Landtag von Baden-Württemberg **Drucksache 14 / 5500**

14. Wahlperiode **01. 12. 2009**

Mitteilung

des Landesbeauftragten für den Datenschutz

29. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg 2008/2009

Schreiben des Landesbeauftragten für den Datenschutz in Baden-Württemberg vom 1. Dezember 2009:

Anbei übersende ich Ihnen unseren 29. Tätigkeitsbericht, der nach § 31 Abs. 1 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 1. Dezember 2009 zu erstatten ist.

Klingbeil

Eingegangen: 01. 12. 2009 / Ausgegeben: 17. 12. 2009

29. Tätigkeitsbericht
des Landesbeauftragten für den Datenschutz
in Baden-Württemberg
2008/2009

INHALTSVERZEICHNIS

Vorwort

Der 29. Tätigkeitsbericht umfasst nach der jüngsten Änderung des Landesdatenschutzgesetzes einen Zeitraum von zwei Jahren, beruht also zu einem wesentlichen Teil auf den Vorarbeiten meines Vorgängers, dessen Amtszeit am 28. Februar 2009 mit dem Eintritt in den Ruhestand endete. Peter Zimmermann hat dem Amt durch seine umfassende Verwaltungserfahrung, sein sicheres Judiz und seine stets abgewogene Haltung zu hohem Ansehen verholfen, wie auch die Presse anerkennend konstatiert hat; hierfür bin ich ihm sehr dankbar. Bedanken darf ich mich auch bei den Abgeordneten des Landtags von Baden-Württemberg für den Vertrauensbeweis, der in der einstimmigen Bestätigung meiner Bestellung zum vierten Landesbeauftragten für den Datenschutz zum Ausdruck kam. Und nicht zuletzt danke ich meinen Mitarbeiterinnen und Mitarbeitern für ihre engagierte Unterstützung, denn dieser Bericht ist trotz der zumeist gewählten Ich-Form das Ergebnis einer Teamarbeit.

Als „Störenfried von Amts wegen“ wurde mein Amtsvorgänger einmal von der Presse bezeichnet. Damit ist eine wichtige Funktion eines Datenschutzbeauftragten angesprochen. Ich werde da keine Ausnahme machen. Der Begriff lässt aber zugleich erkennen, dass meine Befugnisse sehr beschränkt sind und eher in die Kategorie „Mahnen und Warnen“ gehören. Mein „schärfstes Schwert“ sind nun einmal die förmliche Beanstandung und die Benennung von Defiziten in Tätigkeitsberichten wie diesem, dies stets in der Hoffnung, dass der Landtag, die Medien und natürlich möglichst viele Bürgerinnen und Bürger meine Anliegen unterstützen mögen. Andererseits mache ich mir auch nichts vor: Für die meisten Behörden ist Datenschutz eher eine lästige Pflichtübung, zumal auch der private Bereich von einer zunehmenden Preisgabe der Privatsphäre geprägt ist. Nach meinem Eindruck sind Datenschutzverstöße im öffentlichen Bereich zumeist auf fehlendes Problembewusstsein und Gedankenlosigkeit zurückzuführen. Den Appell „Datenschutz sollte Chefsache sein“, den der Herr Innenminister im August 2009 an die Adresse der Unternehmen richtete, kann ich in Bezug auf die Behörden nur wiederholen. Leider fehlen meiner Dienststelle bisher die personellen Kapazitäten für mehr als nachträgliche Reparaturarbeiten als Reaktion auf festgestellte Versäumnisse. Um strukturelle Verbesserungen zu erreichen, wäre zunächst durchgängig mehr Datenschutzbewusstsein der Verantwortlichen erforderlich. Zumindest für die großen Verwaltungsbereiche sollten daher Netzwerke von Ansprechpartnern geschaffen werden, die in Kooperation mit meiner Dienststelle den Datenschutzgedanken in den Behördenalltag hineintragen. Im Bereich der Polizei gibt es hierfür bereits gute Ansätze, zumal die Polizeidirektionen in der Regel über eigene behördliche Datenschutzbeauftragte verfügen. Ein „Kommunales Netzwerk Datenschutz“ ist vor kurzem auf Initiative der Hochschule für öffentliche Verwaltung Kehl gegründet worden. Auch für den Schulbereich, in dem die Schulen datenschutzrechtlich selbst verantwortlich sind, habe ich dem Kultusministerium eine stärkere datenschutzrechtliche Betreuung der Schulen vorgeschlagen. Datenschutzthemen sollten darüber hinaus generell stärker bei der Aus- und Fortbildung, insbesondere bei der von zahlreichen Akteuren betriebenen Vermittlung von Medienkompetenz, Berücksichtigung finden; mit der Landesstiftung Baden-Württemberg bin ich deswegen im Gespräch. Datenschutz ist eben auch eine Bildungsaufgabe.

Die Zuständigkeit meiner Dienststelle ist bislang auf den öffentlichen Bereich beschränkt, was in der Praxis immer wieder zu schwierigen Abgrenzungsfragen führt. Diese werden hoffentlich bald der Vergangenheit angehören, nachdem sich nunmehr auch die CDU-Landtagsfraktion für eine Zusammenlegung meines Amtes mit der derzeit noch im Innenministerium angesiedelten Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich ausgesprochen hat. Damit zeichnen sich auch in Baden-Württemberg modernere und effizientere Strukturen im Datenschutz ab und den Bürgerinnen und Bürgern kann „Datenschutz aus einer Hand“ geboten werden. Wunder sind allerdings auch nach einer Zusammenlegung nicht zu erwarten, weil die Personalausstattung in beiden Bereichen im bundesweiten Vergleich sehr bescheiden ist und bislang nur ein „Pflichtprogramm“ statt einer offensiven Datenschutzstrategie erlaubt. Gerade die oben aufgezeigten Handlungsfelder verdeutlichen, dass hier mehr getan werden kann und getan werden muss.

Den langjährigen Lesern der Tätigkeitsberichte werden bei der Lektüre einige äußerliche Veränderungen auffallen. Aus Datenschutzsicht maßgebliche Entwick-

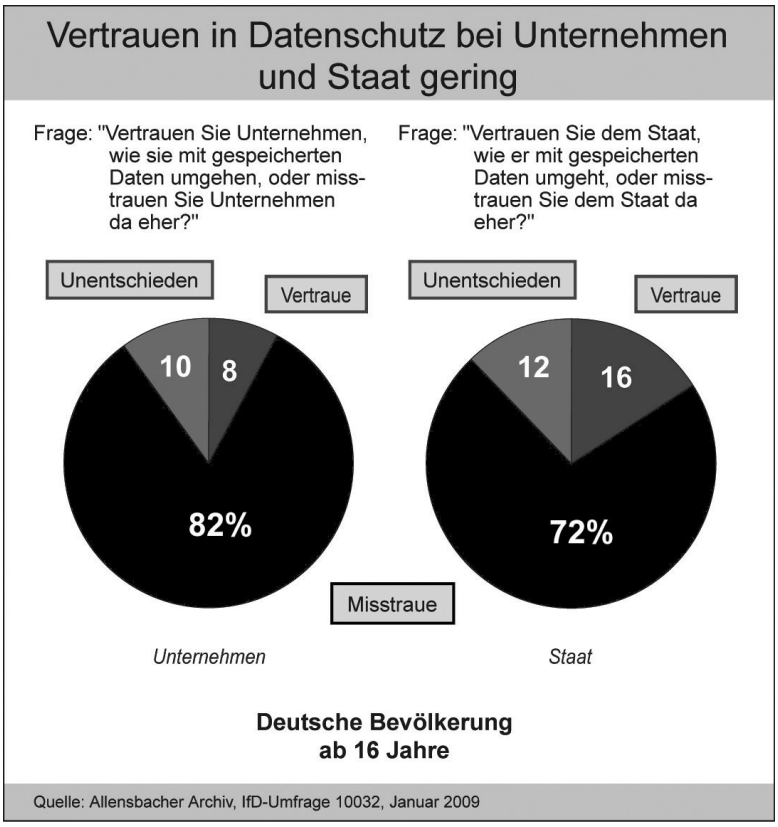
lungen auf europäischer und auf Bundesebene werden nunmehr bereits im 1. Teil dargestellt, außerdem gehe ich dort auf das Querschnittsthema Videoüberwachung ein. Ferner wurde versucht, die Lesbarkeit des Tätigkeitsberichts weiter zu verbessern, soweit das unter den drucktechnischen Rahmenbedingungen einer Landtagsdrucksache möglich war: Die Beiträge sind nun in der Regel knapper gefasst; bei Bedarf werden den Beiträgen jeweils ein Problemaufriss vorangestellt und ein Fazit oder eine Empfehlung angeschlossen (kursiv). Außerdem werden an geeigneter Stelle Gesetzestexte oder passende Zitate optisch hervorgehoben. Für weitere Anregungen und Verbesserungsvorschläge bin ich auch in Zukunft dankbar.

Jörg Klingbeil

1. Teil: Zur Situation

1. Datenschutz in Bewegung

Der Datenschutz ist in Bewegung geraten: Das betraf im Berichtszeitraum 2008/2009 weniger die personellen Veränderungen in der Dienststelle als vielmehr zahlreiche Datenschutzpannen und -skandale, die bundesweit nicht nur zu beachtlichen Schlagzeilen führten, sondern bei vielen Bürgerinnen und Bürgern den Eindruck erweckten, ihre Daten seien nicht mehr sicher, weder bei Behörden noch bei Unternehmen (siehe nachstehendes Ergebnis einer Umfrage des Instituts für Demoskopie Allensbach vom Januar 2009).



Das Thema Datenschutz hatte wieder Konjunktur – wie seit dem Volkszählungsurteil aus dem Jahre 1983 nicht mehr. „Sicherheitslecks“ und die interne Überprüfung von Verbindungsdaten bei einem großen Telekommunikationsunternehmen, Datenschutzverstöße beim Adresshandel, die Videobeobachtung von Mitarbeitern eines Discounters sowie etliche kleinere und größere Datenschutzpannen, aber vor allem wohl der offenkundige Vertrauensverlust in der Bevölkerung führten auf der politischen Ebene zunächst zu einem „Datenschutzgipfel“ beim damaligen Bundesinnenminister am 4. September 2008 und – gewisse Verzögerungen aufgrund der involvierten Interessen blieben nicht aus – zu mehreren Novellierungen des Bundesdatenschutzgesetzes kurz vor dem Ende der 16. Legislaturperiode des Deutschen Bundestags. Parallel hierzu legte der Bundesarbeitsminister wenige Tage vor der Bundestagswahl, ohne Chance auf eine gesetzgeberische Umsetzung, den Entwurf eines Arbeitnehmerdatenschutzgesetzes vor. Das jahrelang im politischen Abseits stehende Themenfeld Datenschutz geriet jedenfalls in ungewohnte Bewegung.

Nach der Bundestagswahl scheint es auf Bundesebene mit frischem Schwung weiterzugehen. Der Koalitionsvertrag von CDU, CSU und FDP vom 26. Oktober 2009 geht im Kapitel „Datenschutz“ nicht nur von der

richtigen Erkenntnis aus, dass ein moderner Datenschutz gerade in der heutigen Informationsgesellschaft von besonderer Bedeutung ist; die Koalitionspartner bekennen sich auch zum Ziel eines hohen Datenschutzniveaus. Die programmatische Aussage im Koalitionsvertrag, dass „die konsequente Anwendung geltenden Rechts, eine gute Ausstattung der Sicherheitsbehörden und die Beseitigung von Vollzugsdefiziten immer Vorrang vor der Erweiterung staatlicher Eingriffsbefugnisse“ haben sollen, und ähnliche Aussagen des neuen Bundesinnenministers lassen hoffen, dass im Sicherheitsbereich mehr Zurückhaltung als in den vergangenen Jahren an den Tag gelegt werden wird. Interessant ist auch der Plan, eine Stiftung Datenschutz zu schaffen.

Auszug aus der Koalitionsvereinbarung, Kap. IV.3 Datenschutz:

Ein moderner Datenschutz ist gerade in der heutigen Informationsgesellschaft von besonderer Bedeutung. Wir wollen ein hohes Datenschutzniveau. Die Grundsätze der Verhältnismäßigkeit, der Datensicherheit und -sparsamkeit, der Zweckbindung und der Transparenz wollen wir im öffentlichen und privaten Bereich noch stärker zur Geltung bringen. Hierzu werden wir das Bundesdatenschutzgesetz unter Berücksichtigung der europäischen Rechtsentwicklung lesbarer und verständlicher machen sowie zukunftsfest und technikneutral ausgestalten. ...

Darüber hinaus werden wir eine Stiftung Datenschutz errichten, die den Auftrag hat, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, Bildung im Bereich des Datenschutzes zu stärken, den Selbstdatenschutz durch Aufklärung zu verbessern und ein Datenschutzaudit zu entwickeln. Wir sind überzeugt, dass mit dieser Lösung auch der Technologiestandort Deutschland gestärkt wird, wenn datenschutzfreundliche Technik aus Deutschland mit geprüfter Qualität weltweit vertrieben werden kann. ...

Kurz nach der Regierungsbildung kündigte nicht nur der neue Bundesinnenminister an, er wolle bald den Entwurf eines Arbeitnehmerdatenschutzgesetzes vorlegen, auch die neue Bundesjustizministerin gab bekannt, sie strebe eine grundlegende Renovierung des Datenschutzrechts an, die für den privaten wie den öffentlichen Bereich gelten solle. In beiden Punkten würde damit eine langjährige Forderung der Datenschutzbeauftragten von Bund und Ländern aufgegriffen (vgl. hierzu Entschließungen vom 26. März und vom 8. Oktober 2009, Anhänge 2 und 19). Auch der Deutsche Bundestag hatte wiederholt ein modernes, leicht verständliches und übersichtliches Datenschutzrecht sowie einen Gesetzentwurf zum Arbeitnehmerdatenschutz eingefordert; insofern entspricht der Koalitionsvertrag im Grunde (nur) der Beschlusslage des Parlaments. Die Datenschutzbeauftragten von Bund und Ländern haben inzwischen Vorarbeiten für eigene Vorschläge zur Modernisierung des Datenschutzrechts aufgenommen.

Zutreffend hat der Bundestag auch ein zunehmendes Auseinanderklaffen von datenschutzrechtlichen Bestimmungen und technologischer Entwicklung konstatiert (vgl. zuletzt Drucksache 16/12271; die Beschlussempfehlung des Innenausschusses wurde in der Plenarsitzung des Deutschen Bundestages am 19. März 2009 einstimmig angenommen).

Auszug aus Drucksache 16/12271

Nr. 2: Der Abstand zwischen den geltenden datenschutzrechtlichen Bestimmungen und der rasanten technologischen Entwicklung mit ihren Folgen in allen Lebensbereichen wird immer größer. Das vom Deutschen Bundestag geforderte moderne, leicht verständliche und übersichtliche Datenschutzrecht wäre nicht nur ein wirtschaftlicher Standortvorteil, sondern könnte auch einen wertvollen Beitrag zur Entbürokratisierung leisten.

Die Einschätzung der neuen Bundesjustizministerin, der Koalitionsvertrag beinhalte den Einstieg in einen Paradigmenwechsel, hin zu einer stärkeren Beachtung der Freiheits- und Bürgerrechte, scheint mir allerdings etwas zu

optimistisch zu sein; zumindest steht die Nagelprobe hierfür noch aus. Bei Lichte betrachtet orientiert sich der Koalitionsvertrag nur an den Grenzen des verfassungsrechtlich Zulässigen, die das Bundesverfassungsgericht im Berichtszeitraum dem Gesetzgeber erneut mehrfach aufgezeigt hat. Dabei hat insbesondere die Entscheidung vom 27. Februar 2008[1], mit der das Bundesverfassungsgericht die Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz kippte, Aufsehen erregt. Denn das Gericht stellte dem im Volkszählungsurteil von 1983 formulierten „Grundrecht auf informationelle Selbstbestimmung“ überraschend eine junge „Schwester“ (um den Präsidenten des Bundesverfassungsgerichts zu zitieren), das „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme“, an die Seite. Damit wollte das höchste deutsche Gericht den wachsenden Gefährdungen Rechnung tragen, die sich aus der für die Persönlichkeitsentfaltung bedeutsamen Nutzung der Informationstechnik, namentlich des Internets, ergeben. Es bleibt zu hoffen, dass die staatlichen Stellen nun eine aktive Rolle einnehmen, um die geforderte Vertraulichkeit und Integrität zu gewährleisten; nur der Hinweis auf die Selbstverantwortung der Nutzer wäre jedenfalls zu wenig. Nur am Rande sei die Bemerkung gestattet, dass mein Amtsvorgänger Peter Zimmermann mit seiner Prognose im letzten Tätigkeitsbericht hinsichtlich des Schicksals der Online-Durchsuchung auf dem Prüfstand des Bundesverfassungsgerichts vollauf Recht behalten hat. Und auch die neuen Gesetze über das Bundeskriminalamt und die Vorratsdatenspeicherung sowie das Antiterrordateigesetz werden in den nächsten Monaten unweigerlich einer kritischen Prüfung durch das höchste deutsche Gericht unterzogen werden; ich würde mich wundern, wenn diese Vorhaben gänzlich ungestreift davonkämen.

Auf europäischer Ebene wird der am 1. Dezember 2009 in Kraft tretende Vertrag von Lissabon auch für den Datenschutz bedeutsame Änderungen mit sich bringen: Die Grundrechte-Charta der Europäischen Union mit ihrem Grundrecht auf Datenschutz wird zum europäischen Primärrecht. Durch die Aufgabe der bisherigen Säulenstruktur ist auch die zwischenstaatliche polizeiliche und justizielle Zusammenarbeit in Strafsachen zu vergemeinschaften; allerdings ist hier erst noch ein einheitliches, möglichst hohes Datenschutzniveau zu schaffen. Ob der im internationalen Vergleich durchaus beachtliche deutsche Datenschutz zum Maßstab auf europäischer Ebene werden oder ob eine Harmonisierung auf einem niedrigeren Niveau erfolgen wird, bleibt abzuwarten. Wegen der Bedeutung des Vertrags von Lissabon ist ihm ein eigener Abschnitt in diesem Tätigkeitsbericht gewidmet, ebenso dem „Stockholmer Programm“, das sich der Europäische Rat im Bereich der inneren Sicherheit noch in diesem Jahr geben will. Angesprochen wird auch die weitere Umsetzung der EU-Dienstleistungsrichtlinie auf Landesebene. Zu den Projekten auf Bundesebene, auf die ich in diesem Bericht eingehe, gehören die Umsetzung des ELENA-Gesetzes, das geplante Bundesmelderegister sowie der elektronische Pass und der elektronische Personalausweis. Mein Anliegen ist in diesem Zusammenhang, im Tätigkeitsbericht auch einige für die Bürgerinnen und Bürger datenschutzrelevante Entwicklungen außerhalb der Landesgrenzen darzustellen, selbst wenn ich dafür nicht originär zuständig bin. Unsere Informationsgesellschaft kennt eben immer weniger nationale und Landesgrenzen.

Im Mittelpunkt dieses Tätigkeitsberichts stehen jedoch wie in den früheren Jahren die zahlreichen neuen Gesetzesvorhaben, Projekte und EDV-Verfahren auf Landesebene sowie selbstverständlich die vielen Eingaben und Beschwerden aus der Bevölkerung, die bei mir tagtäglich eingehen und die vielfach zur Nachschau bei den Behörden vor Ort und hin und wieder auch zu einer Beanstandung geführt haben. Dankend zu erwähnen sind auch die wertvollen Hinweise aus dem Bereich der Medien, durch die meine Mitarbeiter und ich immer wieder auf Missstände, aber auch auf uns bisher unbekannte Vorhaben von Landesbehörden und Kommunen aufmerksam gemacht werden. Leider geschieht es noch zu oft, dass ich erst durch Presseartikel oder Landtagsdrucksachen von Projekten erfahre, über die ich eigentlich von Amts wegen schon lange vorher hätte unterrichtet werden müssen.

[1] http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

Aus der Reihe der Gesetzgebungsvorhaben des Landes sind im Berichtszeitraum besonders die Novellierung des Polizeigesetzes, der Entwurf eines neuen Landesversammlungsgesetzes, das Gesetz über die elektronische Aufsicht im Vollzug, das Justizvollzugsgesetzbuch, das Landeskrebsregistergesetz und dessen Umsetzung sowie die gesetzlichen Grundlagen für den Zugang zu Geodaten zu nennen. Als gewisser Schwerpunkt meiner Tätigkeit haben sich in den zurückliegenden beiden Jahren auch der Bildungsbereich und hierauf bezogene Konzepte und Verfahren herausgestellt. Zu erwähnen sind hier vor allem die Einschulungsuntersuchung sowie der Orientierungsplan für Bildung und Erziehung in Kindergärten und Kindertagesstätten, der erhebliche Eingriffe in das Persönlichkeitsrecht vorsieht und trotz fehlender Rechtsgrundlage zunächst verbindlich eingeführt werden sollte. Aber auch das Verfahren „Kompetenzanalyse Profil AC an Haupt- und Sonderschulen“ machte deutlich, dass die vom Kultusministerium den Schulen (nicht nur bei diesem Verfahren) zugedachte Rolle als datenschutzrechtlich verantwortliche Stelle im Sinne von § 3 Abs. 3 des Landesdatenschutzgesetzes (LDSG) dort weitgehend noch unbekannt ist bzw. dass die Schulen bei der Umsetzung datenschutzrechtlicher Anforderungen offenbar vielfach allein gelassen werden. Ich habe zwar ein gewisses Verständnis dafür, dass nicht jede Schule einen eigenen behördlichen Datenschutzbeauftragten nach § 10 Abs. 1 LDSG bestellen kann oder will, das Gesetz bietet aber auch die Möglichkeit, dass diese Funktion von der Aufsichtsbehörde wahrgenommen wird oder ein Datenschutzbeauftragter für mehrere öffentliche Stellen gemeinsam bestellt wird (§ 10 Abs. 2 LDSG). Die jüngsten Erfahrungen bestätigen mich auch in meiner Forderung, im Landesdatenschutzgesetz – ähnlich wie in den Datenschutzgesetzen einiger anderer Länder und des Bundes – eine gesetzliche Verpflichtung zur Bestellung eines behördlichen Datenschutzbeauftragten zu schaffen; bisher ist das nur fakultativ vorgesehen. Auf diese Weise könnte gegebenenfalls auch eine Entlastung meiner Mitarbeiterinnen und Mitarbeiter erreicht werden.

Diese wäre übrigens dringend erforderlich, denn die Personalausstattung meiner Dienststelle ist leider nach wie vor unzureichend. Aber auch in organisatorischer Hinsicht scheint der Datenschutz auf Landesebene in Bewegung zu kommen: Für das kommende Jahr zeichnet sich eine Zusammenlegung meiner Dienststelle mit der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich ab, nachdem nunmehr auch die CDU-Landtagsfraktion diese Lösung befürwortet. Das ist eine gute Nachricht für den Datenschutz im Lande, weil sich hierdurch die Chance eröffnet, den Rat suchenden Bürgerinnen und Bürgern Datenschutz aus einer Hand zu bieten. Die derzeitige Zuständigkeitsabgrenzung ist vor allem in Anbetracht der vielen privatrechtlichen Betätigungsformen der öffentlichen Hand für die Betroffenen häufig kaum noch zu durchschauen. Wichtig wird nun sein, dass die Dienststelle in ihrem neuen Zuschnitt vernünftig mit Stellen und Sachmitteln ausgestattet wird, damit die politisch gewünschte Schlagkraft der Datenschutzaufsicht Realität werden kann. Bislang ist die personelle und sachliche Ausstattung meiner Dienststelle, aber auch die der im Innenministerium angesiedelten Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich – verglichen mit den Datenschutzaufsichtsbehörden in den anderen Ländern und beim Bund – sehr bescheiden, sodass im Grunde nur das Pflichtpensum bewältigt werden kann. Eine Fusion von zwei notleidenden Aufsichtsbehörden – womöglich noch mit dem Hintergedanken, Synergieeffekte in Form von Personaleinsparungen zu erzielen – wäre jedenfalls der falsche Weg, wenn man es mit einer schlagkräftigen Datenschutzaufsicht ernst meint. Datenschutzaufsicht sollte mehr sein als nur die rückwärtsgewandte Kontrolle (und gegebenenfalls Beanstandung) in Einzelfällen, wenn das Kind schon in den Brunnen gefallen ist. Wie meine Mitarbeiter und ich immer wieder erleben, wäre eine verstärkte Beratung der Behörden sowie die Mitwirkung an der Erarbeitung von wichtigen Konzepten und Projekten vielfach dringend erforderlich; dies muss aus Kapazitätsgründen bisher in der Regel unterbleiben. Wichtig wäre auch eine intensivere Öffentlichkeitsarbeit, nicht zuletzt im Bereich der Bildung, um das Recht auf Privatsphäre stärker im Bewusstsein von Multiplikatoren und Betroffenen zu verankern. Viele Akteure in diesem Bereich haben sich zwar die Verbesserung der Medienkompetenz zum Ziel gesetzt; gelegentlich habe ich aber den Eindruck, dass der Datenschutz auf dem weiten Feld des richtigen

Umgangs mit Tastatur und Computermaus, E-Mail und Internet etwas ins Hintertreffen gerät.

Dabei stellt die stürmische technische Entwicklung, insbesondere die zunehmende Verbreitung des Internets, auch eine große Herausforderung für meine Mitarbeiter und mich dar, wenngleich der nichtöffentliche Bereich noch mehr gefordert sein dürfte. Denn das stark technikabhängige Datenschutzrecht stammt in seiner Grundstruktur weitgehend noch aus den achtziger Jahren des vorigen Jahrhunderts, aus der Zeit der Großrechner und des knappen und teuren Speicherplatzes. Die Gegenwart ist vor allem das Internet: Allein in Deutschland nutzen mittlerweile knapp 70 % der über 14-Jährigen das Internet (Quelle: [N]Onliner-Atlas 2009, siehe *www.initiatived21.de*), weltweit sind es 1,6 Milliarden, in der Altersgruppe der 14- bis 29-Jährigen sind es schon 94,5 %. Nach einer EMNID-Umfrage vom Juli 2009 sind 47 % der Bevölkerung Mitglied in einem sozialen Netzwerk wie Facebook, StudiVZ oder Xing, bei den 14- bis 29-Jährigen liegt der Anteil der Mitglieder in einer Online-Community sogar bei 89 % *(www.tns-emnid.com)*. Wenn man sich anschaut, dass hier viele, zum Teil höchst private Informationen freiwillig preisgegeben werden, dann kann man schon von einer „Generation Sorglos“ reden. Das hierdurch entstandene datenschutzrechtliche Risikopotenzial liegt auf der Hand. Vielen der jungen Internet-User scheint nicht bewusst zu sein, dass das Internet „nichts vergisst“ und dass viele Informationen noch auffindbar sind, wenn sich die Urheber hieran nicht mehr so gerne erinnern wollen. Eine Umfrage des dimap-Instituts im Auftrag der Bundesregierung (Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz) vom Juli 2009 ergab beispielsweise, dass mehr als ein Viertel der befragten Unternehmen gezielt das Internet allgemein für Personalentscheidungen und hiervon immerhin 36 % soziale Netzwerke als Informationsquellen im Bewerbungsprozess nutzen *(www.bmelv.de)*. Wegen Einzelheiten verweise ich auf den Fünften Tätigkeitsbericht des Innenministeriums über den Datenschutz im nichtöffentlichen Bereich 2009, der wertvolle Hinweise enthält und die von den Aufsichtsbehörden des Bundes und der Länder („Düsseldorfer Kreis“) aufgestellten Anforderungen an eine datenschutzkonforme Ausgestaltung sozialer Netzwerke benennt (der Bericht kann von der Homepage des Innenministeriums unter der Adresse *www.innenministerium.baden-wuerttemberg.de/fm7/2028/Fuenfter_Taetigkeitsbericht_2009_Datenschutz.pdf* heruntergeladen werden).

Mit der dezentralen und global verfügbaren Internet-Technik verflüchtigen sich auch die gewohnten datenschutzrechtlichen Anknüpfungspunkte zusehends: Mag beispielsweise die Verantwortlichkeit für die Einstellung von Informationen ins Netz bei einem seriösen Anbieter dank der Angaben im Impressum nach §§ 5, 6 des Telemediengesetzes (TMG) noch eindeutig feststellbar sein, so gilt dies bei Spiegelung der Seite oder des Inhalts, bei jedem gesetzten Link und erst recht bei der Zwischenspeicherung in Suchmaschinen nur noch sehr eingeschränkt oder gar nicht mehr. Ist der Verantwortliche aber nicht bekannt, so können auch die Betroffenenrechte dramatisch an Bedeutung verlieren. Zudem besteht ein erhebliches praktisches Problem hinsichtlich der Zuständigkeit der jeweiligen Aufsichtsbehörde, das sich aus der komplexen und globalisierten Datenverarbeitung im Internet ergibt.

2. Europäische Entwicklung

2.1 Datenschutz und der Vertrag von Lissabon

Der am 13. Dezember 2007 in Lissabon von den europäischen Staats- und Regierungschefs unterzeichnete Vertrag über die Reform der Europäischen Union (EU) wird nach seinem Inkrafttreten auch für den Datenschutz durchgreifende Änderungen mit sich bringen. Die Grundrechte-Charta mit einem Grundrecht auf Datenschutz wird zum europäischen Primärrecht. Die bisher zwischenstaatliche polizeiliche und justizielle Zusammenarbeit in Strafsachen wird vergemeinschaftet; ein einheitliches hohes Datenschutzniveau in diesem Bereich ist noch zu schaffen.

Nach dem vorläufigen Scheitern einer europäischen Verfassung im Jahr 2005 wurde das Reformwerk in abgespeckter Form im Jahr 2007 maß-

geblich unter deutscher Ratspräsidentschaft durchgesetzt. Inzwischen hat die irische Bevölkerung in einem zweiten Referendum grünes Licht gegeben; nachdem zuletzt auch Polen und Tschechien den Vertrag von Lissabon ratifiziert haben, ist er am 1. Dezember 2009 in Kraft getreten. Der Vertrag gestaltet die bisherigen Gemeinschaftsverträge – insbesondere den Vertrag über die Europäische Union und den Vertrag zur Gründung der Europäischen Gemeinschaft (künftig „Vertrag über die Arbeitsweise der Europäischen Union", AEUV) – grundlegend um. So wird u. a. die bisherige Säulenstruktur aufgegeben und die Charta der Grundrechte in das europäische Primärrecht eingebunden (siehe: *http://europa.eu/lisbon_treaty/full_text/index_de.htm*). Der Vertrag von Lissabon bringt auch für den Datenschutz eine Reihe bedeutsamer Änderungen mit sich:

– Artikel 16 Abs. 2 AEUV (bisher Artikel 286 des EG-Vertrages) verpflichtet die europäischen Gesetzgebungsorgane zum Erlass von Datenschutzvorschriften. Diese Pflicht gilt nicht nur hinsichtlich der Verarbeitung personenbezogener Daten durch europäische Institutionen, sondern nunmehr auch für die Datenverarbeitung durch die Mitgliedstaaten.

> *Artikel 16 Abs. 2 AEUV*
>
> *(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.*
>
> *(2) Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.*
>
> *Die auf der Grundlage dieses Artikels erlassenen Vorschriften lassen die spezifischen Bestimmungen des Artikels 39 des Vertrags über die Europäische Union unberührt.*

– Der Vertrag von Lissabon führt zum Wegfall der bisherigen Säulenstruktur; die erste Säule betraf den einheitlichen Wirtschaftsraum Europa, die zweite Säule die gemeinsame Außen- und Sicherheitspolitik und die dritte Säule die zwischenstaatliche polizeiliche und justizielle Zusammenarbeit in Strafsachen. Nunmehr wird auch der bisher der dritten Säule zugehörende Bereich der zwischenstaatlichen polizeilichen und justiziellen Zusammenarbeit vergemeinschaftet und unterliegt fortan grundsätzlich dem Geltungsbereich des Artikels 16 AEUV. Inwieweit die EU-Datenschutzrichtlinie von 1995 (95/46/EG), die nach ihrem Artikel 3 gerade nicht für den Sicherheitsbereich galt, nunmehr hier Anwendung findet, wird noch zu prüfen sein. In jedem Fall ist es erforderlich, auch in diesem Bereich einen allgemein verbindlichen hohen Datenschutzstandard zu schaffen.

– Der Rat der EU-Innen- und Justizminister hat erst am 27. November 2008 einen Rahmenbeschluss über den Datenschutz in der dritten Säule verabschiedet (ABl. EU 2008/L 350/60); ob dieser den Anforderungen des Artikels 16 AEUV entspricht, erscheint jedoch zweifelhaft. Problematisch ist insbesondere, dass er sich nur auf die grenzüberschreitende Kommunikation und nicht auf die Datenverarbeitung in den Mitgliedstaaten selbst bezieht, obwohl die übermittelten Daten im Empfängerland mit den dort erhobenen Daten zusammengeführt werden. So kann kein einheitlicher Datenschutzstandard in Europa erreicht werden. Ebenso unbefriedigend ist das Recht der Betroffenen auf Auskunft geregelt, weil die konkrete Ausgestaltung den Mitgliedstaaten überlassen bleibt. Auch das Europäische Parlament hat auf Regelungsdefizite hingewiesen. Die Konferenz der Datenschutz-

beauftragten von Bund und Ländern hat in einer Entschließung vom 6./7. November 2008 erneut angemahnt, dass ein angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich ist (vgl. Anhang 9).

– Die wohl wichtigste Änderung – wenngleich nicht für den grundrechtlich bereits gut abgesicherten Datenschutz in Deutschland – bringt der Vertrag von Lissabon durch seine Bezugnahme auf die Charta der Grundrechte der EU mit sich; dort ist in Artikel 8 ein Grundrecht auf Datenschutz (ergänzend wäre auch auf Artikel 7 – Achtung des Privat- und Familienlebens – hinzuweisen) normiert, das nun erstmals auf europäischer Ebene rechtsverbindlich wird.

Artikel 8 der Grundrechte der EU

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betreffenden Person oder auf einer sonst gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Welche Entwicklung sich aus der unmittelbaren Geltung der EU-Grundrechte für das nationale Datenschutzrecht ergibt, bleibt abzuwarten. Das bewährte Grundrecht auf informationelle Selbstbestimmung in Deutschland darf durch die europäische Rechtsordnung allenfalls ergänzt, aber – auch im Hinblick auf den „Integrationsvorbehalt“ in Artikel 23 Abs. 1 des Grundgesetzes – keinesfalls verdrängt werden, da die europäischen Grundrechte (noch) kein vergleichbares Schutzniveau gewährleisten (siehe hierzu eingehend Ronellenfitsch: Der Vorrang des Grundrechts auf informationelle Selbstbestimmung vor dem AEUV, Datenschutz und Datensicherheit [DuD], 2009, S. 451 ff.).

Artikel 23 Abs. 1 des Grundgesetzes

Zur Verwirklichung eines vereinten Europa wirkt die Bundesrepublik Deutschland bei der Entwicklung der Europäischen Union mit, die demokratischen, rechtsstaatlichen, sozialen und föderativen Grundsätzen und dem Grundsatz der Subsidiarität verpflichtet ist und einen diesem Grundgesetz im Wesentlichen vergleichbaren Grundrechtsschutz gewährleistet. Der Bund kann hierzu durch Gesetz mit Zustimmung des Bundesrats Hoheitsrechte übertragen. Für die Begründung der Europäischen Union sowie für Änderungen ihrer vertraglichen Grundlagen und vergleichbare Regelungen, durch die dieses Grundgesetz seinem Inhalt nach geändert oder ergänzt wird oder solche Änderungen oder Ergänzungen ermöglicht werden, gilt Artikel 79 Abs. 2 und 3.

2.2 Die Harmonisierung der Sicherheitspolitik nach dem „Stockholmer Programm“: Bleibt der Datenschutz auf der Strecke?

Die Europäische Union will im „Stockholmer Programm“ ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dabei drohen die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für verschärfte Sicherheitsmaßnahmen zurückzubleiben.

„Ein offenes und sicheres Europa im Dienste der Bürger“ lautete die Überschrift des im Sommer 2009 angenommenen Dokuments der Eu-

ropäischen Kommission, welches noch in diesem Jahr durch den Europäischen Rat verabschiedet werden und das Gerüst für Maßnahmen der Union auf den Gebieten der Unionsbürgerschaft, Justiz, Sicherheit, Asyl und Einwanderung für die kommenden fünf Jahre (2010 bis 2014) bilden soll. Damit tritt es die Nachfolge der Programme von Tampere „Auf dem Weg zu einer Union der Freiheit, der Sicherheit und des Rechts“ und von Den Haag „Zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union“ an.

Nimmt man das aktuelle Dokument der Kommission näher unter die Lupe, so fallen viele programmatische Ansätze auf, die in dem noch zu beschließenden Aktionsplan umgesetzt werden sollen. Hierzu gehört auch die Absicht, eine „einheitliche Regelung zum Schutz personenbezogener Daten“ zu finden. Bevor es aber dazu kommen kann, muss das „Stockholmer Programm“ noch einige Hürden im Abstimmungsprozess zwischen Kommission und Europäischem Parlament und vor allem im Europäischen Rat im Dezember 2009 nehmen.

Einwände sind im Beteiligungsverfahren beispielsweise auch vom Landtag von Baden-Württemberg und vom Bundesrat geltend gemacht worden; auf die Landtags-Drucksachen 14/4736 und 14/4876 und die Bundesrats-Drucksache 616/09 mit ihren vielfältigen Forderungen und Anregungen wird verwiesen. Dabei stand jedoch weniger der Datenschutz im Mittelpunkt, vielmehr ging es darum, zentralistische Überlegungen der Kommission, die mit dem Subsidiaritätsgebot nicht in Einklang stehen, sowie Kompetenzerweiterungen der europäischen Institutionen Europol und Eurojust zu verhindern.

Der Europäische Datenschutzbeauftragte hat in seiner Stellungnahme vom 10. Juli 2009 deutlich gemacht, dass aus seiner Sicht verschiedene Aspekte des Datenschutzes besonderer Beachtung bei der Realisierung des Programms bedürfen. Dies umfasst nicht nur den Datenaustausch mit den Vereinigten Staaten von Amerika und mit Drittstaaten, die Nutzung neuer Technologien für einen besseren Datenschutz, sondern auch Aussagen zu der Frage zentralisierter Datenbanken, zur Einrichtung eines Systems zur Erfassung von Einreisen und Ausreisen in das Gebiet der Union, zur Entwicklung von präzisen Normen und Kriterien für die Nutzung biometrischer Daten, zum Informationsaustausch zwischen den Polizeibehörden der Mitgliedstaaten und zur weiteren Entwicklung von Europol und Eurojust, den auf europäischer Ebene agierenden Institutionen für die polizeiliche und justizielle Zusammenarbeit.

Datenschutzrechtliche Anliegen sind im Programm als besonders zu berücksichtigende und lückenlos zu gewährende Bürgerrechte genannt, die aber naturgemäß in einem Spannungsfeld mit den Interessen der inneren Sicherheit, der Justiz und der Migration stehen. In diesem Zusammenhang haben bereits die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung der 76. Konferenz zur justiziellen und polizeilichen Zusammenarbeit in der Europäischen Union gefordert:

- *Bei jeder neuen Initiative ist das Verhältnismäßigkeitsprinzip zu wahren und deren Auswirkung auf das bestehende System von Eingriffsmaßnahmen zu berücksichtigen.*
- *Im Hinblick auf den Kumulationseffekt sind die verschiedenen europäischen Initiativen zudem grundrechtskonform aufeinander abzustimmen. Redundanzen und Überschneidungen müssen verhindert werden.*
- *Ein Rechtsakt muss unverzüglich beschlossen werden, der über den Rahmenbeschlussvorschlag hinaus einen hohen und gleichwertigen Datenschutzstandard bei der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit verbindlich vorschreibt. Die gesamte nationale und grenzüberschreitende Informationsverarbeitung in diesem Bereich muss davon erfasst sein, um ein einheitliches Datenschutzniveau in den EU-Mitgliedstaaten zu gewährleisten.*

– *Ein unabhängiges, beratendes Datenschutzgremium sowie eine unabhängige und umfassende datenschutzrechtliche Kontrolle müssen für die polizeiliche und justizielle Zusammenarbeit eingerichtet bzw. gewährleistet werden.*

(Der vollständige Wortlaut der Entschließung vom 6./7. November 2008 ist dem Anhang 9 zu entnehmen.)

Diese Gedanken griff die 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder bei der Behandlung des Stockholmer Programms wieder auf und zählte insbesondere die folgenden weiteren Schritte auf, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen:

– *Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.*

– *Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.*

– *Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.*

– *Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.*

– *Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.*

(Der vollständige Wortlaut der Entschließung vom 8./9. Oktober 2009 ist dem Anhang 13 zu entnehmen.)

Ebenso forderte die Konferenz die Bundesregierung auf, sich für diese Forderungen – auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für Europol und Eurojust – im weiteren Verfahren einzusetzen.

Es ist seit Jahren in fast allen Bereichen festzustellen, dass die Europäische Kommission Aktivitäten in einer Vielzahl von Aufgabenfeldern entwickelt, die mit den in den Mitgliedstaaten gewachsenen Traditionen nicht immer harmonieren. Gleichzeitig ist zu erkennen, dass eine Vielzahl von Initiativen, Rechtsakten, Richtlinien und Verordnungen sich überschneiden und damit nicht einer in sich schlüssigen Strategie entsprechen. Auch das „Stockholmer Programm“ macht hier bislang keine Ausnahme. Derzeit ist eher zu befürchten, dass es eine weitere Initiative mit einem noch zu beschließenden Aktionsplan wird, der die bisherigen Regelungen allenfalls in Teilen ergänzt oder gar ersetzt. Die grundsätzlichen Forderungen des Datenschutzes auf der Grundlage des Artikel 286 des Vertrags über die Europäische Gemeinschaft (zukünftig Artikel 16 des Vertrages über die Arbeitsweise der Europäischen Union als Teil des Vertrages von Lissabon) werden dann nicht dem in Deutschland entwickelten Verständnis entsprechen, sondern teilweise nur dem Mindeststandard in dem jeweiligen Mitgliedstaat. Dass dieser bei 27 Mitgliedstaaten sehr unterschiedlich ist, ist offensichtlich. Viel entscheidender ist aber die Erkenntnis, dass die Europäische Union gerade dann, wenn es um Forderungen der Vereinigten Staaten von Amerika zur Übermittlung aller möglichen Daten einschließlich der privaten Zahlungsvorgän-

ge innerhalb Europas oder gar nur innerhalb einzelner Mitgliedstaaten geht, Grundsätze des Datenschutzes eher außer Acht lässt, obwohl ein auch nur annähernd gleichwertiger Datenschutzstandard für Unionsbürger jenseits des Atlantiks überhaupt nicht gewährleistet ist. Ob damit ein offenes und sicheres Europa für die Bürger geschaffen wird, ist zumindest aus Sicht des Datenschutzes zweifelhaft. Der erst seit kurzem aufkommende Widerstand gegen das Abkommen zwischen der EU und den USA über die Übermittlung von Finanztransaktionsdaten (SWIFT), der namentlich durch die Regierungen von Frankreich und Deutschland artikuliert wurde, lässt hoffen, dass die Belange des Datenschutzes wieder stärkere Beachtung finden.

2.3 Die Umsetzung der EU-Dienstleistungsrichtlinie

Die Vorgaben der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (Dienstleistungsrichtlinie) sind bis zum 28. Dezember 2009 in nationales Recht umzusetzen. Ziel der Richtlinie ist der Abbau von bürokratischen Hindernissen und zwischenstaatlichen Hemmnissen sowie die Förderung der grenzüberschreitenden Erbringung von Dienstleistungen. Bei der Schaffung einer Rechtsgrundlage für den „Einheitlichen Ansprechpartner" wurde das Thema Datenschutz leider übersehen.

Um die Niederlassungsfreiheit von Dienstleistungserbringern innerhalb der Europäischen Union zu fördern, sollen diese künftig alle Verfahren und Formalitäten, die mit der Aufnahme oder Ausübung bestimmter Dienstleistungstätigkeiten verbunden sind, europaweit elektronisch über „Einheitliche Ansprechpartner" abwickeln können. „Einheitliche Ansprechpartner" sollen hierbei als Verfahrenslotsen und Mittler dienen, deren Aufgabe es ist, Anträge von Dienstleistern entgegenzunehmen und diese an die zuständigen Behörden weiterzuleiten. Dienstleister müssen somit nicht mit den (unter Umständen mehreren) zuständigen Behörden, sondern lediglich mit einer Stelle kommunizieren.

Auf Bundesebene wurde eine Bund-Länder-Arbeitsgruppe von der Wirtschaftsministerkonferenz mit der Umsetzung der Dienstleistungsrichtlinie beauftragt. Sie soll u. a. ein Anforderungsprofil für den „Einheitlichen Ansprechpartner" sowie ein Optionspapier für die Verortung der „Einheitlichen Ansprechpartner" erstellen. Daneben hat die Unterarbeitsgruppe „Screening" ein Prüfraster für die Überprüfung aller die Richtlinie betreffenden Normen erarbeitet. Mit dem Vierten Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften vom 11. Dezember 2008 (BGBl. I, S. 2418) sind zum 1. April 2009 neue Regelungen zur Umsetzung der Dienstleistungsrichtlinie, z. B. im Hinblick auf Befristungen und Genehmigungsfiktionen, im Verwaltungsverfahrensgesetz (VwVfG) in Kraft getreten. Weitere Änderungen befinden sich derzeit im Abstimmungsverfahren (§§ 8 a ff. VwVfG). Die IT-Umsetzung zählt nach dem Beschluss der Ministerpräsidentenkonferenz zu den priorisierten Deutschland-Online-Projekten. Die Federführung hierfür liegt auf Landesebene bei den Ländern Baden-Württemberg und Schleswig-Holstein.

Bezüglich der Umsetzung in Baden-Württemberg hatte der Ministerrat bereits in der Sitzung vom 2. Oktober 2007 die Schaffung von ressortübergreifenden Umsetzungsstrukturen beschlossen. Die Steuerung und Vernetzung der beteiligten Ressorts erfolgt durch eine interministerielle Lenkungsgruppe unter Federführung des Wirtschaftsministeriums. Zur Erarbeitung umsetzungsfähiger Lösungen wurden drei Projektgruppen zu den Bereichen „Einheitlicher Ansprechpartner", „Normenprüfung" sowie „Binnenmarktinformationssystem und elektronische Verfahrensabwicklung" eingerichtet. Für die Projektgruppen „Einheitlicher Ansprechpartner" und „Normenprüfung" ist das Wirtschaftsministerium federführend. Die Projektgruppe „Binnenmarktinformationssystem und elektronische Verfahrensabwicklung" ist dem Innenministerium zugeordnet.

