absatz 3 Nummer 17 BetrVG unterliegt die Einführung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, der Mitbestimmung des Personalrats. Jedoch rechtfertigt eine Dienst- oder Betriebsvereinbarung eine nach den gesetzlichen Bestimmungen rechtswidrige Videoüberwachung nicht. So hat das Bundesarbeitsgericht eine Betriebsvereinbarung, die die Grundrechte der Arbeitnehmer nicht ausreichend achtete, für unwirksam erklärt. Durch die Mitbestimmung des Betriebsrats nach § 87 Absatz 1 Nummer 6 BetrVG solle gerade der Gefahr begegnet werden, dass der Arbeitnehmer zum Objekt einer Überwachungstechnik werde und sein Wissen darum zu erhöhter Abhängigkeit und zur Behinderung der freien Entfaltung seiner Persönlichkeit führe (BAG, Beschluss vom 29. Juni 2004, 1 ABR 21/03, NZA 2004, 1278, 1281). Nach § 75 Absatz 2 BetrVG hätten Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Zwar fehlt eine dem § 75 Absatz 2 BetrVG entsprechende Regelung im Bundespersonalvertretungsgesetz, der Schutz der freien Entfaltung der Persönlichkeit folgt jedoch bereits aus Art. 2 Absatz 1 GG, an den die öffentliche Verwaltung und damit die Dienststellenleitung und die Personalvertretung gebunden sind. Die dargestellte Rechtsprechung ist daher auf die öffentliche Verwaltung übertragbar.

6. Verfahrensverzeichnis und Vorabkontrolle

Hierzu wird auf Abschnitt I Nummer 9 verwiesen.

III. Videoüberwachung von Gebäuden durch die Bundespolizei: § 27 BPolG

Gemäß § 5 Bundespolizeigesetz (BPolG) kann die Bundespolizei Verfassungsorgane des Bundes und Bundesministerien auf deren Ersuchen gegen Gefahren schützen, die die Durchführung ihrer Aufgaben beeinträchtigen. Um derartige Gefahren zu erkennen, darf die Bundespolizei auch Videoüberwachung einsetzen. Die Rechtsgrundlage ist dann § 27 Satz 1 Nr. 2 i. V. m. § 23 Abs. 1 Nr. 4 BPolG. Danach kann die Bundespolizei Videoüberwachung auch zur Eigensicherung ihrer Liegenschaften und zur Überwachung infrastrukturell besonders gefährdeter Objekte – etwa Bahnhöfen und Flughäfen – einsetzen.

Soweit gem. § 27 BPolG Liegenschaften der Bundespolizei, der Verfassungsorgane oder der Bundesministerien videoüberwacht werden, ist der Umfang der Videoüberwachung für jedes Objekt gesondert zu bestimmen. Hierbei sind insbesondere die Gefährdung des Objekts und die Möglichkeit des ungehinderten Zugangs von Personen zu dem Objekt maßgeblich. Dabei sollten grundsätzlich auch die im ersten Teil dieser Orientierungshilfe aufgeführten Gesichtspunkte nach Maßgabe folgender Erwägungen Beachtung finden:

1. Erkennbarkeit

Gemäß § 27 Satz 2 BPolG müssen die eingesetzten Geräte erkennbar sein. Daraus folgt eine Hinweispflicht, für die die Ausführungen in Abschnitt I Nummer 7 entsprechend gelten (vgl. oben Seite 7).

2. Speicherdauer

Nach § 27 BPolG Satz 3 müssen personenbezogene Daten, die durch die Videokameras erhoben worden sind, spätestens nach 30 Tagen vernichtet werden, soweit sie nicht zur Abwehr einer gegenwärtigen Gefahr oder zur Verfolgung einer Straftat oder einer Ordnungswidrigkeit benötigt werden. Den ihr zugebilligten Spielraum bei der Speicherdauer muss die Bundespolizei nach der Maßgabe der Erforderlichkeit und Verhältnismäßigkeit ausfüllen. Insofern ist ein Konzept erforderlich, das aufgrund von kriminalistischen Erfahrungswerten und der Gefahrenlage eine grundrechtsschonende Aufzeichnungspraxis sicherstellt. Eine pauschale Speicherung für die gesetzliche Höchstdauer würde diesen Vorgaben nicht genügen.

Anlage 8

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 17. Januar 2012)

Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen. Der Text lautet wie folgt:

Einwilligung in die Erhebung und Verwendung von Gesundheitsdaten und Schweigepflichtentbindungserklärung[a]

Die Regelungen des Versicherungsvertragsgesetzes, des Bundesdatenschutzgesetzes sowie anderer Datenschutzvorschriften enthalten keine ausreichenden Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen. Um Ihre Gesundheitsdaten für diesen Antrag und den Vertrag erheben und verwenden zu dürfen, benötigt die Versicherung XY[1] daher Ihre datenschutzrechtliche(n) Einwilligung(en). Darüber hinaus benötigt die Versicherung XY Ihre Schweigepflichtentbindungen, um Ihre Gesundheitsdaten bei schweigepflichtigen Stellen, wie z.B. Ärzten, erheben zu dürfen. Als Unternehmen der Lebensversicherung (*Krankenversicherung*)[2] benötigt die Versicherung XY Ihre Schweigepflichtentbindung ferner, um Ihre Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Daten, wie z. B. die Tatsache, dass ein Vertrag mit Ihnen besteht, an andere Stellen, z. B. …[3] weiterleiten zu dürfen.

Die folgenden Einwilligungs- und Schweigepflichtentbindungserklärungen[4] sind für die Antragsprüfung sowie die Begründung, Durchführung oder Beendigung Ihres Versicherungsvertrages in der Versicherung XY unentbehrlich. Sollten Sie diese nicht abgeben, wird der Abschluss des Vertrages in der Regel nicht möglich sein.[5]

Die Erklärungen betreffen den Umgang mit Ihren Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

[a] Der Text der Einwilligungs-/Schweigepflichtentbindungserklärung wurde 2011 mit den Datenschutzaufsichtsbehörden inhaltlich abgestimmt.

- durch die Versicherung XY *[Versicherungsgesellschaft, mit der der Versicherungsvertrag abgeschlossen wird]* selbst (unter 1.),
- im Zusammenhang mit der Abfrage bei Dritten (unter 2.),
- bei der Weitergabe an Stellen außerhalb der Versicherung XY (unter 3.) und
- wenn der Vertrag nicht zustande kommt (unter 4.).

Die Erklärungen gelten für die von Ihnen gesetzlich vertretenen Personen wie Ihre Kinder, soweit diese die Tragweite dieser Einwilligung nicht erkennen und daher keine eigenen Erklärungen abgeben können.[6]

1. Erhebung, Speicherung und Nutzung der von Ihnen mitgeteilten Gesundheitsdaten durch die Versicherung XY

Ich willige ein, dass die Versicherung XY die von mir in diesem Antrag und künftig mitgeteilten Gesundheitsdaten erhebt, speichert und nutzt, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Versicherungsvertrages erforderlich ist.