Die allgemeinen verwaltungsverfahrensrechtlichen Anforderungen der Dienstleistungsrichtlinie wurden zwischenzeitlich mit dem Gesetz zur

Änderung des Landesverwaltungsverfahrensgesetzes und anderer Gesetze vom 30. Juli 2009 (GBl. S. 363) getroffen. Geleitet vom Grundsatz der Einheitlichkeit des Verwaltungsverfahrensrechts des Bundes und der Länder wurden die bundesrechtlichen Regelungen weitgehend in das Landesrecht übernommen. Namentlich führt das Landesverwaltungsverfahrensgesetz eine neue Verfahrensart, das Verfahren über eine einheitliche Stelle (Einheitliche Ansprechpartner), und allgemeine Regelungen über die Genehmigungsfiktion ein. Eine Festlegung von Aufgaben und Zuständigkeiten der Einheitlichen Stelle soll im Verwaltungsorganisationsrecht erfolgen, sodass weitere Änderungen im einschlägigen Fachrecht oder in Ausführungsgesetzen erforderlich werden.

Mit Beschluss des Ministerrats vom 19. Mai 2009 wurde der Entwurf eines Gesetzes über Einheitliche Ansprechpartner für das Land Baden-Württemberg (EA-Gesetz) zur Anhörung freigegeben. Danach ist vorgesehen, dass in Baden-Württemberg die 30 dienstleistungsrichtlinienrelevanten Kammern sowie – auf freiwilliger Basis – die Stadt- und Landkreise die Aufgabe des „Einheitlichen Ansprechpartners“ wahrnehmen. Die elektronische Informationsbereitstellung und Verfahrensabwicklung soll im Grundsatz über das Dienstleistungsportal des Landes Baden-Württemberg („www.service-bw.de“) erfolgen. Eine umfangreiche Verordnungsermächtigung sieht u. a. die Regelung der Einzelheiten der elektronischen Verfahrensabwicklung und der elektronischen Informationsbereitstellung in einer Rechtsverordnung vor.

Artikel 43 der Dienstleistungsrichtlinie weist ausdrücklich darauf hin, dass die Vorschriften zum Schutz personenbezogener Daten eingehalten werden müssen, diese jedoch auf nationaler Ebene festzulegen sind. Obwohl es also offenkundig ist, dass datenschutzrechtlichen Belangen bei der Umsetzung der Richtlinie eine zentrale Bedeutung zukommt, hat es das für das EA-Gesetz verantwortlich zeichnende Wirtschaftsministerium leider nicht für nötig gehalten, meine datenschutzrechtliche Beurteilung im Rahmen des Anhörungsverfahrens einzuholen. Mein Vorgänger hatte in der Vergangenheit bereits eingehend dargelegt, welche datenschutzrechtlichen Anforderungen an die Umsetzung der Dienstleistungsrichtlinie zu stellen sind (vgl. 28. Tätigkeitsbericht für das Jahr 2007, LT-Drucksache 14/2050). Inzwischen wurde der Gesetzentwurf der Landesregierung (LT-Drucksache 14/5345) in den Landtag eingebracht. Natürlich ist mir bewusst, dass angesichts der Tatsache, dass die Dienstleistungsrichtlinie bis Ende des Jahres umzusetzen ist, ein enormer Zeitdruck besteht. Dies darf aber keinesfalls zu Lasten der Gründlichkeit gehen.

Bei der weiteren Umsetzung der Richtlinie sind die geltenden Grundsätze des Datenschutzes wie z. B. der Rechtmäßigkeit, der Erforderlichkeit, der Zweckbindung und der Transparenz der Datenverarbeitung sowie die Betroffenenrechte zu beachten und Sicherheits- und Datenschutzkontrollmaßnahmen verbindlich festzulegen. Meine Dienststelle wird sowohl die Umsetzung der Dienstleistungsrichtlinie in baden-württembergisches Recht weiterhin kritisch begleiten als auch bei der anschließenden praktischen Realisierung prüfen, ob die Rechte der Betroffenen hinreichend gewahrt bleiben.

3. Entwicklung auf Bundesebene

3.1 Die Weiterentwicklung des Datenschutzrechts

Kurz vor dem Ende der 16. Legislaturperiode hat der Deutsche Bundestag drei verschiedene Novellen zum Bundesdatenschutzgesetz (BDSG) beschlossen, die hier nur nachrichtlich dargestellt werden, da sie den nichtöffentlichen Bereich betreffen:

– Die BDSG-Novelle I vom 29. Juli 2009 (BGBl. I, S. 2254) betraf die Tätigkeit von Auskunfteien und beim Einsatz von (Kredit-)Scoring-Verfahren und hatte zum Ziel, für die Betroffenen mehr Transparenz und Rechtssicherheit zu schaffen. Die Änderung tritt am 1. April 2010 in Kraft. Ergänzend hierzu ist die BDSG-Novelle III, ebenfalls

vom 29. Juli 2009 (BGBl. I, S. 2355), zu erwähnen, die u. a. der Umsetzung der Verbraucherkreditrichtlinie dient und am 11. Juni 2010 in Kraft tritt.

– Die BDSG-Novelle II vom 14. August 2009 (BGBl. I, S. 2814) trat bereits am 1. September 2009 in Kraft; sie hatte die besonders umstrittenen Regelungen zum Adresshandel und zur Werbung zum Gegenstand (Stichwort: Listenprivileg). In einem neuen § 32 BDSG wurde außerdem eine Bestimmung zur Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses aufgenommen.

Wegen weiterer Einzelheiten hierzu wird auf die ausführlichen Erläuterungen im Fünften Tätigkeitsbericht des Innenministeriums über den Datenschutz im nichtöffentlichen Bereich (Kap. B, 2.1) verwiesen *(www.innenministerium.baden-wuerttemberg.de/fm7/2028/Fuenfter_Taetigkeitsbericht_2009_Datenschutz.pdf)*.

Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI; vgl. *www.bfdi.bund.de*) geht in seinem 22. Tätigkeitsbericht und in seinem Internetauftritt auf die aktuellen Änderungen des BDSG ein. Auf der Homepage des BfDI ist außerdem eine regelmäßig aktualisierte Übersicht über den Stand der Bundesgesetzgebung mit datenschutzrechtlichem Bezug zu finden (Datenschutz → Gesetze → Übersicht).

Der Blick voraus lässt hoffen: Das Thema Datenschutz scheint in der 17. Legislaturperiode für die Bundesregierung einen gestiegenen Stellenwert zu haben. Hierauf deuten Passagen des Koalitionsvertrages der die Bundesregierung bildenden Parteien hin, auf die an anderer Stelle schon eingegangen wurde (1. Teil, Nr. 1). Auch einige Programmsätze des neuen Bundesinnenministers klingen ungewohnt moderat, wenn man sie mit den gelegentlich markigen Positionsbestimmungen der beiden Amtsvorgänger vergleicht:

Aussagen von Bundesinnenminister Dr. Thomas de Maizière in der Plenardebatte des Deutschen Bundestags am 11. November 2009, Pl.Prot. 17/4

– *„Wenn es nötig ist, sollten wir neue Gesetze für mehr Sicherheit erlassen. Wenn es nicht nötig ist, sollten wir es lassen.“*
– *„Wir sollten unsere öffentlichen Räume, unsere Plätze, unsere Bahnhöfe, unsere Waggons nicht noch mehr entmenschlichen. Kameras sind gut und notwendig, Menschen sind allemal besser.“*
– *„Daher wird der Datenschutz – ich glaube, wir sollten lieber von Datensicherheit sprechen – ein Schwerpunkt der Arbeit in dieser Legislaturperiode sein.“*
– *„Gesetzlicher Handlungsbedarf besteht zum Beispiel beim Arbeitnehmerdatenschutz. Ich werde im nächsten Jahr einen Gesetzentwurf im Rahmen des Bundesdatenschutzgesetzes für ein Arbeitnehmerdatenschutzgesetz vorlegen.“*

Auch die neue Bundesjustizministerin hat den Datenschutz auf ihrer Agenda ganz nach oben gesetzt:

Aussagen von Bundesjustizministerin Sabine Leutheusser-Schnarrenberger in einem Interview in der Tageszeitung „Die Welt“ am 28. Oktober 2009:

„Das größte Projekt (Anm.: die Frage bezog sich auf die mit Vorrang anzugehenden Projekte des Ressorts) wird die umfassende Modernisierung des Datenschutzes sein. Das gilt für den privaten wie für den öffentlichen Bereich. Dazu brauchen wir den Dialog über die Herausforderungen im Internet, der die klassischen Frontstellungen überwindet. Konkret haben wir ein Datenschutz-Gütesiegel verabredet, so eine Art Stiftung Datenschutz für das Internet.“

Mit einer umfassenden Modernisierung des Datenschutzrechts würde in der Tat ein langjähriges Anliegen der Datenschutzbeauftragten von Bund und Ländern aufgegriffen. Zu erinnern ist in diesem Zusammenhang an das bereits im Jahr 2001 erschienene gleichnamige Gutachten von Roßnagel, Pfitzmann und Garstka, das seinerzeit vom Bundesinnenminister in Auftrag gegeben wurde (auch auf meiner Homepage abzurufen: *www.baden-wuerttemberg.datenschutz.de*). Die Datenschutzbeauftragten von Bund und Ländern haben vor kurzem eine Arbeitsgruppe gebildet, um eigene Vorschläge in die nun erneut beginnende Diskussion über eine Modernisierung des Datenschutzrechts einzubringen.

Wegen der nicht unerheblichen Auswirkungen auf die Bürgerinnen und Bürger im Land werden im Folgenden einige aktuelle datenschutzrechtliche Entwicklungen auf Bundesebene, die den öffentlichen Bereich betreffen, vertieft dargestellt.

3.2 Rechtsentwicklung im Sicherheitsbereich

– Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt

Es war der „Hindernislauf des Jahres“, wenn man die Unterlagen und Medienberichte zu der Änderung des Bundeskriminalamtsgesetzes (BKAG), die am letzten Tag des Jahres 2008 verkündet wurde, noch einmal Revue passieren lässt. Ausgangspunkt war die Föderalismusreform, durch die auch dem Bundeskriminalamt präventivpolizeiliche Gefahrenabwehraufgaben im Bereich des internationalen Terrorismus zugestanden wurden. Diese Gesetzesänderung war und ist zwischen Bund und Ländern, den Datenschutzbeauftragten, den berufsständischen Vertretungen, den Medien und vielen anderen Interessenten aus sehr unterschiedlichen Motiven umstritten. Hauptkritikpunkte waren und sind:

- Möglichkeit des Einsatzes geheimdienstlicher Instrumente durch die Polizei,
- datenschutzrechtlich sehr kritische neue Befugnisse wie Durchsuchung, Rasterfahndung, Wohnraumüberwachung, Telekommunikationsüberwachung und Online-Durchsuchung sowie
- der unzureichende Schutz des Zeugnisverweigerungsrechts bestimmter Berufsgruppen.

Zwar erfolgten im Vermittlungsausschuss noch einige Nachbesserungen, sodass das Gesetz am 1. Januar 2009 in Kraft treten konnte; in den kritischen Punkten aus datenschutzrechtlicher Sicht ergab das Verfahren aber keine grundsätzliche Wende zum Guten. Die 17. Legislaturperiode des Deutschen Bundestages lässt nach dem Koalitionsvertrag vom 26. Oktober 2009 erwarten, dass doch noch die eine oder andere „Feinjustierung“ im Interesse des Grundrechtsschutzes, insbesondere in Bezug auf den Schutz des Kernbereichs privater Lebensgestaltung, vorgenommen wird. In Aussicht gestellt wurde u. a., dass für die Entscheidung über die Anordnung von verdeckten Ermittlungsmaßnahmen nach dem Bundeskriminalamtsgesetz künftig ein Richter am Bundesgerichtshof (statt des bisher zuständigen Amtsgerichts am Dienstsitz des Bundeskriminalamts) zuständig sein soll.

Aus datenschutzrechtlicher Sicht ist vor allem die Vielzahl von Eingriffen in das informationelle Selbstbestimmungsrecht sowohl im Umfang als auch in der Tiefe zu weit gefasst. Hinzu kommt die Sorge vor einer Überlappung der Kompetenz des Bundeskriminalamts mit der Zuständigkeit der Länderpolizeien; außerdem drohen die Grenzen zu den Aufgaben des Verfassungsschutzes verwischt zu werden. Gerade das Bundesverfassungsgericht hatte in seiner Entscheidung vom 27. Februar 2008 den Schutz des Kernbereichs der privaten Lebensgestaltung mit seiner Bedeutung für die verfassungsrechtliche Ordnung noch einmal betont. Die Entschließung der

75. Datenschutzkonferenz zu dem ursprünglichen Gesetzentwurf findet sich in Anhang 4.

Bemerkenswert ist dieses Gesetzgebungsverfahren nicht zuletzt deshalb, weil die erwähnte Entscheidung zur Online-Durchsuchung klare Grenzen für eine verfassungsgemäße Lösung aufgezeigt hatte. So ist es nicht verwunderlich, dass die Änderung des Bundeskriminalamtsgesetzes ebenfalls zur Anrufung des Bundesverfassungsgerichts führte.

– Rechtsverordnung nach § 7 Abs. 6 BKAG

Seit Jahren existiert im Bundeskriminalamtsgesetz eine Verordnungsermächtigung für das Bundesministerium des Innern, nach der mit Zustimmung des Bundesrates das Nähere über die Art der Daten, die nach §§ 8 und 9 BKAG gespeichert werden dürfen, geregelt werden kann. Diese Bestimmungen regeln die Datenverarbeitung in Dateien der Zentralstelle, die zu verschiedenen Zwecken errichtet wurden. Das Gesetz regelt ebenfalls die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten. Ein ganz wesentlicher Teil der Datenverarbeitung erfolgt in dem polizeilichen Informationssystem nach § 11 BKAG, einem Datenverbund mit einer Vielzahl von Verbunddateien, für den wiederum die vorgenannten Regelungen entsprechend gelten.

Daher hat eine nähere Bestimmung über zu speichernde Daten erhebliche Auswirkungen auf die kriminalpolizeiliche Tätigkeit in den Ländern. Seit Jahren wurde immer wieder von den Datenschutzbeauftragten gefordert, diese Verordnungsermächtigung für konkrete Regelungen zu den Speicherungsinhalten zu nutzen. Erst nachdem durch das Urteil des Niedersächsischen Oberverwaltungsgericht in Lüneburg vom 16. Dezember 2008, 11 LC 229/08, zu der Verbunddatei „Gewalttäter Sport“ die Unzulässigkeit der Speicherung personenbezogener Daten mangels fehlender Rechtsgrundlage festgestellt wurde und die 77. Konferenz der Datenschutzbeauftragten von Bund und Ländern ihre Forderung für eine rechtliche Festlegung der Speicherungsinhalte erneuerte (siehe Anhang 11), kam Bewegung in die Sache. Der Bundesinnenminister legte einen Arbeitsentwurf vor, zu dem inzwischen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Stellung genommen hat; dabei nahm er auch die Anregungen der Datenschutzbeauftragten der Länder für eine präzise Festlegung der zulässigen Daten auf. Inzwischen fand eine erste Ressortbesprechung auf Bundesebene statt, bei der aber zunächst noch grundsätzliche Fragen, wie etwa eine sinnvolle Abgrenzung in Bezug auf die beiden unterschiedlichen Verordnungsermächtigungen in § 7 Abs. 6 BKAG und in § 484 Abs. 3 StPO, im Vordergrund standen. Des Weiteren wurde über die Methode diskutiert, wie zulässige Datenarten zu regeln sind (z. B. durch Regelbeispiele oder durch eine abschließende Aufzählung). Aus Sicht des Datenschutzes verdient eine enumerative Aufzählung schon in Anbetracht der verfassungsrechtlichen Vorgaben den Vorzug.

3.3 Zensus 2011

2011 findet in allen Staaten der Europäischen Union ein Zensus statt. Im Unterschied zur Volkszählung 1983 gibt es diesmal keine wesentlichen datenschutzrechtlichen Probleme.

Die Vorbereitung der europaweiten Volkszählung 2011 war bereits 2007, als mein Amtsvorgänger in seinem Tätigkeitsbericht über den damaligen Sachstand berichtete, in vollem Gang. Diese Vorbereitung fand 2009 zumindest hinsichtlich der Schaffung der dafür erforderlichen gesetzlichen Grundlagen ihren Abschluss. Aufbauend auf dem Zensusvorbereitungsgesetz wurde im Juli 2009 mit dem Zensusanordnungsgesetz das eigentliche Zensusgesetz 2011 (ZensG) beschlossen und verkündet (BGBl. I, S. 1781). Damit ist nun beispielsweise klar, dass die Statistischen Ämter des Bundes und der Länder zum Stichtag (Berichtszeitpunkt) 9. Mai 2011 eine Bevölkerungs-, Gebäude- und Wohnungszäh-

lung durchführen, die erstmals nicht mehr im Wege einer Befragung aller Einwohner, sondern im Wesentlichen registergestützt, das heißt durch Auswertung vorhandener Melde- und anderer Verwaltungsregister durchgeführt wird; Haushalte werden nur noch auf Stichprobenbasis befragt. Erfreulicherweise hat das Finanzministerium Baden-Württemberg meine Dienststelle auch diesmal frühzeitig eingebunden. Meine datenschutzrechtlichen Anmerkungen blieben letztlich leider unberücksichtigt; allerdings ist mein Einfluss bei Bundesvorhaben auch recht begrenzt. Problematisch ist weiterhin vor allem die in § 8 ZensG vorgesehene Erhebung von Daten in sog. Sonderbereichen (z. B. Gemeinschaftsunterkünfte), weil sie 2011 – im Unterschied zur Volkszählung 1987 – in personenbezogener Form erfolgen soll. Unter dem Strich ist aber festzuhalten, dass, wenn die Volkszählung gesetzeskonform durchgeführt wird, keine durchgreifenden datenschutzrechtlichen Bedenken bestehen. Wegen weiterer Einzelheiten verweise ich auf die Ausführungen des für die Bundesgesetzgebung federführend zuständigen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in seinem 22. Tätigkeitsbericht unter Nummer 5.3 „Neue Ansätze in der amtlichen Statistik“ und 5.5 „Volkszählung 2011“ *(www.bfdi.bund.de)*.

3.4 Gesetz über den elektronischen Entgeltnachweis (ELENA)

Der Bundesgesetzgeber hat im Berichtszeitraum das Gesetz über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen. Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an eine Zentrale Speicherstelle zu dulden.

Am 2. April 2009 ist das ELENA-Verfahrensgesetz in Kraft getreten (BGBl. I, S. 634, 1141). Es sieht vor, dass Arbeitgeber von Januar 2010 an die Einkommensdaten ihrer Beschäftigten an eine Zentrale Speicherstelle übertragen. 2012 beginnt der Regelbetrieb im ELENA-Verfahren. Dann werden die für die Bewilligung von Anträgen auf Arbeitslosengeld, Wohngeld und Bundeselterngeld erforderlichen Daten unter Einsatz von Signaturkarten der Leistungsbezieher abgerufen. Die Idee zu dem Verfahren stammt aus der Ägide der rot-grünen Regierungskoalition auf Bundesebene und trug seinerzeit den Namen „JobCard“.

Aus meiner Sicht ist das Verfahren eines der größten datenschutzrechtlichen Ärgernisse der letzten Jahre, denn das Gesetz führt zu einem riesigen zentralen Datenspeicher, wobei ein großer Anteil der Betroffenen die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals geltend machen wird. So haben die betreffenden Arbeitgeber beispielsweise monatlich Entgeltnachweise elektronisch an die Zentrale Speicherstelle auch für alle Beamten, Richter und Soldaten, aber auch für alle anderen Beschäftigten des öffentlichen Dienstes zu liefern, obwohl dieser Personenkreis nur ausnahmsweise Leistungsbezieher sein wird und sein Gehalt ohne Weiteres durch eine Gehalts- oder Besoldungsmitteilung, die im Behördenverkehr gegenseitig anerkannt wird, jederzeit nachweisen kann. Diese Datensammlung auf Vorrat ist unter dem Gesichtspunkt der Verhältnismäßigkeit, insbesondere der Erforderlichkeit, verfassungsrechtlich bedenklich. Hierauf haben die Datenschutzbeauftragten des Bundes und der Länder wiederholt, unter anderem in ihrer Entschließung vom 6./7. November 2008 (vgl. Anhang 25), hingewiesen. Hinzu kommt die Gefahr, dass eine zentrale Speicherung Begehrlichkeiten anderer Behörden weckt.

In der genannten Entschließung haben die Datenschutzbeauftragten u. a. gefordert, dass der Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten von einer unabhängigen Treuhänderstelle verantwortet werden muss. Das ELENA-Verfahrensgesetz sieht nun vor, dass der Datenbank-Hauptschlüssel durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) verwaltet wird. Ich halte das für keine glückliche Lösung, denn auf diese Weise könnte der BfDI Aufgaben der Exekutive übernehmen, die er ansonsten zu überwachen hat. Eine weitere Forderung des Datenschutzes war, für die abrufenden Stellen sog. starke Authentisierungs-

verfahren vorzuschreiben, um deren Identität sicherzustellen. Auch dem ist der Gesetzgeber nachgekommen. Nicht realisiert wurde allerdings die geforderte Ende-zu-Ende-Verschlüsselung.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Umsetzung des ELENA-Verfahrensgesetzes in den nächsten Jahren aufmerksam beobachten und begleiten. Ob die Regelungen tatsächlich verhältnismäßig sind, muss sich noch in der Praxis und gegebenenfalls auf dem Prüfstand des Bundesverfassungsgerichts erweisen.

3.5 Das geplante Bundesmelderegister

Durch die Föderalismusreform I ist die Gesetzgebungszuständigkeit auf dem Gebiet des Meldewesens ausschließlich auf den Bund übergegangen. Bisher war diese Materie rahmenrechtlich durch den Bund im Melderechtsrahmengesetz sowie in den Meldegesetzen der Länder geregelt.

Das Bundesministerium des Innern hat schon im Jahr 2008 den Referentenentwurf eines Gesetzes zur Fortentwicklung des Meldewesens vorgelegt. In dessen Mittelpunkt steht bzw. stand eine Vorschrift, welche die Einrichtung eines (zentralen) Bundesmelderegisters auf Bundesebene vorsah. Die Verwirklichung dieser Pläne des Bundes hätte zur Folge, dass die Einwohnerdaten künftig auf zwei oder gar drei Ebenen parallel gespeichert werden, nämlich bei den originär zuständigen Meldebehörden (Gemeinden), beim Bund und zusätzlich noch (wie zum Teil schon bisher) auf Landesebene.

In seiner Stellungnahme an das Innenministerium hat mein Vorgänger seinerzeit die massiven rechtlichen Bedenken des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gegen die Einführung eines Bundesmelderegisters unterstützt. Dieser hatte – trotz einiger Verbesserungen im Laufe des Gesetzgebungsvorhabens – weiterhin Zweifel hinsichtlich der Notwendigkeit eines inhaltlich umfänglichen zentralen Bundesmelderegisters geäußert, welches einer Datenspeicherung auf Vorrat für unbestimmte Zwecke angesichts einer Vielzahl zugriffsberechtigter Stellen Vorschub leisten könne. Das Bundesmelderegister eröffne zudem die Möglichkeit einer Verknüpfung mit anderen Daten und könne gegebenenfalls den Weg zu einem allgemeinen Personenkennzeichen bereiten.

Die Ziele, die als Begründung für ein Bundesmelderegister genannt wurden, könnten möglicherweise auch durch eine Vernetzung vorhandener Melderegister, z. B. auf Länderebene, erreicht werden.

Der Referentenentwurf des Bundesinnenministeriums für ein Bundesmeldegesetz hat in der 16. Wahlperiode des Deutschen Bundestags keine Gesetzesreife mehr erlangt. In der Koalitionsvereinbarung vom 26. Oktober 2009 findet sich lediglich der dürre Hinweis, dass der fortbestehende Auftrag aus der Föderalismuskommission I durch ein Bundesmeldegesetz erfüllt werden solle. Es ist zu hoffen, dass dabei auch für das Bundesmelderegister eine datenschutzfreundlichere Lösung gefunden wird.

3.6 Elektronischer Pass und elektronischer Personalausweis

Im 28. Tätigkeitsbericht meiner Dienststelle für das Jahr 2007 (LT-Drucksache 14/2050) wurde bereits darauf hingewiesen, dass auf dem RFID-Chip des neuen elektronischen Reisepasses seit 1. November 2007 zusätzlich Fingerabdrücke des Passinhabers gespeichert werden. Ferner wurde in diesem Beitrag auch über die Eindrücke eines meiner Mitarbeiter anlässlich eines Informationsbesuchs bei einem Testlauf des Passantragsverfahrens berichtet. Am 1. November 2007 wurde das Verfahren zur Beantragung des e-Passes bundesweit in den Produktionsbetrieb übernommen. Nennenswerte Beschwerden von Betroffenen sind mir bisher erfreulicherweise nicht zugegangen.

Ab November 2010 soll auch der Personalausweis nicht nur mit elektronisch gespeichertem Lichtbild und – erfreulicherweise nur auf freiwilliger Grundlage – mit elektronisch gespeicherten Fingerabdrücken

auf dem Funkchip ausgestattet werden. Das entsprechende Gesetz wurde am 18. Juni 2009 verkündet (BGBl. I, S. 1346) und soll im Wesentlichen am 1. November 2010 in Kraft treten. Es ist anzuerkennen, dass der Gesetzgeber aufgrund datenschutzrechtlicher Bedenken nunmehr ausdrücklich klargestellt hat, dass ein Ausweisinhaber keine Nachteile erleiden darf, wenn er sich weigert, seine Fingerabdrücke auf dem Ausweis speichern zu lassen. Wenn es vom Inhaber gewünscht ist, soll der elektronische Personalausweis zukünftig als elektronischer Identitätsnachweis im Internet sowohl gegenüber Behörden als auch bei Rechtsgeschäften mit der Privatwirtschaft dienen. Dem Ausweisinhaber soll es dann aber möglich sein, z. B. gegenüber einem Vertragspartner nur bestimmte personenbezogene Daten, z. B. sein Alter, zu offenbaren.

Noch ist technisch und rechtlich nicht vollständig geklärt, wie ein Ausweisinhaber künftig seine Signatur als zusätzliches Datum für die Gültigkeitsdauer dieser Identitätskarte speichern lassen kann.

Der neue elektronische Personalausweis wird aufgrund seiner Zusatzfunktionen für Zwecke der elektronischen Abwicklung von Rechtsgeschäften und des eGovernment einerseits vielfältige Chancen, andererseits aber auch zahlreiche Risiken im Hinblick auf Datenschutz und Datensicherheit mit sich bringen. Ein Auslesen des Datenflusses und der PIN muss zuverlässig unterbunden werden. Dem im kommenden Jahr vorgesehenen bundesweiten Testbetrieb sehe ich daher mit Spannung entgegen.

4. Videoüberwachung

In Bahnhöfen, in Kaufhäusern, in Parkhäusern, in unterirdischen Haltestellen, in Fahrzeugen des öffentlichen Nahverkehrs, an privaten Hauseingängen sind sie mittlerweile allgegenwärtig: Videokameras, die alle Menschen erfassen, die sich dort – aus welchem Grund auch immer – aufhalten, gehen, stehen oder fahren. Videokameras werden aber auch in und an öffentlichen Dienstgebäuden, im Straßenraum, bei Veranstaltungen aller Art eingesetzt.

Für die von privaten Stellen eingesetzten Kameras gilt das Bundesdatenschutzgesetz. Hierfür ist die Dienststelle des Landesbeauftragten für den Datenschutz bisher nicht zuständig. Die Aufgabe der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich übt das Innenministerium aus, das sich schon häufiger mit Fragen zur Videoüberwachung auseinandersetzen musste, zuletzt in seinem Fünften Tätigkeitsbericht aus diesem Jahr.

Demgegenüber unterliegen die öffentlichen Stellen, die ihre Dienstgebäude und Einrichtungen mit Videokameras ausstatten, um die Besucher in den Räumlichkeiten „im Blick“ zu haben, und die öffentliche Straßen und Plätze überwachen, um kriminellem Tun möglichst schnell begegnen zu können, der Kontrolle durch meine Dienststelle. Vielfach setzen auch Ordnungskräfte die Videotechnik ein, um ihre Einsätze zu dokumentieren und mögliche Störer bildlich zu erfassen. Bereits im 25. Tätigkeitsbericht für das Jahr 2004 (LT-Drucksache 13/3800) hat mein Vorgänger zu derartigen Maßnahmen im Zusammenhang mit Volksfesten grundlegende Ausführungen gemacht. Wie nachfolgend nachzulesen ist, bedurfte es in einem Fall weiterer Nachhilfe, um der informationellen Selbstbestimmung einer Vielzahl von Festbesuchern gerecht zu werden.

Da unter „Videoüberwachung“ vieles verstanden und dementsprechend auch praktiziert wird, ist es notwendig, das Zusammenspiel von rechtlichen Anforderungen und technischen Möglichkeiten näher zu erläutern. Ob eine derartige Maßnahme jeweils den rechtlichen Bedingungen für die Erhebung und Verarbeitung personenbezogener Daten entspricht und mit welchen technischen Mitteln sie realisiert wird, macht in vielen Fällen den Unterschied zwischen zulässig und unzulässig aus.

Die Beobachtung eines aktuellen Geschehens mittels Kamera und Bildschirm durch Übersichtsaufnahmen ist zulässig, wenn dabei personenbezogene Daten Einzelner nicht identifiziert werden können. Selbst das Aufzeichnen wäre dann mangels Eingriff in die Grundrechte der aufgenomme-

nen Personen unproblematisch. In Anbetracht der raschen Entwicklung technisch immer komfortablerer und preiswerterer Geräte dürfte eine derartige Technik, bei der man die aufgenommenen Personen nur schemenhaft erkennt, kaum noch zum Einsatz kommen. Selbst Webcams werden immer leistungsfähiger und drohen allmählich ihren datenschutzrechtlich unproblematischen Einsatzbereich zu überschreiten. Sobald Einzelpersonen oder Fahrzeuge aber individuell erkennbar werden, beginnt der Eingriff in das informationelle Selbstbestimmungsrecht. Das äußere Erscheinungsbild einer Person, das Kraftfahrzeugkennzeichen und alle weiteren Merkmale, die eine Zuordnung zu einer bestimmten Person erlauben, gehören zu den personenbezogenen Daten. Dafür bedarf es nach dem inzwischen 25 Jahre alten Urteil des Bundesverfassungsgerichts zur Volkszählung aus dem Jahr 1983 (BVerfGE 65,1) einer spezifischen Rechtsgrundlage. Dies hat das Gericht in einem Beschluss vom 11. August 2009, 2 BvR 941/08, zum Einsatz von Videoüberwachungsanlagen bei der Verfolgung von Verkehrsordnungswidrigkeiten ausdrücklich noch einmal bestätigt. Wenn dann durch Aufzeichnung des Geschehens eine Reproduzierbarkeit der erhobenen Daten möglich wird, wird der Eingriff in die Persönlichkeitsrechte weiter intensiviert.

Welche rechtlichen Bedingungen für eine derartige Verarbeitung personenbezogener Daten gegeben sind, ist für Baden-Württemberg recht einfach zu beantworten. Es gibt vor allem Regelungen im Polizeigesetz für offene und verdeckte Bildaufzeichnungen; weitere sind in Bundesgesetzen wie der Strafprozessordnung oder dem Bundesdatenschutzgesetz enthalten, letzteres gilt für öffentliche Stellen des Landes nicht. In allen anderen Bereichen der öffentlichen Verwaltung wurde früher nur der bisherige § 13 Abs. 2 Satz 2 LDSG herangezogen. Diese Vorschrift bietet nach der Entscheidung des Bundesverfassungsgerichts vom 23. Februar 2007, 1 BvR 2368/06 (vgl. hierzu 28. Tätigkeitsbericht für das Jahr 2007, LT-Drucksache 14/2050), zu der inhaltlich vergleichbaren Regelung des Bayerischen Datenschutzgesetzes, mangels hinreichender Bestimmtheit jedoch keine ausreichende Rechtsgrundlage für Videoüberwachungen. Konsequenzen sollten aus dieser Entscheidung eigentlich schon längst gezogen worden sein. Vor einem Jahr wurde meine Dienststelle bereits zu einem Arbeitsentwurf zur entsprechenden Änderung des Landesdatenschutzgesetzes angehört. Leider hat ein Vorschlag für eine verfassungskonforme Regelung bis jetzt noch nicht den Weg in den Landtag gefunden.

Bei allen rechtlichen Vorgaben und technischen Möglichkeiten muss in der allerorten geführten Diskussion über Sinn und Zweck der Videoüberwachung bedacht werden, ob sie das leisten kann, was allgemein von ihr erwartet wird. Dass Aufzeichnungen helfen können, Straftäter zu ermitteln, bestreite ich gar nicht. Dem Opfer einer Straftat wird das leider nur bedingt helfen. Wenn neben der Aufzeichnung auch an einem Bildschirm in Echtzeit das Geschehen beobachtet wird, kann dies geeigneter sein. Dann ist es aber auch erforderlich, genügend Personal für die Beobachtung und vor allem für Interventionen am Ort des beobachteten Geschehens einsetzen zu können. Die Kehrseite dieser Medaille ist, dass Daten von einer Vielzahl von Personen, die die überwachten Orte vielleicht sogar täglich passieren müssen, ohne erkennbare Zweckbestimmung und vielleicht sogar gegen deren Willen erhoben werden. Gerade der oben erwähnte jüngste Beschluss des Bundesverfassungsgerichts sollte die Notwendigkeit präziser gesetzlicher Regelungen und deutlicher Hinweise bei der Realisierung der Beobachtung vor Augen führen.

Ein Blick über die Grenzen kann ebenso hilfreich sein. Das Vereinigte Königreich bietet vielerorts flächendeckende Videoüberwachung. Nach Schätzung des dortigen Innenministeriums sind etwa vier Millionen Überwachungskameras im Einsatz. Zu den in London installierten Kameras konstatierte die zuständige Metropolitan Police in einem jüngst veröffentlichten Bericht, dass auf 1.000 Überwachungskameras nur eine aufgeklärte Straftat käme. Die Erwartungen der Bevölkerung seien nach der Analyse des leitenden Polizeivertreters enttäuscht worden, obwohl sie täglich 300-mal von den Kameras erfasst würden. 500 Millionen britische Pfund (derzeit rund 550 Millionen EUR), die zwischen 1996 und 2006 dafür ausgegeben wurden, seien kaum effizient eingesetzt worden. Dies läge nicht zuletzt daran, dass die Aufzeichnungen vielfach nicht gesichtet würden, da auch zu wenig geschul-

tes Personal vorhanden sei. Gewaltverbrechen und spontane Straftaten könnten im Übrigen damit nicht verhindert werden. Diese Analyse macht deutlich, dass die Erwartungen an eine Videoüberwachung im Hinblick auf eine präventive Wirkung oft überzogen sind; Videoüberwachungsmaßnahmen sind jedenfalls kein Allheilmittel.

Die Videoüberwachung erfordert für eine wirksame Prävention einen erheblichen Einsatz an Personal. Es reicht eben nicht, im Nachhinein Aufzeichnungen auszuwerten. Während der Beobachtung müssen erfahrene Kräfte an den Bildschirmen das in dem überwachten öffentlichen Bereich bereitstehende Personal zum raschen Eingreifen führen. In Anbetracht der angespannten Personalsituation der Polizei kann sich die polizeiliche Videoüberwachung nach meinem Eindruck eigentlich nur auf wenige öffentliche Stellen und besonders auffällige Orte beschränken. Ganz abgesehen von diesen praktischen Erwägungen ist es erforderlich, dass ein überwachter Bereich mit eindeutigen Hinweisen auf die Maßnahme gekennzeichnet ist. Selbstverständlich sind diese Hinweise so zu gestalten, dass sie von den Passanten auch zur Kenntnis genommen werden können.

Die rechtlichen Anforderungen an den Einsatz der Videotechnik bekommen auch deshalb zunehmend Gewicht, weil sich immer mehr öffentliche und private Stellen dazu entschließen, aktuelles Geschehen im öffentlichen oder privaten Raum durch Webcams zu beobachten und im Internet einer unbegrenzten Zuschauerzahl zugänglich zu machen. Vereinzelt gibt es bereits Webcams, die von dem einzelnen Zuschauer über das Internet gesteuert werden können, um für ihn interessante Geschehnisse besser zu erfassen. Auf den 6. Teil, 4. Abschnitt, Nr. 1 weise ich hier schon hin. Ob das alles und zu jeder Zeit zulässig ist, welche Möglichkeiten Betroffene haben, sich dagegen zur Wehr zu setzen, wird nicht nur den Datenschutz weiter beschäftigen. Dies machen schon die immer häufigeren Zivilrechtsstreitigkeiten auf Unterlassung von Videoüberwachungen im privaten Umfeld deutlich. Nicht umsonst spricht die Aufsichtsbehörde für den nichtöffentlichen Bereich bereits von einem „Kampf gegen Windmühlen“ (Fünfter Tätigkeitsbericht des Innenministeriums 2009, Kap. B 11).

Nachfolgend berichte ich über Videoüberwachungen, die dem öffentlichen Bereich zuzuordnen waren oder gewesen wären.

4.1 Videoüberwachung an Schulen

Mein Vorgänger hatte schon im 28. Tätigkeitsbericht für das Jahr 2007 (LT-Drucksache 14/2050) sowie in seiner Pressemitteilung vom 30. September 2008 „Videoüberwachung bedarf gesetzlicher Grundlage, Bundesverfassungsgericht ernst nehmen“ (abrufbar über die Internet-Seite meines Amts unter „Der LfD und seine Aufgaben“ → „Pressemitteilungen“ und dem genannten Datum) darauf hingewiesen, dass eine Videoüberwachung von allgemein zugänglichen Orten und Einrichtungen – jedenfalls soweit die Videoüberwachung mit einer Aufzeichnung verbunden ist – einer speziellen gesetzlichen Grundlage bedarf. Im Polizeibereich ist diese Art der Datenverarbeitung geregelt, bislang aber nicht für Schulen. Gleichwohl gibt es im Schulbereich offenbar den verbreiteten Wunsch, zur Bekämpfung etwa von Diebstählen und Vandalismus zum Mittel der Videoüberwachung zu greifen. In vielen Fällen wandten sich insbesondere Schulleiterinnen und Schulleiter sowie Bürgermeisterämter, da im Regelfall die Gemeinden Schulträger sind, an mein Amt und wurden unter Hinweis auf die Entscheidung des Bundesverfassungsgerichts vom 23. Februar 2007 und das noch ausstehende Gesetzgebungsverfahren eingehend beraten. Soweit ich Rückmeldungen erhielt, führte diese Beratung ganz überwiegend dazu, dass im Schulbereich die Rufe nach Videoüberwachung angesichts der klaren rechtlichen Rahmenbedingungen jedenfalls bis auf Weiteres verstummten.

Daneben hatte sich mein Amt aber leider auch mit Fällen zu befassen, in denen Videoüberwachungen an Schulen unter Missachtung der Rechtslage bereits aktiviert worden waren. An erster Stelle ist hier die Videoüberwachung an 17 Mannheimer Schulen zu nennen, auf die mein Amt durch eine Anfrage aus dem Bereich der Stadt Mannheim aufmerksam gemacht worden war. In seiner Pressemitteilung vom

30. September 2008 stellte mein Vorgänger ausdrücklich fest, dass der Betrieb von Videoüberwachungsanlagen durch öffentliche Stellen – sofern mit einer Aufzeichnung des Bildmaterials verbunden – außerhalb des polizeilichen Bereichs in jedem Fall rechtswidrig sei. Wenn Videoüberwachung auch in anderen Bereichen der öffentlichen Verwaltung zugelassen werden soll, müsse der Landtag dafür erst die Grundlage schaffen. Auch wenn die Entscheidung zu einer Videoüberwachung in Bayern ergangen sei, seien die Erkenntnisse des Gerichts wegen der Vergleichbarkeit der Rechtslage in beiden Ländern uneingeschränkt auf Baden-Württemberg übertragbar. Dies bedeute, dass in jedem Fall Videoüberwachungsanlagen mit Aufzeichnungsmöglichkeit, die nach der Entscheidung des Bundesverfassungsgerichts ohne spezielle gesetzliche Grundlage installiert worden sind, sofort abzuschalten sind.

Für bereits eingerichtete Videoüberwachungen sah er eine Übergangslösung bis Ende 2008 als möglich an, die dem Umstand Rechnung trage, dass vor der Entscheidung des Bundesverfassungsgerichts eine Überwachung auch aufgrund allgemeiner datenschutzgesetzlicher Regelungen zugelassen gewesen sei. Soweit eine Gesetzesänderung bis dahin nicht realisiert werden könne, müssten auch die in Betrieb befindlichen Altanlagen abgeschaltet werden. Im Übrigen könne eine solche Übergangslösung für Altanlagen nicht voraussetzungslos in Anspruch genommen werden. Ein rechtmäßiger Betrieb von Videoüberwachungsanlagen verlange, dass die Erforderlichkeit einer Videoüberwachung gründlich untersucht und alternative Lösungsmöglichkeiten sorgfältig geprüft werden. Es seien dann die Maßnahmen zu wählen, die mit den geringsten Eingriffen in das Persönlichkeitsrecht der Betroffenen verbunden sind, was dazu führen könne, dass auf eine Videoüberwachung gänzlich zu verzichten sei. Zudem seien die Überwachungsbereiche deutlich kenntlich zu machen.

In Mannheim hat die Prüfung durch meine Dienststelle ergeben, dass dort an insgesamt 17 Schulen videoüberwacht wurde. Eine einheitliche Linie, welche Schulbereiche überwacht wurden und wie lange das Bildmaterial gespeichert worden war, fehlte offensichtlich. Die Stadt Mannheim wurde daher aufgefordert, entsprechend den oben genannten Grundsätzen zu verfahren. Erhebliche Zweifel bestanden auch, ob die Erforderlichkeit einer Videoüberwachung in jedem Fall hinreichend belegt war. Schließlich darf die Einrichtung einer Videoüberwachung nicht nur an Zweckmäßigkeitsgesichtspunkten ausgerichtet werden, sondern es muss gründlich abgewogen werden, ob das Interesse an einer Videoüberwachung die rechtlichen Interessen der von der Beobachtung Betroffenen wirklich überwiegt.

Die Stadt Mannheim teilte mir auf meine entsprechenden Anfragen mit, man habe dort mit einer schriftlichen Mitteilung vom 17. Dezember 2008 die in städtischer Schulträgerschaft stehenden Schulen darüber unterrichtet, dass eine vorhandene Videoüberwachung mit Ablauf des 31. Dezember 2008 abzuschalten sei, und man gehe davon aus, dass die Videoüberwachungen tatsächlich eingestellt worden seien. Zudem wies die Stadt Mannheim darauf hin, dass die kommunale Verwaltung eine weitergehende Kontrolle für entbehrlich halte, da nach einem Schreiben des Kultusministeriums Baden-Württemberg beim laufenden Schulbetrieb bei der Anbringung und Durchführung der Videoüberwachung die sog. inneren Schulangelegenheiten betroffen seien, für die das Land und nicht die Stadt Mannheim die Verantwortung trage. Ich betrachte diese Angelegenheit damit zunächst als erledigt, behalte mir aber selbstverständlich vor, die Verhältnisse vor Ort zu gegebener Zeit zu kontrollieren.

Einem weiteren Fall ging mein Amt aufgrund von Zeitungsmeldungen nach, in denen unter den Überschriften „Schüler auf dem Weg zum Klo fotografiert“ und „Big Brother vor der Toilette“ über eine Videoüberwachung an einer Grundschule berichtet wurde. Demnach hatte der Schulleiter wegen des Verdachts, dass einige Schüler die Toiletten wiederholt verschmutzt hätten, auf dem Flur vor den Toiletten eine digitale Überwachungskamera nebst Bewegungsmelder installiert, wobei diese

Überwachung nach einem Monat auf Anweisung von Schulträger und Schulamt wieder eingestellt worden sei. Meine Dienststelle bat unter nachrichtlicher Beteiligung des Staatlichen Schulamts sowie des Regierungspräsidiums als oberer Schulaufsichtsbehörde sowohl die Schule als auch die betroffene Stadt – als Schulträger – um Stellungnahme. Eine Stellungnahme der Stadt ist bei meinem Amt bislang leider nicht eingegangen. Dagegen bestätigte die Schule in ihrer raschen Stellungnahme im Wesentlichen den in den Zeitungsmeldungen dargestellten Sachverhalt. Sie räumte einen „fatalen Fehler“ ein und erklärte, man hätte sich dort vor der Durchführung der Maßnahme besser über die schul- und datenschutzrechtlichen Bestimmungen informieren müssen. Ergänzend teilte sie mit, dass der Hausmeister auf Anordnung des Stadtbauamts die Kamera wieder abgebaut habe. Ich betrachte diese Angelegenheit als erledigt und sehe derzeit keinen weiteren Handlungsbedarf.

Diese Fälle können als Musterbeispiele dafür gesehen werden, wie wichtig es für Schulen sein kann, sich rechtzeitig, also im Vorfeld unüberlegter und gegebenenfalls illegaler Maßnahmen, über die Rechtslage zu informieren und sich dazu etwa an die Aufsichtsbehörden der Kultusverwaltung oder natürlich auch an mein Amt zu wenden.

4.2 Videoüberwachung im gemeindlichen Freizeitbad

Die einleitend erwähnten Entscheidungen des Bundesverfassungsgerichts zur Videoüberwachung machen deutlich, dass Behörden und sonstige öffentliche Stellen eine Videoüberwachungsmaßnahme – jedenfalls mit Aufzeichnung des gewonnenen Bildmaterials – nicht auf allgemeine datenschutzrechtliche Regelungen stützen können. Welche erheblichen Eingriffe in das Recht auf informationelle Selbstbestimmung damit verbunden sind, zeigt auch das folgende Beispiel. Es belegt, wie notwendig spezielle gesetzliche Regelungen sind, um Anlass, Zweck und Grenzen des Eingriffs präzise und normenklar festzulegen.

Mitte 2009 wandte sich die Inhaberin einer Schwimmschule an mich. Sie teilte mir mit, in dem kommunalen Freizeitbad, wo sie ihren Beruf ausübe, seien verschiedene Videokameras angebracht. Die Petentin warf ihrem Ex-Mann, der zugleich Betriebsleiter des Freizeitbads war, vor, auch sie und ihre Schwimmkurse während der Scheidungszeit auf diese Weise überwacht zu haben. Jedenfalls habe ihr Ex-Mann gegenüber dem Finanzamt in einer Steuerangelegenheit eine eidesstattliche Versicherung abgegeben, die darauf hindeute. Die Petentin hatte das offenbar auch dem Bürgermeister in einem Gespräch mitgeteilt. Der Bürgermeister habe das zum Anlass genommen, die bisher fehlenden Hinweisschilder auf die Videoüberwachung im Freizeitbad anzubringen.

Nachdem ich mich vergewissert hatte, dass die Petentin mit der Nennung ihres Namens gegenüber der Gemeinde einverstanden ist, bat ich diese um Stellungnahme. Die Anhörung der Gemeinde ergab Folgendes:

Der Bürgermeister stellte die Videoüberwachung nicht in Abrede. Vielmehr teilte er uns mit, dass insgesamt zehn Kameras, davon sieben im Innenbereich, in dem Bad im Einsatz seien. Die Kameras seien deutlich sichtbar aufgehängt. Außerdem würden gut erkennbare Schilder auf die Videoüberwachung hinweisen. Die Überwachungsmaßnahmen dienten zum einen der Abschreckung potenzieller Straftäter. Die vorübergehende Speicherung der Bilder solle außerdem dazu beitragen, Straftaten und Unfälle aufzuklären. Überwacht würden u. a. der Eingangs- und Kassenbereich, der Personalparkplatz, aber auch z. B. das Sportbecken (per Unterwasserkamera). In den Umkleidebereichen, in den Duschräumen sowie im gesamten Saunabereich finde keine Videoüberwachung statt. Der Monitor sei im Schwimmmeisterraum aufgestellt, Zutritt habe dort nur das Personal. Die automatisch gespeicherten Videoaufzeichnungen würden nach einer Woche gelöscht; auf die Aufzeichnungen könne nur der Betriebsleiter zugreifen. Dieser gebe die Aufzeichnungen lediglich bei Straftaten auf Anforderung an Polizei, Staatsanwaltschaft oder Gerichte heraus. Der Bürgermeister versicherte, „konkret“ seien

weder die Petentin noch deren Schwimmkurse überwacht worden. Er ließ mich wissen, dass er zwei Kameras, die für die Überwachung von Außenflächen bestimmt waren, abgeschaltet habe. Leider ging er auf den Kern meines Schreibens, nämlich auf die neue Rechtslage infolge der Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2007 nicht weiter ein, offenbar in der Annahme, dass diese Entscheidung für den Innenbereich des Freizeitbads während der Öffnungszeiten nicht einschlägig sei.

Ich ließ den Bürgermeister und die Petentin wissen, dass ich die Videoüberwachungsmaßnahmen für rechtswidrig halte. Den Bürgermeister forderte ich auf, zur Vermeidung einer förmlichen Beanstandung die Überwachung – jedenfalls mit Aufzeichnung des gewonnenen Bildmaterials – unverzüglich zu beenden. Ich stieß aber leider nicht auf offene Ohren. Der Bürgermeister fühlte sich offenbar immer noch im Recht und hielt die Bundesverfassungsgerichtsentscheidung nicht für einschlägig, da das Freizeitbad nicht öffentlich zugänglich sei (wegen des zu entrichtenden Entgelts) und zum anderen die Besucher durch entsprechende Schilder auf die Videoüberwachung hingewiesen würden. Seit Neuestem enthielten diese Schilder zusätzlich noch folgenden Text: „Mit dem Betreten des ... bzw. dem Lösen einer Eintrittskarte stimmt der Besucher der Videoüberwachung zu."

Da ich dem Bürgermeister nicht mangelnden Willen unterstellte, sondern seine Widerspenstigkeit auf die komplizierte Rechtslage zurückführte, habe ich der Gemeinde nochmals eine kurze Frist für das Abschalten der Videokameras bzw. für das Unterlassen von Aufzeichnungen während der Öffnungszeiten eingeräumt, um eine förmliche Beanstandung nach § 30 LDSG samt Unterrichtung der Rechtsaufsichtsbehörde zu vermeiden.

Daraufhin hat mir der Bürgermeister erfreulicherweise zugesagt, dass künftig während der Öffnungszeiten des Freizeitbads keine Bildaufzeichnungen mehr gefertigt werden.

Die Petentin habe ich hiervon unterrichtet.

Der Landesgesetzgeber sollte im Rahmen der Novellierung des Landesdatenschutzgesetzes die Videoüberwachung durch öffentliche Stellen alsbald so regeln, dass sowohl die Belange des Datenschutzes als auch die Sicherheitsinteressen gewahrt werden können.

4.3 Die unzulässige „Privatisierung" der Videoüberwachung auf dem Biberacher Gigelberg

Das Biberacher Schützenfest, ein Brauchtumsfest mit großer Tradition, das mit dem Festplatz auf dem Gigelberg und einer Vielzahl von Veranstaltungen im ganzen Stadtgebiet das örtliche Leben prägt, war auch 2008 und 2009 sicher – ohne Videoüberwachung. Die polizeilich erfassten Ereignisse wie Körperverletzungen, Widerstandshandlungen, Sachbeschädigungen, Diebstähle, Gewahrsamnahmen oder Ruhestörungen ließen nach Presseberichten im Vergleich zu den Vorjahren erkennen, dass die Zahl bestimmter Delikte gesunken, anderer dagegen gestiegen war. Von vergleichbaren anderen Veranstaltungen im Land unterschied sich dieses über eine Woche dauernde Brauchtumsfest damit nicht.

Bereits im 25. Tätigkeitsbericht für das Jahr 2004 (vgl. LT-Drucksache 13/3800) hatte mein Vorgänger darauf hingewiesen, dass auch größere Volksfeste ohne Verlust an Sicherheit auf eine Videoüberwachung verzichten. Schon damals war man in Biberach aber anderer Ansicht. Trotz einer angekündigten förmlichen Beanstandung wurde erst nach einer Entscheidung des Verwaltungsgerichts auf die Videoüberwachung verzichtet. Umso überraschender waren deshalb Presseanfragen im Jahr 2008, wonach ein Brauchtumsverein nunmehr durch eine entsprechende vertragliche Gestaltung die Videoüberwachung auf dem Gigelberg, dem zentralen Festplatz, durchführen solle.

Die Ahnung, dass die „Privatisierung" der Videoüberwachung dazu dienen sollte, eine Kontrolle durch den Landesbeauftragten für den Da-

tenschutz zu vermeiden, bestätigte sich letztendlich, wie die Prüfung der von meinem Vorgänger informierten Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich ergab (vgl. Fünfter Tätigkeitsbericht des Innenministeriums 2009, Kap. B 11.2). Denn der private Brauchtumsverein sollte, wie sich dabei herausstellte, Aufgaben der Ortspolizeibehörde im Bereich der Gefahrenabwehr und zur Sicherung von Strafverfolgungsmaßnahmen umfassend übernehmen. Zu der gesamten Problematik vertrat das Innenministerium nicht zuletzt wegen der eindeutigen Rechtslage im Polizeigesetz die Auffassung, dass eine Übertragung der hoheitlichen Aufgaben nicht zulässig ist, was – nebenbei bemerkt – mein Vorgänger der Stadt zuvor schon „schwarz auf weiß“ mitgeteilt hatte.

So traten die Beteiligten nach dem Verzicht auf Kameras im Jahr 2008 schon rechtzeitig für das Jahr 2009 den geordneten Rückzug an. Nach dem Fest stellten sie die Erfolge ihres Sicherheitskonzeptes für die Veranstaltung heraus. Wie Presseberichten zu entnehmen war, trug dieses Sicherheitskonzept, das mehr Ordnungskräfte auf Seiten des Veranstalters und eine entsprechende Verstärkung der Einsatzkräfte des Polizeivollzugsdienstes vorsah, nicht nur auf dem Festplatz, sondern auch an anderen Stellen in der Stadt zu einem friedlicheren Verlauf der Veranstaltung bei.

Die Vielzahl der Festbesucher konnte sich darüber rundum freuen, nicht zuletzt auch über den damit verbundenen Verzicht auf Eingriffe in ihr informationelles Selbstbestimmungsrecht.

4.4 Mannheim behält den Schutz vor Kriminalität im Fokus

Bereits im 21. Tätigkeitsbericht für das Jahr 2000 (vgl. LT-Drucksache 12/5740) wurde über die damaligen Absichten der Stadt Mannheim berichtet, an bestimmten Orten der Innenstadt eine Videoüberwachung zur Bekämpfung der Straßenkriminalität zu starten, obwohl die entsprechende Änderung des Polizeigesetzes erst noch in den Landtag eingebracht werden musste. Eine dagegen erhobene Klage wurde letztlich vom Verwaltungsgerichtshof Baden-Württemberg mit Urteil vom 21. Juli 2003, 1 S 377/02, abgewiesen, nachdem im Laufe des Verfahrens hinreichende Belege für die überdurchschnittliche Kriminalitätsbelastung der überwachten Bereiche nachgeschoben worden waren. Ende 2007 wurden die Kameras an drei Standorten abgeschaltet, nachdem die Kriminalitätsentwicklung dort deutlich zurückgegangen war. Zuvor kam jedoch ein weiterer – schon in den ursprünglichen Überlegungen enthaltener – Standort hinzu, der Platz vor dem Hauptbahnhof. Schon in der Prognose für die Rechtfertigung der Anordnung waren Aussagen zur Kriminalitätsbelastung dieses Bereichs enthalten. Auf weitere Nachfragen meiner Dienststelle teilte das Polizeipräsidium im Sommer 2009 die für die befristete Fortsetzung der Videoüberwachung erhobenen Erkenntnisse zu der Kriminalitätsbelastung dieses Platzes mit. Das nur etwa 10.000 Quadratmeter große Gebiet umfasste ca. 0,6 % des innerstädtischen Raumes; dafür sei die Kriminalitätsbelastung im Verhältnis zur Innenstadt 13-mal höher und die Innenstadt sei im Vergleich zum übrigen Stadtgebiet schon überproportional belastet.

Ein Vorfall, der auch den Landtag beschäftigte (vgl. LT-Drucksache 14/2398), betraf die zeitweise „Zweckentfremdung“ einer Kamera am Bahnhofsvorplatz, um den Verkehr außerhalb des eigentlichen Einsatzbereichs zu beobachten. Dort hatte es Beschwerden über eine Blockade der Straßen und Lärmbelästigungen aus Anlass von Unabhängigkeitsfeiern von Kosovo-Albanern gegeben. Bei dieser Videobeobachtung, die eigentlich nur für Übersichtsaufnahmen des Verkehrsflusses gedacht war, hätte – wie das Polizeipräsidium im Nachhinein einräumte – die Möglichkeit des Wiedererkennens von bereits bekannten und durch besondere Merkmale leicht zu identifizierender Personen nicht gänzlich ausgeschlossen werden können. Daher prüfe es weitere technische bzw. mechanische Maßnahmen zur ausschließlichen Fokussierung der Kameras auf den bestimmungsgemäßen Überwachungsbereich. Später wurde uns das Ergebnis der Überlegungen mitgeteilt: Zwei der Kame-

ras konnten jetzt nur in einen anderen als den vorgesehenen Bereich geschwenkt werden, wenn der eingesetzte Videobeobachter dieses freigab. Bei Verlassen des vorgegebenen Einsatzbereichs der Kameras werde dieses automatisch protokolliert. Meine Anregung, außerdem in geeigneter Form den Grund, die betroffene Person und das Ergebnis des „Schwenks“ aktenkundig zu machen, traf auf offene Ohren. Denn das Polizeipräsidium hatte bereits selbst erkannt, dass im manuell geführten Videoprotokoll Angaben zum Grund, zur Eingriffsnorm, zum Anordnenden und zur Dauer der Maßnahme erfasst werden sollten. Nach dem Kameraschwenk, der den Landtag beschäftigt hatte, seien im Einsatztagebuch zwei weitere Fälle erfasst worden. In einem Fall sei ein Raubüberfall und im anderen ein Wohnungsbrand der Anlass gewesen. Auch diese Videoüberwachung war inzwischen Gegenstand eines verwaltungsgerichtlichen Verfahrens, das allerdings durch die Erklärung der Erledigung des Rechtsstreits beendet wurde. Ich werde den Einsatz der Mannheimer Kameras jedenfalls im Auge behalten und zu gegebener Zeit erneut kontrollieren.

Der gesamte Vorgang zeigt, dass es trotz der Änderung des Polizeigesetzes nicht einfach ist, rechtssicher eine Videoüberwachung anzuordnen und durchzuführen. Ohne eine laufende Beobachtung des Geschehens ist sie in ihrer Wirkung zweifelhaft. Videoaufzeichnungen, die lediglich der späteren Auswertung dienen, wenn „das Kind schon in den Brunnen gefallen“ ist, widersprechen dem grundsätzlichen Auftrag der Polizei zur Gefahrenabwehr, also dem Präventionsgedanken.

5. Die Dienststelle in Zahlen

Die Ausstattung meiner Dienststelle blieb im Berichtszeitraum nahezu unverändert, wie man auch den jeweiligen Staatshaushaltsplänen (dort Einzelplan 03, Kap. 0303) entnehmen kann (vgl. im Internet *www.statistik-bw.de/shp/*):

– Die Dienststelle verfügt derzeit – einschließlich meiner Stelle – über elf Beamtenstellen (davon eine des gehobenen Dienstes) und fünf Angestelltenstellen. Dem entsprechen Personalausgaben von knapp 750 T€ (Soll 2009). In Bezug auf das „Betreuungsverhältnis“ (Tausend Einwohner pro Mitarbeiter) liegt meine Dienststelle damit im Ländervergleich auf dem 16. und letzten Platz (Stand: 2008). Erfreulicherweise ist die Personalsituation meiner Dienststelle seit dem 1. Oktober 2009 durch die Abordnung eines Beamten des höheren Polizeivollzugsdienstes verbessert worden.

– Für sächliche Verwaltungsausgaben stehen meiner Dienststelle rund 65 T€ zur Verfügung (Soll 2009). Im Jahr 2010 ist u. a. im Hinblick auf meinen Vorsitz in der Konferenz der Datenschutzbeauftragten von Bund und Ländern eine vorübergehende Erhöhung vorgesehen. Im Jahr 2011 ist ein erhöhter Haushaltsansatz für die Ersatzbeschaffung der Telefonanlage eingeplant. In Bezug auf die Sachmittel in absoluten Zahlen liegt meine Dienststelle im Ländervergleich auf dem 15. und vorletzten Platz (vor dem Saarland). Andere Datenschutzbeauftragte mit vergleichbarem Aufgabenzuschnitt verfügen über die doppelte (Thüringen), vierfache (Bayern) oder gar siebenfache (Hessen) Sachmittelausstattung. Soweit meine Kollegen auch für den nichtöffentlichen Bereich und/oder das Thema Informationsfreiheit zuständig sind, liegen die absoluten Beträge noch erheblich höher.

Das landesweite Projekt der Einführung Neuer Steuerungsinstrumente (NSI), zu dem sich meine Dienststelle unter dem Aspekt des Personaldatenschutzes in früheren Jahren geäußert hatte (vgl. 23. Tätigkeitsbericht für das Jahr 2002, LT-Drucksache 13/1500; 24. Tätigkeitsbericht für das Jahr 2003, LT-Drucksache 13/2650), hat auch vor meiner Dienststelle nicht Halt gemacht. Im Hinblick auf meine Unabhängigkeit und die geringe Größe des Amtes sowie aufgrund der weitgehend durch Eingaben und Beschwerden der Bürger, also ohne meinen Einfluss, vorgegebenen Arbeitsbelastung wurde die Kosten-Leistungsrechnung in Absprache mit dem Innenministerium allerdings nur in vereinfachter Form eingeführt; zum Beispiel findet

keine kostenträgerbezogene Zeit- und Mengenerfassung statt, sondern es werden – insbesondere für die „produktorientierten Informationen“ im Staatshaushaltsplan – gewisse Kennzahlen statistisch erhoben und im Haushalt abgebildet. Dort sind auch folgende Ziele der Dienststelle genannt:

– Unterstützung des Bürgers bei der Wahrnehmung seines Datenschutzrechts,

– Verbesserung des Datenschutzniveaus,

– Förderung des Datenschutzbewusstseins.

Als Messgrößen zur Zielerreichung werden dort die jeweilige Anzahl der Eingaben, Kontrollen und Beratungen aufgeführt. Die entsprechenden Zahlenwerte stellen sich in Ist und Soll wie folgt dar:

		2007	2008	2009	2010	2011
Anzahl der Eingaben	Soll	2000	2000	2000	2000	2000
	Ist	1818	2246	2400*		
Anzahl der Kontrollen	Soll	25	25	20	20	20
	Ist	10	22	19*		
Anzahl der Beratungen	Soll	1500	1500	1000	1000	1000
	Ist	804	953	820*		

Hinsichtlich der Anzahl der Eingaben ist darauf hinzuweisen, dass aufgrund der schwierigen Zuständigkeitsabgrenzung ein Teil an die Aufsichtsbehörde für den nichtöffentlichen Bereich abzugeben ist; umgekehrt gehen uns auch von dort weitergeleitete Eingaben zu.

In der Sitzung der Arbeitsgruppe „Produktinformationen“ des Finanzausschusses vom 30. April 2009 hat eine Abgeordnete angeregt, für meine Arbeit möge eine Kennzahl ausgewiesen werden, wie viele meiner Initiativen „letztlich erfolgreich“ gewesen seien. So gern ich meine Arbeit mit einer entsprechenden Kennzahl „schmücken“ würde: Bisher habe ich noch kein taugliches Abgrenzungskriterium gefunden, was den „Erfolg“ meines Handelns ausmacht. Auf manche Datenschutzprobleme werde ich zum Beispiel von Bürgern zum gleichen Zeitpunkt wie die Presse hingewiesen. Wenn die betroffene Behörde nun aufgrund von Presseanfragen und wegen meiner Recherchen reagiert, kann man darüber streiten, ob dies eher aus Sorge vor kritischen Presseartikeln oder vor einer förmlichen Beanstandung meinerseits erfolgte (oder aus beiden Gründen). Viel Aufwand bedeuten auch die Stellungnahmen zu Gesetzgebungsvorhaben und Projekten, die aber in der Regel schon von den jeweiligen Ministerien sorgfältig geprüft wurden; dass der Datenschutz hier noch „ein Haar in der Suppe“ findet, ist eher die Ausnahme. Und wenn politische Vorfestlegungen – wie etwa beim Entwurf des Polizeigesetzes – zu einer kritischen Reaktion aus datenschutzrechtlicher Sicht führen, dann ist die Frage, welchen „Erfolg“ mein Widerstand hatte, im Grunde überflüssig. Zahlreiche Eingaben führen aufgrund meiner Intervention allerdings zum gewünschten „Erfolg“, etwa in der Weise, dass eine Behörde ihre bisherige Praxis ändert, Formulare anpasst oder Auskunft erteilt. Eine Statistik hierüber führe ich nicht. Vielfach muss ich empörten Bürgern auch mitteilen, dass eine öffentliche Stelle rechtmäßig handelte und warum kein datenschutzrechtlicher Verstoß festgestellt werden konnte. Wenn diese danach die Rechtslage besser verstehen, dann ist das in gewisser Weise auch ein „Erfolg“.

* Hochrechnung aufgrund der Zahlen des 1. bis 3. Quartals 2009.

2. Teil: Öffentliche Sicherheit und Justiz

1. Abschnitt: Öffentliche Sicherheit

1. Gesetzgebung

1.1 Polizeigesetz

Im November 2008 verabschiedete der Landtag eine Änderung des Polizeigesetzes, die unter anderem die Ausweitung der Videoüberwachung, den Einsatz automatischer Kennzeichenlesesysteme, die Verkehrsdatenerhebung in der Telekommunikation, die Ausschreibung zur gezielten Kontrolle und die Speicherung von tatverdächtigen Personen ohne Prognose der Wiederholungsgefahr für zwei Jahre umfasste. Gegen die vorgesehenen Änderungen wurden aus datenschutzrechtlicher Sicht im Gesetzgebungsverfahren erhebliche Bedenken geltend gemacht.

Anders als der Bund bei der Änderung des Bundeskriminalamtsgesetzes hatte die Landesregierung von Anfang an keine Regelung zur Online-Durchsuchung von Datenverarbeitungsanlagen im Gesetzentwurf vorgesehen. Der Verzicht auf diesen erheblichen Eingriff in den grundrechtlich geschützten Bereich, zu dem das Bundesverfassungsgericht aufgrund der Klagen gegen das Bundesgesetz ohnehin noch ausführlich Stellung nehmen dürfte, ist aus meiner Sicht zu begrüßen.

Nachdem ein erster Gesetzentwurf zur Änderung des Polizeigesetzes (PolG) meine Dienststelle Ende des Jahres 2007 erreichte, führte das Urteil des Bundesverfassungsgerichts zum Einsatz von automatischen Kennzeichenlesesystemen in den Polizeigesetzen der Länder Hessen und Schleswig-Holstein (Urteil vom 11. März 2008, 1 BvR 2074/05 und 1 BvR 1254/07) zu einer grundlegenden Überarbeitung der beabsichtigten baden-württembergischen Regelung, die sich dadurch allein schon im Umfang vervielfachte, um alle denkbaren Konstellationen für einen solchen Eingriff zu erfassen. Die erste Entwurfsfassung hatte aus datenschutzrechtlicher Sicht erhebliche Bedenken wegen der Eingriffsintensität und mangelnden Bestimmtheit des Regelungsvorschlags ausgelöst. Von verschiedener Seite wird gleichwohl weiterhin bezweifelt, dass die Gesetzgebungskompetenz für derartige Regelungen überhaupt bei einem Landesgesetzgeber liege, da der Zweck eher dem Bereich der Strafverfolgung zugerechnet werden müsse.

Bedenken bestanden bzw. bestehen neben der vorgenannten Regelung in § 22 a des Polizeigesetzes (PolG) insbesondere gegen die Erweiterung der Möglichkeiten zur Videoüberwachung (§ 21 PolG), zur Erhebung von Telekommunikationsdaten (§ 23 a PolG), zur Ausschreibung von Personen zur gezielten Kontrolle (§ 25 PolG) und gegen die Speicherung personenbezogener Daten für die Dauer von zwei Jahren zur vorbeugenden Bekämpfung von Straftaten, ohne dass eine Prognose zur Wiederholungsgefahr dafür erforderlich ist (§ 38 Abs. 2 PolG).

Die von meinem Vorgänger mehrfach vorgetragenen Bedenken sind teilweise in der LT-Drucksache 14/3165, S. 89, 94, 98, 100, 107 abgedruckt; hiervon wurden aber nur einige berücksichtigt. Grundsätzlich habe ich auch weiterhin Bedenken, dass sich insbesondere die Videoüberwachung peu à peu zu einer Standardmaßnahme entwickelt. Die Entscheidung über die Erforderlichkeit stützt sich nach dem Gesetz nämlich eher auf abstrakte Erwägungen zur polizeilichen Einsatztaktik als auf konkrete tatsächliche Erkenntnisse; auf diese Weise besteht die Gefahr, dass die betroffenen Individualinteressen der Bürger zu weit zurückstehen. Auch die Veränderung der Voraussetzungen für Videoüberwachungen durch den Polizeivollzugsdienst oder die Ortspolizeibehörde kann bezogen auf die Kriminalitätsbelastung des Gemeindegebiets zweifelhaft sein. Auch wenn das in dem in diesem Tätigkeitsbericht (1. Teil, Nr. 4.4) geschilderten Fall zutreffen mag, wäre diese Bezugsgröße in einer Gemeinde ohne bisher einschlägige Belastung bei nur wenigen Fällen schnell gegeben. Das entspräche aber nicht den verfassungsrechtlichen Voraussetzungen für eine Videoüberwachung.

Zu der Erhebung der Telekommunikationsdaten bin ich wie mein Vorgänger der Auffassung, dass dies der bundesrechtlichen Kompetenz zur Strafverfolgung unterliegt und nicht vom Landesgesetzgeber geregelt werden kann.

Ebenso wenig kann ich der Einschätzung des Innenministeriums folgen, welches den Grundrechtseingriff durch eine Ausschreibung zur gezielten Kontrolle für weniger intensiv als den Eingriff durch eine (verdeckte) polizeiliche Beobachtung hielt. Gerade die bei einer gezielten Kontrolle möglichen weiteren Eingriffe wie Identitätsfeststellung, Durchsuchung von Personen und Sachen machen deutlich, wie hier allmählich die Gewichte hin zu immer mehr polizeirechtlichen Befugnissen verschoben werden sollen.

Grundsätzliche Bedenken habe ich weiterhin auch gegen die Einführung der Verdachtsspeicherung ohne Prognose zur Wiederholungsgefahr für bis zu zwei Jahre, die das Prinzip der in § 38 Abs. 1 PolG betonten und datenschutzrechtlich bisher maßgeblichen Erforderlichkeit einer Datenspeicherung durch die Einführung einer Fiktion ersetzt. Diese Gesetzesänderung ist aus Sicht meiner Beratungs- und Kontrollpraxis besonders bitter, betrifft doch ein Großteil der mich tagtäglich erreichenden Briefe und Anrufe betroffener Bürgerinnen und Bürger gerade die Speicherung in den polizeilichen Datenbanken. Wenn man sich vor Augen hält, dass dort selbst Bagatelldelikte eingespeichert werden, bei denen die Staatsanwaltschaft das Verfahren umgehend wegen Geringfügigkeit eingestellt oder die Beteiligten auf den Privatklageweg verwiesen hatte, dann wird vielleicht verständlich, dass ich über den Wegfall des bisher noch verbliebenen Korrektivs, nämlich der Prognose einer Wiederholungsgefahr, besonders verärgert bin. Das aus Polizeikreisen häufig gehörte Argument, man wolle „kriminelle Karrieren“ von Beginn an verfolgen können, wird auf diese Weise ad absurdum geführt. Falls die Einspeicherung aber nur als „Tätigkeitsnachweis“ für die Polizei dienen sollte, dann würde eine statistische Erfassung vollauf ausreichen.

Dass in der Erörterung des Entwurfs im Innenausschuss ein Vertreter des Innenministeriums ohne nähere Begründung ausführen konnte (vgl. Protokoll, LT-Drucksache 14/3373, S. 8),

> *„Die vorgesehene Regelung sei unter dem Aspekt der Verhältnismäßigkeit als sachgerecht zu bewerten. Auch unter dem Gesichtspunkt des Datenschutzes werde diese Regelung in der Praxis zu einem Fortschritt führen. Zwar würden die Daten von Personen, bei denen der Verdacht bestehe, eine Straftat begangen zu haben, grundsätzlich bis zu zwei Jahre gespeichert, jedoch werde sich die Zahl derjenigen, deren Daten auf fünf bis zehn Jahre gespeichert würden, reduzieren. Darüber hinaus werde mit dieser Regelung den Sachbearbeitern vor Ort eine Hilfestellung für die Handhabung derartiger Fälle gegeben.“*

lässt vermuten, dass es sich bei dem erwähnten „Fortschritt“ nicht um die Verbesserung des Datenschutzes handelt, sondern um ein Anzeichen von – vereinfacht gesagt – „Datensammelwut“. Bei näherer Betrachtung könnte man die Aussage – nicht minder fatal – aber auch als verklausulierten Offenbarungseid auffassen, dass nämlich die polizeilichen Informationssysteme nicht mehr nach den europaweit vorgegebenen Prinzipien des Datenschutzes rechtlich zulässig, inhaltlich richtig und technisch sicher geführt werden. Bemerkenswert ist in diesem Zusammenhang, dass ein auch in der Polizei weit verbreiteter Kommentar zum Polizeigesetz in seiner jüngsten Auflage die Meinung vertritt, dass diese Datenspeicherungen mangels Verhältnismäßigkeit verfassungswidrig sein dürften. Hier ist eine Kurskorrektur weiterhin dringend erforderlich.

Welche Datenqualität schon derzeit im landesweiten polizeilichen Auskunftssystem POLAS-BW geboten wird, kann man nicht nur in den

Tätigkeitsberichten der Vergangenheit nachlesen, sondern auch nachfolgend unter Nr. 2.2.

Zusammengefasst kann ich mit der Änderung des Polizeigesetzes unter datenschutzrechtlichen Aspekten nicht zufrieden sein. Die Prinzipien des Grundrechtsschutzes der Bürgerinnen und Bürger sind hier zum Teil ohne erkennbare Notwendigkeit den polizeilichen Interessen untergeordnet worden. Sicherheit zu gewähren, ist die vornehmste Aufgabe der Polizei. Durch zu großzügige Regeln zur Speicherung verdächtiger Bürgerinnen und Bürger wird das grundsätzlich vorhandene Vertrauen in die Objektivität bei der polizeilichen Aufgabenwahrnehmung aber eher in Zweifel gezogen.

1.2 Landesversammlungsgesetz

„Ziel des Gesetzes ist es, das Versammlungsrecht in Baden-Württemberg zu modernisieren und den seit Inkrafttreten des Gesetzes über Versammlungen und Aufzüge (Versammlungsgesetz – VersG) im Jahre 1953 eingetretenen tatsächlichen und rechtlichen Entwicklungen Rechnung zu tragen. Das Landesversammlungsgesetz wird die Rechtsanwendung vereinfachen und das Zusammenwirken von Versammlungsbeteiligten und Behörden erleichtern.“

So lautete die Zielsetzung eines Gesetzentwurfs aus dem Jahr 2007, den das Innenministerium meiner Dienststelle übersandte. Damit war Baden-Württemberg nach Bayern das zweite Land, welches die durch die Föderalismusreform übertragene Gesetzgebungskompetenz rasch ausfüllen wollte.

In dem Bericht über eine Sitzung des Innenausschusses des Landtages am 24. Juni 2009, LT-Drucksache 14/5045, hieß es dann:

> *„Baden-Württemberg strebe jedoch ein Versammlungsgesetz an, das mit verfassungskonformen Regelungen einerseits die Versammlungsfreiheit respektiere und schütze und andererseits natürlich den Sicherheitsbelangen der Bevölkerung Rechnung trage.“*

Dass bis zum heutigen Tage kein Gesetzentwurf in den Landtag eingebracht wurde, hat mehrere gute Gründe, die auch aus datenschutzrechtlicher Sicht gewichtig sind:

Einer der schwerwiegenden Gründe ist die vom Bundesverfassungsgericht in Bezug auf das Bayerische Versammlungsgesetz erlassene einstweilige Anordnung, mit der sowohl bestimmte Bußgeldbestimmungen außer Kraft gesetzt als auch für die Datenerhebung, Bild- und Tonaufzeichnungen, Übersichtsaufnahmen und -aufzeichnungen Einschränkungen gegenüber der gesetzlichen Regelung verfügt wurden (Beschluss vom 17. Februar 2009, 1 BvR 2492/08). Auch wenn hierzulande betont wurde, dass der baden-württembergische Entwurf in vielen Punkten versammlungsfreundlicher als das bayerische Gesetz sei, gibt gerade der zweite Teil der einstweiligen Anordnung zu denken.

Zum anderen wurde der Gesetzentwurf nicht nur in der Anhörung von vielen betroffenen Gewerkschaften, Verbänden und Vereinigungen, sondern auch in den Medien deutlich kritisiert, weil darin zu stark auf die staatlichen Interessen im Verhältnis zur grundrechtlich verbürgten Versammlungsfreiheit nach Artikel 8 des Grundgesetzes abgestellt worden sei. Auch mein Vorgänger und ich haben auf ganz erhebliche Defizite in Hinblick auf das informationelle Selbstbestimmungsrecht von Versammlungsteilnehmern hingewiesen; dies betraf unter anderem Regelungen des Gesetzentwurfs über die Datenerhebung und -verarbeitung sowie zu den Bild- und Tonaufzeichnungen. So enthielt der Entwurf keine Ermächtigungsgrundlage für die eigentliche Datenerhebung, sondern nur allgemeine Grundsätze hierfür. Eine andere Vorschrift sollte erstmals eine bereichsspezifische Rechtsgrundlage für die Datenerhebung schaffen; die als Generalklausel ausgestaltete Ermächtigung, die sogar die verdeckte Datenerhebung umfassen sollte, konnte dem nicht

genügen. Auch die Pflicht zur Unterrichtung einer betroffenen Person im Fall einer verdeckten Datenerhebung, soweit der Verwendungszweck nicht gefährdet ist, erschien in Anbetracht des hohen demokratischen Stellenwerts der Versammlungsfreiheit als zu weitgehend und zu unbestimmt; in der Praxis wäre es unter Berufung auf diese unklare Bestimmung leicht möglich, auf die Unterrichtung zu verzichten.

Die Voraussetzungen für einzelne Datenerhebungen waren im Übrigen unklar: So sollten die Versammlungsbehörde und der Polizeivollzugsdienst Daten einer teilnehmenden Person dann erheben dürfen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigten, dass die Person einen Grund zur Auflösung der Versammlung geben könnte, und die Datenerhebung erforderlich ist, um das Eintreten eines solchen Auflösungsgrundes zu verhindern. Offenbar sollte die Datenerhebung stattfinden, bevor der Grund zur Auflösung eingetreten wäre. Dementsprechend war in der Begründung auch mehrfach von Prognosen die Rede. Für die Prognose, dass ein Teilnehmer einen Auflösungsgrund verursachen wird, wäre es nach meiner Ansicht erforderlich, ihn und sein früheres Verhalten zu kennen, so z. B. bei einem bekannten Hetzredner; dann bedürfte es aber keiner Datenerhebung, weil die Person bereits bekannt ist. Wenn dieses nicht zuträfe, sich aber aufgrund äußerer Umstände ein Auflösungsgrund erkennen ließe, wie z. B. Ankündigungen von Gewalttaten gegenüber anderen Teilnehmern oder von Aufrufen zu Straftaten, würde ein Hinweis an den Veranstalter zwecks Ausschlusses einer solchen Person und das Androhen eines Verbots bzw. einer Auflösung der Versammlung ausreichen. Ganz abgesehen davon sollte das Androhen von Gewalttaten in einer Versammlung nach dem Entwurf ein Straftatbestand sein; für eine Identitätsfeststellung der betreffenden Person würde daher das Strafprozessrecht völlig genügen.

Die ebenfalls vorgesehene Befragung von Versammlungsteilnehmern durch den Polizeivollzugsdienst könnte ohne Weiteres zur Einschüchterung missbraucht werden. Denn wenn Versammlungsteilnehmer angehalten und zur Angabe der Personalien mit der Frage veranlasst werden sollen, ob sie etwas von drohenden Gewalttaten durch andere Teilnehmer wüssten, birgt das vor allem die Gefahr, potenzielle Versammlungsteilnehmer von einer Teilnahme abzuhalten, um nicht von der Polizei registriert zu werden. Die Möglichkeit einer anonymen Teilnahme an Versammlungen entspricht aber dem hohen Stellenwert von Artikel 8 des Grundgesetzes; dies gilt insbesondere für Versammlungen in geschlossenen Räumen.

Von ebenfalls zweifelhafter Güte war die im Entwurf vorgesehene Möglichkeit, dass die Versammlungsbehörde die personenbezogenen Daten der Ordner verlangt. Völlig unklar blieb, warum dieses erforderlich sein sollte, und vor allem, welche Maßstäbe für die Eignung oder Nichteignung dieser Ordner gelten sollten. Erst im Rahmen einer späteren Überarbeitung des Entwurfs wurde die Erhebung der personenbezogenen Daten einer die Versammlung leitenden Person neben den Daten des Veranstalters vorgesehen. Diese Datenerhebung ist wegen der Verantwortlichkeiten auch aus meiner Sicht unzweifelhaft erforderlich. Umso erstaunlicher, dass nach dem Entwurf weiterhin die Anforderung von Daten der Ordner möglich sein soll.

In dem Entwurf war ferner eine neue Bestimmung für verdeckte Bild- und Tonaufzeichnungen von Versammlungsteilnehmern vorgesehen. Aus meiner Sicht fehlten für Geräte zur selbsttätigen Bildaufzeichnung, wenn diese eingesetzt werden sollten, strengere Anforderungen, wie sie bereits im Polizeigesetz enthalten sind. Ebenso bedenklich war die Möglichkeit zur Auswertung der Übersichtsaufnahmen mit dem Ziel der Identifizierung von Einzelpersonen geregelt. Für eine zulässige Bildaufzeichnung wäre zunächst Voraussetzung, dass die Bild- oder Tonaufzeichnung zur Verhinderung des Eintritts der erheblichen Gefahr bei oder im Zusammenhang mit der öffentlichen Versammlung erforderlich ist. Eine Auswertung der Übersichtsaufnahmen nach Ende der Versammlung kann diese Voraussetzung einfach nicht mehr erfüllen. Für die Abwehr einer künftigen erheblichen Gefahr außerhalb der kon-

kreten Versammlung hätte dagegen eine hinreichende Rechtsgrundlage gefehlt. Eine am 21. August 2009 ergangene Entscheidung des Verwaltungsgerichts Münster, 1 K 1403/08, zur Rechtswidrigkeit der Videobeobachtung einer – im Übrigen völlig friedlich verlaufenen – Versammlung gegen Urantransporte macht dies in allen Einzelheiten deutlich. Die Bedenken gegen den Gesetzentwurf waren berechtigt, da bei einer Abwägung von Interessen zur Gewährleistung von Sicherheit und Ordnung gegenüber der Versammlungsfreiheit und auch des informationellen Selbstbestimmungsrechts eine verfassungsrechtlich nicht hinzunehmende Regelung entstanden wäre.

Es bleibt zu hoffen, dass die durch das Bundesverfassungsgericht ausgelöste Denkpause und vor allem dessen Entscheidung in der Hauptsache dazu beitragen wird, verfassungskonforme Regelungen in einem künftigen Landesversammlungsgesetz zu schaffen und damit neben der Versammlungsfreiheit auch dem informationellen Selbstbestimmungsrecht von Versammlungsteilnehmern gerecht zu werden.

2. Polizeiliche Datenverarbeitung

2.1 Szenekundige Beamte und ihre Datenbank

Sehr geehrter Herr,

vom 7. bis 20. Juni 2008 findet in Österreich und der Schweiz die Fußball-Europameisterschaft statt.

Sollten Sie die Absicht haben, zur Europameisterschaft nach Österreich bzw. in die Schweiz zu reisen, wollen wir Sie ausdrücklich um ein gesetzeskonformes Verhalten bitten. Das heißt, Sie sollten

- *sich nicht an Provokationen jeglicher Art beteiligen bzw. nicht auf diese reagieren,*
- *sich nicht an Gewalttätigkeiten jeglicher Art beteiligen,*
- *sich nach Möglichkeit nicht an Örtlichkeiten, an welchen solche Provokationen und Gewalttätigkeiten zu erwarten sind, aufhalten,*
- *Zusammenrottungen von Problemfans meiden,*
- *den Anweisungen der Polizeikräfte vor Ort und dem dortigen Ordnungspersonal an den Spielorten Folge leisten!*

Sie sind Adressat dieses Schreibens, weil Sie in der Vergangenheit im Zusammenhang mit Fußballveranstaltungen polizeilich in Erscheinung getreten sind!

Wir bitten Sie deshalb, sollten Sie die Absicht haben, zur Europameisterschaft zu fahren, sich an Recht und Ordnung zu halten! Das Gleiche gilt auch für die „Public-Viewing“ Veranstaltungen, welche in Deutschland stattfinden werden!

Wir setzen auf Ihre Einsicht, sodass auch Sie dazu beitragen, dass die (Groß-)Veranstaltungen bei der und um die Europameisterschaft 2008 friedliche und tolle Events werden!

Mit freundlichen Grüßen

Ihre Polizei

Dieses oder ähnliche Schreiben gingen im Monat vor der Europameisterschaft einigen Mitbürgern und Mitbürgerinnen in Baden-Württemberg wie auch in anderen Bundesländern zu. Absender war die für sie jeweils zuständige Polizeidienststelle. „Gefährderansprache“ nennen sich diese Schreiben im polizeilichen Sprachgebrauch. Seit Jahren und nach den immer häufigeren Nachrichten über Gewalt als Begleiterscheinung von Sportveranstaltungen, insbesondere bei Fußballspielen hinunter bis zur fünften Liga, scheint es aus polizeilicher Sicht notwendig zu sein, Angehörige von Fangruppen näher zu beobachten und die-

ses die Betroffenen auch wissen zu lassen. Um Maßnahmen zur Vermeidung von gewalttätigen Auseinandersetzungen im Vorfeld besser vorbereiten zu können, festgestellte Störer oder Straftäter leichter zu identifizieren und ordnungsrechtliche Maßnahmen gegen diese Personen besser begründen zu können, gibt es nicht nur eine vom Bundeskriminalamt und den Landeskriminalämtern gemeinsam betriebene Verbunddatei „Gewalttäter Sport“ (zur Rechtsgrundlage s. o. 1. Teil, Nr. 3.2), sondern im Land seit dem Jahr 2005 auch eine Arbeitsdatei für „Szenekundige Beamte (SKB)“, kurz die „SKB-Datenbank“.

Nachdem einem Bürger bereits im Jahr 2007 vom Landeskriminalamt mitgeteilt worden war, dass in den polizeilichen Informationssystemen nichts über ihn gespeichert sei, veranlasste ihn das oben zitierte Schreiben zu einer erneuten Anfrage. Diese wurde an die zuständige Polizeidienststelle weitergeleitet, die ihm dasselbe Ergebnis mitteilte. Ergänzend wurde ihm auch mitgeteilt, dass er von der für gewalttätige Auseinandersetzungen im Zusammenhang mit Fußballspielen zuständigen Organisationseinheit wiederholt in vorderster Reihe mit anderen, zum Teil gewaltbereiten Fans gesehen worden und persönlich bekannt sei. Der Bürger schaltete daraufhin einen Anwalt ein, der sich an meine Dienststelle wandte. Die Antwort der zuständigen Polizeidienststelle half den widersprüchlichen Eindruck zu klären, den der Adressat in der polizeilichen Praxis vermutete. Die Auskunft des Landeskriminalamts war vor dem Hintergrund seiner Zuständigkeit für die zentralen Informationssysteme der Polizei, also das im nachfolgenden Abschnitt näher beschriebene polizeiliche Auskunftssystem des Landes POLAS-BW sowie die von baden-württembergischen Polizeidienststellen veranlassten Speicherungen in den Verbunddateien nach dem Bundeskriminalamtsgesetz, zwar nicht falsch. Vollständig war die Auskunft nach § 45 des Polizeigesetzes (PolG) aber auch nicht. Dort heißt es:

> *Der Polizeivollzugsdienst erteilt nach § 21 des Landesdatenschutzgesetzes Auskunft über die von ihm gespeicherten personenbezogenen Daten; er ist jedoch nicht verpflichtet, über die Herkunft der Daten Auskunft zu erteilen.*

Die zuständige Polizeidienststelle hatte also in ihrem Schreiben ihr Wissen über die Zugehörigkeit des Betroffenen zu einer Fangruppe, die sie als gewaltbereit einstufte, mitgeteilt, nicht aber die Speicherung bestimmter personenbezogener Daten zu dem Adressaten ihres Schreibens in der örtlich vorhandenen SKB-Datenbank erwähnt. Dieser Umstand veranlasste meine Dienststelle, das Innenministerium um eine Klarstellung zu der Auskunftspflicht nach § 45 PolG zu bitten, da eine Auskunftsverweigerung wohl kaum Sinn macht, wenn die Datenbank die Grundlage für Gefährderansprachen ist. Das Innenministerium teilte diese Auffassung, schlug aber wegen der gespaltenen Zuständigkeit für die Auskünfte beim Landeskriminalamt einerseits und bei den immerhin elf Polizeidienststellen, die eine SKB-Datenbank besitzen, andererseits nur eine kurzfristige Zwischenlösung vor, die zwar grob Lücken schließen, aber den Anspruch auf vollständige Auskunft nicht wirklich erfüllen kann. Dies war aus meiner Sicht unbefriedigend.

Um über die tatsächliche Nutzung der Datenbank Klarheit zu gewinnen, kontrollierten meine Mitarbeiter bei der Polizeidienststelle, die den Anlass für den Schriftwechsel gegeben hatte, diese Datenbank. Sie fanden – vereinfacht gesagt – einen elektronischen Karteikasten vor. In dem zu den Einzelpersonen geführten Teil der Datenbank waren neben den üblichen Angaben zur Person und evtl. einem Lichtbild auch Daten zum Arbeitgeber, zu genutzten Fahrzeugen, zu Stadionverboten, zur Zugehörigkeit zu einer Fangruppe einschließlich der Kategorisierung in Hinblick auf die Gewalttätigkeit bei Veranstaltungen, ein Löschdatum, aber auch Freitexteinträge vorgesehen. In dem Teil „Spielteilnahmen“ der Datenbank waren rudimentär Eintragungen enthalten, die auch eine Verknüpfung mit den Daten der seinerzeit gespeicherten Personen ermöglichten, aber nur in diesem Teil der Datenbank; bei den Personen-

daten waren diese Spielteilnahmen nicht erkennbar. Eine systematische Speicherung war bei den Spielteilnahmen nicht möglich, da dies von der Teilnahme der zuständigen Organisationseinheit an den Auswärtsspielen abhing. Es wurde aber zugesichert, dass mit der Löschung eines Personendatensatzes auch die Verknüpfung bei den Spielteilnahmen gelöscht werde. Zweifelhaft waren für mich verschiedene Daten: Warum wurden Angaben zum Arbeitgeber vorgesehen, woher stammten die teilweise vorhandenen Lichtbilder und welchen Hintergrund hatten Angaben in den Freitextfeldern? Wie die Löschung der Daten aufgrund des jeweiligen Löschdatums organisiert war, war aus der Dienstanweisung ebenfalls nicht erkennbar. Nach der Dienstanweisung sollte die Datenbank eine Vielzahl von Vorgängen erschließen, um damit die Grundlage für präventivpolizeiliche Maßnahmen zur Verhinderung von gewalttätigen Auseinandersetzungen bei oder im Zusammenhang mit Sportveranstaltungen zu schaffen. Diesen Zweck kann die Datenbank allenfalls nur teilweise erfüllen, da für Maßnahmen wie beispielsweise ein Ausreiseverbot nach dem Passgesetz vielfältige Akten auf anderen Wegen erschlossen werden müssen, die Datenbank also keine umfassende Erschließung ermöglicht.