2. Abfrage von Gesundheitsdaten bei Dritten

2.1. Abfrage von Gesundheitsdaten bei Dritten zur Risikobeurteilung und zur Prüfung der Leistungspflicht[7]

Für die Beurteilung der zu versichernden Risiken kann es notwendig sein, Informationen von Stellen abzufragen, die über Ihre Gesundheitsdaten verfügen. Außerdem kann es zur Prüfung der Leistungspflicht erforderlich sein, dass die Versicherung XY die Angaben über Ihre gesundheitlichen Verhältnisse prüfen muss, die Sie zur Begründung von Ansprüchen gemacht haben oder die sich aus eingereichten Unterlagen (z. B. Rechnungen, Verordnungen, Gutachten) oder Mitteilungen z. B. eines Arztes oder sonstigen Angehörigen eines Heilberufs ergeben.

Diese Überprüfung erfolgt nur, soweit es erforderlich ist. Die Versicherung XY benötigt hierfür Ihre Einwilligung einschließlich einer Schweigepflichtentbindung für sich sowie für diese Stellen, falls im Rahmen dieser Abfragen Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Informationen weitergegeben werden müssen.

Sie können diese Erklärungen bereits hier (I) oder später im Einzelfall (II) erteilen. Sie können Ihre Entscheidung jederzeit ändern. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:

Möglichkeit I:

☐ Ich willige ein, dass die Versicherung XY – soweit es für die Risikobeurteilung oder für die Leistungsfallprüfung erforderlich ist – meine Gesundheitsdaten bei Ärzten, Pflegepersonen sowie bei Bediensteten von Krankenhäusern, sonstigen Krankenanstalten, Pflegeheimen, Personenversicherern, gesetzlichen Krankenkassen, Berufsgenossenschaften und Behörden[8] erhebt und für diese Zwecke verwendet.

Ich befreie die genannten Personen und Mitarbeiter der genannten Einrichtungen von ihrer Schweigepflicht, soweit meine zulässigerweise gespeicherten Gesundheitsdaten aus Untersuchungen, Beratungen, Behandlungen sowie Versicherungsanträgen und -verträgen aus einem Zeitraum von bis zu zehn Jahren[9] vor Antragstellung an die Versicherung XY übermittelt werden.

Ich bin darüber hinaus damit einverstanden, dass in diesem Zusammenhang – soweit erforderlich – meine Gesundheitsdaten durch die Versicherung XY an diese Stellen weitergegeben werden und befreie auch insoweit die für die Versicherung XY tätigen Personen von ihrer Schweigepflicht.

Ich werde vor jeder Datenerhebung nach den vorstehenden Absätzen unterrichtet, von wem und zu welchem Zweck die Daten erhoben werden sollen, und ich werde darauf hingewiesen, dass ich widersprechen und die erforderlichen Unterlagen selbst beibringen kann.[10]

Möglichkeit II:

☐ Ich wünsche, dass mich die Versicherung XY in jedem Einzelfall informiert, von welchen Personen oder Einrichtungen zu welchem Zweck eine Auskunft benötigt wird. Ich werde dann jeweils entscheiden, ob ich

- in die Erhebung und Verwendung meiner Gesundheitsdaten durch die Versicherung XY einwillige, die genannten Personen oder Einrichtungen sowie deren Mitarbeiter von ihrer Schweigepflicht entbinde und in die Übermittlung meiner Gesundheitsdaten an die Versicherung XY einwillige
- oder die erforderlichen Unterlagen selbst beibringe.

Mir ist bekannt, dass dies zu einer Verzögerung der Antragbearbeitung oder der Prüfung der Leistungspflicht führen kann.

Soweit sich die vorstehenden Erklärungen auf meine Angaben bei Antragstellung beziehen, gelten sie für einen Zeitraum von fünf Jahren[11] nach Vertragsschluss. Ergeben sich nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte[12] dafür, dass bei der Antragstellung vorsätzlich unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde, gelten die Erklärun-

gen bis zu zehn Jahre nach Vertragsschluss.

2.2. Erklärungen für den Fall Ihres Todes

Zur Prüfung der Leistungspflicht kann es auch nach Ihrem Tod erforderlich sein, gesundheitliche Angaben zu prüfen. Eine Prüfung kann auch erforderlich sein, wenn sich bis zu zehn Jahre nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte dafür ergeben, dass bei der Antragstellung unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde. Auch dafür bedürfen wir einer Einwilligung und Schweigepflichtentbindung. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:[13]

Möglichkeit I:

□ Für den Fall meines Todes willige ich in die Erhebung meiner Gesundheitsdaten bei Dritten zur Leistungsprüfung bzw. einer erforderlichen erneuten Antragsprüfung ein wie im ersten Ankreuzfeld beschrieben (siehe oben 2.1. – Möglichkeit I).

Möglichkeit II:

□ Soweit zur Prüfung der Leistungspflicht bzw. einer erforderlichen erneuten Antragsprüfung nach meinem Tod Gesundheitsdaten erhoben werden müssen, geht die Entscheidungsbefugnis über Einwilligungen und Schweigepflichtentbindungserklärungen auf meine Erben oder – wenn diese abweichend bestimmt sind – auf die Begünstigten des Vertrags über.

3. Weitergabe Ihrer Gesundheitsdaten und weiterer nach § 203 StGB geschützter Daten an Stellen außerhalb der Versicherung XY

Die Versicherung XY verpflichtet die nachfolgenden Stellen vertraglich auf die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit.[14]

3.1. Datenweitergabe zur medizinischen Begutachtung

Für die Beurteilung der zu versichernden Risiken und zur Prüfung der Leistungspflicht kann es notwendig sein, medizinische Gutachter einzuschalten. Die Versicherung XY benötigt Ihre Einwilligung und Schweigepflichtentbindung, wenn in diesem Zusammenhang Ihre Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten übermittelt werden. Sie werden über die jeweilige Datenübermittlung unterrichtet.[15]

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten an medizinische

Gutachter übermittelt, soweit dies im Rahmen der Risikoprüfung oder der Prüfung der Leistungspflicht erforderlich ist und meine Gesundheitsdaten dort zweckentsprechend verwendet und die Ergebnisse an die Versicherung XY zurück übermittelt werden. Im Hinblick auf meine Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten entbinde ich die für die Versicherung XY tätigen Personen und die Gutachter von ihrer Schweigepflicht.