Erfreulicherweise wurde ich bereits während der Befassung mit der Datenbank vom Landeskriminalamt darauf hingewiesen, dass man sich dort überlege, wie man nicht nur den Auskunftsanspruch besser sicherstellen, sondern die Datenbank von Grund auf den inzwischen gegebenen Möglichkeiten anpassen könne.

Das Innenministerium hat sich nunmehr deutlich zu meinen Feststellungen geäußert: Zunächst solle die Anwendung durch ein Web-gestütztes Analyse-Werkzeug abgelöst werden; die Prüfung laufe derzeit. Eine solche Anwendung könne ab der Spielsaison 2010/2011 mit einem zentral geführten Datenbestand dazu beitragen, das Risiko unvollständiger Auskünfte zu minimieren. Zu den einzelnen Datenfeldern kündigte das Innenministerium weiter an, dass die Erforderlichkeit der Daten zum Arbeitgeber demnächst geklärt werde. Für die Freitextfelder werde zukünftig eine Regelung zur Nutzung vorgesehen. Für die Lichtbilder solle zukünftig nachvollziehbar hinterlegt werden, auf welcher rechtlichen Grundlage sie erhoben wurden. Nicht zuletzt erwarte es auch die Realisierung von Löschwarnläufen, die in anderen Anwendungen schon seit Jahren Standard sind.

Dieses Beispiel zeigt, dass die Vielfalt der polizeilichen Datenverarbeitungsanwendungen Probleme selbst für den Polizeivollzugsdienst schafft, die nur mit großem Aufwand beseitigt werden können. Lösungen aufgrund einer einheitlichen Software, die wie ein Baukasten für viele Problemstellungen genutzt werden kann, dürften dazu beitragen, dass die Interessen Betroffener besser und vollständiger berücksichtigt werden können. Dass ein „Baukastensystem“ im Hinblick auf die vielseitige Verwendbarkeit und den großen Nutzerkreis besonderer datenschutzrechtlicher und technischer Absicherungen bedarf, steht auf einem anderen Blatt.

2.2 Polizeiliche Informationssysteme – Anspruch und Wirklichkeit

2.2.1 Datenbanken und ihr Zweck

Automatisierte Datenverarbeitung ist in unserer Gesellschaft selbstverständlich geworden. Öffentliche Stellen können ihre Aufgaben ohne diese kaum noch wirkungsvoll wahrnehmen. Deshalb ist es entscheidend, welche Daten gespeichert werden und wie dies geschieht. Dafür gibt es in den unterschiedlichen Bereichen gesetzliche Regeln, die bestimmen, wer was wann zu welchen Zwecken speichern darf. Von besonderer Bedeutung sind für viele Menschen die Datenbanken, in denen die Vorgänge gespeichert werden, die Auskunft über ihre Konflikte mit dem Gesetz geben: Das Verkehrszentralregister für die Verkehrsdelikte, das Bundeszentralregister für die Vorstrafen und das zentrale staatsanwaltschaftliche Verfahrensregister für alle in Deutschland

geführten Ermittlungsverfahren gegen Personen sind mehr oder weniger bekannt. Häufig wird Betroffenen aber erst bei einer Verkehrskontrolle klar, dass auch die Polizei Daten vorhält, spätestens dann, wenn nach der Überprüfung der Papiere mehr oder minder diskret auf einschlägige Erkenntnisse aus teilweise viele Jahre zurückliegenden Vorkommnissen hingewiesen wird oder sogar eingehendere Maßnahmen wie die Durchsuchung des Fahrzeugs oder mitgeführter Sachen folgen. Diesen Überraschungseffekt kann ich aus vielen Eingaben an meine Dienststelle herauslesen.

Rechtsgrundlage für die Speicherung von Erkenntnissen aus Ermittlungsverfahren, die der Polizeivollzugsdienst nach § 163 der Strafprozessordnung (StPO) zu führen hat, ist § 483 Abs. 3 StPO. Danach darf er Daten auch in Dateien speichern, für die die polizeigesetzlichen Regelungen maßgebend sind. Dafür ist im baden-württembergischen Polizeigesetz (PolG) vor allem § 38 Abs. 1 einschlägig:

§ 38 Abs. 1 PolG

Der Polizeivollzugsdienst kann personenbezogene Daten, die ihm im Rahmen von Ermittlungsverfahren bekannt geworden sind, speichern, verändern, und nutzen, soweit und solange dies zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Für Daten, die durch eine Maßnahme nach § 100 c der Strafprozessordnung erhoben wurden, gilt dies nur zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person. Für Daten, die durch eine Maßnahme nach § 100 a der Strafprozessordnung erhoben wurden, gilt dies nur zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung (§ 22 Abs. 5). Die Daten sind zu löschen, wenn die Voraussetzungen für die Speicherung entfallen sind.

Auf dieser Grundlage betreibt die Polizei Baden-Württemberg vor allem das Auskunftssystem POLAS-BW als Landesanwendung. Daneben gibt es noch verschiedene weitere Anwendungen auf Landesebene sowie die aufgrund des Bundeskriminalamtsgesetzes betriebenen Verbunddateien der Polizei, in die auch die baden-württembergischen Polizeidienststellen Daten einspeichern und aus denen sie Daten abrufen können.

Von zentralem Interesse für meine Dienststelle ist vor allem das Auskunftssystem POLAS-BW, da darin alle Vorgänge gespeichert werden, die die jeweils zuständige Polizeidienststelle aufgrund der gesetzlichen Vorgaben für speicherungswürdig hält. Das ist dann der Fall, wenn die betroffene Person verdächtig ist, eine Straftat begangen zu haben. Ein solcher Verdacht kann dadurch bestätigt werden, dass die Person wegen der Tat verurteilt wurde, dass das Ermittlungsverfahren gegen sie zwar eingestellt wurde, aber dennoch ein Restverdacht bleibt, oder dass sie gar mangels Beweises freigesprochen wird. Wie in früheren Tätigkeitsberichten bereits erläutert, gilt die Unschuldsvermutung im Polizeirecht gerade nicht, sodass aus Sicht der Polizei ein (Rest-)Tatverdacht auch dann zur Einspeicherung führen kann, wenn der Betroffene im Strafprozess nach dem Grundsatz „in dubio pro reo“ freigesprochen worden ist. Außerdem muss die Polizei nach ihrer kriminalistischen Erfahrung bei der betreffenden Person grundsätzlich eine Wiederholungsgefahr begründen. Damit ist – durch die Rechtsprechung des Bundesverfassungsgerichts mehrfach bestätigt – die Möglichkeit erfasst, bei der Verfolgung von Straftaten durch gespeicherte Daten zu einem Verdächtigen weitere Anhaltspunkte zu gewinnen; die Förderung der Ermittlungstätig-

keit der Polizei ist ein legitimer Zweck der Datenverarbeitung. Zu der inzwischen erfolgten Erweiterung der Speicherungsvoraussetzungen ohne Prognose bei Ersttätern habe ich bereits oben unter Nr. 1.1 meine Auffassung dargelegt.

2.2.2 Einblick in die polizeiliche Arbeit – natürlich nur nach Einwilligung in Datenbankabfragen?

Die Förderung der Ermittlungstätigkeit ist aber nicht der einzige Verwendungszweck. Der Polizeivollzugsdienst nutzt diese Datenbestände auch für andere Zwecke, die nicht im Polizeigesetz stehen. Dabei greift er auch auf eine Möglichkeit zurück, die das Landesdatenschutzgesetz bietet. § 4 LDSG macht die Zulässigkeit einer Datenverarbeitung nämlich davon abhängig, dass sie entweder gesetzlich erlaubt ist oder soweit ein Betroffener eingewilligt hat. Diese Einwilligung ist im Regelfall schriftlich zu erteilen, nachdem der Betroffene über die beabsichtigte Datenverarbeitung und deren Zweck aufgeklärt wurde.

Dieses Instrument wird vom Polizeivollzugsdienst – wie bereits in früheren Tätigkeitsberichten geschildert (vgl. 27. Tätigkeitsbericht für das Jahr 2006, LT-Drucksache 14/650, und 28. Tätigkeitsbericht 2007, LT-Drucksache 14/2050) – in unterschiedlichen Fallkonstellationen bei Bedarf genutzt. Zum Beispiel erfuhr ich durch die Anfrage einer Betroffenen, dass die Polizei von Rechtsreferendaren eine entsprechende Einwilligung verlangt, die bei einer Polizeidienststelle für einen begrenzten Zeitraum die polizeiliche Praxis kennen lernen wollen.

Warum die Polizei bei Rechtsreferendaren für Hospitationen einen Abruf aus POLAS-BW benötigt, ist mir nicht klar. Denn diese stehen in einem öffentlich-rechtlichen, beamtenähnlich ausgestalteten Ausbildungsverhältnis der Justizverwaltung und wurden daher schon auf ihre Zuverlässigkeit geprüft. Das Innenministerium sieht die Überprüfung anhand der polizeilichen Informationssysteme vor Beginn einer freiwilligen Ausbildungsstation bei der Polizei aus verschiedenen Gründen dennoch als notwendig an. Es sei allerdings bisher kein Fall bekannt geworden, in dem eine fehlende Einwilligung zur Verweigerung einer Hospitation geführt habe.

Im Rahmen unserer Nachforschungen sind wir ferner der Frage nachgegangen, ob ähnliche Überprüfungen auch bei anderen Personengruppen erfolgen, die den Polizeialltag näher kennen lernen wollen, z. B. Journalisten. Auf unsere Nachfrage schloss nach Angaben des Innenministeriums eine Dienststelle nicht aus, dass in Einzelfällen Medienvertreter, denen der Polizeivollzugsdienst Einblicke in den polizeilichen Alltag gewähren möchte, um eine Einwilligung gebeten werden könnten. Dies sei bisher aber nicht geschehen. Denn die Begleitung von Einsätzen oder Ermittlungen durch Journalisten komme nur selten vor. Dabei werde darauf geachtet und gewährleistet, dass keine personenbezogenen oder geheimhaltungsbedürftigen Daten erkennbar seien. Soweit sich Medienvertreter bei der Polizei aufhielten, würden sie grundsätzlich durch Polizeibeamte betreut und begleitet, sodass Einfluss auf Informationsinhalte und Datenzugang genommen werden könne. Der ursprünglich aus der Datenverarbeitung stammende und mittlerweile (auch) für Kriegsberichterstatter verwendete Begriff hierfür ist wohl „embedded“.

Ob die Freiwilligkeit einer Einwilligung in den genannten Fällen tatsächlich gegeben ist, kann man in Anbetracht der Folgen einer Verweigerung in Frage stellen. Ob eine solche Abfrage bezogen auf den Anlass verhältnismäßig ist, ist ebenfalls mehr als fraglich. Letztlich bezweifele ich, dass die Qualität der gespeicherten Daten für die Beurteilung so verlässlich ist, wie es Innenministerium und Polizeivollzugsdienst immer behaupten.

2.2.3 Die üblichen Verdächtigen – wessen Daten sind in polizeilichen Auskunftssystemen zu finden?

Jeder, der von der Polizei verdächtigt wird, eine Straftat begangen zu haben, kann mit seinen Daten in den Informationssystemen gespeichert werden. Zumeist erfolgt dies bereits dann, wenn die Polizei ihre Ermittlungsergebnisse an die Staatsanwaltschaft vorlegt. Aber es sind auch schon Speicherungen bei Beginn der Ermittlungen möglich, z. B. Angaben aus erkennungsdienstlichen Maßnahmen. Diese sind jedoch innerhalb einer kurzen Frist zu löschen, wenn keine weiteren Angaben zu der Person gespeichert werden.

Eingaben Betroffener an meine Dienststelle beziehen sich in größerer Zahl auf die Frage nach Inhalt und Dauer von Speicherungen in den polizeilichen Informationssystemen. Anlässe sind häufig Verkehrskontrollen oder Überlegungen, ob frühere Kontakte mit der Polizei nicht Probleme beim Studium, im Beruf oder bei sonstigen Tätigkeiten bereiten könnten. Dann kann man eine unentgeltliche Auskunft bei der Polizei beantragen. Einige verzichten darauf und wenden sich stattdessen an mich nach § 27 LDSG.

Für meine Dienststelle bieten diese Eingaben immer wieder eine willkommene Möglichkeit, den konkreten Fall, aber auch die generelle Praxis der Datenverarbeitung unter die Lupe zu nehmen. Zu flächendeckenden Kontrollen ist meine Dienststelle personell leider nicht in der Lage, aber die Summe der bisherigen Erkenntnisse lässt auf verbreitete Schwachstellen schließen. Diese aufzudecken ist im Interesse der Betroffenen. Denn nur erforderliche, geeignete und richtige Daten in den polizeilichen Auskunftssystemen verletzen deren informationelles Selbstbestimmungsrecht nicht. Im Interesse des Polizeivollzugsdienstes müsste dies eigentlich auch sein, denn falsche und ungeeignete Daten machen nur unnötig Arbeit.

Zwei Eingaben aus unterschiedlichen Gegenden des Landes ließen grundsätzliche Zweifel an der Richtigkeit der gespeicherten Informationen zu. In beiden Fällen hatten die Staatsanwaltschaften die strafrechtlichen Ermittlungsverfahren nach § 170 Abs. 2 StPO eingestellt; aus den Entscheidungsgründen war herauszulesen, dass kein strafbares Verhalten vorlag. Zwar war mir zuvor mitgeteilt worden, dass die in POLAS-BW gespeicherten Daten im Rahmen der Sachbearbeitung gelöscht worden seien, jedoch hatten meine Mitarbeiter und ich den Verdacht, dass dies erst aufgrund unserer Nachfrage erfolgt war. Bei Einsichtnahme in die Akten stellte sich dann heraus, dass in einem Fall die Speicherung des (nicht strafbaren) Tatverdachts sogar erst nach Eingang der Entscheidung der Staatsanwaltschaft erfolgte. Die aus den Akten entnommene Begründung ließ nur den Schluss zu: Dem Sachbearbeiter war es egal, wie die Staatsanwaltschaft den Vorgang beurteilt hatte, für ihn war der Betroffene speicherungswürdig; es war daher nur konsequent, dass in dem Feld für die Erfassung der justiziellen Entscheidung lakonisch „Entscheidung liegt noch nicht vor“ gespeichert war. Die eigentlich für die Plausibilität von Speicherungen Zuständigen, der Prüfdienst und der Datenstationsleiter, unterbanden diese in jeder Hinsicht unzulässige Erfassung leider nicht. Eine entsprechende Aktivität ließ sich aus dem Vorgang jedenfalls nicht entnehmen. Immerhin hat es das Landeskriminalamt in diesem Zusammenhang geschafft, bei dieser Dienststelle für die Zukunft eine Speicherpraxis zu beenden, die sogar der Dienstanweisung für POLAS-BW widersprach.

In dem anderen Fall war die Speicherung des Tatverdachts zunächst zulässig gewesen, beim Eingang der Einstellungsverfügung der Staatsanwaltschaft kam es aber zu dem gleichen Fehler: Der Sachbearbeiter bejahte den (nicht strafbaren) Tatverdacht

und sah die Wiederholungsgefahr aufgrund des Konsums von Betäubungsmitteln als gegeben an. Prüfdienst und Datenstationsleiter nahmen auch hier keine Korrekturen vor. Die Prognose einer Wiederholungsgefahr dürfte nach der Lebenserfahrung vielleicht nicht falsch sein, aber ohne Tatverdacht fehlt jegliche rechtliche Grundlage für die Speicherung. Nebenbei: In diesem Fall musste auch die Verarbeitung von Daten durch die Fahrerlaubnisbehörde auf den gesetzlich vorgegebenen Umfang beschränkt werden.

Das Landeskriminalamt nahm die von meiner Dienststelle geprüften Fälle zum Anlass für einen generellen Appell an die Dienststellen, künftig sorgfältiger bei der Datenverarbeitung vorzugehen.

Weitere bemerkenswerte Fälle waren:

– Ein Bürger hisste in seinem Garten die Deutschlandflagge. Auf ihr war das Bild einer Banane aufgedruckt. Die Polizei musste nach den strafprozessualen Bestimmungen ermitteln, denn Verunglimpfung des Staates und seiner Symbole ist nach § 90 a des Strafgesetzbuches grundsätzlich strafbar. Das sah die Staatsanwaltschaft in diesem Fall aber nicht so und stellte das Verfahren gleich ein. Daraufhin wehte die Flagge unverändert wieder über den Beeten. In POLAS-BW erfolgte eine Erfassung nur im Hinblick auf die polizeiliche Kriminalstatistik (PKS). Ein sog. PKS-Fall darf für die üblichen Auskünfte nicht genutzt werden und wird automatisch nach 13 Monaten gelöscht. Dies kann nach meiner Einschätzung noch als angemessen angesehen werden.

– Ein Student, der mit einigen Freunden eine Veranstaltung besuchte, geriet wegen seines auffälligen Verhaltens mit einer Polizeistreife in Konflikt. Er musste letztlich mit zur Wache. Ein Freund, der das polizeiliche Vorgehen mit dem Handy filmen wollte, wurde von einem Polizeibeamten unter Androhung der Wegnahme davon abgehalten. Auf der Wache beleidigte der Student noch einen anderen Polizeibeamten. Ergebnis: Student und Polizeibeamter trafen sich vor Gericht wieder – beide als Angeklagte! Beide wurden rechtskräftig mit dem Vorbehalt einer Geldstrafe verwarnt, die Verurteilung erfolgte bei dem Studenten wegen Beleidigung, bei dem Polizeibeamten wegen Nötigung. Dass der Polizeibeamte nicht in POLAS-BW gespeichert war, wurde bei einem der nachfolgend beschriebenen Kontrollbesuche festgestellt. Der Student war es dagegen schon, aber nicht nur mit Beleidigung, sondern auch mit Widerstand gegen Vollstreckungsbeamte, der vom Gericht als nicht erwiesen angesehen worden war. Die justizielle Entscheidung fand sich im Datensatz, aber nicht der Hinweis auf den Vorbehalt der Geldstrafe.

  Auf unsere Nachfrage korrigierte die Dienststelle den Datensatz. Zunächst wurde der Eintrag des Vorbehalts in der justiziellen Entscheidung, der schon von Anfang an mitgeteilt worden war, nachgeholt. Dann bewertete man das Geschehen als Fall von geringer Bedeutung, was zu einer Verkürzung der Aussonderungsprüffrist von fünf auf drei Jahre führte. Sollte bis Ende Oktober 2009 kein neuer Vorgang hinzugekommen sein, dürfte der Datensatz gelöscht sein. Ein zumindest erträgliches Ende einer nicht unbedingt qualitätsvollen Datenverarbeitung.

– Der dritte Fall hatte medial seinerzeit Wirkung weit über den Ort des Geschehens hinaus: Es ging um einen Geburtstagsempfang eines Prominenten in einem besonders festlichen Rahmen. Jahre später erfuhr die Staatsanwaltschaft, dass bei

der Finanzierung der Feierlichkeiten nicht alles mit rechten Dingen zugegangen sei. Zusammen mit der Polizei wurde daraufhin ein strafprozessuales „Vollprogramm“ einschließlich Durchsuchung von Wohn-, Geschäfts- und Büroräumen bei allen Verdächtigen durchgeführt. Wiederum einige Jahre später war im Pressespiegel des Innenministeriums zu lesen, dass das Strafverfahren bei zwei verantwortlichen Personen in zweiter Instanz gegen hohe Geldbußen durch das Berufungsgericht eingestellt worden war. Eine fast zehn Monate nach der Einstellung des Verfahrens eher beiläufig veranlasste Abfrage in POLAS-BW ergab, dass die beiden ehemaligen Angeklagten noch mit dem erstinstanzlichen Urteil als justiziellem Ausgang gespeichert waren. Deshalb wurden die Akten bei der zuständigen Polizeidienststelle angefordert. Die Durchsicht ergab, dass nicht nur diese beiden Personen nach Abschluss der polizeilichen Ermittlungen in dem Auskunftssystem gespeichert wurden. Auch weitere Verdächtige waren gespeichert worden. Die Antwort der Polizeidienststelle ergab, dass die Einstellungsentscheidungen schon seit mehreren Monaten vorlagen. Zum Zeitpunkt der von meiner Dienststelle veranlassten Abfrage hätten sie gespeichert sein können. Daten der weiteren Verdächtigen wurden aber nur in einem Fall kurz nach der Einstellung des Ermittlungsverfahrens durch die Staatsanwaltschaft gelöscht. Die restlichen Verdächtigen blieben mit ihren Daten wegen des Restverdachts einer Straftat gespeichert. Nachdem die Angelegenheit weit über fünf Jahre zurücklag und alle Personen, zu denen bisher Daten gespeichert waren, nicht erneut derart auffällig geworden waren, löschte die Polizeidienststelle alle Datensätze. Diese Entscheidung halte ich für richtig, da der ursprüngliche Tatverdacht gegeben, die Wiederholungsgefahr – im Vergleich mit den Maßstäben der Polizei in anderen, noch zu beschreibenden Fällen – allenfalls nur vertretbar begründet war.

Ein Problem aus der Vielzahl an Eingaben an meine Dienststelle ist seit Jahren die Dauer der Speicherung. Nach den gesetzlichen Bestimmungen hat die Polizei Aussonderungsprüffristen zu vergeben. Im Regelfall sind es fünf Jahre, bei Fällen geringer Bedeutung sind es drei Jahre. Die Behandlung gerade der Fälle geringer Bedeutung führt mir immer wieder vor Augen, dass dies in den Dienststellen sehr unterschiedlich gehandhabt wird. Während es bei einer Erstspeicherung meistens klappt, geht es bei der Zuspeicherung solcher Fälle zu vorhandenen Erkenntnissen sehr uneinheitlich zu. Einige Dienststellen vergeben mehr oder minder automatisch gleich die fünfjährige Regelfrist. Erläuterungen der Dienststellen hierfür stimmen nach meinem Verständnis des Gesetzeswortlauts damit nicht immer überein. Wenn aus dem Aktenrückhalt beispielsweise erkennbar wird, dass es sich um gewohnheits- oder gewerbsmäßiges Tun handelt, sollte das in den Unterlagen für die Datenerfassung auch deutlich gemacht werden. Begründungen wie die, dass bei einem zweiten Vorgang die Vergünstigung der kürzeren Speicherfrist nicht mehr gewährt werden könne, verkennt die Notwendigkeit der an der Person und an der Tat jeweils auszurichtenden Begründung für die Speicherfrist. Dass es auch anders geht, habe ich verschiedenen anderen Vorgängen entnehmen können, in denen Polizeidienststellen mehrfach Vorgänge zu derselben Person als Fälle von geringer Bedeutung speicherten.

Ich verschweige nicht, dass ich in dieser Frage mit dem Landeskriminalamt nicht einer Meinung bin, das bei vorhandenen Datenbeständen eine kürzere Speicherungsfrist von nachfolgenden Erkenntnissen nicht zulassen will. Allerdings habe ich darauf hingewiesen, dass viele Dienststellen die Formulierung in der Dienstanweisung zu POLAS-BW, die in solchen Fällen entweder das Beibehalten oder das Erhöhen des bereits vorhandenen höchsten

Aussonderungsprüfdatums vorsieht, offenbar als Einladung verstehen, die Speicherungsdauer zu erhöhen und das mit der Frist, die schon im letzten Fall vergeben wurde. Das können dann auch mal zehn Jahre sein. Ob die jüngste Tat dieses rechtfertigt, wird hingegen nicht geprüft, zumindest ist dies aus dem Aktenrückhalt in der Regel nicht ablesbar. Diese Art der Speicherung führt dazu, dass in vielen Fällen Erkenntnisse mitgeschleppt werden, die für die Beurteilung einer Person in Hinblick auf die vorbeugende Bekämpfung von Straftaten eher irrelevant sind. Dieser von mir und meinen Vorgängern wiederholt kritisierte „Mitzieheffekt“ wird zwar gesehen, aber wohl aus „Tradition“ unverändert in Kauf genommen. Das Prinzip der Erforderlichkeit einer Datenspeicherung wird damit bewusst und gewollt verletzt.

Trotz des Bemühens des Landeskriminalamts als der verantwortlichen Dienststelle für die zentralen polizeilichen Informationssysteme konnte ich keine grundsätzliche Verbesserung hinsichtlich der Richtigkeit und Vollständigkeit der Datenspeicherungen feststellen. Aus vielen Einzelfällen habe ich vielmehr den Eindruck gewonnen, dass die polizeiliche Datenverarbeitung einige strukturelle Schwächen aufweist. Dazu später mehr.

2.2.4 Sind Polizeibeamte Menschen wie du und ich? Betrachtungen zur Speicherpraxis in POLAS-BW

Polizeibeamte sind Menschen wie du und ich, das wusste ich schon vor den vier Kontrollbesuchen bei Polizeidienststellen. Auch die Einsichtnahme in eine Vielzahl von Akten, in denen es darum ging, ob und wie sie mit dem Gesetz in Konflikt gekommen sind, bestätigte diese Feststellung. Interessant war es dagegen zu erfahren, wie sich diese Erkenntnis in den polizeilichen Informationssystemen zur vorbeugenden Bekämpfung von Straftaten niederschlägt.

Anlass war ein Pressebericht: Ein Polizeibeamter zahlte eine Geldbuße, damit ein gegen ihn geführtes Ermittlungsverfahren wegen einer größeren Zahl identischer Vorwürfe eingestellt wurde. Für die Speicherung in den polizeilichen Auskunftssystemen ist eine solche justizielle Entscheidung eine zulässige Grundlage, wie schon in den Tätigkeitsberichten der vergangenen Jahre nachzulesen war. Da solche Entscheidungen üblicherweise zu einer Verlängerung einer bei der Abgabe der Ermittlungsakte an die Staatsanwaltschaft bereits laufenden Speicherfrist führen, bestand meinerseits Interesse zu erfahren, ob dieser Polizeibeamte mit den Daten aus dem Ermittlungsverfahren gespeichert war. Gerade im Vergleich mit „gewöhnlichen“ Verdächtigen wollte meine Dienststelle Näheres zu Inhalt und Dauer einer theoretisch denkbaren Speicherung erfahren. Es blieb bei der Theorie, denn in POLAS-BW gab es diesen Beamten und seinen Fall nicht.

Dieses weckte nicht nur im Einzelfall, sondern generell unser Interesse an der polizeilichen Speicherungspraxis in den Fällen, in denen Ermittlungen gegen Polizeibeamte geführt wurden. Deshalb schickte ich dem Innenministerium einen umfangreichen Fragenkatalog und bat um Auskunft zu der bisherigen Praxis. Nach über sieben Monaten erhielt ich schließlich Antwort. Für die Jahre 2006 bis 2008 waren Disziplinarakten durchgeschaut und dann die Fälle mit POLAS-BW abgeglichen worden. Anspruch auf Vollständigkeit wollte das Innenministerium nicht erheben. Meine nicht übertriebenen Erwartungen wurden aber im Wesentlichen bestätigt.

Mitgeteilt wurden 415 Ermittlungsverfahren. In 272 Fällen ging es um Straftaten im Zusammenhang mit der Dienstausübung und in 143 Fällen um außerdienstliche Vorgänge. 275 Vorgänge – also immerhin 66 % – waren nicht gespeichert, obwohl nur in 61 Fällen kein Tatverdacht gegeben war. Bei

den innerdienstlichen Vorgängen ergab die Durchsicht bei den Kontrollbesuchen tendenziell einen Verzicht auf die Speicherung. Drei in anderen Ländern geführte Ermittlungsverfahren waren nicht zu berücksichtigen. Weniger als fünf Jahre gespeichert waren von 138 Fällen 24, also 17 %. Davon wurden 13 als PKS-Fall und fünf als Fall von geringer Bedeutung erfasst. Die restlichen sechs waren kurzfristige Speicherungen zu Beginn der Ermittlungen, ein Erstfall sowie ein Prüffall nach der Neuregelung des § 38 Abs. 2 PolG. Von den betroffenen Polizeibeamten waren 28 mehr als einmal in POLAS-BW erfasst worden.

Der Vollständigkeit wegen ist zu erwähnen, dass Verkehrsdelikte – egal von wem begangen – nicht in POLAS-BW gespeichert werden. Daher relativiert dies etwas die vorgenannten Zahlen, da teilweise solche Ermittlungsverfahren mitgezählt worden waren.

Die Speicherungsquoten unterschieden sich zwischen den sieben „Erhebungsbezirken", die das Innenministerium in Anlehnung an § 70 PolG gebildet hatte. Dies waren die vier Regierungspräsidien, das Polizeipräsidium Stuttgart, das Landeskriminalamt und das Bereitschaftspolizeipräsidium. Am höchsten lag die Speicherquote im Bezirk Freiburg mit 64 %, gefolgt vom Bezirk Tübingen mit 49 %, dem Bereitschaftspolizeipräsidium mit 44 %, dem Bezirk Karlsruhe mit 34 % und den restlichen drei mit 28 %, 25 % und 24 %. Dabei darf nicht übersehen werden, dass in diesen „Erhebungsbezirken" die Zahl der Angehörigen des Polizeivollzugsdiensts sehr unterschiedlich ist. Welche Gründe in der Mehrzahl der Fälle zu keiner Speicherung führten, ließ sich nach den Angaben des Innenministeriums häufig nicht mehr feststellen. Es ließ mich aber wissen, dass Fälle offensichtlich haltloser Anschuldigungen gegen Polizeibeamte, die nicht zu dienstaufsichtsrechtlichen Prüfungen geführt hätten, in der Statistik nicht erfasst seien.

In vier Dienststellen nahm ein Mitarbeiter meiner Dienststelle im Rahmen von Kontrollbesuchen Einblick in die dort auf meinen Wunsch zusammengeführten Ermittlungs- und Disziplinarakten. Die besuchten Dienststellen unterstützten die Durchführung der Kontrolle in konstruktiver Weise.

Die Kontrollbesuche ergaben, dass die Speicherung oder Nichtspeicherung von Erkenntnissen nicht von der Laufbahngruppe des verdächtigten Polizeibeamten abhängig war. Entscheidend war die Zugehörigkeit zum Polizeivollzugsdienst als solche jedoch schon. Gerade Angehörige einer ermittelnden Dienststelle konnten sicher sein, dass Entscheidungen über eine Speicherung in POLAS-BW nur nach der Beteiligung Vorgesetzter oder durch diese selbst getroffen wurden. Dabei spielten für die Prognose einer Wiederholungsgefahr – soweit dies bei Nichtspeicherungen erkennbar war – die Konsequenzen aus dem Disziplinarrecht eine Rolle. Es liegt mir fern, dieses zu kritisieren. Jedoch würde ich mir bei jeder Entscheidung über eine Speicherung oder Nichtspeicherung in polizeilichen Auskunftssystemen die gleiche Sorgfalt bei der Prognose wünschen, ungeachtet der Tätigkeit der betroffenen Person.

Das andernorts beschriebene Problem trat auch in diesen Fällen auf: Der Ausgang des justiziellen Verfahrens war häufig nicht gespeichert, obwohl das Verfahren schon abgeschlossen war. Dieses könnte daran liegen, dass die zuständige Staatsanwaltschaft der Polizeidienststelle den Verfahrensausgang mitteilt, aber nicht (immer) der ermittelnden Organisationseinheit nach § 482 StPO und Nr. 11 der Mitteilungen in Strafsachen (MiStra).

Bei den Kontrollbesuchen lag in den Disziplinarakten stets die Mitteilung nach Nr. 15 MiStra an den Leiter der Polizeidienststelle, also den disziplinarrechtlich Verantwortlichen für die Angehörigen seiner Dienststelle, vor. Diese gehören zur Personalakte, unterliegen einem erheblich strengeren Schutz nach dem Landesdatenschutzgesetz und dem Landesbeamtengesetz. Allerdings sollte in geeigneter Form auch für die Vollständigkeit und Richtigkeit der gespeicherten Daten in den Akten und Dateien der ermittelnden Organisationseinheit gesorgt werden.

Nachfolgend werden beispielhaft einige der kontrollierten Fälle dargestellt, um die Praxis im Umgang mit § 38 PolG zu verdeutlichen:

– In dem zweiten der unter 2.2.3 erwähnten Fälle war neben dem Studenten auch der Polizeibeamte wegen einer Straftat verurteilt worden. Im Gegensatz zu dem Studenten war zu dem Polizisten nichts gespeichert. Wie mir mitgeteilt wurde, seien ursprünglich gespeicherte Daten mangels Anhaltspunkten für eine Wiederholungsgefahr gelöscht worden. Da die Unterlagen fehlten, konnte dies nicht weiter geprüft werden.

– Gegen drei Polizeibeamte wurde in dem Erhebungszeitraum wegen des Verrats von Dienstgeheimnissen ermittelt. Abgeschlossen sind die Verfahren noch nicht. Sie waren jeweils einmal vorher auffällig und in POLAS-BW erfasst worden, sodass bereits jetzt der weitere Vorgang zugespeichert wurde. Näher geprüft wurde dieser Fall aus Zeitgründen nicht.

– Eine Dienstgruppenführerin wurde von einem Mitglied der Dienstgruppe sexuell belästigt und vertraute dies der Beauftragten für Chancengleichheit an. Das durch diese angestoßene Ermittlungsverfahren wurde gegen eine Geldbuße eingestellt. Diese Einstellung und das Disziplinarverfahren hätten dem Polizeibeamten sein Fehlverhalten deutlich gemacht und daher sei eine Speicherung der Daten aus dem Ermittlungsverfahren mangels Wiederholungsgefahr nicht erfolgt, ließ der Dienststellenleiter meine Dienststelle wissen. Er führte weiter aus, dass die Beamtin die Annäherungsversuche nicht von Anfang an entschieden und deutlich zurückgewiesen habe. Der betroffene Beamte habe diese Versuche nach solchen Hinweisen sofort unterlassen und im Übrigen die notwendige Einsicht in ein zukünftig korrektes Verhalten in einem persönlichen Gespräch mit ihm erkennen lassen.

– Auch ein Polizeibeamter ist mal privat unterwegs. In nicht mehr nüchternen Zustand beschädigte der betreffende Beamte eine Sache ganz erheblich. Seine Dienststelle ermittelte nicht nur; die Einstellung des Verfahrens gegen eine Geldbuße war in dem Datensatz in POLAS-BW enthalten. Die Frist zur Aussonderungsprüfung betrug fünf Jahre. Auf seinen zweiten Antrag hin löschte die Dienststelle den Datensatz nach drei Jahren, da sich bei ihm inner- und außerdienstlich eine deutliche Änderung zum Positiven gezeigt habe.

– Nach einem Einsatz in einem nicht einfachen Umfeld wurde gegen zwei Angehörige des Polizeivollzugdienstes wegen Körperverletzung im Amt und Beleidigung einer Person, gegen die Zwangsmaßnahmen erforderlich waren, ermittelt. Am Ende wurde der eine zu einer hohen Geldstrafe verurteilt, die andere erreichte in der zweiten Instanz eine Einstellung gegen die Auflage, dem Opfer eine Entschädigung zu zahlen. Nach der Stellungnahme der ermittelnden Dienststelle sind die Daten zu beiden in POLAS-BW zunächst gespeichert, aber nach dem justiziellen Ende gelöscht worden. Eine Wiederholungsgefahr sei verneint worden, denn beide Polizeibeamten seien trotz vieler vergleichbarer Einsätze zum ersten Mal auffällig geworden. Nebenbei hieß es: Bei dem einen Angehörigen sei

im Disziplinarverfahren auch eine Entfernung aus dem Dienst möglich gewesen, bei der anderen sei kein disziplinärer Überhang gesehen worden.

– Ein Polizeibeamter wurde mehrfach wegen Ermittlungen, die zuletzt Vorgänge wie eine Beleidigung oder eine „einfache“ Körperverletzung zum Gegenstand hatten, in POLAS-BW gespeichert. Da er schon in der Vergangenheit auffällig geworden war, wurden die zuletzt gespeicherten Vorgänge – obwohl sie in dem Katalog der Fälle von geringer Bedeutung nach § 5 Abs. 3 der Durchführungsverordnung zum Polizeigesetz (DVO PolG) genannt sind – mit der Regelfrist von fünf Jahren erfasst. Die bearbeitende Dienststelle verwies zu dieser Speicherfrist auf entsprechende Richtlinien des Landeskriminalamts.

– Drei Polizeibeamte, die wegen identischer Betrugsvorwürfe im Zusammenhang mit der Dienstausübung aufgefallen waren, konnten die Ermittlungsverfahren gegen Zahlung von Geldbußen beenden. Nach Darstellung der Dienststelle wurden die Vorgänge in POLAS-BW als PKS-Fälle gespeichert, da eine Wiederholungsgefahr bei allen verneint wurde und der Schaden gering gewesen sei.

– In zwei Fällen einer Dienststelle konnte festgestellt werden, dass die Daten in POLAS-BW, insbesondere zum justiziellen Ausgang, nicht mit den von meiner Dienststelle getroffenen Feststellungen übereinstimmten. Die Nachfragen seien zum Anlass genommen worden, die Eintragungen zu korrigieren, lautete die Antwort der Dienststelle.

– In einem anderen Fall wurde gegen einen Beamten, der ursprünglich im Verdacht der Beteiligung an einer anderen Straftat stand, wegen ungenehmigter Nebentätigkeiten innerhalb der Dienstzeit und unter Verwendung eines Dienstfahrzeugs ermittelt. Gegen Zahlung einer Geldbuße wurde das Verfahren eingestellt. Seine Daten in POLAS-BW wurden auf seinen Antrag vor Ablauf von noch nicht einmal zwei Jahren gelöscht. Aus den Akten konnte nicht entnommen werden, was diese Entscheidung des Sachbearbeiters nach Rücksprache mit dem behördlichen Datenschutzbeauftragten begründete.

– Beleidigungen auf sexueller Grundlage kommen auch bei Polizeibeamten vor. In einem Fall wurde eine Beamtin als Sexualpartnerin im Internet von einem Kollegen, der sich wahrheitswidrig als ihr Lebenspartner ausgab, „angeboten“. Auf einen Strafantrag verzichtete die Beamtin, nachdem ihr der Urheber des unmoralischen Angebots bekannt wurde. In einem anderen Fall wurden mehrere SMS mit sexuellen Inhalten zwischen einem Beamten und einer anderen Beamtin gewechselt, die sich dann beleidigt sah und Anzeige erstattete. Daten wurden beide Male nicht gespeichert, da die Dienststelle keine Anhaltspunkte für die Begehung weiterer Straftaten bei den Beamten sah.

– In dem für die Erhebung und Kontrollbesuche ursächlichen Fall aus dem Pressebericht war die Speicherung nicht erfolgt, da eine Wiederholungsgefahr verneint wurde. Mir wurde erklärt, die sachbearbeitende Dienststelle sei der Auffassung gewesen, dass dem Beamten durch das Ermittlungsverfahren und die öffentliche Berichterstattung darüber sein Irrtum über die zugrunde liegende Rechtslage hinreichend deutlich geworden sei.

Die Begründungen der einzelnen Dienststellen kann man akzeptieren oder nicht. Meiner Meinung nach ist die Polizei gut beraten, nicht nur bei Polizeibeamten sorgfältig vorzugehen. Das beginnt bei dem Aktenrückhalt, setzt sich bei den Überlegungen zum Tatverdacht und zur Wiederholungsgefahr fort

und endet auch bei der Festlegung der Parameter für die Aussonderungsprüffrist nicht. Allein schon die deutlich größere Sorgfalt bei der Bearbeitung von Vorgängen mit Polizeibeamten als Verdächtigen zeigt, dass dies möglich sein muss.

Während der Erstellung dieses Tätigkeitsberichts erreichten mich noch zwei Eingaben von Polizeibeamten. In einem Fall stellte sich heraus, dass eine eigentlich vorgesehene automatische Löschung von erkennungsdienstlichen Unterlagen doch nicht funktioniert hatte, was die Dienststelle dann manuell realisierte. Und in dem anderen sieht sich ein Polizeibeamter zu Unrecht gespeichert, da seine Handlung durch Notwehr gerechtfertigt sei. Hierzu musste meine Dienststelle zunächst einmal eine Stellungnahme und die Akten anfordern.

Die kurz vor Redaktionsschluss des Berichts eingegangene Antwort lässt erkennen, dass die Daten inzwischen gelöscht sind. Allerdings räumte die Dienststelle auch ein, dass der Löschprozess wegen programmbedingter Automatismen nicht nachzuvollziehen sei. Auch hier werde ich mich weiter um die offenen Fragen kümmern müssen.

2.2.5 Verbessert werden kann vieles, man muss es nur wollen!

Grundsätzlich ist die Notwendigkeit der Speicherung von Daten zur vorbeugenden Bekämpfung von Straftaten, vor allem wenn es um die Förderung polizeilicher Ermittlungen geht, unbestritten. Umso mehr ist dabei aber auf eine hohe Datenqualität zu achten. Dies ist ein Thema, dem sich auch eine Arbeitsgruppe beim Landeskriminalamt seit einiger Zeit widmet. Dass die Qualität der Datenspeicherung verbessert werden kann, ist nach einem mir zugegangenen Evaluationsbericht dieser Gruppe kaum zu bestreiten. Hierzu soll auch die Realisierung des Projektes ComVor, also die Einführung eines Vorgangsbearbeitungssystems, welches Quelldatenbank für die verschiedenen polizeilichen Informationssysteme werden soll, beitragen.

Ob die von mir bemängelten Probleme mit Hilfe des Projekts ComVor überzeugend gelöst werden können, hängt von vielen Voraussetzungen ab. Generelles Ziel muss sein, dass die Datenbanken der Polizei einen hohen Datenschutzstandard erreichen. Die Polizei wäre auch gut beraten, wenn sie sich frühzeitiger von Daten trennen würde, deren Erkenntnisgewinn minimal ist. Auf die Speicherung von Bagatelldelikten, wie wechselseitiger Beleidigungen u. Ä., wurde bereits im 27. Tätigkeitsbericht für das Jahr 2006 (LT-Drucksache 14/650) eingegangen. Der Wert der Speicherung von Ermittlungsverfahren, in denen die Staatsanwaltschaft die Beteiligten auf den Privatklageweg verweist, erschließt sich mir vor dem Hintergrund der oben skizzierten Fälle von „gewöhnlichen" Menschen und Polizeibeamten nicht. Wenn es dem Polizeivollzugsdienst nur um eine Art „Tätigkeitsnachweis" in POLAS-BW gehen sollte, dann reicht eine statistische Erfassung („PKS-Fall") aus.

Bei einer Fortbildungsveranstaltung haben mir die behördlichen Datenschutzbeauftragten der Polizeidienststellen des Landes vor einigen Monaten berichtet, dass es gerade in der Datenverarbeitung an dem notwendigen Personal fehlt. Die neben dem Sachbearbeiter für die Qualität der einzuspeichernden Daten sorgenden Prüfdienste und Datenstationsleiter seien hierzu wegen anderer Aufgaben nicht mehr in der Lage. Das Landeskriminalamt schrieb mir, dass dies nicht auf alle Dienststellen zuträfe. Die Besetzung mit Polizeibeamten und Tarifangestellten sei sehr unterschiedlich, nicht zuletzt, weil sich auch die von den einzelnen Dienststellen zu erbringende Effizienzrendite jeweils unter-

schiedlich auswirke. Nach meinem Eindruck besteht aber aufgrund zu vieler Aufgaben oder zu geringer Personalausstattung, verstärkt durch eine tradierte, umfassende Speicherpraxis, die generelle Gefahr, dass eine sorgfältige, das informationelle Selbstbestimmungsrecht achtende Datenverarbeitung nicht mehr gewährleistet ist. Wie das Landeskriminalamt inzwischen erklärte, fehle zwar derzeit ein Instrument für die Feststellung von Defiziten, die Thematik solle aber zukünftig aufgegriffen werden.

Um die Qualität der zu speichernden Daten zu verbessern, schlage ich folgende konkrete Maßnahmen vor:

- *In der Aus- und Fortbildung ist Datenschutz über die bisherigen Ansätze hinaus stärker zu thematisieren und zu vermitteln;*
- *justizielle Verfahrensausgänge sind unverzüglich zu verarbeiten und im Aktenrückhalt für die Dateiinhalte aufzunehmen;*
- *Speicherungen von Daten in Fällen, in denen kein strafrechtlicher Tatverdacht (mehr) gegeben ist, müssen verhindert oder unverzüglich gelöscht werden;*
- *es ist zu prüfen, ob eine zusätzliche automatisierte Überwachung bestimmter Datenfelder, insbesondere des Datenfelds, in dem der Ausgang des justiziellen Verfahrens einzutragen ist, eine notwendige Korrektur beschleunigen kann;*
- *die Nachvollziehbarkeit der Datenverarbeitung im Aktenrückhalt ist zu verbessern; Gründe für eine Speicherung, ausgehend von dem Tatverdacht und der Wiederholungsgefahr, müssen nachvollziehbar für weitere zu beteiligende Organisationseinheiten sein; insbesondere bei der Fortdauer der Speicherung bei Einstellung des Ermittlungsverfahrens ist dies in angemessener Form darzulegen;*
- *die Dauer der Speicherung von Fällen geringer Bedeutung mit einer dreijährigen Frist entsprechend der gesetzlichen Regelung ist sicherzustellen; bereits gespeicherte Erkenntnisse dürfen nicht verhindern, kürzere Fristen zu vergeben;*
- *erleichterte Erfassung von PKS-Fällen und Ausdehnung auf Bagatelldelikte, damit eine Konzentration auf wesentliche Vorgänge und die Kernaufgaben der Polizei möglich wird.*

Ich bin gespannt, welche Überlegungen das Innenministerium und das Landeskriminalamt anstellen werden, um POLAS-BW zu einem wirklich tauglichen Instrument für die Polizeiarbeit zu machen. Danach kommt dann das schwerste Stück der Arbeit, die Umsetzung in die Praxis. Ich werde auch diese Phase kritisch, aber konstruktiv begleiten.