3.2. Übertragung von Aufgaben auf andere Stellen (Unternehmen oder Personen)

Die Versicherung XY führt bestimmte Aufgaben, wie zum Beispiel die Risikoprüfung, die Leistungsfallbearbeitung oder die telefonische Kundenbetreuung, bei denen es zu einer Erhebung, Verarbeitung oder Nutzung Ihrer Gesundheitsdaten kommen kann, nicht selbst durch, sondern überträgt die Erledigung einer anderen Gesellschaft der XY-Gruppe oder einer anderen Stelle. Werden hierbei Ihre nach § 203 StGB geschützten Daten weitergegeben, benötigt die Versicherung XY Ihre Schweigepflichtentbindung für sich und[16] soweit erforderlich für die anderen Stellen.[17]

Die Versicherung XY führt eine fortlaufend aktualisierte Liste[18] über die Stellen[19] und Kategorien von Stellen[20], die vereinbarungsgemäß Gesundheitsdaten für die Versicherung XY erheben, verarbeiten oder nutzen unter Angabe der übertragenen Aufgaben. Die zurzeit gültige Liste ist als Anlage der Einwilligungserklärung angefügt.[21] Eine aktuelle Liste kann auch im Internet unter (*Internetadresse*) eingesehen oder bei (*Ansprechpartner nebst Anschrift, Telefonnummer, ggf. E-Mailadresse*) angefordert werden. Für die Weitergabe Ihrer Gesundheitsdaten an und die Verwendung durch die in der Liste genannten Stellen benötigt die Versicherung XY Ihre Einwilligung.

Ich willige ein,[22] dass die Versicherung XY meine Gesundheitsdaten an die in der oben erwähnten Liste genannten Stellen übermittelt und dass die Gesundheitsdaten dort für die angeführten Zwecke im gleichen Umfang erhoben, verarbeitet und genutzt werden, wie die Versicherung XY dies tun dürfte. Soweit erforderlich, entbinde ich die Mitarbeiter der XY Unternehmensgruppe und sonstiger Stellen[23] im Hinblick auf die Weitergabe von Gesundheitsdaten und anderer nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.3. Datenweitergabe an Rückversicherungen

Um die Erfüllung Ihrer Ansprüche abzusichern, kann die Versicherung XY Rückversicherungen einschalten, die das Risiko ganz oder teilweise übernehmen. In einigen Fällen bedienen sich die Rückversicherungen dafür weiterer Rückversicherungen, denen sie ebenfalls Ihre Daten[24] übergeben. Damit sich die Rückversicherung ein eigenes Bild über das Risiko oder den Versicherungsfall machen kann, ist es möglich, dass die Ver-

sicherung XY Ihren Versicherungsantrag oder Leistungsantrag der Rückversicherung vorlegt. Das ist insbesondere dann der Fall, wenn die Versicherungssumme besonders hoch ist oder es sich um ein schwierig einzustufendes Risiko handelt.

Darüber hinaus ist es möglich, dass die Rückversicherung die Versicherung XY aufgrund ihrer besonderen Sachkunde bei der Risiko- oder Leistungsprüfung sowie bei der Bewertung von Verfahrensabläufen unterstützt.

Haben Rückversicherungen die Absicherung des Risikos übernommen, können sie kontrollieren, ob die Versicherung XY das Risiko bzw. einen Leistungsfall richtig eingeschätzt hat.

Außerdem werden Daten über Ihre bestehenden Verträge und Anträge im erforderlichen Umfang an Rückversicherungen weitergegeben, damit diese überprüfen können, ob und in welcher Höhe sie sich an dem Risiko beteiligen können.**[25]** Zur Abrechnung von Prämienzahlungen und Leistungsfällen können Daten über Ihre bestehenden Verträge an Rückversicherungen weitergegeben werden.

Zu den oben genannten Zwecken werden möglichst anonymisierte bzw. pseudonymisierte Daten, jedoch auch personenbezogene Gesundheitsangaben verwendet.

Ihre personenbezogenen Daten werden von den Rückversicherungen nur zu den vorgenannten Zwecken verwendet. Über die Übermittlung Ihrer Gesundheitsdaten an Rückversicherungen werden Sie durch die Versicherung XY unterrichtet**[26]**.

Ich willige ein, dass meine Gesundheitsdaten – soweit erforderlich – an Rückversicherungen übermittelt und dort zu den genannten Zwecken verwendet werden. Soweit erforderlich, entbinde ich die für die Versicherung XY tätigen Personen im Hinblick auf die Gesundheitsdaten und weiteren nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.4. Datenaustausch mit dem Hinweis- und Informationssystem (HIS)[27]

Die Versicherungswirtschaft nutzt zur genaueren Risiko- und Leistungsfalleinschätzung das Hinweis- und Informationssystem HIS, das derzeit die informa Insurance Risk and Fraud Prevention GmbH (informa IRFP GmbH, Rheinstraße 99, 76532 Baden-Baden, www.informa-irfp.de) betreibt. Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten, und erhöhte Risiken kann die Versicherung XY an das HIS melden. Die Versicherung XY und andere Versicherungen fragen Daten im Rahmen der Risiko- oder Leistungsprüfung aus dem HIS ab, wenn ein berechtigtes Interesse besteht.**[28]** Zwar werden dabei keine Gesundheitsdaten weitergegeben, aber für eine Weitergabe Ihrer nach § 203 StGB geschützten Daten benötigt die Versicherung XY Ihre Schweige-

pflichtentbindung. Dies gilt unabhängig davon, ob der Vertrag mit Ihnen zustande gekommen ist oder nicht.

Ich entbinde die für Versicherung XY tätigen Personen von ihrer Schweigepflicht, soweit sie Daten aus der Antrags- oder Leistungsprüfung an den jeweiligen Betreiber des Hinweis- und Informationssystems (HIS)[29] melden.

Sofern es zur Prüfung der Leistungspflicht erforderlich ist, können über das HIS Versicherungen ermittelt werden, mit denen Sie in der Vergangenheit in Kontakt gestanden haben, und die über sachdienliche Informationen verfügen könnten. Bei diesen können die zur weiteren Leistungsprüfung erforderlichen Daten erhoben werden (siehe unter Ziff. 2.1).

3.5. Datenweitergabe an selbstständige Vermittler

Die Versicherung XY gibt grundsätzlich keine Angaben zu Ihrer Gesundheit an selbstständige Vermittler weiter. Es kann aber in den folgenden Fällen dazu kommen, dass Daten, die Rückschlüsse auf Ihre Gesundheit zulassen, oder gemäß § 203 StGB geschützte Informationen über Ihren Vertrag Versicherungsvermittlern zur Kenntnis gegeben werden.

Soweit es zu vertragsbezogenen Beratungszwecken erforderlich ist, kann der Sie betreuende Vermittler Informationen darüber erhalten, ob und ggf. unter welchen Voraussetzungen (z. B. Annahme mit Risikozuschlag, Ausschlüsse bestimmter Risiken) Ihr Vertrag angenommen werden kann.