2.3 Identitätsfeststellungen, Durchsuchungen, Fahndungsmaßnahmen und DNA-Proben – Datenschutz im polizeilichen Alltag

Eine Razzia und ihre Folgen

Die Polizei kann die Identität einer Person feststellen, wenn sie sich an einem Ort aufhält, an dem erfahrungsgemäß Straftäter sich verbergen, Personen Straftaten verabreden, vorbereiten oder verüben, sich ohne erforderliche Aufenthaltserlaubnis treffen oder der Prostitution nachgehen – § 26 Abs. 1 Nr. 2 des Polizeigesetzes (PolG).

Diese Vorschrift ist vor allem Kennern des Polizeirechts bekannt, enthält sie doch die Beschreibung „verrufener“ Orte. Ob ein Ort dazu gehört, ergibt sich nach vielfältiger Rechtsprechung und Kommentaren aus den Erfahrungen und tatsächlichen Anhaltspunkten sowie nach den örtlichen Verhältnissen und Erkenntnissen der Polizeibehörden oder

Polizeidienststellen. Wenn es dann einen solchen Ort gibt, kann die Identität aller Personen festgestellt werden, die sich dort aufhalten. Sofern dabei ausnahmslos alle Personen kontrolliert werden, handelt es sich um eine Razzia. Welche Auswirkungen eine solche polizeiliche Maßnahme hatte, erfuhren die Besucher einer bekannten Veranstaltungsstätte in einem Konstanzer Gewerbegebiet im Mai 2008.

Das Ereignis wurde in den lokalen Medien aufgrund der Hinweise vieler betroffener Besucher eingehend kommentiert und führte nicht nur zu Presseanfragen, sondern auch zu Eingaben an meine Dienststelle.

Anlass für die Aktion, bei der rund 280 Kontrollkräfte, neben den Polizeibeamten auch Angehörige des Zolls mit Rauschgiftspürhunden sowie drei Angehörige der Thurgauer Kantonspolizei und der Schweizer Grenzwacht, etwa 400 Gäste in ihrem Freizeitvergnügen störten, war der Verdacht, dass in der Veranstaltungsstätte mit Betäubungsmitteln gehandelt werde. Die mehrere Stunden dauernde Aktion, die umfassend von Videotrupps der Bereitschaftspolizei dokumentiert wurde, führte zu 14 Ermittlungsverfahren wegen Drogendelikten und weiteren sechs wegen Verstößen gegen das Waffengesetz, wegen Widerstands gegen Vollstreckungsbeamte, wegen eines Eigentumsdelikts und wegen einer Beleidigung. Zwei Ordnungswidrigkeitenverfahren wegen falscher Namensangabe, 35 positive Drogenvortests und 17 aufgefundene Betäubungsmittel, die nicht zugeordnet werden konnten, rundeten das Ergebnis der Razzia ab.

Entscheidend für viele Gäste waren aber die weiter angeordneten Maßnahmen wie Erfassung jedes Einzelnen mit einer Videokamera sowie eine Durchsuchung der jeweiligen Person und mitgeführten Sachen, zu der auch das Auslesen der IMEI-Nummer der Mobiltelefone gehörte, um diese mit dem Sachfahndungsbestand abzugleichen. Zur Erläuterung: Die „International Mobile Station Equipment Identity“ [IMEI] ist eine 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät eindeutig identifiziert werden kann. Aus den Schreiben an meine Dienststelle wurde ebenso deutlich, dass ein Aufsuchen der Toiletten nicht ohne Weiteres möglich war und ein Austrinken der Gläser Probleme mit den eingesetzten Polizeibeamten bereitete. In einem Fall wurde einem Gast, der durch die Aktion verletzt worden war, außer einer Erstversorgung vor Ort nur der Rat erteilt, sich in ein Krankenhaus zu begeben. Die meisten Reaktionen ließen erkennen, dass sich die Gäste auch um ihr Vergnügen gebracht sahen, da sie nach den polizeilichen Maßnahmen anschließend des Platzes verwiesen wurden.

Nachdem in der Veranstaltungsstätte bestimmte Räume noch durchsucht werden sollten, wurde der zunächst nicht anwesende Betreiber, der die Halle an einen Veranstalter vermietet hatte, hinzu gerufen. Ob die handelnden Einsatzkräfte den Überblick verloren hatten oder mangelnde Kommunikation ursächlich war: Dem Betreiber erging es wie den in der Halle anwesenden Gästen, er und sein Fahrzeug wurden erst einmal gründlich durchsucht. Allerdings hat sich die Polizeidirektion im Nachhinein bei dem Betreiber ausdrücklich für diese Maßnahme entschuldigt.

Auf die Anfragen hin, die meine Dienststelle erreichten, musste mein Vorgänger zunächst darauf hinweisen, dass er sich nur um die Erhebung und Verarbeitung der personenbezogenen Daten während dieser Razzia kümmern könne. Ob die Maßnahme polizeirechtlich zulässig und verhältnismäßig war, haben die übergeordneten Behörden oder die Verwaltungsgerichtsbarkeit zu klären.

Die rechtlichen Bedingungen für die Erhebung der Daten der Gäste waren nach den einschlägigen Bestimmungen des Polizeigesetzes aufgrund der Allgemeinverfügung gegeben. Denn die Daten wurden offen bei den Betroffenen erhoben und die Voraussetzungen des § 20 Abs. 2 PolG waren erfüllt. Dies traf auch auf die Anordnung der Durchsuchung und die Anfertigung der Lichtbilder mittels Videokamera zu. Betont wurde seitens der Polizeidirektion, dass die Einzelaufzeichnung der Gäste in einem „Videotor“ keine erkennungsdienstliche Maßnahme sei,

sondern auf § 21 Abs. 3 PolG gestützt werde (Weiteres zu dieser Bestimmung ist im 1. Teil unter Nr. 4.3 und 4.4 enthalten.). Ausdrücklich wurde darauf hingewiesen, dass alle Aufzeichnungen – seien es Videoaufnahmen oder die Erhebungen zu den einzelnen Personen – drei Wochen nach der Maßnahme gelöscht und vernichtet worden seien, sobald keine Bezüge zu den Ermittlungsverfahren oder sonstigen polizeirechtlichen Maßnahmen mehr gegeben waren. Dies entspricht den gesetzlichen Regelungen in § 37 Abs. 1 PolG zur Speicherung, Veränderung und Nutzung von Daten, soweit und solange dies zur Wahrnehmung der polizeilichen Aufgabe erforderlich ist, und in § 46 Abs. 1 PolG zur Löschung nicht mehr benötigter Daten.

Gegen die Hinzuziehung der Schweizer Beamten, die die Überprüfung schweizerischer Staatsbürger unterstützten, war vor dem Hintergrund des deutsch-schweizerischen Vertrags aus dem Jahre 1999 über die polizeiliche Zusammenarbeit, der seit dem 2. Oktober 2001 in Kraft ist (BGBl. II, S. 946), ebenfalls nichts einzuwenden.

Die im Schriftverkehr geäußerten Befürchtungen, aus den Mobiltelefonen seien mehr Informationen als die IMEI-Nummer ausgelesen worden, konnten nach einem Selbstversuch meiner Mitarbeiter im Rahmen eines anderen Kontrollbesuchs im Nachhinein eher ausgeschlossen werden, da das Auslesen auch eines relativ einfachen Gerätes nicht in wenigen Minuten erfolgen kann, sondern erheblich mehr Zeit in Anspruch nimmt.

Zusammengefasst bleibt nur festzuhalten, dass auch ein Freizeitvergnügen ein abruptes Ende finden kann, wenn es in einer Umgebung stattfindet, die von anderen Menschen zu gesetzeswidrigem Tun genutzt wird. Datenschutzrechtlich gab es mit Ausnahme der unzulässigen Maßnahmen gegenüber dem Betreiber der Halle keine unzulässigen Erhebungen und Datenverarbeitungen. Ob die polizeirechtliche Maßnahme insgesamt rechtmäßig war, soll Gegenstand eines verwaltungsgerichtlichen Verfahrens gewesen sein, dessen Ausgang meinen Mitarbeitern und mir allerdings nicht bekannt ist.

Wattestäbchen und das informationelle Selbstbestimmungsrecht

Der Mord an einer Polizeibeamtin und der Mordversuch an ihrem Kollegen in Heilbronn sind noch nicht vergessen. Wer die Tat begangen hat, ist nach über zwei Jahren immer noch ungeklärt. Die sofort angelaufenen Ermittlungen brachten zunächst Erkenntnisse mit Bezügen zu vielen anderen Taten, die sich inzwischen aber als Trugspuren herausgestellt haben. Bevor man aber diese Erkenntnis gewinnen konnte, wurden im Rahmen der strafprozessualen Maßnahmen viele Ansätze zur Ermittlung genutzt. Im Vordergrund stand eine auch am Tatort festgestellte DNA-Spur, die sich später als Verunreinigung des zur Probeentnahme verwendeten Wattestäbchens herausstellte. Bis es soweit war, wurden in vielen Fällen DNA-Proben erhoben. Dass bei einer solchen Straftat auf der Grundlage des § 81 h der Strafprozessordnung (StPO) nach gerichtlicher Anordnung nur mit schriftlicher Einwilligung bei den Personen, die auf den Täter vermutlich zutreffende Prüfungsmerkmale erfüllen, Körperzellen entnommen, molekulargenetisch auf das DNA-Identifizierungsmuster und das Geschlecht untersucht und mit DNA-Identifizierungsmustern von Spurenmaterial automatisch abgeglichen werden können, ist grundsätzlich zulässig.

Ein Beschwerdeführer, der als Schwerbehinderter nach seiner Einschätzung kaum als Täter in Frage kam, fühlte sich gleichwohl von der für seinen Wohnsitz zuständigen Polizeidirektion zu der Abgabe der Einwilligungserklärung genötigt. Bei der Überprüfung durch meine Dienststelle stellte sich heraus, dass ein Hinweis auf ihn bei der Sonderkommission eingegangen war, dem natürlich nachgegangen werden musste. Die Spur führte – wie nicht anders zu erwarten war – nicht weiter, sodass seine DNA-Probe vernichtet wurde und nur in den Spurenakten der Hinweis auf das negative Ergebnis der Überprüfung seiner DNA verblieb. Gegen diese Verfahrensweise konnte ich keine Bedenken äußern und unterrichtete den Beschwerdeführer entsprechend.

Etwas anders verlief eine Aktion in den Landkreisen Heilbronn und Ludwigsburg Ende des letzten Jahres. Durch Presseberichte wurde bekannt, dass Passanten und Autofahrer an neuralgischen Punkten bei Kontrollen um die Abgabe freiwilliger DNA-Proben gebeten wurden. Dazu fragten wir bei der ermittelnden Polizeidirektion an. Eine Antwort erhielten wir von der übergeordneten Dienststelle. Nachdem verschiedene Anlagen zu der Antwort meine Dienststelle verspätet erreichten, wurden im Mai 2009 noch weitere Nachfragen zu dem Vorgehen notwendig. Erst vor kurzem erhielt ich eine Reaktion auf die Fragen.

Aus der Antwort dieser Dienststelle auf mein erstes Schreiben, die inhaltlich mit der Antwort des Innenministeriums in der LT-Drucksache 14/3990 identisch war, ging hervor, dass in 80 % der im Landkreis Ludwigsburg durchgeführten 321 Erhebungen von DNA-Proben eine Rechtsgrundlage überhaupt nicht gegeben war, da diese von dem seinerzeit gültigen Beschluss des Amtsgerichts nicht gedeckt waren. Ganz abgesehen davon wurden DNA-Proben nicht nur nach der einleitend genannten Rechtsgrundlage, sondern auch nach § 81 e StPO erhoben. Die Staatsanwaltschaft wurde darüber bei Beginn der Fahndungsmaßnahmen in Kenntnis gesetzt. Die Rechtsvorschrift passte zu den durchgeführten Probenahmen in dem Fahndungskonzept jedoch nicht. Die hiernach vorgesehenen Probenerhebungen wurden ab März 2009 nicht mehr durchgeführt, nachdem alle beteiligten Dienststellen durch das Landeskriminalamt nach einer kritischen Prüfung der Rechtslage entsprechend angewiesen worden waren. Dass es bei den erwähnten Kontrollen an neuralgischen Punkten keine in die Irre führenden Spuren gab, lag daran, dass die Proben in der Regel nicht mit den Wattestäbchen der Lieferfirma erhoben wurden, die die Spurenprobleme verursacht hatten.

Die mit den Ermittlungsmaßnahmen zusammenhängenden Erörterungen im Landtag, die sich auch aus der LT-Drucksache 14/5045 zu den Anträgen in den LT-Drucksachen 14/4259, 14/4359 und 14/4364 ergeben, machen deutlich, auf welchen Ebenen die Erkenntnisse zu den Trugspuren seit wann diskutiert wurden.

Meine Aufgabe ist es, die datenschutzrechtlichen Anliegen auch in dieser Situation deutlich zu machen. Ich bedauere es sehr, dass es gerade bei der Aufklärung eines solchen Verbrechens, trotz allen Verständnisses für die unter hohem Erfolgsdruck stehenden Ermittler, zu den schlichtweg nicht gesetzlich gerechtfertigten Probenahmen kam. Nicht verstehen kann ich, dass den Einsatzkräften nicht die Unterlagen zur Verfügung gestellt wurden, um DNA-Proben nur nach dem vom Amtsgericht vorgegebenen Personenraster zu erheben. Insoweit wurde das Persönlichkeitsrecht einer Vielzahl Betroffener verletzt. Beruhigen kann die Aussage, dass alle insoweit entnommenen Proben inzwischen vernichtet worden seien, nur bedingt.

Abschließend stellt sich für mich wieder die grundsätzliche Frage, wie zukünftig gewährleistet werden kann, dass der Polizeivollzugsdienst sich an gesetzliche, richterliche oder sonstige verbindliche Vorgaben tatsächlich hält. Sensibilisierung für die Anliegen des Datenschutzes ist dafür ein nicht unwesentlicher Beitrag.

2. Abschnitt: Justiz

1. Gesetzgebung

1.1 Forderungsmanagement der Justiz oder Inkasso im Auftrag des Fiskus

Auf der Rechtsgrundlage des § 9 a des Landesjustizkostengesetzes wird künftig ein privates Inkassounternehmen die Landesoberkasse bei der Beitreibung ausstehender Gerichtskosten unterstützen.

Nichts ist umsonst im Leben – diese alte Spruchweisheit gilt bekanntlich auch für die Dienste der Justiz. Der Bürger kann aus verschiedenen Gründen zu ihrem Schuldner werden: Gerichtskosten sind zu zahlen,

bewilligte Prozesskostenhilfe ist zurückzuerstatten, Zulassungs- und Prüfungsgebühren müssen entrichtet werden etc. Manche Gerichtskostenschuldner können oder wollen jedoch nicht zahlen – und nicht immer gelingt es dem Land, seine Forderungen am Ende durchzusetzen. So kritisierte der Rechnungshof Baden-Württemberg in einer Beratenden Äußerung aus dem Jahr 2005, dass die zuständige Landesoberkasse jährlich Justizkostenforderungen in Millionenhöhe niederschlage und nicht mehr weiterbearbeite.

Wie nun, wenn die zuständige Landesoberkasse gegen Erfolgsprovision einfach ein Inkassounternehmen beauftragen würde, niedergeschlagene Forderungen beizutreiben? Mit dieser Idee wurde meine Dienststelle konfrontiert und um eine Einschätzung gebeten, ob ein entsprechendes Pilotprojekt aus datenschutzrechtlicher Sicht Bedenken begegne. Es wird kaum überraschen, dass sich mein Vorgänger im Jahr 2008 sehr skeptisch äußerte: Die Übermittlung personenbezogener Daten an ein privates Inkassounternehmen stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht des Forderungsschuldners dar, für den seinerzeit eine hinreichende Rechtsgrundlage nicht zu erkennen war, zumal die Frage im Raume stand, ob das legitime Ziel, die Außenstände zu verringern, nicht auch durch eine personelle und sachliche „Ertüchtigung“ der Landesoberkasse erreicht werden konnte. Unser Fazit lautete daher, dass eine Einbindung Privater in das Forderungsmanagement der Justiz schon in der Projektphase allenfalls auf der Grundlage einer bereichsspezifischen und normenklaren gesetzlichen Vorschrift denkbar sei, die freilich erst noch geschaffen werden musste.

Die beteiligten Ressorts akzeptierten diesen Standpunkt und machten sich an die Arbeit. Einige Monate später wurde uns ein mittlerweile Gesetz gewordener Entwurf eines „Gesetzes zur Änderung des Landesjustizkostengesetzes sowie zur Anpassung von Rechtsvorschriften“ präsentiert, dem man anmerkte, dass er von dem für die Aufsicht über den Datenschutz im nichtöffentlichen Bereich zuständigen Fachreferat des Innenministeriums intensiv begleitet worden war. Durch das Gesetz ist in Gestalt eines § 9 a eine neue, sehr detaillierte Vorschrift in das Landesjustizkostengesetz eingeführt worden (GBl. 2008, S. 333), die – vereinfacht dargestellt – aus zwei Regelungskomplexen besteht: Während die Absätze 1 bis 3 der Norm die Landesoberkasse ermächtigen, zum Zweck der Forderungsbeitreibung künftig bei privaten Auskunfteien die aktuelle Anschrift des säumigen Schuldners zu ermitteln sowie sog. Negativauskünfte einzuholen, die Rückschlüsse auf dessen Zahlungsfähigkeit erlauben, darf sie nach Maßgabe der Absätze 4 bis 7 darüber hinaus ein sorgfältig auszuwählendes privates Unternehmen mit unterstützenden Beitreibungsmaßnahmen beauftragen. Bevor Letzterem jedoch personenbezogene Daten des Schuldners übermittelt werden, ist dieser regelmäßig letztmals zur Zahlung aufzufordern und ihm damit Gelegenheit zu geben, den weiteren Einziehungsprozess durch Zahlung doch noch abzuwenden. Flankiert werden diese Bestimmungen durch Detailregelungen, die gewährleisten sollen, dass die in den nichtöffentlichen Bereich übermittelten Schuldnerdaten dort nur für den Übermittlungszweck verarbeitet und im Übrigen alsbald wieder gelöscht werden.

Damit war der Forderung nach einer bereichsspezifischen und normenklaren gesetzlichen Regelung entsprochen worden; insofern konnte meine Dienststelle für das Pilotprojekt, das unterdessen mit der Auswahl des privaten Projektpartners in seine entscheidende Phase eingetreten sein dürfte, letztlich „grünes Licht“ geben.

Freilich ist das letzte datenschutzrechtliche Wort damit noch nicht gesprochen. Vielmehr halte ich es für unabdingbar, dass die Ergebnisse der Gesetzesnovelle nach Abschluss der dreijährigen Pilotphase sorgfältig und ergebnisoffen evaluiert werden. Dabei dürfen nicht alleine die Erwartungen im Vordergrund stehen, die mit der Einbindung eines privaten Inkassounternehmens in das Forderungsmanagement der Justiz verbunden sind; vielmehr wird auch zu hinterfragen sein, ob sich die in § 9 a des Landesjustizkostengesetzes getroffenen Vorkehrungen zum Schutz des informationellen Selbstbestimmungsrechts der Forderungs-

schuldner in der Praxis bewährt haben. Ebenso wie das Innenministerium im Fünften Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich 2009 (Kap. A 2.5) möchte ich bereits jetzt darauf hinweisen, dass vergleichbare rechtliche Regelungen zu schaffen sind, wenn das Justizmodell auf andere Forderungen des Landes und der Kommunen übertragen werden soll.

Nach Abschluss der dreijährigen Pilotphase sind die Ergebnisse des auf der Grundlage des § 9 a des Landesjustizkostengesetzes durchgeführten Pilotprojektes unter besonderer Berücksichtigung seiner Folgen für das informationelle Selbstbestimmungsrecht der Betroffenen sorgfältig zu evaluieren. Eine Übertragung des Modells auf andere Bereiche bedarf ähnlich präziser Rechtsgrundlagen.

1.2 Gesetz über die elektronische Aufsicht im Vollzug der Freiheitsstrafe – die „elektronische Fußfessel“ kommt!

Im Rahmen eines Modellversuchs soll im baden-württembergischen Justizvollzug als alternative Form des Strafvollzugs die „elektronische Fußfessel“ erprobt werden. Mit einem „Gesetz über die elektronische Aufsicht im Vollzug der Freiheitsstrafe“ (EAStVollzG, GBl. 2009, S. 360) hat der Landesgesetzgeber hierfür die rechtlichen Voraussetzungen geschaffen.

Ein Gesetz, das die „elektronische Aufsicht im Vollzug“ zum Gegenstand hat, mag zunächst wenig spektakulär anmuten. Tatsächlich schickt sich das Land Baden-Württemberg jedoch an, im Strafvollzug neue Wege zu beschreiten, die aus datenschutzrechtlicher Sicht nicht ohne Brisanz sind, denn es geht um nichts weniger als um eine umfassende Kontrolle des Tagesablaufs eines Probanden mit elektronischen Hilfsmitteln, die es, abgestuft nach seinem individuellen Flucht- und Rückfallrisiko, äußerstenfalls sogar ermöglichen sollen, ein lückenloses Bewegungsprofil über ihn zu erstellen. Aus der Warte der Betroffenen mag sich die elektronische Aufsicht freilich als eine Vergünstigung darstellen, da sie anderenfalls eine Haftstrafe in der Justizvollzugsanstalt antreten bzw. auf Vollzugslockerungen während der Haft verzichten müssten.

Erprobt werden soll die elektronische Aufsicht im Rahmen eines Modellversuchs zunächst als Mittel zur Überwachung eines Hausarrests. Diesem können zum einen Probanden unterstellt werden, die anderenfalls eine Ersatzfreiheitsstrafe verbüßen müssten, weil sie ihre Geldstrafe nicht begleichen können; zum anderen soll der elektronisch überwachte Hausarrest aber auch als Instrument der Entlassungsvorbereitung zum Einsatz kommen. Voraussetzung ist jeweils, dass der Proband über eine Wohnung mit Telefonanschluss sowie eine Arbeit oder Ausbildungsstätte verfügt und in den elektronisch überwachten Hausarrest, den er selbst bei der zuständigen Justizvollzugsanstalt beantragen muss, einwilligt. Sieht die Justizvollzugsanstalt die formellen Voraussetzungen als erfüllt an, so erarbeitet in einem nächsten Schritt eine vom Gesetz bewusst nicht näher bestimmte „für die elektronische Aufsicht zuständige“ Stelle, bei der es sich gegebenenfalls auch um eine private Organisation handeln können soll, gemeinsam mit dem Gefangenen einen Vollzugsplan, der im Detail bestimmt, was der Proband während der Zeit seines Hausarrests zu tun oder zu unterlassen hat. Dieses Vollzugsprogramm kann Regelungen über Arbeit, Ausbildung, Freizeit und Sport enthalten, den Probanden zur Teilnahme an Einzel- und Gruppentherapien sowie besonderen Erziehungs- und Schulungsprogrammen verpflichten und Weisungen über den Aufenthalt, den Verzicht auf Alkohol und andere Drogen etc. vorsehen. Abschließend entscheidet der Leiter der zuständigen Justizvollzugsanstalt über die Bewilligung des Hausarrests.

Ferner soll die elektronische Aufsicht ohne Hausarrest im Bereich der Vollzugslockerungen zum Einsatz kommen und Spielräume schaffen, das heißt um bei solchen Gefangenen Ausgänge, Freigang oder Hafturlaub zu gewähren, bei denen die Voraussetzungen hierfür ohne elektronische Überwachung nicht erfüllt wären. Auch hier setzt die elektronische Aufsicht stets die Einwilligung des Betroffenen voraus.

Was ist nun unter der „elektronischen Aufsicht“ konkret zu verstehen? Der Landesgesetzgeber hat absichtlich darauf verzichtet, sich auf eine bestimmte Technik festzulegen; stattdessen beschreibt das Gesetz lediglich die Anforderungen, welche von dieser zu erfüllen sind. Die elektronische Aufsicht soll es ermöglichen, die An- und Abwesenheit des Gefangenen in seiner Wohnung technisch zu beaufsichtigen und ein Bewegungsprofil des Probanden zu erstellen. Nur beispielhaft benennt die Begründung als mögliche technische Lösungen die (Mobil-)Funkzellenortung, die Ortung des Betroffenen über GPS-Koordinaten sowie die sog. Radio-Frequenz-Identifikation (RFID). Dabei soll die zuständige Stelle, die gemeinsam mit dem Gefangenen das Vollzugsprogramm erarbeitet hat, mit dessen (elektronischer) Überwachung betraut werden; lediglich die Entscheidung über Sanktionen bei etwaigen Verstößen gegen das Vollzugsprogramm bleibt der zuständigen Justizvollzugsanstalt vorbehalten.

Diese Konzeption des Gesetzgebers ist auf Zustimmung, aber auch auf Kritik gestoßen, wobei die meisten vorgetragenen Einwände freilich keine Fragen des Datenschutzes betreffen. Auch aus datenschutzrechtlicher Warte stimmt jedoch nachdenklich, dass die nach dem Gesetz grundsätzlich mögliche Übertragung der Aufgaben der elektronischen Aufsicht auf eine private Organisation gleichsam ein Einfallstor für eine weitere (Teil-)Privatisierung des Strafvollzugs darstellt. Dies gilt umso mehr, als – anders als in der Gesetzesbegründung dezidiert behauptet – nicht erst die der Justizvollzugsanstalt vorbehaltenen Sanktionen wegen etwaiger Verstöße gegen den Vollzugsplan, sondern bereits die der „zuständigen Stelle“ obliegenden elektronischen Überwachungsmaßnahmen als solche einen durchaus gewichtigen Grundrechtseingriff darstellen.

Andererseits konnten wir uns mit dem federführenden Justizministerium in einer anderen nicht unwichtigen Detailfrage einigen. Die Aufgaben, die der Gesetzgeber der „für die elektronische Aufsicht zuständigen Stelle“ zugewiesen hat, gehen aus datenschutzrechtlicher Sicht jedenfalls über eine bloße Auftragsdatenverarbeitung hinaus, mit der Konsequenz, dass die Verarbeitung personenbezogener Daten durch die „zuständige Stelle“ nicht mehr der Justizvollzugsanstalt als quasi eigene Datenverarbeitung zugerechnet werden kann. Da das Justizministerium dies wohl zunächst anders gesehen hatte, wies der ursprüngliche Gesetzentwurf insoweit eine gewisse dogmatische Unschärfe auf, die jedoch in Absprache mit meiner Dienststelle im Zuge des Gesetzgebungsverfahrens behoben wurde.

Trotz der skizzierten Kritikpunkte haben wir das Gesetz im Übrigen nicht prinzipiell abgelehnt. Zwar stellt die elektronische Aufsicht, zumal wenn ein umfassendes Bewegungsbild des Gefangenen erstellt wird, zweifelsohne einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Probanden dar; die Alternative vor Augen, ihre Ersatz- oder Restfreiheitsstrafe in der Justizvollzugsanstalt zu verbüßen oder auf Vollzugslockerungen zu verzichten, dürften die meisten Betroffenen diesen Eingriff jedoch als das geringere Übel empfinden. Da überdies die elektronische Aufsicht in jedem Falle das Einverständnis des Betroffenen voraussetzt, sahen wir keinen Grund, uns dem gesetzgeberischen Anliegen, dieses Instrument in einem von vornherein eng begrenzten Rahmen als alternative Vollzugsform zu erproben, grundsätzlich zu verweigern.

Dessen ungeachtet halte ich eine ergebnisoffene Evaluation des Modellversuchs unter besonderer Berücksichtigung seiner datenschutzrechtlichen Auswirkungen für unverzichtbar. Einen Automatismus dergestalt, dass das einmal eingeführte Instrumentarium um seiner selbst willen beibehalten oder gar auf weitere Bereiche des Justizvollzugs erstreckt wird, darf es aus datenschutzrechtlicher Sicht nicht geben.

Nach Abschluss des angekündigten Modellversuchs ist ergebnisoffen zu evaluieren, ob sich die „elektronische Aufsicht im Vollzug“ bewährt hat. Meine Dienststelle wird die weitere Entwicklung kritisch beobachten.

1.3 Justizvollzugsgesetzbuch

In einem vier Bücher umfassenden Justizvollzugsgesetzbuch hat das Land den Strafvollzug in Baden-Württemberg unter Einbeziehung des Untersuchungshaftrechts auf eine neue rechtliche Grundlage gestellt. Für den Datenschutz ergeben sich daraus bislang keine wesentlichen Änderungen.

Seit im Zuge der Föderalismusreform Artikel 74 Abs. 1 des Grundgesetzes (GG) geändert worden ist, haben die Bundesländer auf dem Gebiet des Strafvollzugs nach Maßgabe des Artikels 70 Abs. 1 GG das alleinige Recht der Gesetzgebung. Von dieser neuen ausschließlichen Zuständigkeit hat das Land Baden-Württemberg bereits mit dem Erlass zweier Gesetze über den Jugendstrafvollzug sowie über den Datenschutz im Justizvollzug, über die mein Vorgänger in seinem 28. Tätigkeitsbericht für das Jahr 2007 (vgl. LT-Drucksache 14/2050) berichtet hatte, Gebrauch gemacht; im Übrigen galt hierzulande bis vor kurzem jedoch das Strafvollzugsgesetz des Bundes fort.

Dies hat sich mittlerweile geändert, denn der Landtag hat am 4. November 2009 ein „Gesetz zur Umsetzung der Föderalismusreform im Justizvollzug“ beschlossen (GBl. S. 545), das am 1. Januar 2010 in Kraft tritt. Dieses stellt den Strafvollzug in Baden-Württemberg auf eine neue, rein landesrechtliche Rechtsgrundlage. Die bisherigen Landesgesetze über den Justizvollzug, das heißt das Jugendstrafvollzugsgesetz, das Justizvollzugsdatenschutzgesetz sowie ein Gesetz über die Verhinderung von Mobilfunkverkehr auf dem Gelände von Justizvollzugsanstalten wurden in ein vier Bücher umfassendes „Justizvollzugsgesetzbuch“ (JVollzGB) ebenso integriert wie landesrechtliche Regelungen, welche an die Stelle des Strafvollzugsgesetzes des Bundes treten. Nicht zuletzt wurde im Rahmen dieses Justizvollzugsgesetzbuchs das Untersuchungshaftrecht, für das gesetzliche Bestimmungen bis dato weitgehend fehlen, erstmals umfassend kodifiziert.

Das Justizvollzugsgesetzbuch hat aus datenschutzrechtlicher Sicht kaum Änderungen der bisherigen Rechtslage zur Folge. Denn das bisherige, am 1. August 2007 in Kraft getretene Justizvollzugsdatenschutzgesetz wurde weitgehend unverändert als „Abschnitt 7“ des ersten Buchs des Justizvollzugsgesetzbuchs übernommen und so gleichsam „vor die Klammer gezogen“. Der Geltungsanspruch der datenschutzrechtlichen Regelungen wurde dadurch nicht erweitert, denn schon nach dem bisher geltenden Recht waren die Bestimmungen des Justizvollzugsdatenschutzgesetzes umfassend für den Vollzug von gerichtlich angeordneten Freiheitsentziehungen in Justizvollzugsbehörden anzuwenden.

Freilich sind einige wichtige datenschutzrechtliche Fragen, namentlich Bestimmungen über die Überwachung der Besuche, des Schriftverkehrs und der Telefonate des Gefangenen, bisher nicht im Justizvollzugsdatenschutzgesetz geregelt gewesen. Auch im Justizvollzugsgesetzbuch wurden diesbezügliche Bestimmungen nicht in den besagten Abschnitt 7 des ersten Buchs integriert, sondern sind in den einzelnen Büchern über die Untersuchungshaft, den allgemeinen Erwachsenenstrafvollzug und den Jugendstrafvollzug enthalten. Da sich der Landesgesetzgeber jedoch an den Bestimmungen des Strafvollzugsgesetzes des Bundes orientiert hat, ergibt sich auch insoweit kein Bruch mit der bisherigen Praxis des Justizvollzugs.

Meine Dienststelle hatte im Übrigen Gelegenheit erhalten, bereits zu dem Referentenentwurf des Gesetzes Stellung zu nehmen. Einige unserer Detailanregungen sind in die endgültige Fassung des Gesetzes eingeflossen. Bedauerlich erscheint mir jedoch, dass der Landesgesetzgeber die Untersuchungshaft im Hinblick auf den Besucherverkehr, den Schriftwechsel des Untersuchungsgefangenen und dessen Telefonate weitgehend wie die normale Strafhaft behandelt. Meines Erachtens wäre es im Hinblick auf die – für den Untersuchungsgefangenen bis zu seiner etwaigen Verurteilung geltende – Unschuldsvermutung geboten gewesen, die Befugnis der Vollzugsbehörden, in elementare Grundrechte des Gefangenen einzugreifen, stärker zu beschränken.

Aus datenschutzrechtlicher Sicht ist zu bedauern, dass das Justizvollzugsgesetzbuch des Landes keine differenzierte Regelung für den Bereich der Untersuchungshaft vorsieht.

2. Kontrollbesuch bei der Neustart gGmbH, Einrichtung Heilbronn

Die Aufgaben der Bewährungshilfe, der Gerichtshilfe und des Täter-Opfer-Ausgleichs werden in Baden-Württemberg von der Neustart gGmbH wahrgenommen, die im Land neben der Stuttgarter Geschäftszentrale neun Einrichtungen unterhält. Bei einer dieser zentralen Standorte, der Einrichtung Heilbronn, haben wir Anfang 2008 einen Kontrollbesuch durchgeführt.

Seit 2007 werden die Aufgaben der Bewährungs- und Gerichtshilfe und des Täter-Opfer-Ausgleichs in Baden-Württemberg flächendeckend von der Neustart gGmbH wahrgenommen, einem freien Träger, der nach Maßgabe des § 7 Abs. 1 des Landesgesetzes über die Bewährungs- und Gerichtshilfe sowie die Sozialarbeit im Gerichtsvollzug (LBGS) beliehen worden ist. Bei der Neustart gGmbH handelt es sich um eine Tochter des österreichischen Vereins Neustart/Wien, welcher in unserem Nachbarland seit 50 Jahren justiznahe Sozialarbeit durchführt und bei der Schaffung ähnlicher Strukturen in Baden-Württemberg Pate stand.

Als beliehener Träger gilt die Neustart gGmbH gemäß § 2 Abs. 2 Satz 3 LDSG ungeachtet dessen, dass sie ihrer Rechtsform nach eine juristische Person des Privatrechts ist, aus datenschutzrechtlicher Sicht als öffentliche Stelle, soweit sie die ihr übertragenen hoheitlichen Aufgaben der öffentlichen Verwaltung wahrnimmt. Vor diesem Hintergrund entschloss sich mein Vorgänger, bei einer ausgewählten Einrichtung der Neustart gGmbH Anfang 2008 eine Kontrolle durchzuführen, um sich ein Bild von der Organisation und den Abläufen einer typischen Organisationseinheit der Neustart gGmbH zu machen. Die Wahl fiel auf Heilbronn.

Um es vorwegzunehmen: Die Kontrolle hat keine schwerwiegenden datenschutzrechtlichen Mängel an den Tag gebracht. Vielmehr machte die Einrichtung Heilbronn insgesamt einen guten Eindruck.

Das besondere Augenmerk galt der sog. Klientendokumentation „KliDoc“, welche unter Verwendung eines Accounts einer Mitarbeiterin aus der Einrichtung Heilbronn vor Ort stichprobenweise geprüft wurde. Es handelt sich bei KliDoc um ein automatisiertes Verfahren zur Dokumentation der Betreuung der Probanden, welches ursprünglich vom Verein Neustart/Wien entwickelt worden ist. Dieser betreibt denn auch die IT-Infrastruktur für die Anwendung, auf welche die Neustart gGmbH über einen Browser zugreift. Rechtlich ist diese grenzüberschreitende Kooperation zwischen der deutschen Neustart gGmbH und ihrer österreichischen „Mutter“ in einem Vertrag geregelt, welcher die Administration der Klientendokumentation durch den Verein „Neustart/Wien“ als Datenverarbeitung im Auftrag ausweist, das heißt als eine Datenverarbeitung, für welche der Auftraggeber – also die Neustart gGmbH – in datenschutzrechtlicher Hinsicht allein verantwortlich bleibt. Dass der Auftragnehmer in Österreich ansässig ist, stellt dabei kein grundsätzliches Problem dar, da öffentliche Stellen nach Maßgabe des § 3 Abs. 5 LDSG nicht nur inländische Stellen, sondern auch Personen und Stellen aus anderen Mitgliedstaaten der Europäischen Union mit der Verarbeitung personenbezogener Daten im Auftrag betrauen dürfen. Nicht verschwiegen sei allerdings, dass die Arbeit mit KliDoc im Hinblick auf die berufliche Schweigepflicht staatlich anerkannter Sozialarbeiter und staatlich anerkannter Sozialpädagogen bei manchen Beteiligten dennoch Vorbehalten begegnet; diese Kontroverse war jedoch nicht Gegenstand unserer Vor-Ort-Kontrolle.

In KliDoc werden neben den Personalien des Probanden und dessen Angaben zu seiner beruflichen, finanziellen, sozialen und gesundheitlichen Situation auch Daten über den erteilten Auftrag und den gerichtlichen Auftraggeber, die Ziele der Betreuung, die Betreuungskontakte sowie gegebenenfalls auch Daten einer Lebenspartnerin bzw. eines Lebenspartners des Klienten dokumentiert. Die Erhebung und Speicherung dieser personenbezogenen Daten muss sich am datenschutzrechtlichen Grundsatz der Erforderlichkeit

messen lassen. Es konnte jedoch nicht festgestellt werden, dass einzelne Datenfelder, welche die Klientendokumentation ausweislich ihres Verfahrensverzeichnisses dem Sachbearbeiter zur Verfügung stellt, schlechthin überflüssig wären. Freilich steht – wie wir in unserem Kontrollbericht an die Neustart gGmbH betont haben – der zuständige Bewährungshelfer in der Pflicht, eigenverantwortlich zu prüfen, welche dieser Informationen für die Bearbeitung des konkreten Bewährungshilfefalles im strengen datenschutzrechtlichen Sinne erforderlich, das heißt unverzichtbar sind, und die Datenerhebung auf diese zu beschränken.

Neben Art und Umfang des gespeicherten Datenbestandes war insbesondere die Struktur der vergebenen Zugriffsberechtigungen im Rahmen der Klientendokumentation von Interesse. Wesentliche Mängel vermochten meine Mitarbeiter jedoch auch insoweit nicht festzustellen.

Erhebliche Bedenken bestanden jedoch im Hinblick auf den geplanten ergänzenden Einsatz mobiler Speichermedien. Damit hat es folgende Bewandtnis: Das Bewährungshilfekonzept der Neustart gGmbH sieht vor, bei der Betreuung ihrer Probanden neben hauptamtlichen Mitarbeitern in geeigneten Fällen vermehrt auch ehrenamtliche Bewährungshelfer einzusetzen. Diese ehrenamtlichen Mitarbeiter erhalten jedoch keinen Zugang zur Klientendokumentation; stattdessen soll ihnen – nach einer zum Zeitpunkt des Kontrollbesuchs zumindest in Heilbronn allerdings noch nicht realisierten Planung – jeweils ein kennwortgeschützter USB-Stick mit personenbezogenen Daten des Probanden zur weiteren Verarbeitung am heimischen Computer zur Verfügung gestellt werden.

Um den evidenten datenschutzrechtlichen Risiken einer solchen Praxis entgegenzuwirken, gibt die Neustart gGmbH den ehrenamtlichen Bewährungshelfern umfangreiche organisatorische Regelungen zum Umgang mit den USB-Sticks an die Hand; so werden ihnen Vorgaben zur Nutzung von Sicherheitssoftware wie etwa einer Firewall und eines Virenscanners am Computer gemacht. Da es sich hierbei jedoch um Computer handelt, die sich im Privatbesitz der ehrenamtlichen Bewährungshelfer befinden, können diese auf vollkommen unterschiedliche Weise und mit der Software verschiedenster Hersteller installiert und konfiguriert sein. Hinzu kommt noch, dass nicht jedermann gleichermaßen im Umgang mit Computern versiert ist. Daher halte ich es für sehr fraglich, ob alle Ehrenamtlichen mit solchen Vorgaben praktisch zurechtkommen. Andere Unwägbarkeiten kommen hinzu: So mag ein anderer Nutzer, etwa ein Familienangehöriger, ohne Wissen des ehrenamtlichen Bewährungshelfers die Konfiguration des Computers verändern und dadurch das Sicherheitsniveau verringern. Im schlimmsten Fall steht zu befürchten, dass sensible Probandendaten ungeachtet entgegenstehender Vorgaben am Ende doch auf privaten Rechnern gespeichert werden, sei es infolge schlichter Bedienungsfehler, sei es durch technische Mechanismen, etwa durch eine aktivierte Wiederherstellungsfunktion oder durch vom Betriebssystem automatisch angefertigte Speicherabbilder.

Mein Vorgänger hat in seinem Kontrollbericht daher dezidiert davon abgeraten, Probandendaten mittels USB-Sticks in Umlauf zu setzen. In einer ersten Reaktion hierauf hat die Neustart gGmbH sich zwar gesprächsbereit gezeigt, jedoch darauf hingewiesen, dass insoweit auch wirtschaftliche Aspekte eine Rolle spielten. Dies kann – bei allem Verständnis dafür, dass auch ein freier Träger sparsam zu wirtschaften hat – aus datenschutzrechtlicher Warte sicherlich nicht das letzte Wort sein.

Die Einrichtung Heilbronn hat aus datenschutzrechtlicher Sicht insgesamt einen positiven Eindruck hinterlassen. Ich bleibe mit der Neustart gGmbH wegen datenschutzrechtlicher Anforderungen im Gespräch und werde die weitere Entwicklung aufmerksam beobachten.

3. Teil: Bildungsbereich

1. Von Schlüsselszenen und Lernspuren – der Orientierungsplan für Bildung und Erziehung in baden-württembergischen Kindergärten und weiteren Kindertageseinrichtungen

Der „Orientierungsplan für Bildung und Erziehung in baden-württembergischen Kindergärten und weiteren Kindertageseinrichtungen" sollte ursprünglich ungeachtet einer fehlenden normenklaren Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten verbindlich eingeführt werden.

Der o. g. Orientierungsplan, der in seiner ursprünglichen Fassung für eine Pilotphase bereits 2006 vom Kultusministerium herausgegeben worden war, enthält in der aktuellen Fassung auf über 146 Seiten eine Fülle von Ausführungen, etwa über das Grundverständnis von Bildung und Erziehung, die sich daraus ergebenden Ziele und die Kooperationsfelder des Kindergartens sowie konkrete Anhaltspunkte für die pädagogische Arbeit. Dabei hängt er die Messlatte fachlich sehr hoch. Dies hat zur Folge, dass die Umsetzung des Orientierungsplans in der praktischen Arbeit mit nicht unerheblichem Aufwand verbunden ist, der auf kommunaler Seite bereits zum Hinweis auf die finanziellen Folgen geführt hat (Stichwort: Konnexitätsprinzip).

Auch datenschutzrechtlich ist der Plan von Brisanz: Insbesondere die Aussagen zur „verpflichtenden Dokumentation von Entwicklungsverläufen und Bildungsprozessen" und zu „Fotos von Schlüsselszenen oder Videosequenzen", die, „unter der Voraussetzung, dass Eltern damit einverstanden sind", „greifbare Lernspuren einer persönlichen Bildungsbiografie" bilden sollen, werfen die Frage auf, aus welcher gesetzlichen oder sonstigen Vorschrift sich die Verpflichtung zur Dokumentation von Entwicklungsverläufen und Bildungsprozessen eigentlich ergeben soll. Denn auch dem Kultusministerium sollte bekannt sein, dass es für Eingriffe in das informationelle Selbstbestimmungsrecht einer normenklaren gesetzlichen Grundlage oder gegebenenfalls einer Einwilligung der Betroffenen bedarf. Die mir zunächst entgegengehaltenen Vorschriften des Gesetzes über die Betreuung von Kindern in Kindergärten, anderen Kindertageseinrichtungen und der Kindertagespflege (KiTaG) oder des Achten Buchs des Sozialgesetzbuchs (SGB VIII) haben im Wesentlichen programmatischen Charakter und sind im Hinblick auf den mit der verbindlichen Umsetzung des Orientierungsplans verbundenen Grundrechtseingriff nicht normenklar genug. Die vom Kultusministerium ebenfalls angedachte Lösung über den Abschluss öffentlich-rechtlicher Vereinbarungen mit (notwendigerweise allen!) kommunalen und kirchlichen Trägern von Kindergärten und weiteren Kindertageseinrichtungen halte ich weder für praktikabel noch – im Hinblick auf die Einbeziehung der Kinder bzw. Erziehungsberechtigten – für einen gleichwertigen Ersatz einer gesetzlichen Regelung. Schließlich wäre es bei dieser Variante erforderlich, dass die Erziehungsberechtigten völlig freiwillig der Anwendung des Orientierungsplans in Bezug auf ihr Kind zustimmen.

Die Fragestellung nach dem Rechtscharakter und den Rechtsfolgen zog sich wie ein roter Faden durch alle hier bearbeiteten Fälle, seit mein Amt 2007 aufgrund einer Eingabe erstmals mit dem Orientierungsplan befasst war. Zwar hat das Kultusministerium inzwischen erklärt, der Orientierungsplan solle keine förmliche Verwaltungsvorschrift darstellen; damit bleibt jedoch mangels gesetzlicher Grundlage offen, welche der darin enthaltenen Aussagen tatsächlich rechtliche Verbindlichkeit beanspruchen. Diese Fragen haben durchaus praktische Bedeutung: Für die kommunalen Kindergartenträger landauf, landab war, wie sich in vielen Anfragen zeigte, vielfach unklar, ob sie sich an die Vorgaben des Orientierungsplans halten müssen oder ob diese nur den Charakter von Anregungen und Empfehlungen haben. Damit waren diese Kindergartenträger zwangsläufig oft auch nicht in der Lage, den Eltern der Kindergartenkinder klare Informationen zu vermitteln, insbesondere für die gesetzlich gebotene Aufklärung der Eltern bei der Einholung der datenschutzrechtlichen Einwilligung für Foto- und Filmaufnahmen von ihren Kindern zu sorgen. Auf dieses Problem hat mein Amtsvorgänger bereits vor Jahren auch das Kultusministerium schriftlich hingewiesen. Ich habe den Eindruck, dass diese Hinweise leider längere Zeit

nicht die nötige Beachtung gefunden haben. Erst in diesem Jahr kam auf wiederholtes Nachfassen von mir endlich Bewegung in die Sache. Ich habe dem Kultusministerium, aber auch anderen maßgeblichen Beteiligten, beispielsweise von kommunaler und kirchlicher Seite, die datenschutzrechtlichen Anforderungen auch persönlich eingehend erläutert. Ich denke, dass die Botschaft nun beim Kultusministerium angekommen ist.

Festzuhalten bleibt, dass die fachliche und handwerkliche Arbeit am Entwurf des Orientierungsplans zunächst einmal zu Ende gebracht werden muss. Hierzu gehört auch die Klärung der wesentlichen Rechtsfragen. Selbstverständlich werde ich das Kultusministerium bei Bedarf im Rahmen meiner Möglichkeiten auch weiterhin beraten und unterstützen; seine Hausaufgaben muss das Ministerium aber zunächst selbst erledigen.

Ungeachtet der anerkennenswerten pädagogischen Zielsetzung, die aus dem Orientierungsplan spricht, sollte die Landesregierung noch einmal selbstkritisch prüfen, ob eine verbindliche Einführung wirklich das Gebot der Stunde ist. Meines Erachtens könnte der Orientierungsplan als pädagogische „Handreichung“ oder als programmatischer „Leitfaden“ für die kommunalen und kirchlichen Einrichtungsträger eine ebenso wertvolle „Orientierung“ wie ein verbindlicher „Plan“ bieten, den Trägern aber die Art und Weise der Umsetzung freistellen. Jenseits der ungeklärten Frage nach einer hinreichenden Rechtsgrundlage bestehen meinerseits auch unter dem Aspekt der Datenvermeidung und Datensparsamkeit generelle Bedenken gegen immer stärker ausufernde Beobachtungs- und Dokumentationspflichten im Kontext von menschlicher Zuwendung und sozialer Betreuung. Die Erfahrungen im Krankenhaus- und Pflegebereich haben zumindest eines deutlich gemacht: Die Zeit, die für die Dokumentation erforderlich ist, steht für die persönliche Zuwendung nicht mehr zur Verfügung.

Am 24. November 2009 haben sich das Land und die Kommunalen Landesverbände über eine stufenweise Umsetzung des Orientierungsplans verständigt. Danach soll dem steigenden Betreuungsaufwand durch einen verbesserten Personalschlüssel Rechnung getragen werden. Zur Verbindlichkeit des Orientierungsplans wurde etwas kryptisch erklärt, dass es – entsprechend den Prinzipien von Pluralität, Trägerautonomie und Konzeptvielfalt – in der Verantwortung der Träger und Einrichtungen stehe, wie die im Orientierungsplan genannten Ziele im pädagogischen Alltag erreicht werden.

Ob der Orientierungsplan in der weiteren Umsetzung mehr „Orientierung“ oder mehr „Plan“ sein wird, wird sich zeigen. Ich bleibe dabei: Frühkindliche Entwicklungsverläufe und Bildungsprozesse sollten allenfalls bei konkretem Bedarf und auch dann nur auf wirklich freiwilliger Basis dokumentiert und ausgewertet werden.

2. „Kompetenzanalyse Profil AC“ – ohne datenschutzrechtliche Kompetenz?

Schulleiter werden mit datenschutzrechtlichen Problemen offenbar vielfach allein gelassen. Dies gilt auch für ein landesweites EDV-Verfahren, das an Haupt- und Sonderschulen eingesetzt wird.

Durch die Lektüre der LT-Drucksache 14/4379 vom 22. April 2009 bin ich auf das an allen Haupt- und Sonderschulen in Baden-Württemberg eingesetzte EDV-Verfahren „Kompetenzanalyse Profil AC“ aufmerksam geworden. Mit diesem Verfahren werden sensible, personenbezogene Daten verarbeitet, denn es sollen die Stärken und Schwächen der Schülerinnen und Schüler erkannt und dargestellt sowie individuelle Kompetenzprofile erstellt werden. Bedauerlich war hierbei zunächst, dass ich erst auf diesem Wege von dem Verfahren erfuhr. Das Kultusministerium hatte mich vorher nämlich nicht eingeweiht und auch die beteiligten Schulen hatten meinem Amt die nach § 11 LDSG vorgeschriebenen Verfahrensverzeichnisse bis dahin nicht übermittelt. Warum diese Verzeichnisse sinnvoll sind, darauf gehe ich im 7. Teil dieses Tätigkeitsberichts unter Nr. 2 ein. Daraufhin habe ich mich an das Kultusministerium gewandt, welches mir mitteilte, dass das automatisierte Verfahren bereits seit dem Schuljahr 2007/2008 laufe, und bestätigte, dass hierbei tatsächlich besonders sensible Daten von Schülern

verarbeitet würden. Verantwortliche Stelle im Sinne des Landesdatenschutzgesetzes sei aber die jeweilige Schule, die das Verfahren einsetze; da die Schulen in der Regel keinen Datenschutzbeauftragten hätten, lägen die Voraussetzungen des § 11 Abs. 2 LDSG grundsätzlich vor. Aufgrund bestimmter Umstände und Erwägungen (angeführt wurde die „Verwaltungsvereinfachung"), habe das Ministerium jedoch darauf verzichtet, die Schulen anzuweisen, meiner Dienststelle jeweils ein Verfahrensverzeichnis zu übersenden. Nun ist zwar die Verwaltungsvereinfachung ein wichtiges Ziel, dass aber ein Ministerium mir mitteilt, es halte aus diesem Grund die Erfüllung gesetzlicher Pflichten nicht für erforderlich, ist zumindest ungewöhnlich. Denn § 32 Abs. 1 LDSG sieht vor, dass öffentliche Stellen Verfahrensverzeichnisse nur dann meinem Amt nicht zu übermitteln haben, wenn sie einen behördlichen Datenschutzbeauftragten bestellt haben.

Zur weiteren Klärung habe ich mir zunächst vom Kultusministerium eine Liste der beteiligten Schulen übersenden lassen, daraus 21 zufällig ausgewählte Schulen direkt angeschrieben und um Auskunft zum Einsatz des Verfahrens „Kompetenzanalyse Profil AC" sowie um Vorlage des Verfahrensverzeichnisses gebeten. Obwohl in diesem Schreiben die Pflicht, mein Amt bei der Ausübung seiner Aufgaben zu unterstützen, explizit angesprochen wurde, hat rund die Hälfte der angeschriebenen Schulen innerhalb der eingeräumten Frist überhaupt keine Stellungnahme abgegeben, was jeweils eine förmliche Beanstandung gemäß § 30 LDSG nach sich zog. Diese Tatsache sowie die Antworten der anderen Schulen und diverse Telefonkontakte lassen den Schluss zu, dass im Schulbereich offenbar teilweise elementare datenschutzrechtliche Grundkenntnisse fehlen. Einige Schulleiter räumten mit entwaffnender Offenheit ein, dass man sich keiner datenschutzrechtlichen Verantwortung bewusst und das Verfahren zentral vorgegeben worden sei. Dieses Eingeständnis steht in krassem Gegensatz zu der Aussage des Kultusministeriums, wonach die jeweilige Schule die datenschutzrechtlich verantwortliche Stelle sei; dies scheint den Schulen bzw. den Schulleitern aber niemand gesagt zu haben.

Soweit öffentliche Schulen das Verfahren einsetzen und keine Eintragungen in das Verfahrensverzeichnis gemacht haben, verstößt dieses Verhalten der Schulen zudem auch gegen die vom Kultusministerium selbst erlassene Verwaltungsvorschrift „Verarbeitung personenbezogener Daten durch öffentliche Schulen und Einsichtnahme in schulische Prüfungsunterlagen und deren Aushändigung" vom 2. August 2005. Im Rahmen unserer Kontakte äußerten insbesondere die Schulleiter immer wieder, dass diese Verwaltungsvorschrift entweder nicht bekannt sei oder von einem juristischen Laien nicht verstanden und nicht als hilfreich betrachtet würde.

Mittlerweile hat das Ministerium für Kultus, Jugend und Sport reagiert und an die betroffenen Schulen ein Muster für ein Verfahrensverzeichnis herausgegeben. Die daraufhin in meinem Amt eingegangenen Verfahrensverzeichnisse waren jedoch vielfach unvollständig und inhaltlich nicht korrekt; teilweise wurde das Formular ohne Eintragungen übersandt. Daher war es mir bis heute nicht möglich zu überprüfen, ob und inwieweit die datenschutzrechtlichen Vorschriften durch die Anwendung des Verfahrens „Kompetenzanalyse Profil AC" eingehalten werden. Mir drängt sich nicht nur in diesem Zusammenhang der Eindruck auf, dass die Schulen bzw. die Schulleiter, die in erster Linie ihren pädagogischen Auftrag im Auge haben und auch sonst vielfältigen Herausforderungen ausgesetzt sind, in datenschutzrechtlicher Hinsicht ziemlich allein gelassen werden. Hierfür sprechen auch die deutlichen Worte, die von Seiten einiger verunsicherter Schulleiter an meine Mitarbeiter bei Nachfragen zu dem genannten EDV-Verfahren gerichtet wurden. So wurde wiederholt völliges Unverständnis dafür geäußert, dass

a) erst das Verfahren „von Stuttgart" aus vorgegeben wurde,

b) in Schulungsveranstaltungen erklärt worden sei, datenschutzrechtlich sei „alles in Ordnung", und

c) gewissermaßen als „krönender Abschluss" nun meine Kritik komme.

Dabei wurde vereinzelt auch freimütig eingeräumt, dass man weder wisse, was ein Verfahrensverzeichnis sei, noch die datenschutzrechtlichen Anforderungen kenne; auch die Bemerkung, dass man „Wichtigeres" zu tun habe,

bekamen wir zu hören. Auch ich habe Verständnis dafür, dass der Datenschutz bei den Schulleitern nicht ganz oben auf der Agenda steht. Nur: So, wie es derzeit läuft – oder besser: nicht läuft –, kann es im Schulbereich nicht bleiben.

Aus meiner Sicht sollten die Schulen bzw. Schulleiter von der Kultusverwaltung datenschutzrechtlich stärker „an die Hand" genommen und hierdurch zugleich entlastet werden. Ob allein Schulungen ausreichen, um die erkannten Defizite auszugleichen, scheint mir fraglich. Zielführender dürfte es sein, wenn bestimmte Stellen innerhalb der Kultusverwaltung, sei es auf Kreisebene oder auf Ebene der Regierungsbezirke oder in einer zentralen Einrichtung des Ressorts, für die Schulen die Rolle der behördlichen Datenschutzbeauftragten nach § 10 Abs. 2 LDSG übernehmen und die Schulen zielgerichtet betreuen.

3. „Offene Mathe-Foren" und eine Vielzahl anderer Probleme an einem Gymnasium

Im Schulbetrieb lauern zahlreiche datenschutzrechtliche Fallstricke. Das Problembewusstsein der Verantwortlichen ist manchmal aber nur schwach ausgeprägt.

Es begann damit, dass mein Amt durch besorgte Eltern auf ein sog. „Mathe-Forum" an einem Gymnasium angesprochen wurde. Dabei müssten, so hieß es, Schülerinnen und Schüler von insgesamt vier Klassen benotete Mathematik-Übungen machen. Wer sich nicht daran halte und nicht wöchentlich teilnehme, bekomme eine schlechte Benotung. Meine Mitarbeiter gingen der Sache sogleich nach und mussten feststellen, dass im Internet-Angebot des Gymnasiums zu den dort betriebenen „Mathe-Foren" eine Vielzahl von Namen, insbesondere von Schülerinnen und Schülern, und diesen zuordenbare weitere Angaben frei abrufbar waren. Somit konnte weltweit jeder, der über einen Internet-Zugang verfügt, lesen, wie sich welche Gymnasiasten und punktuell auch die Lehrkraft mit Blick auf die Mathematikaufgaben äußerten. Dabei ergab sich, wie stets im realen Leben, kein Bild problemloser und perfekter Bewältigung der Aufgaben. Es drängten sich in einigen Fällen – stets auf die mit vollem Namen genannten Gymnasiasten beziehbar – vielmehr die heiklen Fragen auf, ob denn alle Aufgaben mit dem nötigen Engagement, Ernst und Sachverstand bearbeitet werden oder ob hier Defizite zu beklagen sind. Daraufhin bat mein Amt die Schule rasch um kurzfristige Stellungnahme zu den hier eingegangenen Mitteilungen sowie zum Ergebnis unserer eigenen Internet-Recherche und wies zudem darauf hin, dass die Schule gegebenenfalls eine nun selbst als rechtswidrig erkannte Datenverarbeitung unverzüglich zu beenden hat.

Die Schule reagierte prompt, zunächst in Gestalt der Lehrkraft, die diese „Mathe-Foren" konzipiert und eingesetzt hatte. Dabei zeigte sich, um mit dem Erfreulichen zu beginnen, dass die datenschutzrechtlich illegalen „Mathe-Foren" auf unser Schreiben sofort abgestellt worden waren. Unerfreulich und besorgniserregend war dagegen, dass die Schule, auch in den späteren Äußerungen des Schulleiters, ein tiefgreifendes Unverständnis für datenschutzrechtliche Anforderungen und somit gravierende Defizite und Probleme erkennen ließ. Jedenfalls war der dringende Beratungs- und Kontrollbedarf augenfällig und führte zu einem Vor-Ort-Termin an der Schule. Die eingehende Beratung durch meine Mitarbeiter fiel allerdings beim Schulpersonal auf unfruchtbaren Boden. Die Schulleitung äußerte zwar wiederholt, auch unter Hinweis auf die einschlägige Verwaltungsvorschrift des Kultusministeriums zur Verarbeitung personenbezogener Daten durch öffentliche Schulen, dass man den Datenschutz als wichtig betrachte und ernst nehme. Im Gesamtbild erwiesen sich diese Worte leider als bloße Lippenbekenntnisse. Zur Erklärung wurde mehrfach geltend gemacht, dass die Verwaltungsvorschrift des Kultusministeriums unverständlich und somit für die Schule nicht hilfreich sei. So verwundert es nicht, dass der Schulleiter sich kaum um diese „Mathe-Foren" und deren datenschutzrechtliche Zulässigkeit gekümmert und stattdessen auf die Aussage der zuständigen Lehrkraft verlassen hatte, dass „alles in Ordnung" sei. Im Hinblick auf die Vorbildfunktion, die Lehrkräfte gegenüber den Schülerinnen und Schülern auch

in Sachen des Datenschutzes haben, war das offen erkennbare Desinteresse des Schulleiters weder verständlich noch akzeptabel.

Die datenschutzrechtliche Kontrolle brachte zudem weitere Verstöße zutage: So wurde beispielsweise gravierend gegen die Vorschriften des Landesdatenschutzgesetzes über die Datenverarbeitung im Auftrag verstoßen. Am Gymnasium waren, allein zu schulischen Zwecken und in schulischer Verantwortung, verschiedene automatisierte Verfahren im Einsatz. Sämtliche administrativen Aufgaben in Zusammenhang mit dem technischen Betrieb dieser Verfahren wurden vollumfänglich durch den städtischen Schulträger wahrgenommen. Die nach dem Landesdatenschutzgesetz für solche Situationen vorgesehene schriftliche Auftragserteilung durch die Schule war aber unterblieben. Es war auch nicht feststellbar, dass dies wenigstens mündlich erfolgt war. Die Schule war sich vielmehr ihrer Verantwortung gar nicht bewusst gewesen und hatte den Mitarbeitern meines Amts zu erklären versucht, das Kultusministerium oder dem Gymnasium übergeordnete Stellen der Kultusverwaltung seien hier im Sinne des Landesdatenschutzgesetzes verantwortlich. Für keines dieser Verfahren existierte ein Verfahrensverzeichnis, wie es für die automatisierten Verfahren einer öffentlichen Stelle nach § 11 LDSG vorgeschrieben ist. Weitere Mängel zeigten sich im technischen und organisatorischen Bereich. So befanden sich beispielsweise Tagebücher unbeaufsichtigt und frei zugänglich im Flur vor dem Sekretariat. Diese Tagebücher enthalten erfahrungsgemäß u. a. Krankheits- und Fehlzeiten von Schülerinnen und Schülern sowie Eintragungen wegen Zuspätkommens und disziplinarische Einträge. Der Hinweis des Schulleiters, dass diese Dokumente über Nacht im Sekretariat eingeschlossen würden und derzeit keine Schüler mehr im Haus seien, half nicht darüber hinweg, dass eine unbefugte Kenntnisnahme der darin enthaltenen personenbezogenen Daten am Tag des Kontrollbesuchs tatsächlich möglich war, zumal sich am Ende des Kontrollbesuchs gezeigt hat, dass durchaus noch Schüler in der Schule zugegen waren.

Auf den Internet-Seiten der Schule befanden sich für jedermann frei zugänglich Bilder von – ehemaligen – Schülern, teilweise in Großaufnahmen. Keiner der auf diesen Bildern vorhandenen Schüler hatte, wie sich leider zeigte, eine schriftliche Einwilligungserklärung für diese Verarbeitung personenbezogener Daten erteilt. Beim Kontrollbesuch sicherte der Schulleiter zu, diese Bilder schnellstmöglich zu entfernen. Jedoch waren diese Bilder auch nach dem Kontrollbesuch für einige Tage immer noch auf der Internet-Seite vorhanden.

Mein Amtsvorgänger hat alle festgestellten Verstöße gegenüber dem Kultusministerium förmlich nach § 30 LDSG beanstandet. Das Ministerium nahm daraufhin gegenüber meinem Amt zu den einzelnen Punkten Stellung und erklärte dabei u. a., das Regierungspräsidium sei gebeten worden, mit dem Schulleiter ein Gespräch zu führen, ihn auf die Verpflichtung zur Einhaltung der einschlägigen datenschutzrechtlichen Bestimmungen hinzuweisen sowie diese bei Bedarf zu erläutern. Dies ist im Ergebnis zu begrüßen. Es wird aber auch deutlich, welch hoher Aufwand für derartige „Nach- und Aufräumarbeiten“ entfaltet werden muss, wenn es am nötigen Datenschutzbewusstsein fehlt.

Die Schulen sollten von der Kultusverwaltung auch in datenschutzrechtlicher Hinsicht stärker betreut werden. Bislang besteht gelegentlich der Eindruck, dass sich die jeweiligen Schulen und die Kultusverwaltung die datenschutzrechtliche Verantwortung für die an den Schulen eingesetzten Verfahren gegenseitig zuschieben wollen.

4. Die Tücken des Verfahrens „winprosa“

Auf einen Hinweis aus dem Kreis datenschutzbewusster Abiturienten befasste sich mein Amt im Berichtszeitraum auch mit dem EDV-Verfahren „winprosa“. Dieses wird von einer Privatfirma vermarktet und, so war im Verlauf der datenschutzrechtlichen Prüfung zu erfahren, an beinahe allen baden-württembergischen Gymnasien eingesetzt, hauptsächlich zur Verwaltung der von den Schülerinnen und Schülern gewählten Kurse sowie zur Erfassung und Bearbeitung von Schülerleistungsdaten (Noten und Zeugnis-

sen) in der gymnasialen Oberstufe. Insider behaupteten nun, dass es für Abiturienten, deren Daten mit „winprosa“ verwaltet werden, mit relativ einfachen Mitteln, etwa durch wiederholtes Ausprobieren, möglich sei, die Daten der anderen Abiturienten auszuspähen. Ein rascher Kontrollbesuch bei einem Gymnasium im Großraum Stuttgart ließ mehrere datenschutzrechtliche Mängel erkennen. Von besonderer Bedeutung war die mangelnde Datenträger-, Zugriffs- und Transportkontrolle. Im Einzelnen:

Schülern wurden für unterschiedliche Zwecke Datenexporte aus dem System zur Verfügung gestellt:

- Schüler der Klassenstufe 11 erhielten einen Export zur Zusammenstellung ihrer Kurswahl.
- Die Schüler der Oberstufen erhielten ein Jahrgangspaket, in dem sie ihre Noten sehen und zudem vom System Varianten durchrechnen lassen konnten, welche Abiturnote sie in Abhängigkeit von welcher Klausurnote bzw. Zeugnisnote erhalten würden.
- Für die Schüler der Klassenstufe 13 stand eine Exportfunktionalität zur Auswahl der Prüfungsthemen im Abitur bereit.

Diese Exporte wurden den Schülern per Downloadmöglichkeit auf der Internet-Seite der Schule oder auf den vernetzten Computern im sog. Schülernetz in einem Computerraum der Schule, zu dem Schüler mitunter auch ohne ständige Aufsicht der Lehrkörper Zugang hatten, angeboten. Die Datenexporte enthielten grundsätzlich jeweils den gesamten aktuellen Datenbestand – verschlüsselt – eines Jahrgangs, auch die zum Zeitpunkt des Exports in das System bereits eingegebenen Noten. Die Exporte bestanden aus verschiedenen einzelnen Dateien, wobei eine Datei die eigentlichen Daten mit den Namen der Schülerinnen und Schüler und den jeweils gewählten Fächern und Bewertungen enthielt. In einer anderen Datei wurden die für den jeweiligen Export erteilten Zugriffsberechtigungen hinterlegt. Die Schülernamen waren in einer weiteren Datei im Klartext lesbar. Durch die Zugriffsberechtigung sollte eigentlich geregelt werden, dass ein Schüler nur seine eigenen Daten sehen kann. Dazu erhielt jeder Schüler ein Login, das aus dem Abiturjahr und der persönlichen Schülernummer bestand, sowie ein Passwort, welches sich aus den letzten vier Ziffern der in einem Schulverwaltungssystem automatisch vergebenen Schüler-ID zusammensetzte. Eine automatische Sperrung nach einer definierten Anzahl von Fehleingaben fand nicht statt.

Die Exportdateien für die oben genannten drei Anwendungsfälle bestanden jeweils u. a. aus den Daten „Schülername“, „gewählte und bereits besuchte Kurse“ sowie „Zeugnisnoten“ und enthielten somit mehr als nur die persönlichen Daten eines einzelnen Schülers, nämlich auch die Daten aller Mitschüler eines Jahrganges. Auch der besuchte Religionsunterricht war auslesbar. Zwar lagen diese Informationen verschlüsselt vor und über eine Berechtigungsverwaltung war zunächst geregelt, dass ein Schüler nur seine eigenen Daten sehen konnte. Es war jedoch durchaus wahrscheinlich, dass ein Schüler das Passwort eines Mitschülers erraten konnte, zumal die Regeln, aus denen sich Benutzername und Passwort zusammensetzten, im frei zugänglichen Handbuch von „winprosa“ (Downloadmöglichkeit auf der Internet-Seite des Herstellers der Software) für alle Schüler verfügbar waren. Zudem war es aufgrund eines fehlenden Sperrmechanismus bei Falscheingaben möglich, durch einfaches „Herumprobieren“ oder auch durch ein einfach zu programmierendes Tool zur automatisierten Simulation von Passworteingaben an Daten Dritter heranzukommen.

Meine Mitarbeiter haben daher bereits am Tag nach dem Kontrollbesuch das Gymnasium – als Sofortmaßnahme – darum gebeten, dieses potenzielle Risiko auszuschließen und die Exportfunktionalität für Schüler nicht mehr zu verwenden. Zudem sollte die Downloadmöglichkeit im Internet deaktiviert werden. Es ist zu begrüßen, dass diese Deaktivierung noch am selben Tag erfolgte.

Insgesamt konnten die mit dem Verfahren verbundenen datenschutzrechtlichen Probleme ausgeräumt werden, ohne dass es einer Beanstandung durch meinen Amtsvorgänger bedurfte.

5. Prüfungspläne mit Namen von Abiturienten haben im Internet nichts zu suchen

Meine Dienststelle wurde von aufmerksamen Bürgerinnen und Bürgern darauf hingewiesen, dass ein bestimmtes Gymnasium vollständige Listen aller Abiturienten in Form der Teilnahmelisten an den mündlichen bzw. Präsentationsprüfungen im Internet veröffentlichte. Die von meinen Mitarbeitern im Internet daraufhin durchgeführten Stichproben ergaben auch bei anderen Gymnasien ein ähnliches Bild: Die Veröffentlichungen enthielten neben den Namen und Vornamen der Schülerinnen und Schüler bestimmter, auch bereits zurückliegender Abiturjahrgänge Angaben über deren jeweilige Prüfungsfächer und die Tage und Uhrzeiten, an denen bestimmte Prüfungen abzulegen waren.

Um es sogleich auf den Punkt zu bringen: Eine solche weltweite Streuung personenbezogener Daten im Internet ist mit den dienstlichen Erfordernissen der Gymnasien in keiner Weise zu rechtfertigen und somit ohne die Einwilligung der betroffenen Schülerinnen und Schüler oder gegebenenfalls der jeweiligen Erziehungsberechtigten schlicht illegal. Datenschutzrechtliche Einwilligungen wurden in den von meinem Amt geprüften Fällen offenbar nicht erteilt. Nachdem eines der Gymnasien die Pläne nach Erhalt eines kritischen Hinweises sofort aus dem Internet entfernte, sah mein Amtsvorgänger davon ab, den mit der Veröffentlichung der Prüfungspläne verbundenen Rechtsverstoß förmlich zu beanstanden. Es ist aus datenschutzrechtlicher Sicht natürlich sehr zu begrüßen, wenn ein Gymnasium auf einen kritischen und berechtigten Hinweis umgehend reagiert und die Situation bereinigt. Gleichwohl sollten personenbezogene Daten erst dann im Internet veröffentlicht werden, wenn eine sorgfältige Prüfung ergab, dass dies datenschutzrechtlich zulässig ist. Nur dann können rechtswidrige Eingriffe in das Recht auf informationelle Selbstbestimmung von Schülerinnen und Schülern oder anderen Betroffenen wirksam vermieden werden.

Wegen der Bedeutung dieser Sache für verschiedene Gymnasien in Baden-Württemberg hat mein Vorgänger auch das Kultusministerium darum gebeten, sich in eigener Verantwortung mit dem Thema zu befassen und auf die Beachtung datenschutzrechtlicher Vorschriften hinzuwirken; schließlich ist das Kultusministerium oberste Schulaufsichtsbehörde. Das Ministerium hat die Gymnasien in Baden-Württemberg inzwischen darauf hingewiesen, dass die Veröffentlichung von Prüfungsplänen für Abiturienten in Form von Teilnahmelisten an den mündlichen Prüfungen bzw. Präsentationsprüfungen im Internet aus datenschutzrechtlichen Gründen nicht zulässig ist. Ich hoffe, dass solchen Problemen damit dauerhaft ein Riegel vorgeschoben ist. Jedenfalls sind mir dazu bislang keine weiteren Beschwerden bekannt geworden.

6. Datenschutz an einer Schule im Zusammenhang mit einem Masernfall

Bei dem Wort Masern kommt einem vieles in den Sinn, insbesondere etwa das Mitgefühl mit den Erkrankten, der Schutz der Menschen in deren Umgebung und die Vermeidung einer Epidemie. Der Datenschutz wird dabei eher nicht im Fokus stehen. Im Zusammenhang mit einem Masernfall an einer sehr großen Schule gerieten im April 2008 aber ausnahmsweise auch datenschutzrechtliche Fragen in den Blickpunkt.

Ein Bürger hatte sich mit einer Datenschutzbeschwerde gegen die Sicherheitsvorkehrungen einer Schule gewandt und vorgetragen: Alle Schülerinnen und Schüler hätten an einem bestimmten Tag das Schulgebäude nur noch gegen Vorlage ihres Impfausweises oder einer ärztlichen Laborbescheinigung über eine vorherige Masernerkrankung betreten dürfen. Als Nachweis für die Vorlage hätten sie jeweils ein rotes Bändchen (technisch den Bändchen vergleichbar, die im Rahmen von All-inclusive-Urlaubsreisen von Hotels verwendet werden) ums Handgelenk gebunden bekommen. Gleichzeitig sei darum gebeten worden, dieses Bändchen für die Dauer von knapp zwei Wochen nicht mehr abzulegen. Der Bürger hielt dies für unzulässig, denn auf diese Weise müssten die betroffenen Kinder auch außerhalb des Schulgebäudes, im außerschulischen, sozialen Umfeld, wie

etwa Sportverein, Schwimmbad, Freizeitgruppe, Erkennungsmerkmale tragen, die Rückschlüsse auf den jeweiligen Gesundheitszustand zulassen. Die datenschutzrechtliche Prüfung meines Amtsvorgängers ergab Folgendes:

An der Schule wurden tatsächlich rote Bändchen als Zeichen der durchgeführten Kontrolle ausgegeben. Andere Möglichkeiten des Vorgehens, beispielsweise tägliche Eingangskontrolle, Stempelkennzeichnung oder Schließung der gesamten Schule für den Quarantänezeitraum, waren zuvor zwischen Schule und dem zuständigen Gesundheitsamt zwar diskutiert, aber verworfen worden. Das ausgewählte Verfahren erschien der Schule angemessen: Es vereinfache die schulischen Aufgaben und enthalte nach Auffassung der Schule keine unzumutbare Härte, zumal für einen derart begrenzten Zeitraum. Die Schüler seien per Durchsage und Aushang aufgefordert worden, die Bändchen nicht zu entfernen. Falls dies doch einmal erforderlich sei, könnten die Schüler jederzeit gegen Vorlage des Impfpasses bzw. nach Kontrolle der Liste bei der Schulleitung ein neues Bändchen bekommen. Eine Bestrafung wegen Verlust der Bändchen erfolge nicht.

Trotz der ungewöhnlichen Fallkonstellation begegnete der geschilderte Sachverhalt letztlich keinen durchgreifenden datenschutzrechtlichen Bedenken; mein Amtsvorgänger sah auch keinen Anlass zur förmlichen datenschutzrechtlichen Beanstandung gegenüber der Schule. Denn Masern sind eine meldepflichtige Krankheit nach dem Infektionsschutzgesetz. Somit war die Schule nicht nur berechtigt, sondern sogar verpflichtet, einen dort auftretenden Masernfall bei der Gestaltung des Schulbetriebs zu berücksichtigen und über ihr Vorgehen nach pflichtgemäßem Ermessen zu entscheiden. Dass die Schule den Schutz personenbezogener Daten bei der Ermessensbetätigung völlig unberücksichtigt ließ, war nicht erkennbar. Gleichwohl sind einige Hinweise angebracht, damit in vergleichbaren Fällen dem Datenschutz noch in stärkerem Maß Rechnung getragen werden kann:

Öffentliche Stellen haben generell die grundlegenden Gebote der Datenvermeidung und Datensparsamkeit zu beachten. Somit müssen öffentliche Schulen diese Gebote auch berücksichtigen, wenn sie angesichts dort aufgetretener Masern (oder anderer meldepflichtiger Krankheiten) die Konsequenzen hinsichtlich des Schulbetriebs prüfen. Wenn dabei mehr als eine Möglichkeit des Vorgehens besteht, sollte – sofern dies mit Blick auf die zu erfüllenden Dienstpflichten vertretbar ist – die datenschutzfreundlichste Möglichkeit gewählt werden.

Bei ihrer Ermessensbetätigung ist auch das Wesen des Rechts auf informationelle Selbstbestimmung von betroffenen Schülerinnen und Schülern und eventuellen sonstigen Betroffenen angemessen zu berücksichtigen, denn die Betroffenen sollten grundsätzlich selbst darüber entscheiden können, welche Informationen sie hinsichtlich ihrer Person wem in welcher Weise preisgeben. Eingriffe in dieses Grundrecht bedürfen einer gesetzlichen Grundlage. Eine gesetzliche Grundlage, die es der Schule erlaubt, von ihren Schülerinnen und Schülern das Tragen der roten Bändchen außerhalb des Schulgebäudes zu fordern, gibt es nicht. Somit waren (und sind) die Schülerinnen und Schüler rechtlich nicht verpflichtet, diese Bändchen außerhalb des Schulgebäudes bzw. -geländes zu tragen. Die Schule hat nach ihrer Mitteilung die Schülerinnen und Schüler per Durchsage und Aushang aber dazu „aufgefordert“, die Bändchen nicht zu entfernen. Dazu ist hervorzuheben, dass eine Aufforderung in vielen Fällen als Mitteilung verstanden werden kann, dass die oder der Aufgeforderte (rechtlich) in gewisser Weise dazu verpflichtet sei. Die Eingabe des besorgten Bürgers ließ erkennen, dass die Aufforderung der Schule wohl tatsächlich – zumindest teilweise – so verstanden worden war. Solche Probleme lassen sich von vornherein dadurch vermeiden, dass die Schule ihre Schülerinnen und Schüler klar und unmissverständlich über die Freiwilligkeit des Tragens der Bändchen außerhalb des Schulgebäudes informiert.

Das Tragen der roten Bändchen außerhalb des Schulgebäudes ist in datenschutzrechtlicher Hinsicht nicht generell irrelevant. Denn es kann, auch wenn die Wahrscheinlichkeit nicht sonderlich groß sein mag, nicht von vornherein ausgeschlossen werden, dass sich für Betrachter mit entsprechendem Zusatzwissen aus dem Tragen des Bändchens Informationen über den Träger ergeben.

7. Die Kopie des Personalausweises in der Schulkartei

Ob Schüler Kopien ihrer Personalausweise für die Schulkartei zur Verfügung stellen müssen, ist datenschutzrechtlich mehr als zweifelhaft.

Mit einer Eingabe wurde uns u. a. mitgeteilt, dass an einer Schule bei Beginn des neuen Schuljahrs von den Schülern verlangt worden sei, eine Kopie ihres Personalausweises abzugeben. Dabei sei den Schülern gesagt worden, dass sie diese Kopie abgeben müssten. Auf unsere Bitte um Stellungnahme teilte uns die Schule Folgendes mit:

Man lasse sich dort seit diesem Schuljahr bei der Schüleraufnahme tatsächlich eine Kopie des Personalausweises vorlegen, um die Identität der Schülerinnen und Schüler festzustellen, die Aufnahmebedingungen zu überprüfen (z. B. Notwendigkeit einer Aufenthaltsgenehmigung) und Zeugnisse erstellen zu können. Die jeweilige Kopie des Ausweises werde während des Schulbesuchs zur „Schülerkartei“ genommen. Es sei vorgesehen, die Kopie nach Schulabgang zu vernichten.

Die Bearbeitung dieser Angelegenheit, die noch weitere Aspekte zum Gegenstand hat, ist zum Zeitpunkt des Redaktionsschlusses für diesen Tätigkeitsbericht noch im Gange. Die hier angesprochenen Umstände sind aus meiner Sicht aber so bemerkenswert, dass – selbstverständlich ohne dem endgültigen Ergebnis vorgreifen zu wollen – einige Anmerkungen angezeigt sind:

Eine öffentliche Schule hat bei der Erhebung und Speicherung personenbezogener Daten, beispielsweise auch in Gestalt der Kopien der Personalausweise von Schülerinnen und Schülern, den datenschutzrechtlichen Erforderlichkeitsgrundsatz mit den darin verankerten Geboten der Datenvermeidung und der Datensparsamkeit zu beachten. Auf den konkreten Fall bezogen heißt das mit anderen Worten: Die Schule darf die Kopien der Personalausweise nur dann verlangen (nach der Terminologie des Landesdatenschutzgesetzes: erheben) und speichern, wenn dies für die Erfüllung der dienstlichen Aufgaben der Schule erforderlich ist. Dabei ist zu beachten, dass der datenschutzrechtliche Erforderlichkeitsbegriff in einem strengen Sinn zu verstehen ist: Eine Erhebung, Speicherung oder sonstige Datenverarbeitung ist nur dann erforderlich, wenn ohne sie die Erfüllung dienstlicher Aufgaben nicht oder nur eingeschränkt möglich ist. Dagegen reicht es nicht aus, dass eine Datenverarbeitung etwa als nahe liegend, praktisch oder bequem angesehen wird. Auf der Grundlage der eingangs genannten Stellungnahme der Schule habe ich ganz erhebliche Zweifel, dass die Erhebung und Speicherung der Personalausweiskopien in allen Fällen dem Erforderlichkeitsgrundsatz entspricht. Denn es ist zunächst nicht nachvollziehbar, dass sich die Schule in jedem Fall der Schulaufnahme mit der Frage nach der Notwendigkeit einer Aufenthaltsgenehmigung befasst. Selbst wenn sich diese Frage im Einzelfall stellen sollte, ist damit die Erhebung der Kopie des Personalausweises und deren Speicherung bis zum Schulabgang keineswegs automatisch gerechtfertigt. Entsprechend den Geboten der Datenvermeidung und der Datensparsamkeit kann es etwa völlig ausreichen, dass die Schule sich in begründeten Einzelfällen den Personalausweis zeigen lässt und gegebenenfalls die darin enthaltenen relevanten Informationen notiert, evtl. mit dem Vermerk, dass der Personalausweis bei der Aufnahme im Original vorgelegt wurde. Es ist auch in keiner Weise nachvollziehbar, weshalb die Kopie von Personalausweisen für die Erstellung von Zeugnissen benötigt wird. Soweit es der Schule darum geht, die Personalien der Schülerinnen und Schüler in deren jeweilige Zeugnisse einzutragen, liegt es nahe, diese Personalien beispielsweise der jeweiligen Schülerakte oder gegebenenfalls einer Datei mit den Schülerstammdatensätzen zu entnehmen, ohne dass im Entferntesten die Nutzung von Personalausweiskopien hierfür erforderlich wäre.

Soweit die Schule nach alledem dennoch eine Datenerhebungsbefugnis für Personalausweiskopien haben sollte, stellt sich die weitere Frage, ob die Schülerinnen und Schüler rechtlich verpflichtet sind, solche Kopien an die Schule herauszugeben. Das ist nach den derzeit hier vorliegenden Informationen nicht der Fall. Bei der weiteren Bearbeitung ist noch eingehend zu prüfen, ob die Betroffenen bei der Datenerhebung in der gesetzlich gefor-

derten Weise (vgl. § 14 LDSG) unterrichtet wurden und ob im Fall minderjähriger Schülerinnen und Schüler beachtet wurde, dass nach der – auch vom Kultusministerium vertretenen – „Faustformel 16“ auch bereits 16-jährige Schülerinnen und Schüler ausreichend einsichtsfähig und somit datenschutzmündig sein können.

Schulische Datensammlungen sollten sich auf den unbedingt erforderlichen Umfang beschränken.

8. Personenbezogene Daten von Studenten im Internet – Datenschutzverstoß an einer Pädagogischen Hochschule

Ein Student wies uns darauf hin, dass personenbezogene Daten von sämtlichen Studenten der Fachrichtung Sport einer Pädagogischen Hochschule im Internet abrufbar seien. Zwar gebe es, so teilte der Betroffene weiter mit, eine gewisse „Verschlüsselung“ und einen Zugangsschutz, doch seien diese nach seinen Vermutungen leicht zu umgehen.

Eine sofortige Überprüfung durch mein Amt ergab, dass die betreffende Pädagogische Hochschule tatsächlich personenbezogene Daten von Studenten in einer Excel-Tabelle gespeichert hatte, die jeder mit einem einfachen Download auf seinen Rechner herunterladen konnte. Diese Tabelle enthielt neben den Namen und den Vornamen aller Studenten insbesondere auch deren Matrikelnummern, das Studienfach und dessen Gewichtung, die Anzahl der Fachsemester sowie die besuchten Lehrveranstaltungen. Die Pädagogische Hochschule hatte eigentlich gewollt, dass ein Student aus dieser Tabelle nur seine eigenen Daten angezeigt bekommt, indem er ein persönliches Kennwort eingibt. Es war jedoch in der Tat leicht möglich, die Daten aller Studenten einzusehen.

Auf unsere Nachfrage führte die Pädagogische Hochschule zwar zu ihrer Rechtfertigung ins Felde, dass die Excel-Tabelle kennwortgeschützt sei und ein Nutzer neben der von ihm selbst eingegebenen Matrikelnummer nur jeweils seine eigenen Daten sehen könne. Sogar von einer Manipulation war die Rede. Eine Überprüfung durch meine Mitarbeiter ergab jedoch, dass dieser „Schutz“ dergestalt realisiert wurde, dass beim Öffnen der Datei das erste Datenblatt (sog. Sheet) angezeigt wird und zudem die Blattregisterkarten (sog. Reiter oder Tabs) der anderen Datenblätter ausgeblendet sind. Dies stellt selbstverständlich keinen hinreichenden Kennwortschutz dar, denn zum einen genügt die Eingabe der Matrikelnummer, um die angemeldeten Lehrveranstaltungen eines Studenten lesen zu können. Zum anderen ist es möglich, durch einfaches Einblenden der Blattregisterkarten Zugriff auf alle in der Datei vorhandenen Informationen zu erhalten. Dieses Einblenden kann über die „erweiterten Excel-Optionen“ erfolgen. Von einer Manipulation, wie die Pädagogische Hochschule zunächst uns gegenüber behauptet hatte, konnte somit nicht gesprochen werden, geschweige denn von einem wirksamen Sicherheitsmechanismus. Bereits mit „Bordmitteln“ des Excel-Programms war es möglich, sich die Daten aller Studenten anzeigen zu lassen. Der Passwortschutz war also keineswegs ausreichend. Grundsätzlich ist zwar die Verarbeitung von personenbezogenen Daten über derartige Online-Lehrveranstaltungsanmeldungen aus datenschutzrechtlicher Sicht nicht von vornherein unzulässig. Wenn alle datenschutzrechtlichen Anforderungen beachtet werden, kann ein solches Verfahren durchaus eingeführt werden und den Vorzug gegenüber einem traditionellen Verfahren unter Nutzung eines sog. Schwarzen Bretts erhalten. Im Ergebnis ist, auch aufgrund einer eigenen Recherche im Internet, festzustellen, dass die technischen und organisatorischen Maßnahmen der Hochschule unzureichend waren. Zwar hat die Pädagogische Hochschule unmittelbar nach unserer Intervention das Verfahren eingestellt, dennoch hat mein Vorgänger für diesen datenschutzrechtlichen Verstoß eine förmliche Beanstandung nach § 30 LDSG ausgesprochen.

Sicherheitsmechanismen müssen mit größter Sorgfalt festgelegt werden, um personenbezogene Daten vor unberechtigten Zugriffen wirksam zu schützen.

4. Teil: Personalwesen

1. Rechnungsprüfungsamt gleicht Personaldaten ab

Maßstab für Umfang und Tiefe der Prüfung durch ein Rechnungsprüfungsamt dürfen nicht die umfassenden Möglichkeiten einer modernen Analyse-Software zum Verknüpfen unterschiedlicher Datenbestände sein.

Im Jahr 2008 glichen sowohl bei einer Gemeinde als auch bei einem Landratsamt die Rechnungsprüfungsämter die Bankverbindungsdaten (das heißt Bankleitzahl und Kontonummer, also keine Umsatz- oder Überweisungsdaten) von Beschäftigten mit den entsprechenden Daten anderer Personen computergestützt ab.

Das Rechnungsprüfungsamt der Gemeinde glich die Bankverbindungsdaten von 1 796 Beschäftigten mehrerer Ämter und Eigenbetriebe der Gemeinde mit den entsprechenden Daten der Lieferanten dieser Ämter und Eigenbetriebe – jeweils getrennt – ab. Zweck des Datenabgleichs war nach Mitteilung des Rechnungsprüfungsamts das Aufdecken „doloser Handlungen“, das heißt insbesondere, ob Beschäftigte Geld auf eigene Konten überwiesen haben. Die Ämter und Eigenbetriebe waren nach Mitteilung des Rechnungsprüfungsamts jeweils aufgrund ihrer höheren „Korruptionsgefährdung“ ausgewählt worden, weil dort regelmäßig Aufträge vergeben und Zahlungen veranlasst würden. Konkrete Anfangsverdachtsmomente für „dolose Handlungen oder Korruption“ hätten allerdings nicht vorgelegen. Der Abgleich ergab keine „Treffer“.

Das Rechnungsprüfungsamt des Landratsamts glich die Bankverbindungsdaten aller Beschäftigten des Landratsamts (1 760 Abrechnungsfälle) mit den entsprechenden Daten der Empfänger der wirtschaftlichen Hilfen ab, welche das Sozialdezernat (ohne die Wohngeldstelle) gewährte. Anlass hierfür war, dass ein Beschäftigter in der Vergangenheit Gelder veruntreut hatte. Der Abgleich ergab „Treffer“, also Übereinstimmungen dieser Bankverbindungsdaten. Das Rechnungsprüfungsamt stellte nach Mitteilung des Landratsamts jedoch keine „Auffälligkeiten“ fest, die einen Verdacht auf Unregelmäßigkeiten begründeten.

Diese Datenabgleiche waren in der Weise, wie sie konkret erfolgt sind, im Ergebnis datenschutzrechtlich unzulässig. Es würde den Rahmen dieses Berichts sprengen, das hier im Einzelnen darzustellen. Deswegen spreche ich nachfolgend nur einzelne Punkte an. Einzelheiten sind dem Abschnitt I meines Berichts an den Landtag zum Datenabgleich bei der Gemeinde (LT-Drucksache 14/4675) zu entnehmen (diese ist über die Internet-Seite des Landtags von Baden-Württemberg – *www.landtag-bw.de* – abrufbar). Hinsichtlich des Datenabgleichs beim Landratsamt stellten sich, ungeachtet der unterschiedlichen Sachverhalte, letztlich vergleichbare Fragen.

Die Aufgaben des Rechnungsprüfungsamts sind in der Gemeindeordnung geregelt; seine Befugnisse werden in § 14 Abs. 2 der Gemeindeprüfungsordnung (GemPrO) konkretisiert. Das entspricht weitgehend den Vorschriften über die Ausgestaltung der Prüfung durch den Rechnungshof Baden-Württemberg.

> *§ 14 Abs. 2 GemPrO*
>
> *Die Gemeinde hat den Prüfer bei seinen Aufgaben zu unterstützen. Der Prüfer kann alle Auskünfte und Unterlagen verlangen sowie eigene Erhebungen vornehmen, die zur Erfüllung seiner Aufgaben erforderlich sind.*

Zunächst ist darauf hinzuweisen, dass der Zielkonflikt zwischen Rechnungsprüfung und Datenschutz in Bezug auf personenbezogene Daten über Beschäftigte bisher nur unzureichend beleuchtet, geschweige denn gelöst worden ist. Deswegen besteht insoweit noch weiterer Klärungsbedarf. Dieser erstreckt sich insbesondere darauf, welche Aufgaben ein Rechnungsprüfungsamt konkret wahrnehmen darf und welche einzelnen Maßnahmen zum Verarbeiten personenbezogener Daten geeignet und notwendig sind, um diese Aufgaben zu erfüllen.