Der Vermittler, der Ihren Vertrag vermittelt hat, erfährt, dass und mit welchem Inhalt der Vertrag abgeschlossen wurde. Dabei erfährt er auch, ob Risikozuschläge oder Ausschlüsse bestimmter Risiken vereinbart wurden.

Bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler kann es zur Übermittlung der Vertragsdaten mit den Informationen über bestehende Risikozuschläge und Ausschlüsse bestimmter Risiken an den neuen Vermittler kommen. Sie werden bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler vor der Weitergabe von Gesundheitsdaten informiert sowie auf Ihre Widerspruchsmöglichkeit hingewiesen.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten und sonstigen nach § 203 StGB geschützten Daten in den oben genannten Fällen – soweit erforderlich – an den für mich zuständigen selbstständigen Versicherungsvermittler übermittelt und diese dort erhoben, gespeichert und zu Beratungszwecken genutzt werden dürfen.

4. Speicherung und Verwendung Ihrer Gesundheitsdaten wenn der Vertrag nicht zustande kommt[30]

Kommt der Vertrag mit Ihnen nicht zustande, speichert die Versicherung XY Ihre im Rahmen der Risikoprüfung erhobenen Gesundheitsdaten für den Fall, dass Sie erneut Versicherungsschutz beantragen. Außerdem ist es möglich, dass die Versicherung XY zu Ihrem Antrag einen Vermerk an das Hinweis- und Informationssystem meldet, der an anfragende Versicherungen für deren Risiko- und Leistungsprüfung übermittelt wird (siehe Ziffer 3.4.). Die Versicherung XY speichert Ihre Daten auch, um mögliche Anfragen weiterer Versicherungen beantworten zu können. Ihre Daten werden bei der Versicherung XY und im Hinweis- und Informationssystem bis zum Ende des dritten Kalenderjahres nach dem Jahr der Antragstellung[31] gespeichert.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten – wenn der Vertrag nicht zustande kommt – für einen Zeitraum von drei Jahren ab dem Ende des Kalenderjahres der Antragstellung zu den oben genannten Zwecken speichert und nutzt.[32]

Ort, Datum	Unterschrift Antragsteller/in oder mitzuversichernde Person
Ort, Datum	Unterschrift gesetzlich vertretene Person (bei Vorliegen der erforderlichen Einsichtsfähigkeit, frühestens ab Vollendung des 16. Lebensjahres)
Ort, Datum	Unterschrift des gesetzlichen Vertreters

Hinweise zur Anwendung der Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung und Verwendung von Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

Der vorliegende Text einer Einwilligungs- und Schweigepflichtentbindungsklausel ist vom GDV mit den Datenschutzaufsichtsbehörden abgestimmt worden. Der Verbraucherzentrale Bundesverband war ebenfalls an den Gesprächen beteiligt. Die Klausel wird flankiert durch Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft (Code of Conduct). Zweck ist, lediglich für die tatsächlich einwilligungsbedürftigen Datenerhebungs- und -verwendungsprozesse eine Einwilligungs- und Schweigepflichtentbindungserklärung einzuholen. Andere Datenverarbeitungen werden in einem Code of Conduct konkretisiert. Sowohl die Klausel als auch der Code of Conduct werden in regelmäßigen Abständen gemeinsam überarbeitet, um aktuelle Entwicklungen der Datenverarbeitung und gesetzliche Änderungen zu berücksichtigen.

Hinweise zur Klausel - BAUSTEINSYSTEM

Die Texte stellen einen maximalen Rahmen für Einwilligungs- und Schweigepflichtentbindungserklärungen dar. Wegen des im BDSG verankerten Prinzips der Datensparsamkeit sind nur die Textpassagen zu verwenden, die benötigt werden. Soweit im Rahmen einer Versicherungssparte oder eines Versicherungsprodukts bestimmte Datenverarbeitungen nicht erfolgen, wie etwa die Erhebung von Gesundheitsdaten bei Dritten zur Risikoprüfung, ist der Text entsprechend zu kürzen. Werden Datenverarbeitungen beschrieben, die das Unternehmen nicht durchführt oder nicht plant, wie zum Beispiel die Datenweitergabe zur medizinischen Begutachtung oder die Datenweitergabe an Rückversicherer, ist der entsprechende Absatz / Satz nicht zu verwenden.

Zu beachten ist dabei jedoch, dass die in Abschnitt 2.1. angebotenen Wahlmöglichkeiten bestehen bleiben müssen. Das heißt, wenn für die Datenerhebung bei Dritten mit dem Antrag eine Einwilligung eingeholt werden soll, müssen auch beide Alternativen (Pauschaleinwilligung / Einzelfalleinwilligung) angeboten werden. Erfolgt keine Wahl, muss spätestens unmittelbar vor der Datenerhebung eine Einwilligung eingeholt werden. Die dafür zu gestaltenden Erklärungen sollten sich an den hier vorliegenden orientieren.

Die vorliegende Einwilligungs- und Schweigepflichtentbindungsklausel bezieht sich auf Gesundheitsdaten und darüber hinaus auf weitere nach § 203 Abs. 1 StGB geschützte Daten, wie die Tatsache des Bestehens eines Versicherungsvertrags. Gesundheitsdaten können in allen Versicherungssparten anfallen, auch dort, wo dies nicht sofort vermutet wird, z.B. in der Reisegepäckversicherung (Verletzungen durch Raub) und in der Kfz-Versicherung (Verletzungen durch Unfall). Die Einwilligungs- und Schweigepflichtentbindungserklärungen müssen vor der jeweils ersten Verarbeitung von Gesundheitsdaten im Unternehmen dem Antragsteller bzw. Versicherungsnehmer vorgelegt werden, soweit sie für bevorstehende Datenerhebungen, -verarbeitungen oder -nutzungen benötigt werden.

Sollen andere besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt werden, wie bspw. die Information über eine Gewerkschaftszugehörigkeit zur Prämienberechnung in speziellen Tarifen gewerkschaftsnaher Unternehmen, ist mit dem betreffenden Antrag eine entsprechende Einwilligungserklärung vom Antragsteller einzuholen. Diese kann z. B. wie folgt formuliert und gestaltet werden:

Ich willige in die Erhebung, Verarbeitung und Nutzung meiner Angaben zur Gewerkschaftszugehörigkeit ein, soweit dies zur* Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung *dieses Vertrages, insbesondere zur Berechnung meiner Versicherungsprämie, erforderlich ist.

---

[1] Hier und im Folgenden kann anstelle von „die Versicherung XY“ der Name des verwendenden Unternehmens oder nach einmaliger Nennung (etwa „wir, die Versicherung XY“) jeweils „wir“ eingefügt werden.
[2] Hier kann die konkrete Sparte genannt werden.
[3] Das Beispiel soll verdeutlichen, dass Versicherer diese Daten nicht willkürlich an x-beliebige Stellen weitergeben. Daher können hier einige für die verwendende Versicherung typische Beispiele genannt werden, die die Breite der Weitergabemöglichkeiten erkennen lassen, wie z. B. Assistancegesellschaften, HIS-Betreiber oder IT-Dienstleister.
[4] Die Klausel ist zunächst nur für Kranken-, Lebens- und Berufsunfähigkeitsversicherungen zu verwenden, weil in diesen Sparten von Vertragsbeginn an Gesundheitsdaten erhoben und verwendet werden. In anderen Sparten ist der Text entsprechend anzupassen und ggf. nur auszugsweise zu verwenden. In Abstimmung mit den Sparten Unfall und Haftpflicht wird den Unternehmen ein angepasster Vorschlag zur Verfügung gestellt.
[5] Verweis auf die Folgen der Verweigerung der Einwilligung gemäß § 4a Abs. 1 Satz 2 BDSG
[6] Werden bei einem Versicherungsprodukt generell keine Kinder und / oder gesetzlich vertretende Personen mitversichert, ist der Absatz bzw. der entsprechende Satz zu streichen. Werden Kinder oder andere gesetzlich vertretene Personen mitversichert, unterschreiben diese ab dem 16. Lebensjahr eine eigene Erklärung, wenn davon auszugehen ist, dass diese einsichtsfähig sind. Diese Erklärung ist aus zivilrechtlichen Gründen auch vom gesetzlichen Vertreter (in der Regel dem Versicherungsnehmer) zu unterzeichnen (siehe unten, Unterschriftenfelder). Damit verbleibt die Entscheidung über das tatsächliche Bestehen der Einsichtsfähigkeit bei dem gesetzlichen Vertreter.
[7] Wenn Unternehmen stets eine Einwilligung im Einzelfall einholen, wird Ziffer 2.1 gestrichen und der Erläuterungstext über dem grauen Kasten wird für die Einzelfalleinwilligung entsprechend angepasst.
[8] Der 2008 in Kraft getretene § 213 VVG führt enumerativ die Stellen auf, bei denen der Versicherer mit Einwilligung des Betroffenen dessen Gesundheitsdaten erheben darf. Hinsichtlich der fehlenden sonstigen Heilberufe (Heilpraktiker, Physiotherapeut, Psychotherapeut) sowie der Versicherer, die keine Personenversicherer im herkömmlichen Sprachgebrauch sind, aber dennoch zur Regulierung von Personenschäden Gesundheitsdaten verarbeiten, wird § 213 VVG weit ausgelegt, vgl. auch Eberhardt in: Münchener Kommentar, § 213 VVG, Rn. 35-40.
[9] Entsprechend der Annahmepolitik der Versicherungsunternehmen kann für alle oder bestimmte Antragsfragen ein kürzerer Zeitraum zugrunde gelegt werden.
[10] Umsetzung der Unterrichtungs- und Hinweispflicht nach § 213 Abs. 2 S. 2 i.V.m. Abs. 4 VVG
[11] Bei der privaten Krankenversicherung ist wegen § 194 Abs. 1 Satz 4 VVG eine Frist von drei Jahren einzusetzen. Bei vorsätzlichem Verhalten gilt auch für die PKV die Zehn-Jahresfrist.
[12] Anhaltspunkte für vorsätzlich falsche Angaben können sich etwa aus Unstimmigkeiten zwischen der Erkrankung und den Angaben im Antrag ergeben. Eine Überprüfung kann dann ergeben, dass es am Vorsatz fehlt und die Datenerhebung für den Betroffenen keine negativen Konsequenzen hat.
[13] Bei Abschnitt 2.2 ist es möglich, das zweite Ankreuzfeld nicht zu nutzen, sodass keine Wahlmöglichkeit besteht und nur das erste Feld angekreuzt werden kann. Der letzte erläuternde Satz vor dem grau unterlegten Feld entfällt dann. Wird das erste (einzige) Ankreuzfeld dann nicht angekreuzt, würde bei einer gerichtlichen Prüfung entweder eine andere Willenserklärung herangezogen (z.B. Testament) oder bei Fehlen einer solchen auf den mutmaßlichen Willen des Betroffenen abgestellt. Ein automatischer Übergang der höchstpersönlichen Verfügungsbe-

fugnis auf Erben oder Bezugsberechtigte des Vertrags erfolgt regelmäßig nicht. Bei Anbieten einer echten Wahlmöglichkeit und einem vorliegenden Kreuz erscheint der Bestand der Erklärungen vor Gericht als wahrscheinlicher, sodass die Bezugnahme auf den mutmaßlichen Willen in einem möglichen Zivilprozess nicht nötig erscheint.

14 Die vertragliche Verpflichtung auf Einhaltung von Datenschutz und Datensicherheit auch für Stellen, die eigenverantwortlich Aufgaben übernehmen, ergibt sich aus dem künftigen Art. 21 Abs. 4 Code of Conduct (CoC). Diese Verpflichtung wurde dort für die Funktionsübertragung an Dienstleister als datenschutzrechtlicher Mehrwert für die Betroffenen vereinbart. Rückversicherer werden nicht als Dienstleister des Erstversicherers im Sinne von Art. 21 angesehen, wenn sie den Erstversicherer im Rahmen von Rückversicherungsverträgen bei der Risiko- und Leistungsprüfung unterstützen. Sofern der Erstversicherer Rückversicherer außerhalb von Rückversicherungsverträgen als Dienstleister einsetzt und diese noch nicht vertraglich auf die Einhaltung von Datenschutz und Datensicherheit verpflichtet hat, ist dies nachzuholen (vgl. auch Hinweis 18).

15 Die Unterrichtungspflicht wurde aufgenommen, um mehr Transparenz zu schaffen. Hierfür ist mitzuteilen, welche konkreten Daten, für welchen Zweck, an welche Stelle übermittelt werden sollen.

16 Der Satzteil “für sich und” ist nur für die Kranken, Leben- und Unfallversicherung zu verwenden.

17 Die Mitarbeiter anderer Stellen werden von ihrer Schweigepflicht entbunden, wenn sie ihrerseits im Rahmen der von ihnen zu erledigenden Aufgaben nach § 203 StGB geschützte Daten an den Versicherer oder an andere Stellen, wie z. B. mit der IT-Wartung beauftragte Subunternehmen weitergeben.