Im Ergebnis halte ich „anlasslose“ Überprüfungen (also Überprüfungen ohne konkreten Anfangsverdacht, wie er etwa Voraussetzung eines strafrechtlichen Ermittlungsverfahrens wäre) durch das Rechnungsprüfungsamt mit Blick darauf, dass es dabei letztlich auch um Steuergelder geht, nicht von vornherein und unter allen Umständen für unzulässig. Das hängt damit zusammen, dass die Rechnungsprüfung gegenüber anderen Nutzungszwecken gesetzlich privilegiert ist. Zum Wesen der Rechnungsprüfung gehört denknotwendig das Erhellen von Sachverhalten, die zu Beginn der Prüfung nicht bzw. nicht vollständig bekannt sind, bei denen aber aufgrund von praktischen Erfahrungen und logischen Schlussfolgerungen nicht auszuschließen ist, dass prüfungsrelevante Feststellungen im Verlauf der Prüfung getroffen werden können. Aus Sicht des Datenschutzes darf Anlass für einen Datenabgleich des Rechnungsprüfungsamts allerdings nicht lediglich ein hypothetisch denkbares Fehlverhalten x-beliebiger Beschäftigter sein. Wenn das Rechnungsprüfungsamt den Prüfungsgegenstand und die zu überprüfenden Personen auswählt sowie den Prüfungsumfang und die Prüfungstiefe festlegt, muss es aufzuklärende Geschehensabläufe (und sich daraus ergebende Schäden) zugrunde legen, die nicht nur abstrakt plausibel, sondern die auch mit einer hinreichenden Wahrscheinlichkeit anzutreffen sind.

Ich neige deswegen zur Auffassung, dass das Rechnungsprüfungsamt mit dem Ziel des Aufdeckens „doloser Handlungen“ unter gewissen Voraussetzungen die Daten der Mitarbeiter von Organisationseinheiten mit strukturellem Gefährdungspotenzial überprüfen darf. Hierzu kann in geeigneten Fällen beispielsweise auch ein elektronischer Abgleich von Kontendaten von Lieferanten mit Kontendaten von bestimmten Beschäftigten mit Hilfe einer Analyse-Software in einer Vielzahl von Fällen gehören. Für solche Datenabgleiche sind jedoch künftig geeignete „Spielregeln“ zu entwickeln und differenzierte verfahrensmäßige Sicherungen zur Wahrung der Grundrechte der Betroffenen vorzusehen. Diese Vorkehrungen müssen für mehr Transparenz und für eine stärkere Konkretisierung der geplanten Maßnahmen und der erzielten Ergebnisse sorgen und damit dem Verhältnismäßigkeitsgrundsatz stärker zur Geltung verhelfen.

Das Nutzen der Beschäftigtendaten durch das Rechnungsprüfungsamt muss – gemessen am (zulässigen) Prüfungszweck – zudem verhältnismäßig sein, also geeignet, erforderlich und im Hinblick auf den damit verbundenen Eingriff in das Recht der Beschäftigten auf informationelle Selbstbestimmung angemessen, das heißt auch im engeren Sinne verhältnismäßig. Erforderlich ist ein Abgleich personenbezogener Daten, um einen vom Rechnungsprüfungsamt zulässigerweise verfolgten Zweck zu erfüllen, wenn dafür kein anderes, gleich wirksames und das Persönlichkeitsrecht weniger einschränkendes Mittel zur Verfügung steht. Die Angemessenheit ist aufgrund einer konkreten Gesamtabwägung der Intensität des Eingriffs und des Gewichts der ihn rechtfertigenden Gründe festzustellen; maßgeblich sind dafür die Gesamtumstände. Dabei spielen die – allerdings noch näher zu präzisierenden – Aufgaben und Befugnisse des Rechnungsprüfungsamts eine nicht unwesentliche Rolle. Hier sind aus meiner Sicht insbesondere folgende Punkte zu beachten:

– Das Rechnungsprüfungsamt hat von gleich gewichtigen Prüfungsthemen oder gleich effektiven Prüfungsmethoden diejenigen vorzuziehen, welche das Verarbeiten von weniger oder weniger bedeutsamen personenbezogenen Daten erfordern. Eine strukturelle Analyse ohne personenbezogene Daten ist daher, soweit möglich, einer Analyse mit personenbezogenen Daten vorzuschalten.

– Stichprobenweise Untersuchungen besonders relevanter Sachverhalte haben stets Vorrang vor flächendeckenden Prüfungen unter undifferenzierter Einbeziehung der Daten aller Beschäftigten. Bei einem Datenabgleich ist der Kreis der Betroffenen soweit wie möglich einzugrenzen und allenfalls stufenweise auszudehnen.

– Es sind ausschließlich die Daten über die Beschäftigten heranzuziehen, die, etwa im Falle von „Treffern“, auch benötigt werden. Das war im konkreten Fall etwa hinsichtlich der vom Rechnungsprüfungsamt der Ge-

meinde verarbeiteten Anschriften der Beschäftigten nicht der Fall: Zur „späteren Identifizierung von ‚Treffern' " genügten nämlich die eindeutigen Personalnummern, die das Rechnungsprüfungsamt ebenfalls herangezogen hatte, und für einen um Namen und Anschriften erweiterten Abgleich waren sie bereits deswegen nicht notwendig, weil kein solcher Abgleich erfolgte.

– Wünschenswert wäre ein weitgehendes Pseudonymisieren der zu verarbeitenden Daten, denn dann müsste der Personenbezug erst bei „Treffern" hergestellt werden.

– Zu den Gründen, die einen Datenabgleich durch das Rechnungsprüfungsamt rechtfertigen können, gehört das beachtliche Interesse des Arbeitgebers und des Steuerzahlers an einer sparsamen und zweckentsprechenden Verwendung öffentlicher Haushaltsmittel und am Aufdecken bewusster Falschzahlungen.

– Die Fürsorgepflicht des Arbeitgebers gebietet einen möglichst schonenden Umgang mit Beschäftigtendaten.

– Die Bankleitzahl und Kontonummer eines Beschäftigten, also die Information, dass dieser bei einer bestimmten Bank ein Konto unterhält, ist für sich betrachtet nicht besonders schutzwürdig. Die Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung der Beschäftigten ist insoweit relativ gering.

– Dem Ziel einer größtmöglichen Transparenz entspräche es, bereits vorab die entsprechenden Beschäftigten unmissverständlich darauf hinzuweisen, dass unter bestimmten Voraussetzungen personenbezogene Daten über sie zum Aufdecken „doloser Handlungen" abgeglichen werden. Sollte das nicht möglich sein, ohne den Prüfungszweck zu gefährden, dann sollten die Betroffenen aus Sicht des Datenschutzes jedenfalls im Nachhinein über den Datenabgleich und die dabei verarbeiteten Datenarten allgemein benachrichtigt werden.

– Etwaige „Treffer", die sich als Verdachtsfälle darstellen, sind unverzüglich aufzuarbeiten. Auch dabei sind die schutzwürdigen Belange der Betroffenen zu wahren. In Anbetracht der möglichen Rufschädigung wären die im Zusammenhang mit solchen Verdachtsfällen gewonnenen Daten zudem vor unbefugten Zugriffen und zweckwidriger Verwendung besonders zu schützen. Wenn sich der Verdacht nicht bestätigt, sind die gewonnenen Daten unverzüglich irreversibel zu löschen. Die Betroffenen sind auch hierüber umgehend zu unterrichten.

Unabhängig von diesen rechnungsprüfungsrechtlichen Fragen fehlte es bei den geprüften Datenabgleichen jeweils an der Vorabkontrolle und an einem vollständigen Verfahrensverzeichnis:

– Die Daten wurden ohne die nach § 12 Abs. 1 LDSG vorgeschriebene Vorabkontrolle abgeglichen.

> *§ 12 Satz 1 Halbsatz 1 LDSG*
>
> *Wer für den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten zuständig ist, das mit besonderen Gefahren für das Persönlichkeitsrecht verbunden sein kann, insbesondere aufgrund der Art oder der Zweckbestimmung der Verarbeitung, darf das Verfahren erst einsetzen, wenn sichergestellt ist, dass diese Gefahren nicht bestehen oder durch technische oder organisatorische Maßnahmen verhindert werden; ...*

Der Einsatz eines Programms zum Abgleich von Bankverbindungsdaten (Kontonummern und Bankleitzahlen) konnte hier mit besonderen Gefahren für das Persönlichkeitsrecht verbunden sein (es genügte, dass das so sein konnte; ob das tatsächlich so war und ob diese besonderen Gefahren gegebenenfalls durch technische oder organisatorische Maßnahmen verhindert werden konnten, wäre bei der Vorabkontrolle selbst zu beantworten gewesen). Denn bei den Abgleichen wurden personenbezogene Daten

aus unterschiedlichen Zusammenhängen verknüpft (von Beschäftigten einerseits und von Lieferanten bzw. von Empfängern wirtschaftlicher Hilfen andererseits). Dadurch kann auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen (vgl. Bundesverfassungsgericht, Volkszählungsurteil vom 15. Dezember 1983, 1 BvR 209/83 u. a., BVerfGE 65, 1, 45).

– Die Einträge in die Verfahrensverzeichnisse zu der Analyse-Software entsprachen nicht den gesetzlichen Vorgaben. Zu diesem allgemeinen Problem verweise ich auch auf die Ausführungen unter Nr. 2 im 7. Teil dieses Berichts. Die Gemeinde erschwerte unsere Prüfung zu diesem Punkt insbesondere dadurch, dass sie uns mehrere voneinander abweichende Auszüge aus dem Verfahrensverzeichnis zuleitete, die zudem noch teilweise unvollständig, widersprüchlich und nicht geeignet waren, einen hinreichenden Überblick über die Art und Weise des Verarbeitens personenbezogener Daten mit dem Verfahren zu verschaffen.

Das Innenministerium Baden-Württemberg hat zwischenzeitlich eine Arbeitsgruppe „Kommunale Rechnungsprüfung und Datenabgleich" ins Leben gerufen. Sie soll, wie von mir angeregt, für künftige Datenabgleiche geeignete „Spielregeln" entwickeln, die insbesondere dem Verhältnismäßigkeitsgrundsatz beim Nutzen von Beschäftigtendaten stärker zur Geltung verhelfen und die besondere Rolle der unabhängigen Rechnungsprüfung nach der Gemeindeordnung berücksichtigen sollen. In dieser Arbeitsgruppe sind neben dem Innenministerium Baden-Württemberg und dem Regierungspräsidium Stuttgart die Kommunalen Landesverbände, die Gemeindeprüfungsanstalt Baden-Württemberg, der Rechnungshof Baden-Württemberg und mein Amt vertreten.

2. Dienstherr fragt heimlich Krankheitsgründe ab

Ein Dienstherr (bzw. Arbeitgeber) fragte die Vorgesetzten nach ihnen bekannten Gründen für Erkrankungen von Beschäftigten.

Aufgrund eines Hinweises aus der Presse wurden meine Mitarbeiter und ich auf einen Vorgang in einer Gemeinde im Regierungsbezirk Tübingen aufmerksam, der dort bereits für Schlagzeilen gesorgt hatte. Das Haupt- und Personalamt der Gemeinde hatte nämlich jahrelang jährliche Umfragen unter den Führungskräften der Verwaltung durchgeführt, um Einzelheiten über die Krankheitsgründe von Mitarbeitern in Erfahrung zu bringen. Zuletzt ging es um Beschäftigte mit „mehr als 20 Krankheitstagen und/oder mehr als fünf Kurzerkrankungen" im Kalenderjahr. Der Dienstherr bat hierbei u. a. darum, „den Grund für die Erkrankungen nicht beim Mitarbeiter direkt zu erfragen". Die Befragungsaktion gehörte zum „Gesundheitsmanagement" der Gemeinde und verfolgte nach Mitteilung der Gemeinde u. a. das Ziel, bei Langzeiterkrankten und Mitarbeitern mit häufig auftretenden Kurzzeiterkrankungen mögliche Bezüge zwischen den Erkrankungen und den Arbeitsplatzbedingungen zu erkennen und künftigen Erkrankungen durch geeignete Maßnahmen vorzubeugen. Als mein Amt den Vorgang kontrollierte, speicherte der Dienstherr nach seiner Mitteilung keine solchen Angaben zu Krankheitsursachen mehr.

Nach den Gründen befragt, machte das Stadtoberhaupt u. a. geltend, seine Vorgehensweise habe den heute geltenden „Vorgaben für ein betriebliches Eingliederungsmanagement" entsprochen. Er verwies dazu auf § 84 Abs. 2 des Neunten Buchs des Sozialgesetzbuchs (SGB IX).

Der hier bedeutsame § 84 Abs. 2 Sätze 1 und 3 SGB IX lautet:

> *[1] Sind Beschäftigte innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig, klärt der Arbeitgeber mit der zuständigen Interessenvertretung im Sinne des § 93, bei schwerbehinderten Menschen außerdem mit der Schwerbehindertenvertretung, mit Zustimmung und Beteiligung der betroffenen Person die Möglichkeiten, wie die Arbeitsunfähigkeit möglichst überwunden werden und mit welchen Leistungen oder Hilfen erneuter Arbeitsunfähigkeit vorgebeugt und der*

Arbeitsplatz erhalten werden kann (betriebliches Eingliederungsmanagement).

[3] Die betroffene Person oder ihr gesetzlicher Vertreter ist zuvor auf die Ziele des betrieblichen Eingliederungsmanagements sowie auf Art und Umfang der hierfür erhobenen und verwendeten Daten hinzuweisen.

Diesen Vorgaben hatte die Gemeinde indessen nicht entsprochen:

– Die Krankheitsgründe wurden bereits bei mehr als 20 Krankheitstagen (diese entsprechen vier Wochen bei einer Fünf-Tage-Woche) oder mehr als fünf Kurzerkrankungen abgefragt und nicht erst dann, wenn Beschäftigte innerhalb eines Jahres länger als sechs Wochen arbeitsunfähig waren.

– Nach der gesetzlich verlangten „Zustimmung" des Betroffenen wurde nicht gefragt. Das Haupt- und Personalamt wandte sich lediglich an deren Vorgesetzte.

– Anders als gesetzlich vorgeschrieben, wies der Dienstherr nicht zuvor auf die Ziele des betrieblichen Eingliederungsmanagements und auf die Datenverarbeitung hin.

Auch wenn ein Dienstherr aus „Fürsorge" nach den Krankheitsgründen seiner Beschäftigten fragt, darf er das nicht hinter deren Rücken tun. Außerdem muss er die Vorschriften über das betriebliche Eingliederungsmanagement beachten. Fürsorge des Dienstherrn und informationelle Selbstbestimmung sind so ohne weiteres miteinander in Einklang zu bringen.

3. Grundsätzlich keine Namen von Beschäftigten ins Internet

Dürfen personenbezogene Daten über Beschäftigte ins Internet? Diese Frage ist weiterhin aktuell. Sie ist datenschutzfreundlich zu beantworten.

Das Veröffentlichen von Beschäftigtendaten im Internet war bereits mehrfach Gegenstand der Tätigkeitsberichte meiner Amtsvorgänger. Beispielsweise wurde im 23. Tätigkeitsbericht für das Jahr 2002 (LT-Drucksache 13/1500) darauf hingewiesen, dass ein Veröffentlichen von Beschäftigtendaten im Internet grundsätzlich nur mit Einwilligung zulässig ist; Ausnahmen seien nur hinsichtlich der Namen, dienstlichen Funktion und dienstlichen Erreichbarkeit von leitenden Beschäftigten sowie von Beschäftigten mit regelmäßigen Außenkontakten vertretbar, wobei auf die Umstände des jeweiligen Einzelfalls abzustellen sei. Im 26. Tätigkeitsbericht für das Jahr 2005 (LT-Drucksache 13/4910) wurde zudem gefordert, dass stets sorgfältig geprüft werden sollte, ob auf die Angabe des Namens des Beschäftigten verzichtet werden kann, weil die Angabe der dienstlichen Funktion und der dienstlichen Erreichbarkeit genügt. Dabei wurde darauf hingewiesen, dass beispielsweise eine funktionsbezogene E-Mail-Adresse ohne den Namen des Beschäftigten auskommt.

Im Berichtszeitraum sind meine Mitarbeiter und ich dagegen immer wieder auf Internet-Seiten öffentlicher Stellen gestoßen, die nicht diesen Kriterien entsprachen. So fand meine Dienststelle auf der Internet-Seite einer Schule u. a. weltweit uneingeschränkt abrufbare Elternbriefe. Darin waren nicht nur neue Lehrkräfte mit Namen und Unterrichtsfächern genannt, sondern es war auch zu lesen, dass zwei namentlich genannte Lehrerinnen „mit Beginn der Mutterschutzfrist beurlaubt" wurden. Das war rechtswidrig und gemäß § 30 LDSG zu beanstanden, vor allem, weil meine Dienststelle eben diese Schule wenige Monate zuvor auf die datenschutzrechtlichen Anforderungen an das Veröffentlichen personenbezogener Daten über Lehrkräfte und Schüler hingewiesen hatte. Das lässt aus meiner Sicht auch mit Blick auf das weitere Defizit, was den Datenschutz an Schulen betrifft (dazu mehr beispielsweise im 25. Tätigkeitsbericht für das Jahr 2004, LT-Drucksache 13/3800, sowie im 3. Teil dieses Berichts), auf strukturelle Missstände schließen. Die Kultusverwaltung sollte jedenfalls wirksame Maßnahmen treffen, das an vielen Schulen erkennbar fehlende Datenschutzbewusstsein wieder zu beleben.

Immerhin hielt auch das Kultusministerium die beanstandeten Veröffentlichungen in dem konkreten Fall für rechtswidrig. Es kündigte an, bei der

beabsichtigten Neufassung der Verwaltungsvorschrift „Datenschutz an öffentlichen Schulen“ unserer Bitte zu entsprechen, die für die Schulen wichtige Frage nach der Zulässigkeit einer Veröffentlichung personenbezogener Daten über Lehrkräfte durch Schulen aufzugreifen. Meine Dienststelle hat sich zu Entwürfen dieser Verwaltungsvorschrift geäußert. Das Kultusministerium hat sie nach unserer Kenntnis bisher nicht in Kraft gesetzt. Wenn das geschieht und in der Verwaltungsvorschrift klare Vorgaben enthalten sind, dann bleibt zu hoffen, dass die weitere Umsetzung zu einer Anhebung des Datenschutzniveaus führen wird.

Aufgrund der Entwicklungen in letzter Zeit halte ich – über den Bereich der Schulen hinaus – das Veröffentlichen bzw. Zugänglichmachen personenbezogener Daten über Beschäftigte im Internet auch generell für kritisch. Ich halte es nur dann für zulässig, wenn eine normenklare Rechtsvorschrift es erlaubt oder wenn der Betroffene nach umfassender Aufklärung über die damit verbundenen Folgen bzw. Gefahren eingewilligt hat; dies sollte auch für leitende Beschäftigte sowie Beschäftigte mit regelmäßigen Außenkontakten gelten. Insoweit schreibe ich die bisherige Position meiner Dienststelle weiter fort. Hierbei spielt eine wesentliche Rolle, dass das Veröffentlichen bzw. Zugänglichmachen personenbezogener Daten im Internet besondere Gefahren für das Recht auf informationelle Selbstbestimmung begründet:

– Internet-Veröffentlichungen haben eine andere Qualität als herkömmliche Veröffentlichungen, etwa in Printmedien. Sie sind mit besonderen Gefahren für das Persönlichkeitsrecht aller Betroffenen verbunden. Das ergibt sich insbesondere daraus, dass Daten im Internet weltweit abrufbar und damit weltweit verfügbar sind, dass sie mit anderen Daten (auch aus anderen Quellen) verknüpfbar sind und dass die Daten, insbesondere wenn sie von Suchmaschinen erfasst sind, kaum mehr „aus der Welt zu schaffen“ sind, auch wenn sie auf der Internet-Seite, von der sie stammen, gelöscht sind. Den letztgenannten Problemkreis reißt der 26. Tätigkeitsbericht für das Jahr 2005 an (LT-Drucksache 13/4910). Das betrifft nicht nur Beschäftigte. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont in ihrer Entschließung vom 8./9. Oktober 2009 „Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur“, dass die zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft unser aller Persönlichkeitsrecht gefährden (vgl. Anhang 3).

– Ich begrüße daher auch die im Koalitionsvertrag vom 26. Oktober 2009 zum Ausdruck kommende Haltung der Bundesregierung, wonach die Risiken der Digitalisierung, die es ermöglicht, quasi auf Knopfdruck Daten zusammenzuführen und durch die Auswertung digitaler Spuren umfassende Persönlichkeitsprofile zu bilden, nicht durch staatliches Handeln verstärkt werden dürfen. Nach dem Koalitionsvertrag soll auch geprüft werden, wie durch die Anpassung des Datenschutzrechts der Schutz personenbezogener Daten im Internet verbessert werden kann, wobei auch von jedem Einzelnen ein verantwortungsvoller Umgang mit seinen persönlichen Daten im Internet erwartet wird.

Jegliches Verarbeiten eines personenbezogenen Datums unterliegt dem gesetzlichen Verbot mit Erlaubnisvorbehalt (das Verarbeiten ist verboten, außer es ist durch Rechtsvorschrift oder Einwilligung erlaubt, vgl. § 4 Abs. 1 LDSG). Das gilt auch für personenbezogene Daten über Beschäftigte einer öffentlichen Stelle.

Im Volkszählungsurteil des Bundesverfassungsgerichts (vom 15. Dezember 1983, 1 BvR 209/83 u. a., BVerfGE 65, 1, 45) heißt es zur Tragweite des Rechts auf informationelle Selbstbestimmung für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt, u. a.:

„Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und anderer-

seits von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr.

Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs."

Dazu ist Folgendes festzuhalten:

– Bei einem Veröffentlichen von Daten im Internet gibt es keinen wirksam festlegbaren Verwendungszusammenhang. Diese Daten können zu allen denkbaren Zwecken verwandt werden.

– Wenn eine öffentliche Stelle auf ihrer Internet-Seite einen Ansprechpartner namentlich nennt, erklärt sie damit regelmäßig zugleich, dass er dort beschäftigt ist.

– Weil das Veröffentlichen bzw. Zugänglichmachen personenbezogener Daten über Beschäftigte im Internet besondere Gefahren für das Recht auf informationelle Selbstbestimmung begründet, dürfen personenbezogene Daten über Beschäftigte ausnahmslos nur dann übers Internet abrufbar sein, wenn eine normenklare Rechtsvorschrift diese Veröffentlichungsform ausdrücklich erlaubt, zumindest jedoch bewusst einbezieht, oder wenn der Betroffene eingewilligt hat. Das ist bei § 12 Abs. 5 des Landeshochschulgesetzes (LHG) der Fall. Nach der Gesetzesbegründung dazu kann das dort geregelte Veröffentlichen unter Umständen auch die Aufnahme personenbezogener Daten in Internet-Auftritten umfassen (LT-Drucksache 13/3640, S. 184).

  § 12 Abs. 5 LHG

  Die Hochschulen dürfen in ihren Veröffentlichungen bei Angaben über die dienstliche Erreichbarkeit ihrer Mitglieder und Angehörigen ohne deren Einwilligung nur Name, Amts-, Dienst- und Funktionsbezeichnung, Telefon- und Telefaxnummern sowie E-Mail- und Internet-Adressen aufnehmen, soweit die Aufgabe der Hochschule und der Zweck der Veröffentlichung dies erfordern. Betroffene können der Veröffentlichung widersprechen, wenn ihr schutzwürdiges Interesse wegen ihrer besonderen persönlichen Situation das Interesse der Hochschule an der Veröffentlichung überwiegt. Andere als die in Satz 1 aufgeführten Angaben dürfen nur veröffentlicht werden, soweit die Betroffenen eingewilligt haben.

  Dagegen stellt etwa § 36 Abs. 1 LDSG keine solche normenklare Rechtsvorschrift dar.

  § 36 Abs. 1 LDSG

  Personenbezogene Daten von Beschäftigten dürfen nur verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienst- oder Betriebsvereinbarung es vorsieht.

– Die Meinung, mit dem Nennen des Namens, der Dienstbezeichnung, der dienstlichen Telefonnummer und der dienstlichen E-Mail-Adresse eines Beamten würden „keine in irgend einer Hinsicht schützenswerten perso-

nenbezogenen Daten preisgegeben“, sodass sich die Frage nach einer für Eingriffe in individuelle Rechte erforderlichen Ermächtigungsgrundlage nicht stelle (vgl. Bundesverwaltungsgericht, Beschluss vom 12. März 2008, 2 B 131.07, Rdnr. 8), bezog sich auf einen Einzelfall bei einer Bibliothek in Rheinland-Pfalz. Ich teile diese Auffassung auch mit Blick auf das Volkszählungsurteil nicht. Das gilt auch für das weitere Argument des Gerichts, dass eine juristische Person des öffentlichen Rechts, soweit sie befugt ist, ihre behördliche und organisatorische Struktur zu regeln, auch ohne ausdrückliche gesetzliche Ermächtigung befugt sei, dem außenstehenden Benutzer, für dessen Bedürfnisse sie eingerichtet ist, einen Hinweis darauf zu geben, welche natürlichen Personen als Amtswalter (Beschäftigte) mit der Erfüllung einer bestimmten Aufgabe betraut und damit in einer auf Außenkontakt gerichteten Behörde für das Publikum die zuständigen Ansprechpartner seien, und dass es allein im organisatorischen Ermessen der Behörde liege, ob sie diesen Hinweis etwa durch Übersichtstafeln, Namensschilder oder auf ihrer Internet-Seite gebe.

Auch wenn die Entscheidung des Dienstherrn (bzw. Arbeitgebers) für einen „personalisierten“ Behördenauftritt im Internet in dessen „Organisationsermessen“ liegt, so macht das eine normenklare Rechtsvorschrift nicht entbehrlich, die es erlaubt, personenbezogene Daten über Beschäftigte im Internet zu veröffentlichen bzw. zugänglich zu machen. Das gilt auch dann, wenn es um personenbezogene Daten über Beamte geht und diese in ihrer Stellung als Amtsträger betroffen sind.

Der Dienstherr kann den Anliegen, die für „personalisierte“ Behördenauftritte im Internet vorgebracht werden, auch Rechnung tragen, ohne personenbezogene Daten über Beschäftigte im Internet preiszugeben:

– Dritte können den zuständigen Beschäftigten bei einer öffentlichen Stelle auch erreichen, wenn nur dessen Sachgebiet, die Telefondurchwahl und beispielsweise eine funktionsbezogene E-Mail-Adresse angegeben sind. Die zusätzliche Angabe des Namens trägt nicht dazu bei, dass sie die öffentliche Stelle besser oder schneller erreichen.

  Mir erschließt sich auch deswegen nicht, aufgrund welcher Vorstellungen und mit welcher Zielrichtung darauf hingewiesen wird, kein Bediensteter einer Behörde habe Anspruch darauf, von Publikumsverkehr und von der Möglichkeit, postalisch oder elektronisch von außen mit ihm Kontakt aufzunehmen, abgeschirmt zu werden, es sei denn, legitime Interessen z. B. der Sicherheit geböten dies (vgl. Bundesverwaltungsgericht, Beschluss vom 12. März 2008, 2 B 131.07, Rdnr. 8). Das ist eine Selbstverständlichkeit. Doch was soll das damit zu tun haben, ob auf der Internet-Seite einer öffentlichen Stelle zusätzlich zur dienstlichen Telefondurchwahlnummer und zur etwaigen dienstlichen funktionsbezogenen E-Mail-Adresse der Name des Beschäftigten genannt wird oder nicht? Das wird niemanden dazu bringen oder davon abhalten, sich an den Beschäftigten zu wenden.

– Für „personalisierte“ Behördenauftritte wird auch ins Feld geführt, es wirke sich positiv auf das Verhältnis „des Bürgers zur Verwaltung“ aus, wenn er wisse, dass er sich an den richtigen Ansprechpartner wende und nicht mit einer Stelle kommunizieren müsse, die mit seiner Angelegenheit nicht vertraut sei. Müsse der Einzelne die Behörde als solche anschreiben, bleibe für ihn das weitere Prozedere ungewiss und die Verwaltung erscheine ihm als anonymes, schwer zu durchschauendes Gebilde. Diese Belange sind mit Angaben ohne Personenbezug ohne Probleme erfüllbar.

– Ebenso wird gelegentlich vorgebracht, bei mehreren Mitarbeitern mit demselben Nachnamen innerhalb einer Behörde könne der Dritte am Vornamen erkennen, ob er es mit derselben oder mit einer anderen Person zu tun habe. Durch die Angabe der Amtsbezeichnung werde erkennbar, wo sich der Beamte nach seiner Stellung innerhalb des Ämtergefüges befinde. Ähnliches treffe auf Funktionsbezeichnungen zu. Diese Aspekte mögen zwar für manche Personen interessant sein. Trotzdem

kann dienstlichen Belangen mit Angaben ohne Personenbezug (etwa der dienstlichen Telefondurchwahlnummer des Leiters eines bestimmten Referats einer Behörde) Rechnung getragen werden.

– Die Öffentlichkeit könne, so wird auch hervorgehoben, infolge entsprechender Angaben im Internet Handlungen bestimmten Amtswaltern zuordnen. Personalisierte Behördenauftritte förderten deshalb die Verwaltungstransparenz. Sofern es um für die Öffentlichkeit bedeutsame Vorgänge geht, sind Auskünfte zu den konkreten Vorgängen aus meiner Sicht jedoch grundsätzlich beim letztlich verantwortlichen Leiter der öffentlichen Stelle oder bei der Pressestelle zu erfragen. Zudem ist Angaben zu Zuständigkeiten nicht stets zu entnehmen, welcher Beschäftigte tatsächlich mit einem konkreten Vorgang befasst ist. Abgesehen davon tritt nach außen in der Regel ohnehin allein die Behörde als Einheit in Erscheinung, unabhängig davon, welcher Beschäftigter (als Organwalter der Behörde) jeweils tatsächlich gehandelt hat.

– Wenn ich selbst ein Anliegen an eine öffentliche oder private Stelle habe und mit dieser Kontakt aufnehmen will, kommt es mir entscheidend darauf an, dass ich den zuständigen Beschäftigten möglichst schnell erreiche. Ob ich dazu vorab dessen Namen erfahre und ob die Stelle sich in ihrem Internet-Auftritt als „modern“ darzustellen versucht, ist für mich dabei von nachrangiger Bedeutung. Soweit im Zusammenhang mit „personalisierten“ Behördenauftritten auf die Privatwirtschaft verwiesen wird, will ich den Blick auf die dort verbreiteten Callcenter lenken. Dort gibt es – meines Wissens – gerade keine Zuständigkeiten eines bestimmten Beschäftigten für bestimmte Fragen oder für bestimmte Kunden. Ich fühle mich jedoch weder schlecht noch unpersönlich behandelt, wenn ich dort anrufe, ohne dass ich zuvor den Namen des Gesprächspartners aus dem Internet erfahren habe. Jedenfalls hängt die Qualität eines Callcenters nicht vom Namen des Gesprächspartners ab.

Die Gefahren, die mit dem Veröffentlichen bzw. Zugänglichmachen personenbezogener Daten im Internet verbunden sind, sind zu verringern:

– Die Internet-Seite einer öffentlichen Stelle sollte nicht als Treffer genannt werden, wenn ein Dritter (etwa der neugierige Nachbar) bei einer Suchmaschine den Namen des Beschäftigten als Suchkriterium eingibt. Dazu sind im 26. Tätigkeitsbericht für das Jahr 2005 (LT-Drucksache 13/4910), auf den ich insoweit verweise, zwei Varianten dargestellt. Hierbei ist die datenschutzfreundlichere Variante, personenbezogene Daten aufgrund eines Dialogs anzuzeigen (dort 2. Punkt), der Variante vorzuziehen, die Seiten entsprechend zu kennzeichnen (dort 1. Punkt).

  Die Wirksamkeit der Kennzeichen-Variante hängt davon ab, dass die Suchmaschinen-Betreiber das Kennzeichen beachten und die Seiten nicht indexieren; das Kennzeichen schließt einen Zugriff der Suchmaschinen auf die Seiten mit den personenbezogenen Daten nämlich nicht technisch aus. Deswegen kann jede inländische oder ausländische Stelle – nicht nur die Suchmaschinen-Betreiber – diese Daten uneingeschränkt zu jedem beliebigen Zweck erfassen und weiter verarbeiten.

  Bei der Dialog-Variante besteht diese Gefahr jedenfalls derzeit im Allgemeinen nicht: Dabei können die Suchmaschinen bereits technisch nicht auf die Daten zugreifen, weil die Seiten mit den personenbezogenen Daten, die im Rahmen eines Dialogs abgerufen werden müssen, vor den Suchmaschinen verborgen sind.

– Selbst dann, wenn eine normenklare Rechtsvorschrift oder eine informierte Einwilligung es erlaubt, personenbezogene Daten über das Internet zugänglich zu machen, sind die Daten der Betroffenen vor einer zweckentfremdenden Verwendung so weit wie möglich zu schützen und nicht „ohne Not“ unbeschränkten Zugriffen preiszugeben. Dazu ist aus Sicht des Datenschutzes ein Zugriff von Suchmaschinen auf diese Daten mittels der datenschutzfreundlicheren Dialog-Variante technisch auszuschließen. Das gilt auch bei Einwilligungen der Betroffenen nach umfas-

sender Aufklärung über die Risiken. Zudem bestehen bei Beschäftigten wegen des bestehenden Abhängigkeitsverhältnisses Besonderheiten: Der betroffene Beschäftigte willigt möglicherweise nur deswegen ein, weil er nicht als illoyal oder „schwierig“ gelten möchte oder bei einer Weigerung Nachteile befürchtet. Jedenfalls wurde mir schon von „Stress“ in der Belegschaft einer öffentlichen Stelle berichtet, als der Vorgesetzte auf die Veröffentlichung der Namen der Mitarbeiter (mit Fotos) gedrängt habe.

Dem Grundsatz der Datenvermeidung ist bei Internet-Seiten mehr Gewicht als bisher beizumessen. Personenbezogene Daten, die nicht von einer Internet-Seite abrufbar sind, können auch nicht beliebig weiterverarbeitet werden. Das ist der wirksamste Schutz von Daten.

Personenbezogene Daten über Beschäftigte sind ausschließlich aufgrund einer normenklaren Rechtsvorschrift im Internet zu veröffentlichen bzw. zugänglich zu machen oder aufgrund einer informierten Einwilligung der Beschäftigten. Die Einwilligung sollte sich lediglich auf die Dialog-Variante beziehen, das heißt keinen Zugriff von Suchmaschinen zulassen.

4. E-Mail-Kontrollen am Arbeitsplatz

Darf der Dienstherr E-Mails seiner Beschäftigten kontrollieren?

Der Dienstherr (bzw. Arbeitgeber) muss seinen Beschäftigten nicht erlauben, den dienstlichen Internet-Zugang oder die dienstliche E-Mail-Funktion privat zu nutzen. Erteilt er jedoch eine solche Erlaubnis, dann darf er sie grundsätzlich an einschränkende Voraussetzungen knüpfen, etwa in Gestalt einer angemessenen Kontrolle. Hinweise hierzu sind in der „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz“ des Arbeitskreises Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. September 2007 dargestellt (abrufbar über die Internet-Seite meines Amts unter „Service“ → „Gemeinsame Materialien von BfD und LfDs“). Auch meine Pressemitteilung vom 27. Juli 2009 (abrufbar über die Internet-Seite meines Amts unter „Der LfD und seine Aufgaben“ → „Pressemitteilungen“ und dem genannten Datum) befasst sich mit der Kontrolle von E-Mails. Deswegen spreche ich nachfolgend lediglich einzelne Punkte an.

Der Dienstherr darf grundsätzlich stichprobenweise prüfen, ob die Beschäftigten die E-Mail-Funktion in zulässiger Weise nutzen (etwa ausschließlich dienstlich oder zwar auch privat, aber nur in einem bestimmten Rahmen). Dabei muss er u. a. Folgendes beachten (unabhängig davon, ob ausschließlich dienstliche oder auch private Nutzung erlaubt ist):

- Der Dienstherr muss das Protokollieren, das Auswerten und die Kontrolle des Nutzens der E-Mail-Funktion so regeln, dass er dabei jeweils keine, ansonsten möglichst wenige personenbezogene Daten verarbeitet. Das gilt auch für das sonstige Verarbeiten personenbezogener Daten im Zusammenhang mit E-Mails. Diese Regelungen müssen eindeutig sein.
- Der Dienstherr muss die Beschäftigten umfassend über Art und Umfang des Verarbeitens ihrer personenbezogenen Daten informieren. Dazu gehören auch mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen.

Wenn der Dienstherr das Nutzen der E-Mail-Funktion durch die Beschäftigten kontrolliert, dann muss er sich insbesondere an die Grundsätze der Datenvermeidung, der Datensparsamkeit und der Transparenz halten. Die Beschäftigten sind über die Vorgehensweise vorab umfassend in Kenntnis zu setzen.

5. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheit

1. ESU – die neue Einschulungsuntersuchung

Ende des Jahres 2008 wurde die neu konzipierte Einschulungsuntersuchung auf der Grundlage der Verwaltungsvorschrift des Ministeriums für Arbeit und Soziales zur Durchführung der Einschulungsuntersuchung (ESU-VwV) vom 28. November 2008 (GABl. S. 381) in Verbindung mit § 2 Abs. 2 der Schuluntersuchungsverordnung flächendeckend in Baden-Württemberg eingeführt. In der Praxis stößt die Einschulungsuntersuchung bei Erzieherinnen, Eltern und Gesundheitsämtern auf massive Kritik. Dabei spielen nicht nur fachliche Gesichtspunkte, sondern vor allem auch datenschutzrechtliche Bedenken eine große Rolle.

Wesentliche Elemente der Neukonzeption der Einschulungsuntersuchung sind die Vorverlagerung der Untersuchung in das Kindergartenalter (24 bis 15 Monate vor der Einschulung), die Fokussierung auf Kinder mit Entwicklungsrisiken und die vermehrte Einbeziehung zusätzlicher Befunde. Damit sollen frühzeitig Entwicklungsverzögerungen bei Vorschulkindern festgestellt werden, um rechtzeitig geeignete Fördermaßnahmen einleiten zu können. Eine weitere Untersuchung im folgenden Jahr soll die Schulreife sicherstellen. Im Rahmen eines zweijährigen Modellprojektes wurde 2006/ 2007 die neue Einschulungsuntersuchung in zehn Stadt- und Landkreisen erprobt.

Mein Amt erhielt bereits in einem sehr frühen Verfahrensstadium, nämlich bereits vor dem Start der zweijährigen Modellphase, Gelegenheit, zu Fragen des Datenschutzes Stellung zu nehmen (vgl. 26. Tätigkeitsbericht für das Jahr 2005, LT-Drucksache 13/4910, 27. Tätigkeitsbericht für das Jahr 2006, LT-Drucksache 14/650). Erfreulicherweise wurde mein Vorgänger erneut beteiligt, als es um die Schaffung der Rechtsgrundlagen für die flächendeckende Einführung der Einschulungsuntersuchung ging. Hinsichtlich der umfangreichen Datenerhebung im Rahmen der neuen Einschulungsuntersuchung hat meine Dienststelle erhebliche Zweifel geäußert, ob diese auf einer tragfähigen Rechtsgrundlage, hier der ESU-VwV, basiert. Denn die wesentlichen Bestimmungen zu Inhalt und Grenzen der Verarbeitung personenbezogener Daten müssen in einem Gesetz getroffen werden, aus dem klar und eindeutig die rechtliche Betroffenheit der Kinder und gegebenenfalls auch anderer Beteiligter unmittelbar erkennbar ist. Es ist mit dem Grundrecht auf informationelle Selbstbestimmung und dem Prinzip des Vorbehalts des Gesetzes nicht zu vereinbaren, solche Bestimmungen einer Verwaltungsvorschrift, hier also der ESU-VwV, vorzubehalten. Auch die Schuluntersuchungsverordnung, die wiederum auf dem Gesundheitsdienstgesetz beruht, stellt aus datenschutzrechtlicher Sicht keine hinreichende Rechtsgrundlage dar. Trotz der von meinem Vorgänger wiederholt geäußerten Befürchtung, dass damit einer rechtswidrigen Verarbeitung von sensiblen Daten Tür und Tor geöffnet ist, wurden seine Bedenken nicht berücksichtigt. Auch ich kann das nur bedauern.

Selbst wenn eine ausreichende Rechtsgrundlage vorliegen würde, ist eine Datenerhebung nicht völlig frei, sondern muss sich an den Grundsätzen der Erforderlichkeit, Geeignetheit und Verhältnismäßigkeit orientieren. Darauf hat meine Dienststelle vor allem im Hinblick auf die landeseinheitlich zu verwendenden Formularsätze nach der ESU-VwV hingewiesen. Besonders kritisch sehe ich hier die Eltern- und Erzieherinnenfragebögen, auch nachdem der Elternfragebogen, verglichen mit seiner ersten Fassung, entschärft wurde und freiwillig ist. Im Kern hat die datenschutzrechtliche Kritik bisher aber nichts gefruchtet.

Vor diesem Hintergrund war es meinem Vorgänger und mir wichtig, die Einschulungsuntersuchung weiter im Auge zu behalten. Meine Mitarbeiter haben sich deshalb rund sechs Monate nach der flächendeckenden Einführung in einem Gesundheitsamt, in einem Kindergarten und in einer Grundschule über die Umsetzung informiert. Dabei stand die Frage im Vor-

dergrund, ob die bisherige Einschätzung, dass die umfangreichen Datenerhebungen in Form der Eltern- und Erzieherinnenfragebögen nicht erforderlich und teilweise ungeeignet sind und dass gegebenenfalls auch datenschutzfreundlichere Verfahrensweisen denkbar wären, zutrifft.

So haben wir zum Thema „Elternfragebogen“ stets die Auffassung vertreten, dass sich nicht bei allen Fragen der Zweck und die Erforderlichkeit der Datenerhebung erschließt. Dies gilt beispielsweise für die Frage nach der Geburt des Kindes (normale Geburt/Frühgeburt/Mehrlingsgeburt/Komplikationen). Wir meinen: Entscheidend für die Beurteilung der Schulfähigkeit und eventuell notwendiger Fördermaßnahmen ist der tatsächliche Entwicklungsstand des Kindes zum Zeitpunkt der Untersuchung. Die Gründe, die gegebenenfalls zu einer Entwicklungsverzögerung bzw. -defiziten geführt haben, sind für diese Feststellung zunächst nicht entscheidend. Soweit für die Beurteilung und Festlegung von Fördermaßnahmen die nachgefragten Informationen erforderlich sind, können diese selbstverständlich erhoben werden, aber nicht generell zu einem Zeitpunkt, an dem noch gar nicht feststeht, ob diese Informationen im Einzelfall benötigt werden. Entsprechendes gilt auch für die Fragen, die mit der Schulfähigkeit des Kindes zunächst nichts zu tun haben, wie Fragen nach gesundheitlichen und anderen Problemen in der Familie, nach dem Medienverhalten der Kinder, dem Bildungsstand und der Berufstätigkeit der Eltern und nicht zuletzt nach Verhalten und Stimmung der Kinder. Soweit diese Fragen ohne konkreten Anlass gestellt werden, sehe ich hier die Gefahr einer vorzeitigen Stigmatisierung. Auf jeden Fall wäre dies eine (unzulässige) Datenerhebung auf Vorrat.

Das von uns kontrollierte Gesundheitsamt erachtete demgegenüber die Erhebung aller im Fragebogen erhobener Daten für wichtig und auch erforderlich, um ein möglichst differenziertes Bild des jeweiligen Kindes zu erhalten und darauf aufbauend, unter Berücksichtigung des familiären und sozialen Hintergrundes, die im Einzelfall geeigneten Fördermaßnahmen treffen zu können. Diese Auffassung verkennt jedoch, dass mit Hilfe der Untersuchung die Schulfähigkeit des Kindes beurteilt werden soll und daher auch nur die zur Beurteilung geeigneten und erforderlichen Daten erhoben werden dürfen (§ 13 Abs. 1 LDSG). Denn nicht alle Daten, die zu irgendeinem Zeitpunkt zu einem bestimmten Zweck erforderlich sein könnten und deren Erhebung daher wünschenswert erscheint, dürfen erhoben werden. Dies hat das Bundesverfassungsgericht in seinem Urteil vom 15. Dezember 1983 (1 BvR 209/83) – dem sog. Volkszählungsurteil – deutlich gemacht. Danach müssen sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken. Die Tatsache, dass das Ausfüllen des Elternfragebogens freiwillig geschieht, ändert daran nichts.

Dass mein Vorgänger und ich mit unserer datenschutzrechtlichen Beurteilung nicht völlig falsch liegen, hat das Gesundheitsamt der Landeshauptstadt Stuttgart bestätigt. Das Gesundheitsamt Stuttgart beschreitet, abweichend von der bei anderen Gesundheitsämtern üblichen Verfahrensweise, aber noch im Rahmen der ESU-VwV, einen eigenen Weg, den sog. „Stuttgarter Weg“. Nach Angaben des Gesundheitsamts Stuttgart wurde dort in Zusammenarbeit mit Elternvertretern, Mitarbeiterinnen von Kindertageseinrichtungen, Bereichsleitern und Trägern eine an die Verhältnisse der Stadt Stuttgart angepasste Variante der Einschulungsuntersuchung erarbeitet: Vorrangiges Ziel sei dabei eine gute Beratung der Eltern, der pädagogischen Fachkräfte und der Lehrerinnen und Lehrer, um die Förderung der Kinder zu optimieren. Insbesondere verzichte der „Stuttgarter Weg“ auf den Elternfragebogen, stattdessen finde eine ärztliche Befragung der Eltern im Rahmen der Untersuchung des Kindes durch einen Kinderarzt statt. Die für die kindliche Entwicklung und die anstehende Einschulung relevanten medizinischen Daten würden durch die persönliche ärztliche Anamnese erhoben. Konkret werde nach Vorerkrankungen, Geburtsanamnese, schweren Krankheiten, Behinderung, Fördermaßnahmen und Geschwistern gefragt. Sozialdaten würden hingegen nur dann nachgefragt, soweit dies im Einzelfall erforderlich sei. Die Daten würden statistisch nicht verarbeitet. Diese Vorgehensweise trage nach den bisherigen Erfahrungen des Gesundheitsamts den Befürchtungen der Eltern Rechnung und habe zu einer hohen Akzeptanz bei den Betroffenen geführt. Wichtig sei für das Gesundheitsamt,

dass dadurch im Einzelfall sichergestellt werden könne, dass auch nur die für die Beurteilung des Kindes erforderlichen Daten erhoben werden. Was erforderlich sei, ergebe sich im Gespräch mit den Eltern im Rahmen der Untersuchung.