18 In der Liste werden die Stellen und Kategorien von Stellen aufgezählt, die Gesundheitsdaten erheben, verarbeiten oder nutzen. Ebenfalls gemeint sind Stellen und Kategorien von Stellen, die einfache personenbezogene Daten, die nach § 203 StGB geschützt sind, wie z. B. die Information, dass ein Lebensversicherungsvertrag besteht, verwenden. Nicht gemeint sind Stellen, die im Rahmen der ihnen zugewiesenen Aufgaben keine Gesundheitsdaten verarbeiten, diese aber theoretisch einsehen können (Bsp. Personen oder Unternehmen, die mit der IT-Wartung betraut sind). In die Liste werden sowohl Dritte im datenschutzrechtlichen Sinn als auch Auftragdatenverarbeiter, bei denen Abgrenzungsschwierigkeiten zur Funktionsübertragung bestehen (siehe Endnote 23), aufgenommen. Rückversicherer werden als Dienstleister des Erstversicherers angesehen, wenn sie ohne einen Rückversicherungsvertrag nur als Dienstleister des Erstversicherers tätig werden.

19 Werden Aufgaben im Wesentlichen von einem Unternehmen an ein anderes Unternehmen der XY-Versicherungsgruppe oder an eine externe Stelle abgegeben, ist die andere Stelle namentlich anzugeben unter Bezeichnung der Aufgabe. Hierunter fallen z. B. Stellen, die die Aufgaben Risikoprüfung, Leistungsfallbearbeitung oder Serviceleistung für das Unternehmen übernehmen.

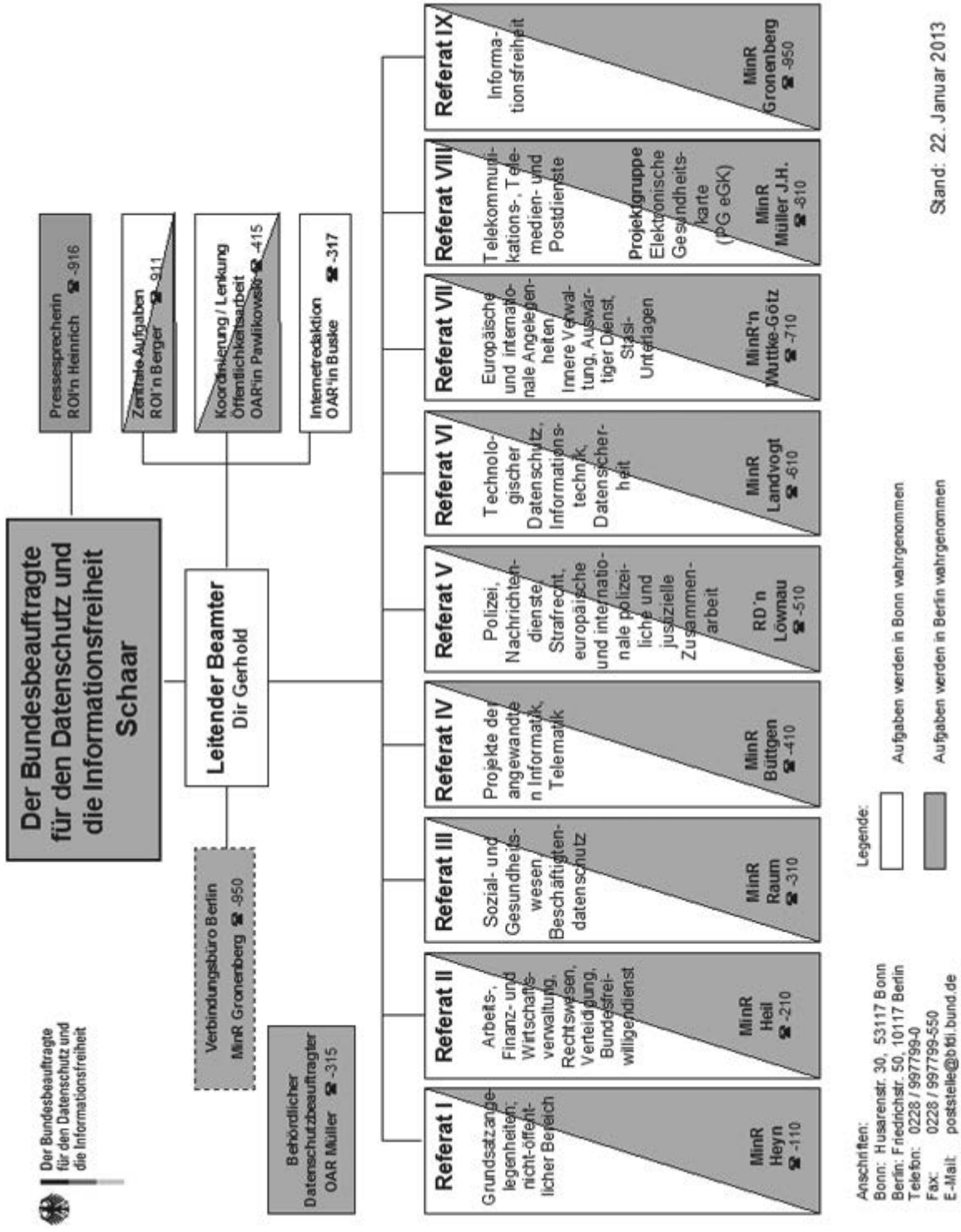
20 Fehlt es an einer systematischen automatisierten Datenverarbeitung, können die Stellen, an die Gesundheitsdaten weitergegeben werden bzw. die zur Erfüllung ihrer Aufgabe selbst Gesundheitsdaten erheben, in Kategorien zusammengefasst werden unter Bezeichnung der Aufgabe. Dies gilt auch für Stellen, die nur einmalig tätig werden, wie z.B. Krankentransporte.

21 Die Liste der Dienstleister soll in der Form, in der die Einwilligungs- und Schweigepflichtentbindungserklärung erteilt wird, als Anlage mitgegeben werden.

22 Die Einwilligung gilt in jedem Fall für die Datenübermittlung an eigenverantwortliche Dienstleister. Sie ist außerdem bei Abgrenzungsschwierigkeiten zwischen Auftragsdatenverarbeitung und Funktionsübertragung einzuholen. Das Einwilligungserfordernis gilt nicht, wenn es sich in Übereinstimmung mit der zuständigen Datenschutzaufsichtsbehörde um eine eindeutige Auftragsdatenverarbeitung handelt. In diesen Fällen sollte dennoch eine Schweigepflichtentbindung eingeholt werden.

23 „und sonstige Stellen“ – Dieser Passus wird gestrichen, wenn keine schweigepflichtgebundenen Dienstleister und Auftragnehmer eingeschaltet sind.

[24] Sollen Gesundheitsdaten an den Rückversicherer des Rückversicherers übermittelt werden, ist eine spezielle Einwilligung zu prüfen.
[25] Für die Kumulkontrolle ist eine Schweigepflichtentbindung erforderlich, da nach § 203 StGB geschützte Daten weitergegeben werden, jedoch keine Gesundheitsdaten.
[26] Die Unterrichtungspflicht des Erstversicherers ersetzt die anderenfalls von den Datenschutzbehörden geforderte ausführliche Erklärung entsprechend dem Baustein 2.1. zur Erhebung von Gesundheitsdaten bei Dritten. Zu unterrichten ist über die konkret übermittelten Daten, den Zweck der Übermittlung und den Empfänger der Daten.
[27] Da keine einwilligungsbedürftigen besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG (Gesundheitsdaten) an das HIS gemeldet werden, betrifft die Schweigepflichtentbindung nur die nach § 203 StGB geschützten Daten, hier etwa die Tatsache, dass ein Versicherungsvertrag besteht.
Da nur die Sparten Unfall und Leben von § 203 Abs. 1 Nr. 6 StGB erfasst werden und mit dem HIS arbeiten, ist der Passus für die anderen Sparten zu streichen. Im Fall der Nutzung ist die Information des Versicherungsnehmers über das Hinweis- und Informationssystem dann in anderer Weise sicherzustellen. Soweit Gesundheitsdaten im Leistungsfall im Rahmen der Detailanfrage ausgetauscht werden, gelten die Einwilligungserklärungen unter 2.1.
[28] Ein berechtigtes Interesse für die Abfrage zum Zweck der Risiko- und Leistungsprüfung ist stets gegeben mit Ausnahme des Erlebensfalls in der Lebensversicherung.
[29] Durch die Formulierung „an den jeweiligen Betreiber“ sowie die Aufnahme von „derzeit“ im ersten Satz des erläuternden Textes wird deutlich gemacht, dass sich der Betreiber des HIS ändern kann. Die Schweigepflichtentbindungserklärung soll auch künftige Betreiber erfassen.
[30] Der Passus ist zu streichen, wenn eine Speicherung von Antragsdaten bei Nichtzustandekommen des Vertrags nicht erfolgt.
Daten über nicht zustande gekommene Verträge sind bei dem Versicherungsunternehmen spätestens drei Jahre gerechnet vom Ende des Kalenderjahres nach Antragstellung zu löschen. Auch im Hinweis- und Informationssystem werden diese Daten entsprechend gelöscht. Gesetzliche Aufbewahrungspflichten oder -befugnisse bleiben hiervon unberührt. Werden Schadensersatzansprüche gegen das Unternehmen geltend gemacht oder bei Prüfungen durch Behörden kann sich eine längere Aufbewahrung auch aus § 28 Abs. 6 Nr. 3 BDSG rechtfertigen.
[31] Es zählt das Datum der Unterschrift im Antrag.
[32] Die Nutzung ist nur zu eigenen Zwecken des Versicherers zulässig. Die Übermittlung an ein anderes Unternehmen ist nur auf der Basis einer von diesem einzuholenden Einwilligung/Schweigepflichtentbindung nach Ziffer 2.1. zulässig.


Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Schaar
Leitender Beamter Dir Gerhold
Pressesprecherin ROI'n Heinrich -916
Zentrale Aufgaben ROI'n Berger -911
Koordinierung / Lenkung Öffentlichkeitsarbeit OAR'in Pawlikowska -415
Internetredaktion OAR'in Buske -317
Verbindungsbüro Berlin MinR Gronenberg -950
Behördlicher Datenschutzbeauftragter OAR Müller -315
Referat I Grundsatzangelegenheiten, nicht-öffentlicher Bereich MinR Heyn -110
Referat II Arbeits-, Finanz- und Wirtschaftsverwaltung, Rechtswesen, Verteidigung, Bundesfreiwilligendienst MinR Heil -210
Referat III Sozial- und Gesundheitswesen Beschäftigtendatenschutz MinR Raum -310
Referat IV Projekte der angewandten Informatik, Telematik MinR Büttgen -410
Referat V Polizei, Nachrichtendienste, Strafrecht, europäische und internationale polizeiliche und justizielle Zusammenarbeit RD'n Löwnau -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
Legende:
Aufgaben werden in Bonn wahrgenommen
Aufgaben werden in Berlin wahrgenommen
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
Stand: 22. Januar 2013

Sachregister

Als Fundstelle ist die Nummer des Abschnitts oder des Beitrages angegeben, in dem der Begriff verwendet wird.

Abkürzungsverzeichnis/Begriffe

A2LL	**A**lg II-**L**eistungen zum **L**ebensunterhalt
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
ADAMS	Anti Doping Administration and Management System
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
ALLEGRO	**Al**g II-**Le**istungsverfahren **Gr**undsicherung **O**nline
Alt.	Alternative
AND	Andere Nachrichtendienste
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
AOS	Allianz Ortungs Services GmbH
APAK	Abschlussprüferaufsichtskommission
APEC	Asia Pacific Economic Cooperation
ARGE	Arbeitsgemeinschaften nach dem Sozialgesetzbuch II
Art.	Artikel
AS	Autorisierte Stelle
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
BAFzA	Bundesamt für Familie und zivilgesellschaftliche Aufgaben
BAG	Bundesamt für Güterverkehr
BAköV	Bundesakademie für öffentliche Verwaltung
BAMF	Bundesamt für Migration und Flüchtlinge
BArchG	Bundesarchivgesetz
BASt	Bundesanstalt für Straßenwesen
BAZ	Bundesamt für den Zivildienst
BBG	Bundesbeamtengesetz
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BBR	Bundesanstalt für Bauwesen und Raumordnung
BBSR	Bundesinstitut für Bau-, Stadt- und Raumforschung
BCR	Binding Corporate Rules; verbindliche unternehmensinterne Datenschutzregelungen
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
bDSB	behördlicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
Bea	Bescheinigungen elektronisch annehmen
BerCA	Berechtigungszertifikateanbieter
BevStatG	Bevölkerungsstatistikgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BFD	Bundesbeauftragter für den Datenschutz
BFD	Bundesfinanzdirektion
BfDBW	Beauftragter für den Datenschutz in der Bundeswehr
BFDG	Bundesfreiwilligendienstgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BfD/BA	Beauftragter für den Datenschutz der Bundesanstalt für Arbeit
BFH	Bundesfinanzhof
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BISp	Bundesinstitut für Sportwissenschaft
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
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	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT	Bundestag
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
CBPR	Cross Border Privacy Rules
CC	Common Criteria
CD / CD-ROM	Compact Disc - Read Only Memory
CDR	Call Data Records
CIA	Central Intelligence Agency, USA
DB	Deutsche Bahn
d.h.	das heißt
DDR	Deutsche Demokratische Republik
DECT	Digital Enhanced Cordless Telecommunications

DHR	Deutsches Hämophilieregister
DIBAS	Digitalisierung von Schriftgut der Bundesagentur für Arbeit
DLZ	Dienstleistungszentrum
DMDA	akkreditierte De-Mail-Diensteanbieter
DNS	Domain Name System
DNT	Do not track
Dok.	Dokument
DPAG	Deutsche Post AG
DPI	Deep Packet Inspection
DPIA	Data Protection Impact Assessment
DPMA	Deutsches Patent- und Markenamt
DRM	Digital Rights Management (Digitales Rechte Management)
Drs.	Drucksache
DRV Bund	Deutsche Rentenversicherung Bund
DSK	Datenschutzkommission (Österreich)
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
DWH	Data Warehouse
E-Akte	elektronische Akte
eAT	elektronischer Aufenthaltstitel
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
EnWG	Energiewirtschaftsgesetz
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
ERP	Enterprise Resource Planning = Software der Firma SAP
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
FATCA	Foreign Account Tax Compliance Act (US Gesetz zur Erfassung von Vermögenswerten von in den USA steuerpflichtigen Personen und Gesellschaften auf Konten im (US-)Ausland
FATF	Financial Action Task Force on Money Laundering (Arbeitskreis Maßnahmen zur Geldwäschebekämpfung)
FAQ	Frequently Asked Questions (häufig gestellte Fragen)
FBI	Federal Bureau of Investigation, USA
FDZ	Forschungsdatenzentrum
ff.	folgende
FFI	Foreign Financial Institution (ausländische Finanzinstitute)
FG	Finanzgericht
FGO	Finanzgerichtsordnung
FH Bund	Fachhochschule des Bundes für öffentliche Verwaltung
FIFA	Fédération Internationale de Football Association
Finanzagentur	Bundesrepublik Deutschland Finanzagentur GmbH
FKS	Finanzkontrolle Schwarzarbeit

FTC	Federal Trade Commission
FVG	Finanzverwaltungsgesetz
G.10	Artikel 10 Gesetz
GAC	Governmental Advisory Committee
GASIM	Gemeinsames Analyse- und Strategiezentrum Illegale Migration
GBA	Generalbundesanwalt beim Bundesgerichtshof
gem.	gemäß
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
GG	Grundgesetz
ggf.	gegebenenfalls
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GIW	Geoinformationswirtschaft
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
HEGA	**H**andlungs**e**mpfehlung/**G**eschäfts**a**nweisung der BA
HIS	Hinweis- und Informationssystem
HKP	häusliche Krankenpflege
HPC	Health Professional Card
HSM	Hardware Security Modul
HTTP	Hypertext Transfer Protocol
HVBG	Hauptverband der gewerblichen Berufsgenossenschaften
HZA	Hauptzollamt
IATA	International Air Transport Association
i.d.F.	in der Fassung
i.d.R.	in der Regel

i.S.d.	im Sinne des (der)
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
ICANN	Internet Corporation for Assigned Names and Numbers
ICAO	International Civil Aviation Organization
ICHEIC	International Commission on Holocaust Era Insurance Claims
ICO	The Information Commissioner's Office
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	Internal Market Information System (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
IPv6	Internet Protocol Version 6
IRS	Internal Revenue Service (Bundessteuerbehörde der USA)
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISPPI	International Standard for the Protection of Privacy and Personal Information
IT	Informationstechnik
IVBB	Informationsverbund Berlin-Bonn
JI-Rat	Rat der Innen- und Justizminister der Europäischen Union
KBA	Kraftfahrt-Bundesamt
KdU	**K**osten **d**er **U**nterkunft und Heizung
KEV	Kontrolleinheit Verkehrswege
KFU	Krebsfrüherkennungsrichtlinien
Kfz	Kraftfahrzeug
KIWI	Kindergeld-Windows-Implementierung
KOM	Europäische Kommission
KWG	Kreditwesengesetz

LfD	Landesbeauftragter für den Datenschutz
LfV	Landesamt für Verfassungsschutz
LG	Landgericht
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
MSISDN	Mobile Subscriber ISDN Number
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
NFC	Near Field Communication
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
OCR	Optical Character Recognition (Optische Zeichenerkennung)
o.g.	oben genannt
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
OK	Organisierte Kriminalität, aber auch: Organisationskomitee
OLAF	Europäisches Amt für Betrugsbekämpfung

OMS	Optimierte Meldeverfahren in der sozialen Sicherung
Opol	Operational Point of Contact
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten
P23R	Prozessdatenbeschleuniger
PassG	Passgesetz
PbD	Privacy by Design
PC	Personalcomputer
PCAOB	Public Company Accounting Oversight Board (amerikanische Aufsichtsbehörde für Wirtschaftsprüfer)
PCC	Privacy Commissioner of Canada
PDA	Personal Digital Assistant
PEI	Paul-Ehrlich-Institut
PEP	politisch exponierte Personen
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
RLTk	Richtlinie Telekommunikation
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
SchuFV	Verordnung über die Führung des Schuldnerverzeichnisses

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
UAS	Unmanned Aerial Systems
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
VerBIS	Vermittlungs-, Beratungs- und Informationssystem - IT-Fachverfahren der Bundesagentur für Arbeit für die Bereiche Vermittlung und Beratung
VG	Verwaltungsgericht
vgl.	vergleiche
VIS	Europäisches Visa-Informationssystem
VN	Vereinte Nationen
VOIP	Voice over IP
VPN	Virtual Private Network (dt. virtuelles privates Netz)

vpS	Vorbeugender personeller Sabotageschutz
VS	Verschlusssache
VwVfG	Verwaltungsverfahrensgesetz
W3C	World Wide Web Consortium
WADA	Welt-Anti-Doping-Agentur
WAP	Wireless Application Protocol
WehrRÄndG	Wehrrechtsänderungsgesetz 2011
WiMax	Wordwide Interoperability for Microwave Access Standard gemäß IEEE 802.16a für lokale Funknetze
WLAN	Wireless Local Area Network
WM	Weltmeisterschaft
WoGG	Wohngeldgesetz
WP	Working Paper
WPersAV	Personalaktenverordnung Wehrpflichtige
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
ZAV	Zentrale Auslands- und Fachvermittlung der Bundesagentur für Arbeit
ZDG	Zivildienstgesetz
ZensG 2011	Zensusgesetz 2011
ZFdG	Zollfahndungsdienstgesetz
ZFER	Zentrales Fahrerlaubnisregister
ZIS	Zollinformationssystem
ZIVIT	Zentrum für Informationsverarbeitung und Informationstechnik
ZKA	Zollkriminalamt
ZNwG	Zentrum für Nachwuchsgewinnung
ZORA	Zukunftsorientierte Retailanwendung
ZPO	Zivilprozessordnung
ZSS	Zentrale Speicherstelle
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

Übersicht alle Tätigkeitsberichte

Tätigkeitsbericht	Berichtszeitraum	Bundestagsdrucksachennummer
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
23.	2009 – 2010	17/5200

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.datenschutz.bund.de

Bonn 2013

Dieser Bericht ist als Bundestagsdrucksache 17/13000 erschienen.

Druck:
Silber Druck oHG
Am Waldstrauch 1
34266 Niestetal