Unter Berücksichtigung der Grundsätze der Erforderlichkeit und Geeignetheit der Datenerhebung sowie der Datensparsamkeit begrüße ich diese Vorgehensweise. Das Beispiel des Gesundheitsamts Stuttgart zeigt, dass eine kritische Hinterfragung der Einschulungsuntersuchung, namentlich des Elternfragebogens, zu einer wesentlich datenschutzfreundlicheren Verfahrensweise führt, die das Ziel der Einschulungsuntersuchung mindestens in gleichem Maße wie das (übliche) Verfahren nach der ESU-VwV erreicht.

Im Übrigen hat das Gesundheitsamt Stuttgart auch meine Bedenken hinsichtlich des Erzieherinnenfragebogens bestätigt. Dort wird auf den zweiten Teil (Teil B) dieses Fragebogens (Anlage 3 der ESU-VwV) verzichtet; stattdessen erfolge – so das Gesundheitsamt – eine differenzierte Beratung der Kindertageseinrichtungen und Schulen. Wenngleich aus datenschutzrechtlicher Sicht die mit dem Erzieherinnenfragebogen erhobenen Daten unkritischer erscheinen als die Fragen des Elternfragebogens, zeigt auch hier das Vorgehen der Stadt Stuttgart, dass eine umfangreiche Datenerhebung in den Kindertageseinrichtungen entbehrlich ist, da die erforderlichen Daten gegebenenfalls in Gesprächen und im Rahmen von Beratungen der Erzieherinnen, wiederum auf den Einzelfall bezogen, gewonnen werden können.

Soweit die so gewonnenen Daten zur Beurteilung der Schulreife des Kindes nicht geeignet und/oder nicht erforderlich sind, bleibt die Frage, wozu diese Daten dann letztendlich noch benötigt werden. Die Einschulungsuntersuchung ist eine staatliche Pflichtuntersuchung, mit der u. a. mittels der Eltern- und Erzieherinnenfragebögen zunächst ausschließlich die Schulreife des Kindes festgestellt werden soll. Darüber hinaus können nach Nr. 7.6 der ESU-VwV bei der Einschulungsuntersuchung erhobene personenbezogene Daten für Zwecke der Epidemiologie und Gesundheitsberichterstattung verarbeitet und in anonymisierter Form veröffentlicht werden. Dies ist aber eindeutig nicht der erklärte Sinn und Zweck der Eltern- und Erzieherinnenfragebögen. Fragen, die zur Beurteilung der Schulreife nicht geeignet oder erforderlich sind, sind aus datenschutzrechtlicher Sicht – trotz der vorgesehenen Freiwilligkeit – auch für statistische Zwecke im vorgesehenen Umfang nicht ohne weiteres hinnehmbar. Vielmehr ist hier allein schon deshalb ein restriktiver Maßstab anzulegen, weil ansonsten aus datenschutzrechtlicher Sicht unzulässige Vorratsdatenspeicherungen entstehen. Ich habe deshalb, bisher ebenfalls erfolglos, insoweit eine Präzisierung gefordert, welche Daten für Zwecke der Epidemiologie und Gesundheitsberichterstattung erforderlich und geeignet sind.

Ein ähnliches Bild ergab sich für meine Mitarbeiter nach dem Besuch eines städtischen Kindergartens, der die Neukonzeption bereits eingeführt hat. Auf den Elternfragebogen und den Erzieherinnenfragebogen angesprochen, wurde erklärt, dass hierfür eigentlich keine Notwendigkeit gesehen werde, da die abgefragten Informationen ohnehin schon weitgehend bekannt seien. Der Kindergarten führe regelmäßig Elterngespräche und dokumentiere die Ergebnisse; außerdem erfolgten regelmäßig Dokumentationen des Entwicklungsstandes der Kinder und etwaiger Besonderheiten. Im Übrigen würden die Fragen des Erzieherinnenfragebogens, die im Zusammenhang mit der Beurteilung der Schulreife für nicht relevant gehalten werden, nicht beantwortet. Auch von dieser Seite werden also meine Bedenken bestätigt, dass die nach der ESU-VwV vorgesehene umfangreiche Datenerhebung keinesfalls erforderlich ist.

Schließlich wollten meine Mitarbeiter bei einem Informations- und Kontrollbesuch noch wissen, wie die Grundschulen mit der neuen Einschulungsuntersuchung umgehen. Hier mussten wir jedoch feststellen, dass die ausgewählte Grundschule zu diesem Zeitpunkt in die neue Einschulungsuntersuchung noch nicht eingebunden war: Weder hatte das Gesundheitsamt der Schule die Ergebnisse der untersuchten fünfjährigen Kinder mitgeteilt noch fand insoweit eine Kooperation von Gesundheitsamt, Kindergarten und Schule in Form des beabsichtigten „Runden Tisches“ statt. Eine Beurteilung, welche Auswirkungen die Erkenntnisse aus der Einschulungsunter-

suchung bei der Einschulung durch die Grundschulen haben, war mir daher nicht möglich.

Um keine Missverständnisse aufkommen zu lassen: Ich sehe die Verlagerung der Untersuchung in das vorletzte Kindergartenjahr und die dadurch geschaffene Möglichkeit, Kindern mit Förderbedarf eine gezielte Förderung zukommen lassen zu können, um damit bessere Ausgangsbedingungen für den Schulstart zu schaffen, positiv. Allerdings darf dabei nicht das eigentliche Ziel der Einschulungsuntersuchung – die Beurteilung der Schulreife – aus den Augen verloren werden. Dies bedeutet aus datenschutzrechtlicher Sicht, dass nur die Daten im Rahmen der Einschulungsuntersuchung erhoben und verarbeitet werden dürfen, die für die Prüfung der Schulreife des Kindes geeignet und erforderlich sind. Dass dazu nicht das Ausfüllen umfangreicher Fragebögen notwendig ist, zeigt beispielhaft der „Stuttgarter Weg". Ungeachtet der für mich nach wie vor ungelösten Problematik der fehlenden Rechtsgrundlage, rate ich nachdrücklich zu landesweit datenschutzfreundlicheren Verfahrensweisen. Der „Stuttgarter Weg" kann hier Vorbild sein – andere Wege sind denkbar und möglich.

2. Krebsregister für Baden-Württemberg

2.1 Neue Entwicklungen im baden-württembergischen Krebsregister

Wie im 25. Tätigkeitsbericht für das Jahr 2004 (vgl. LT-Drucksache 13/3800) und im 26. Tätigkeitsbericht für das Jahr 2005 (vgl. LT-Drucksache 13/4910) mein Vorgänger dargelegt hat, gab es auch aus datenschutzrechtlicher Sicht begründeten Anlass, das Landeskrebsregister neu zu ordnen. Inzwischen hat der Landtag von Baden-Württemberg das Gesetz über die Krebsregistrierung in Baden-Württemberg (Landeskrebsregistergesetz – LKrebsRG) am 21. Februar 2006 beschlossen (GBl. S. 54). Meine Dienststelle hat die weitere Umsetzung eng begleitet.

Das Krebsregister Baden-Württemberg hat die Aufgabe, fortlaufend und einheitlich personenbezogene Daten über das Auftreten und den Verlauf von Krebserkrankungen einschließlich ihrer Frühstadien zu verarbeiten. Das Landeskrebsregistergesetz sieht dazu die Schaffung räumlich, organisatorisch und personell voneinander getrennter Einrichtungen vor – einer Vertrauensstelle, einer klinischen Landesregisterstelle und eines epidemiologischem Krebsregisters. Mit der Krebsregisterverordnung vom 20. März 2009 (GBl. S. 157) wurden die Träger der drei Einrichtungen des Krebsregisters Baden-Württemberg benannt.

Bereits im Rahmen der Erstellung des Landeskrebsregistergesetzes hat meine Dienststelle darauf hingewirkt, dass die Daten der Krebserkrankungen mit Personenbezug nicht unverschlüsselt an das klinische Krebsregister übermittelt werden. Unser Ziel war es, den verarbeiteten Daten zu einem möglichst frühen Zeitpunkt den Personenbezug zu nehmen, sie also nur in pseudonymisierter Form und verschlüsselt zu übermitteln. Dies wurde nunmehr so realisiert. Darüber hinaus haben wir bei der Festlegung des Prozessablaufes und insbesondere bei der Festlegung der technischen und organisatorischen Maßnahmen Anregungen und Hinweise gegeben, die erfreulicherweise berücksichtigt wurden. So wurde ein grundsätzlicher Architekturentwurf sowie eine Netzwerkarchitektur erstellt, an der auch die Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich aus dem Innenministerium Baden-Württemberg mitgewirkt hat. Alle Verfahrensverzeichnisse wurden durch mein Amt geprüft; mittlerweile wurde ein einheitliches, durchgängiges Sicherheitsniveau aller beteiligten Stellen erreicht. Hier war es vor allem wichtig, eine verlässliche, umfangreiche Protokollierung, insbesondere von lesenden und schreibenden Zugriffen auf die personenbezogenen Daten der Betroffenen zu erstellen. Immerhin handelt es sich bei den übertragenen und verarbeiteten Daten um besonders sensible medizinische Daten von Krebserkrankungen. Und schließlich konnte nach intensiver Beratung durch meine Dienststelle die Vertrauensstelle bei der Deutschen Rentenversicherung in Karlsruhe, die klinische Landesregisterstelle bei der Baden-Württembergischen Krankenhausgesell-

schaft e. V. in Stuttgart und das epidemiologische Krebsregister am Deutschen Krebsforschungszentrum Heidelberg angesiedelt werden.

Ich werde auch weiterhin die Umsetzung und den dann folgenden Betrieb des Krebsregisters kritisch im Auge behalten und zu einem späteren Zeitpunkt die Umsetzung sowie die Einhaltung der datenschutzrechtlichen Vorschriften im Rahmen eines Kontrollbesuches vor Ort überprüfen. Von dem Ergebnis dieser Prüfungen wird dann an dieser Stelle wieder zu berichten sein.

2.2 Hautkrebs-Screening

Auch bei der Einbeziehung des Hautkrebs-Screenings in das landesweite Krebsregister sind die datenschutzrechtlichen Anforderungen zu beachten.

Hautkrebserkrankungen nehmen seit Jahren immer mehr zu und sind inzwischen die häufigsten Krebserkrankungen in Deutschland. Seit dem 1. Juli 2008 haben gesetzlich Versicherte ab 35 Jahren alle zwei Jahre einen Anspruch auf eine Früherkennungsuntersuchung auf Hautkrebs, das sog. Hautkrebs-Screening. Das Ministerium für Arbeit und Soziales bat mich um Prüfung, ob die im Rahmen des Screening-Programms erhobenen Daten bei der Kassenärztlichen Vereinigung Baden-Württemberg vorübergehend so hinterlegt werden können, dass eine (spätere) Übermittlung an das im Aufbau befindliche Krebsregister Baden-Württemberg möglich ist.

Unsere datenschutzrechtliche Prüfung hat Folgendes ergeben:

– Die Kassenärztlichen Vereinigungen dürfen gemäß § 285 Abs. 2 des Fünften Buches des Sozialgesetzbuchs (SGB V) Einzelangaben über die persönlichen und sachlichen Verhältnisse der Versicherten nur erheben und speichern, soweit dies zur Erfüllung der in § 285 Abs. 1 Nr. 2, 5, 6 sowie in §§ 106 a und 305 SGB V genannten Aufgaben erforderlich ist.

  Nach § 285 Abs. 2 in Verbindung mit Absatz 1 Nr. 2 SGB V ist die Erhebung und Speicherung zulässig, soweit dies zur Sicherstellung der Vergütung der vertragsärztlichen Versorgung einschließlich der Überprüfung der Zulässigkeit und Richtigkeit der Abrechnung erforderlich ist. In der Richtlinie des Bundesausschusses der Ärzte und Krankenkassen über die Früherkennung von Krebserkrankungen (Krebsfrüherkennungs-Richtlinie) vom 15. November 2008 ist vorgesehen, dass die im Rahmen des Früherkennungsprogramms durchgeführte Untersuchung und eventuelle Abklärungsdiagnostik zu dokumentieren ist. Die vollständige Dokumentation ist Voraussetzung für die Abrechnungsfähigkeit der Früherkennungsmaßnahme. Danach ist die Erhebung und Speicherung der Daten zwar zum Zwecke der Abrechnung der Maßnahme zulässig, nicht aber zur – auch nur zeitweisen – Hinterlegung dieser Daten für andere Zwecke.

  Gemäß § 285 Abs. 2 in Verbindung mit Abs. 1 Nr. 6 SGB V können Daten zur Durchführung der Qualitätssicherung (§ 136) erhoben und gespeichert werden. Diese Regelung setzt allerdings voraus, dass die Qualitätssicherung durch die Kassenärztliche Vereinigung selbst durchgeführt wird. Da vorliegend die Qualitätssicherung ausschließlich durch das Krebsregister erfolgen soll, konnten wir auch insoweit keine Rechtsgrundlage für eine zeitweise Zumeldung an die Kassenärztliche Vereinigung sehen.

– Da wir die bereichsspezifischen Regelungen des Sozialgesetzbuchs insoweit als abschließend verstehen, ist eine entsprechende oder ergänzende Anwendung des Landesdatenschutzgesetzes im Geltungsbereich des Sozialgesetzbuchs ausgeschlossen. Somit kommt ein Rückgriff auf die nach den allgemeinen Regelungen des Landesdatenschutzgesetzes mögliche Einwilligung der Patienten als Ermächtigungsgrundlage, die das Ministerium für Arbeit und Soziales in Betracht gezogen hatte, nicht in Frage.

Die Besorgnis des Ministeriums für Arbeit und Soziales, die im Rahmen des Hautkrebs-Screenings erhobenen Daten könnten für das Krebsregister, das die Meldemöglichkeit der Hautärzte voraussichtlich erst ab dem Jahr 2011 ermöglicht, verloren gehen, kann ich zwar nachvollziehen. Dies kann und darf allerdings nicht dazu führen, dass mit der Hinterlegung der entsprechenden Daten – parallel zum Krebsregister – eine klinische Datenbank bzw. ein klinisches Register, bezogen auf Hautkrebserkrankungen, bei der Kassenärztlichen Vereinigung aufgebaut wird. Eine solche Datenbank wäre durch § 285 SGB V oder eine anderweitige Rechtsvorschrift des Sozialgesetzbuchs nicht gedeckt.

Da die Ärzte die von ihnen erhobenen Daten zehn Jahre aufbewahren müssen, habe ich dem Ministerium empfohlen, ein für alle Beteiligten vertretbares Verfahren zu finden, das eine vollständige Übermittlung der entsprechenden Datensätze an das Krebsregister durch die Ärzte im Jahr 2011 gewährleistet.

3. Kontrollbesuch bei der Zentralen Stelle Mammographie-Screening Baden-Württemberg

3.1 Mammographie-Screening

Am 1. Dezember 2006 begann nach jahrelanger intensiver Vorarbeit mit Eröffnung der ersten Mammographie-Screening-Einheit in der Region Stuttgart ein flächendeckendes Programm zur Früherkennung von Brustkrebs. Nachdem wir in den vergangenen Jahren die gesetzlichen (Neu-)Regelungen zum Mammographie-Screening in beratender Funktion begleitet hatten (vgl. 25. Tätigkeitsbericht für das Jahr 2004, LT-Drucksache 13/3800, 26. Tätigkeitsbericht für das Jahr 2005, LT-Drucksache 13/4910), haben wir nun deren praktische Umsetzung bei der Zentralen Stelle für das Einladungswesen beleuchtet.

Mammographie-Screening ist ein Früherkennungsprogramm von Brustkrebs mit Hilfe einer Röntgenuntersuchung. Angeboten wird dieses Programm allen Frauen von 50 bis 69 Jahren. Frauen dieser Altersgruppe werden alle zwei Jahre persönlich und schriftlich zu einer Früherkennungsuntersuchung eingeladen. Diese Einladung erfolgt in Baden-Württemberg über die Zentrale Stelle Mammograhie-Screening (im Folgenden „Zentrale Stelle“) mit Sitz in Baden-Baden. Die Kassenärztliche Vereinigung Baden-Württemberg hat sich mit den Krankenkassenverbänden auf Landesebene darauf geeinigt, dass die Zentrale Stelle bei der Kassenärztlichen Vereinigung Baden-Württemberg angesiedelt sein soll und in Form einer Arbeitsgemeinschaft gemäß § 219 des Fünften Buches des Sozialgesetzbuchs (SGB V) betrieben wird. Die Kosten der Zentralen Stelle werden von den Verbänden der Krankenkassen getragen.

Mit dem Gesetz über die Zentrale Stelle zur Durchführung des Einladungswesens im Rahmen des Mammographie-Screenings vom 28. Juli 2005 (GBl. S. 584), der Verordnung des Ministeriums für Arbeit und Soziales über die Altersgruppe der einzuladenden Frauen im Rahmen des Mammographie-Screenings vom 23. Dezember 2005 (GBl. 2006 S. 13) und der Änderung der Verordnung des Innenministeriums zur Durchführung des Meldegesetzes vom 28. Januar 2008 (GBl. S. 61) hat der Landesgesetzgeber die rechtlichen Voraussetzungen für die Einführung des Mammographie-Screenings geschaffen.

Im Gebiet der Kassenärztlichen Vereinigung Baden-Württemberg gibt es insgesamt zehn Screening-Einheiten. Sie werden von programmverantwortlichen Ärztinnen und Ärzten geleitet, die mit ihrem Team das Screening-Programm vor Ort mit jeweils mehreren Standorten für die Mammographie-Untersuchungen durchführen. Die Teilnahme am Screening-Programm ist freiwillig und kostenfrei. Wegen weiterer Informationen siehe *www.mammascreen-bw.de*.

3.2 Kontrollbesuch bei der Zentralen Stelle

Durch das Gesetz über die Zentrale Stelle zur Durchführung des Einladungswesens im Rahmen des Mammographie-Screenings wurde diese

als öffentliche Stelle errichtet und unterliegt als solche meiner datenschutzrechtlichen Kontrolle. Um beurteilen zu können, ob das Mammographie-Screening-Programm den Anforderungen des Datenschutzes Rechnung trägt, haben sich meine Mitarbeiter im Berichtszeitraum das Verfahren bei der Zentralen Stelle angesehen. Bei der Überprüfung des Verfahrens standen die Rechte der Frauen im Vordergrund, die nicht am Screening teilnehmen wollen und sich auch wiederholt mit ihren datenschutzrechtlichen Anliegen durch Anfragen und Eingaben an meine Dienststelle gewandt hatten.

Von dem Kontrollbesuch ist Folgendes berichtenswert:

Grundsätzlich hat die Zentrale Stelle bei ihrer Tätigkeit die einschlägigen Bestimmungen des Landesdatenschutzgesetzes zu beachten. Nach § 4 Abs. 1 LDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn entweder die eingeladenen Frauen in die Untersuchung eingewilligt haben oder es eine Rechtsgrundlage für die Durchführung der Untersuchung gibt.

Was die Datenübermittlungen im Zusammenhang mit dem Mammographie-Screening anbelangt, sind grundsätzlich zwei Übermittlungsvorgänge zu unterscheiden:

– Adressherausgabe durch die Meldebehörde

  Rechtsgrundlage hierfür ist § 14 der Meldeverordnung (MVO), der wie folgt lautet:

> *§ 14 MVO*
> *Datenübermittlungen an die Zentrale Stelle zur Durchführung des Einladungswesens im Rahmen des Mammographie-Screenings*
>
> *Zum Zwecke der persönlichen Einladung zur Teilnahme am Mammographie-Screening darf die Meldebehörde der Zentralen Stelle zur Durchführung des Einladungswesens im Rahmen des Mammographie-Screenings alle drei Monate folgende Daten der bei ihr mit alleiniger Wohnung oder mit Hauptwohnung gemeldeten Frauen übermitteln, die nach der Mammographie-Altersgruppenverordnung einzuladen sind:*
>
> 1. *Familiennamen,*
> 2. *Vornamen,*
> 3. *frühere Namen,*
> 4. *Doktorgrad,*
> 5. *Tag und Ort der Geburt,*
> 6. *gegenwärtige Anschrift (alleinige Wohnung oder Hauptwohnung).*

  Beim Kontrollbesuch konnten wir feststellen, dass die Übermittlung seitens der Meldestellen gesetzeskonform erfolgt. Allerdings enthielt die sog. Verfahrensbeschreibung der Zentralen Stelle in der Darstellung der Datenbankstruktur das Feld „Staatsangehörigkeit“. Dieses Datum darf mangels einer entsprechenden Rechtsgrundlage von der Meldestelle nicht übermittelt werden. Ein Blick in die von den Meldebehörden an die Zentrale Stelle übermittelten Daten zeigte, dass tatsächlich keine Übermittlungen im Feld „Staatsangehörigkeit“ erfolgt sind und dieses Feld bei der Zentralen Stelle auch nicht befüllt und auf keiner Anwendermaske sichtbar war. Dennoch habe ich dazu geraten, die Verfahrensbeschreibung an die Rechtslage anzupassen.

– Durchführung der Einladung durch die Zentrale Stelle

  Im Rahmen des Mammographie-Screening-Programms sollen personenbezogene Gesundheitsdaten von Frauen zwischen 50 und 69 Jahren in regelmäßigen Abständen durch bestimmte ärztlich geleitete Screening-Einheiten erhoben werden. Die Information der Scree-

ning-Einheit durch die Zentrale Stelle beruht auf einer (bundes-)gesetzlichen Grundlage (§ 82 Abs. 1, § 81 Abs. 3 des Fünften Buches des Sozialgesetzbuchs in Verbindung mit den Regelungen des Bundesmanteltarifvertrags-Ärzte). Nachdem für diese Datenübermittlung eine Rechtsgrundlage vorhanden ist, handelt es sich um eine zulässige Form der Datenverarbeitung gemäß § 4 Abs. 1 Nr. 1 LDSG, sodass diese datenschutzrechtlich grundsätzlich nicht zu beanstanden ist. Einer ausdrücklichen Zustimmung zur Datenweitergabe durch die betroffenen Frauen bedarf es demzufolge nicht.

Allerdings ist hierbei zu beachten, dass das Programm zur Früherkennung von Brustkrebs durch Mammographie-Screening nur ein Angebot an die betroffenen Frauen ist, die dieses auf freiwilliger Basis nutzen können. Datenschutzrechtlich bedeutet dies Folgendes:

Die Erhebung personenbezogener Gesundheitsdaten von Frauen zwischen 50 und 69 Jahren durch die Screening-Einheiten ist nach § 4 LDSG nur dann zulässig, wenn die betroffenen Frauen hierin eingewilligt haben, da es eine gesetzliche Teilnahmepflicht nicht gibt. Voraussetzung für eine rechtmäßige freiwillige Datenerhebung ist aber – wie grundsätzlich in allen (Einwilligungs-)Fällen –, dass die von der Zentralen Stelle eingeladenen Frauen auch hinreichend deutlich darüber aufgeklärt werden, dass sie aufgrund ihrer eigenen freien Willensbestimmung an den vorgeschlagenen Röntgenuntersuchungen teilnehmen können – oder auch nicht. Hierbei sind verschiedene Reaktionen der Teilnehmerinnen denkbar, auf die die Zentrale Stelle zur Wahrung der Datenschutzrechte der Betroffenen differenziert reagieren muss. Wir haben deshalb verschiedene Fallkonstellationen vor Ort näher geprüft und festgestellt, dass die hierfür vorgesehenen Verfahrensweisen datenschutzkonform sind und in der Praxis auch beachtet werden:

- Erklärt eine eingeladene Frau die Verweigerung der Teilnahme, wird eine Sperre auf Lebenszeit für die Teilnehmerin eingetragen. Sie erhält folglich bis zu einem Widerruf keine Einladungen. Der Datensatz in der Meldeliste wird gelöscht. Dies gilt auch in den Fällen, in denen Frauen mitgeteilt haben, dass sie derzeit nicht teilnehmen wollen, bereits in Behandlung sind oder den angebotenen Termin verschoben haben.

- Meldet sich die Frau hingegen nicht, wird zunächst davon ausgegangen, dass sie am Mammographie-Screening teilnehmen möchte. Bis 15 Tage nach dem (Erst-)Einladungstermin wird gewartet, ob die Screening-Einheit die Teilnahme meldet. Medizinische Daten erhält die Zentrale Stelle dabei nicht. Meldet die Screening-Einheit die Teilnahme, wird der Status auf „teilgenommen“ gesetzt und der Datensatz in der Meldeliste gelöscht. Meldet die Screening-Einheit keine Teilnahme, wird ein Erinnerungsschreiben mit einem neuen Termin verschickt und der Status auf „erinnert“ gesetzt.

  Es können nun die gleichen Fallvarianten eintreten wie bei der Ersteinladung: Es wird zunächst abgewartet, ob in den 15 Tagen nach dem Termin eine Teilnahmebestätigung durch die Screening-Einheit eingeht. Bestätigt die Screening-Einheit die Teilnahme, wird der Status auf „teilgenommen“ gesetzt und der Datensatz in der Meldeliste gelöscht. Hat die Frau auch auf das zweite Schreiben nicht reagiert und ist nicht zur Untersuchung gekommen, wird der Status auf „Erinnerung erfolglos“ gesetzt und der Datensatz aus der Meldeliste gelöscht.

– Verschiedene Frauen hatten sich bei meiner Dienststelle darüber beklagt, dass aufgrund der Absenderangabe und des einprägsamen Logos auf den Einladungsschreiben andere Menschen, z. B. beim Einwerfen eines Einladungsschreibens in den Briefkasten, erkennen können, dass es sich um ein Schreiben der Zentralen Stelle handelt und daraus auch Rückschlüsse auf das Alter der Frauen möglich seien.

Die Zentrale Stelle hat dieses Problem sofort aufgegriffen und verschiedene Entwürfe von Absenderangaben mit aufgedruckten kleineren Logos für die Einladungskuverts vorgestellt. In Abstimmung mit meinem Amt wurde die Adressangabe bzw. das Logo noch weiter geändert und ist datenschutzrechtlich nicht mehr zu beanstanden.

– In mehreren Eingaben, die meine Dienststelle in der Vergangenheit erreicht haben, haben Frauen – nicht ganz zu Unrecht – bemängelt, dass aus den Einladungs-/Erinnerungsschreiben der Zentralen Stelle für sie der Eindruck entstanden sei, dass es sich bei der Krebsvorsorgeuntersuchung nicht um ein Angebot zur freiwilligen Teilnahme, sondern um die Aufforderung zu einer verpflichtenden Untersuchung – ähnlich wie bei der Reihen-Röntgenuntersuchung in früheren Jahren aus anderem Anlass – handelte.

  Wir konnten einvernehmlich mit der Zentralen Stelle erreichen, dass die Einladungsvordrucke bzw. Erinnerungsschreiben so geändert wurden, dass in diesen nunmehr deutlich zum Ausdruck kommt, dass es sich beim Mammographie-Screening-Programm lediglich um ein an die Adresse der Frauen gerichtetes Angebot zur freiwilligen Teilnahme handelt.

– Das Verfahren sah zunächst vor, dass die personenbezogenen Daten der eingeladenen Frauen unmittelbar nach Versand der Einladung an die Screening-Einheit übermittelt werden, bei der die Untersuchung durchgeführt werden soll. Hier stellte sich die Frage, ob es – aus Gründen der Datensparsamkeit – nicht möglich ist, eine geraume Zeit abzuwarten, ob sich die Frauen aufgrund der Einladung melden (oder die Teilnahme ablehnen). Danach wäre es möglich, der Screening-Einheit nur die Daten von Frauen weiterzumelden, die mit hoher Wahrscheinlichkeit zum vorgeschlagenen Untersuchungstermin auch tatsächlich erscheinen werden.

  Meine Mitarbeiter konnten einen möglichen Ansatz für eine technische Lösung aufzeigen, bei der gewährleistet ist, dass die Datensätze erst nach einer bestimmten Zeit an die Screening-Einheiten übermittelt werden. So ist sichergestellt, dass Datensätze von Frauen, die eine Teilnahme ablehnen, nicht unnötig weitergegeben werden.

Gegen die Datenerhebung und -verarbeitung bei der Zentralen Stelle bestehen keine datenschutzrechtlichen Bedenken. Gleichwohl hat die Zentrale Stelle dafür Sorge zu tragen, dass auch künftig beim Mammographie-Screening die datenschutzrechtlichen Anforderungen beachtet werden. Ich werde die weitere Entwicklung im Auge behalten.

4. Die elektronische Gesundheitskarte – alle Jahre wieder: Termin zur Einführung erneut verschoben

Eigentlich sollte die elektronische Gesundheitskarte bereits ab 1. Januar 2006 die Krankenversichertenkarte ersetzen. Die Einführung hat sich jedoch mehrfach verzögert (vgl. 26. Tätigkeitsbericht für das Jahr 2005, LT-Drucksache 13/4910, 27. Tätigkeitsbericht für das Jahr 2006, LT-Drucksache 14/650, 28. Tätigkeitsbericht für das Jahr 2007, LT-Drucksache 14/2050). Der Zeitpunkt der flächendeckenden Einführung in Baden-Württemberg steht weiterhin in den Sternen.

Mit dem Gesetz zur Modernisierung der gesetzlichen Krankenversicherung wurden die Krankenkassen verpflichtet, die bisherige Krankenversichertenkarte zu einer elektronischen Gesundheitskarte zu erweitern. § 291 a Abs. 2, 3 des Fünften Buchs des Sozialgesetzbuchs (SGB V) legt fest, dass die Gesundheitskarte über einen verpflichtenden administrativen Teil (Name, Geburtsdatum, Geschlecht und Anschrift, Angaben zur Krankenversicherung wie Krankenversichertennummer, Versichertenstatus, persönlicher Zuzahlungsstatus, elektronisches Rezept) und einen freiwilligen medizinischen Teil (z. B. Dokumentation über eingenommene Arzneimittel, Notfalldaten, elektronischer Arztbrief, elektronische Patientenakte, vom Versicherten

selbst zur Verfügung gestellte Gesundheitsdaten) verfügen soll, ergänzt um eine detaillierte Auflistung der einzelnen Funktionen und Anwendungen. In einem weiteren Schritt sollen mit Einverständnis des Versicherten Arztbriefe mit Hilfe der Gesundheitskarte gespeichert bzw. weitergeleitet werden. Die elektronische Patientenakte (EPA) soll langfristig die letzte Ausbaustufe der Gesundheitskarte sein.

Die elektronische Gesundheitskarte ist durch die hohe Zahl der beteiligten Akteure und die technischen Neuerungen sehr komplex. Versicherte, Apotheken, niedergelassene Ärzte und Zahnärzte, Krankenhäuser und Krankenkassen gilt es über die sog. Telematik-Infrastruktur, eine abgeschottete, nur für diese Zwecke eingerichtete Computerinfrastruktur, zu vernetzen.

In enger Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder wurden die wesentlichen datenschutzrechtlichen Anforderungen formuliert und gesetzlich festgelegt (§ 291 a Abs. 4 bis 6 SGB V). Bei dem technischen Ausbau des Projekts muss nun sichergestellt werden, dass diese gesetzlichen Anforderungen auch angemessen umgesetzt werden.

Aus datenschutzrechtlicher Sicht gilt dabei mein besonderes Augenmerk nach wie vor der Wahrung der Rechte der Betroffenen: Von gesetzlicher Seite aus ergeben sich Anforderungen in Bezug auf das Auskunftsrecht des Betroffenen über den Inhalt der gespeicherten Daten und ihrer Herkunft sowie ein Berichtigungsanspruch hinsichtlich falscher und ein Löschungsanspruch hinsichtlich unzulässig gespeicherter Daten. Durch wirkungsvolle technische Sicherheitsvorkehrungen ist ferner sicherzustellen, dass ein unbefugter Zugriff auf personenbezogene Daten auf der Karte selbst oder in der Telematik-Infrastruktur verhindert wird. Zudem darf ein Zugriff Dritter auf die meisten eigenen Daten nur durch ein bewusstes Handeln des Patienten möglich sein:

– Zugriffskontrolle

  Für die Daten, außer den Notfalldaten, ist eine doppelte Autorisierung durch den Versicherten mittels der elektronischen Gesundheitskarte und PIN sowie durch den Zugriffsberechtigten, beispielsweise den Arzt, mit Hilfe des sog. elektronischen Heilberufeausweises mit PIN vorgesehen. Beide Komponenten verfügen über eine qualifizierte elektronische Signatur und ermöglichen auf diese Weise prinzipiell eine verlässliche Authentifizierung.

– Protokollierung

  Es muss erfasst werden, von wem welche Art von Zugriff auf welche Daten stattgefunden hat. Dabei ist es erforderlich, dass die letzten 50 Zugriffe protokolliert werden. Diese Zugriffe dürfen nur für eine Datenschutzkontrolle herangezogen werden. Eine Verwendung für andere Zwecke muss ausgeschlossen werden. Die Protokolldaten sind durch geeignete Vorkehrungen gegen zweckwidrige Verwendung und sonstigen Missbrauch zu schützen.

Diese sicherlich einleuchtenden datenschutzrechtlichen Anforderungen sind jedoch in der Realität bislang nur sehr eingeschränkt umgesetzt. Insbesondere die Maßnahmen zur Wahrung der Patientenrechte, wie die Klärung, welche Stelle vom Betroffenen angesprochen werden kann, wenn es um die Auskunftserteilung geht, sowie Fragen zur Durchsetzung eines Lösch- oder Sperranspruchs, sind bislang weitgehend unbeantwortet. Nach wie vor datenschutzrechtlich unklar bzw. – wenn es bei den derzeitigen Überlegungen bliebe – sogar bedenklich ist das Verfahren zur PIN-Eingabe. Wenn beispielsweise demenzkranke, ältere Patienten sich die PIN nicht merken können, so soll der Arzt diese für den Patienten eingeben. Doch dadurch ist der Arzt möglicherweise auch in der Lage, ohne Mitwirken des Patienten auf alle personenbezogenen Daten auf der elektronischen Gesundheitskarte zuzugreifen.

Vorbereitet wird die schrittweise Einführung der elektronischen Gesundheitskarte im Rahmen einer Testphase. In bundesweit sieben Testregionen, darunter im Stadt- und im Landkreis Heilbronn (Testregion Heilbronn), findet die Erprobung der elektronischen Gesundheitskarte statt. Ursprünglich

waren die Testvorhaben bis zum 31. Dezember 2007 geplant gewesen, diese Laufzeit wurde jedoch aufgrund von Projektverschiebungen um zwei Jahre verlängert.

Die am Testbetrieb teilnehmenden Ärzte der Testregion Heilbronn haben zum 31. Juli 2009 alle Verträge zum Gesundheitskartentest gekündigt. Grund hierfür war die Unzufriedenheit der Ärzte mit dem System. Bemängelt wurde insbesondere, dass die Arbeitsabläufe länger dauern als mit der bisherigen Krankenversichertenkarte und zumeist mehr Arbeitsschritte aufweisen würden, ohne dass aber zusätzliche Informationen oder eine bessere Qualität herauskämen. Der Stopp des Testbetriebs bedeutete gleichzeitig eine weitere Verschiebung der flächendeckenden Einführung der elektronischen Gesundheitskarte in der Region, die für das 3. Quartal 2010 vorgesehen war. Aber auch von politischer Seite ist erneut mit Verzögerungen zu rechnen, nachdem die neue Bundesregierung beabsichtigt, nunmehr eine Bestandsaufnahme des Gesamtprojektes durchzuführen. Damit ist derzeit völlig offen, ob und in welcher Weise die Einführung der elektronischen Gesundheitskarte weiter erfolgt.

Wie bereits in den vorausgegangenen Tätigkeitsberichten dargestellt, wird im weiteren Verlauf des Projektes von meiner Seite darauf geachtet werden, ob die datenschutzrechtlichen Anforderungen und vor allem die Rechte der Betroffenen auch tatsächlich berücksichtigt werden. Man darf gespannt bleiben.

2. Abschnitt: Die gesetzliche Krankenversicherung

1. Eigenmächtige Ermittlungen einer Krankenkasse

Ein bei einer gesetzlichen Krankenkasse Versicherter teilte uns mit, er habe die Reparatur- bzw. Ersatzkosten für eine Brille, die bei einem Arbeitsunfall beschädigt wurde, bei seiner Unfallversicherung geltend gemacht. Diese beauftragte einen Mitarbeiter, ohne Wissen des Versicherten Recherchen in dem von ihm beauftragten Brillenfachgeschäft sowie bei seiner Mutter vorzunehmen, um festzustellen, ob seine Angaben über die Beschädigung der Brille auch stimmen. Ihre Zweifel an der Richtigkeit der Unfallschilderung stützte die Unfallversicherung insbesondere darauf, dass der Versicherte fünf Jahre zuvor bereits einen nahezu identischen Arbeitsunfall gemeldet hatte.

Die Unfallversicherung vertrat die Rechtsauffassung, sie habe den Untersuchungsgrundsatz, der sich aus § 199 Abs. 1 Satz 2 des Siebten Buches des Sozialgesetzbuchs (SGB VII) in Verbindung mit § 20 und § 21 des Zehnten Buches des Sozialgesetzbuchs (SGB X) ergebe, zu beachten. Daraus ergebe sich ihre Berechtigung, von sich aus alle Umstände ermitteln zu dürfen, die für die Entscheidung „zweckmäßig“ erscheinen, auch wenn sie von den Verfahrensbeteiligten nicht vorgetragen wurden. Sie könne danach Auskünfte jeder Art einholen und auch (dritte) Personen formlos anhören. Die Auswahl sei lediglich an die Grundsätze der Effektivität und der Verwaltungsökonomie gebunden. Sie müsse sich – wenn sie mehrere Beweismittel zur Verfügung habe – lediglich fragen, mit welchem Beweismittel sie voraussichtlich einen sicheren Beweis erheben könne und welche Beweismittel ihr schneller zur Verfügung stünden.

Diese Auffassung konnte mein Amtsvorgänger so nicht teilen, als ihm der Fall 2008 auf den Tisch kam. Die Unfallversicherung verkannte nämlich bei ihrer Auslegung einen wesentlichen datenschutzrechtlichen Grundsatz, der in § 67 a Abs. 2 SGB X enthalten ist. Danach sind Sozialdaten grundsätzlich beim Betroffenen zu erheben (sog. Direkterhebungsgrundsatz). Für das Spannungsverhältnis zwischen dem von der Versicherung ins Feld geführten Amtsermittlungsgrundsatz (§§ 20 ff. SGB X) und dem Direkterhebungsgrundsatz nach § 67 a Abs. 2 SGB X ergibt sich ein Vorrang zugunsten der Datenermittlung beim Betroffenen selbst. Dies folgt bereits unmittelbar aus der Bestimmung des § 37 Satz 3 des Ersten Buches des Sozialgesetzbuchs (SGB I), der einen Vorrang des Zweiten Kapitels des SGB X vor dessen Erstem Kapitel statuiert. Mit anderen Worten: Der Amtsermittlungsgrundsatz, der es Sozialbehörden ansonsten in gewissen Grenzen freistellt, auf welche

Weise sie den entscheidungserheblichen Sachverhalt ermitteln wollen, wird insoweit eingeschränkt.

§ 199 Abs. 1 Satz 1 SGB VII statuiert den allgemeinen datenschutzrechtlichen Erforderlichkeitsgrundsatz auch für den Bereich der gesetzlichen Unfallversicherung. Dieser ist auch im Rahmen der Vorgehensweise zur Aufklärung von Arbeitsunfällen nach §§ 20 ff. SGB X zu beachten. Die dort aufgeführten Beweismittel (vgl. § 21 SGB X) können dabei vom Sozialversicherungsträger nicht beliebig allein nach Zweckmäßigkeitsgesichtspunkten ausgewählt werden. Maßstab beim konkreten Vorgehen muss dabei insbesondere auch sein, wie man das Grundrecht des Versicherten auf Datenschutz beachtet, ohne gleichzeitig den Aufklärungserfolg nachhaltig zu gefährden. Im geschilderten Schadensfall hatte die Versicherung auf die an sich nahe liegende Möglichkeit verzichtet, den Versicherten zunächst um Übersendung der noch vorhandenen beschädigten Brille zu bitten. Stattdessen wurde die Befragung der Mutter des Versicherten bzw. eines Verkäufers des Brillenfachgeschäfts als besser für die Prüfung der Frage angesehen, ob der konkrete Schaden an der Brille ursächlich von dem geschilderten Unfall herrühren kann. Nachdem aber weder die Mutter noch der Mitarbeiter des Brillenfachgeschäfts unmittelbare Zeugen des Unfalls gewesen waren, erschien diese Vorgehensweise zur Erreichung des damit verfolgten Ziels kaum geeignet und war damit auch datenschutzrechtlich nicht in Ordnung. Unabhängig hiervon wäre die Unfallversicherung verpflichtet gewesen, den Versicherten davon in Kenntnis zu setzen, dass aufgrund der Unfallschilderung und der bis dahin vorhandenen Beweislage eine Übernahme der Unfallkosten nicht möglich ist und – soweit der Versicherte damit einverstanden ist – weitere Rückfragen im Brillenfachgeschäft bzw. bei seiner Mutter in Betracht zu ziehen sind. Auch ein diesbezüglicher – und aus Sicht des Datenschutzes erforderlicher – Hinweis auf eine Datenerhebung bei Dritten unterblieb.

Die Unfallversicherung hat sich letztendlich unserer Auffassung angeschlossen und bestätigt, dass sie künftig im Rahmen ihrer Vorgehensweise zur Sachverhaltsaufklärung bei Arbeitsunfällen den Direkterhebungsgrundsatz beachten und die Mitarbeiter in geeigneter Weise entsprechend unterrichten wird. Die von uns empfohlenen datenschutzrechtlichen Anforderungen wurden zwischenzeitlich in Schulungs- und Fortbildungsmaßnahmen berücksichtigt.

2. Keine Arztberichte und Entlassungsberichte an Krankenkassen

(Fach-)Arztberichte und Entlassungsberichte haben bei Krankenkassen grundsätzlich nichts verloren. Inakzeptabel sind daher Verfahrensweisen, bei denen Krankenkassen bei Ärzten, Krankenhäusern oder Reha-Einrichtungen hochsensible und detaillierte Berichte anfordern.

Mit der Erhebung medizinischer Daten durch gesetzliche Krankenkassen musste sich meine Dienststelle in der Vergangenheit immer wieder beschäftigen (vgl. 19. Tätigkeitsbericht für das Jahr 1998, LT-Drucksache 12/3480, 20. Tätigkeitsbericht für das Jahr 1999, LT-Drucksache 12/4600, und 21. Tätigkeitsbericht für das Jahr 2000, LT-Drucksache 12/5740). Dies hindert mehrere Kassen aber nach wie vor nicht, sich ärztliche Berichte und Entlassungsberichte vorlegen zu lassen. Die Versicherten sollen hierzu ihr Einverständnis erklären. Nachdem diese Verfahrensweise immer wieder beanstandet wurde und längere Zeit keine entsprechenden Eingaben Betroffener mehr bei uns eingingen, nahmen wir an, dass unsere datenschutzrechtliche Auffassung Eingang in die Verwaltungspraxis aller meiner Zuständigkeit unterstehenden Krankenkassen gefunden hat. Insofern war es schon ärgerlich, als im Lauf des Jahres 2008 Fälle bekannt wurden, in denen – immer noch oder schon wieder – Krankenkassen Arztberichte und vollständige ärztliche Entlassungsberichte für den Medizinischen Dienst an sich selbst übermitteln lassen wollten.

Meine Haltung zu dieser Problematik ist nach wie vor eindeutig: Die Krankenkassen haben in den in § 275 des Fünften Buches des Sozialgesetzbuchs (SGB V) genannten Fällen (z. B. Arbeitsunfähigkeit, Leistungen zur medizinischen Rehabilitation) den Medizinischen Dienst mit einer Begutachtung

bzw. Prüfung zu beauftragen. Werden hierzu medizinische Informationen von Leistungserbringern benötigt, müssen sie diese dem Medizinischen Dienst unmittelbar übermitteln (§ 276 Abs. 2 Satz 1, 2. Halbsatz SGB V). Eine darüber hinausgehende pauschale Datenerhebung durch die Kassen selbst sieht das Fünfte Buch des Sozialgesetzbuchs nicht vor. Der Gesetzgeber hat mit der Einräumung dieser eigenständigen Datenerhebungskompetenz des Medizinischen Dienstes entschieden, dass die Krankenkassen diese Informationen gerade nicht erhalten sollen. Die Kassen dürfen lediglich um die Übermittlung der Behandlungsdaten unmittelbar an den Medizinischen Dienst ersuchen. Dies verdeutlicht auch die Regelung des § 277 Abs. 1 Satz 1 SGB V, wonach der Medizinische Dienst der jeweiligen Krankenkasse nur das Ergebnis der Begutachtung mitteilen darf, nicht aber die Informationen, aufgrund derer der Medizinische Dienst zu seiner Bewertung gekommen ist.

Die Einholung einer Einwilligung des Versicherten zur Übermittlung des Berichts an die Krankenkassen halte ich bereits deshalb für unzulässig, weil die Abfrage einer Einwilligung des Versicherten dem Leistungsträger zusätzliche Möglichkeiten der Datengewinnung eröffnen würde, die nach dem Willen des Gesetzgebers gerade nicht vorgesehen sind. Das Fünfte Buch des Sozialgesetzbuchs regelt für die Krankenkassen und den Medizinischen Dienst nämlich abschließend, in welchen Fällen Sozialdaten erhoben werden dürfen (§ 275 ff., § 284 ff. SGB V). Eine darüber hinausgehende Einwilligungslösung sieht das Sozialgesetzbuch nicht vor. Abgesehen davon wäre auch das Element der Freiwilligkeit in Zweifel zu ziehen, da der Versicherte die Nichtgewährung von Leistungen befürchten könnte, wenn ihm die Krankenkasse eine Einwilligung abverlangt.

Aufgrund der an mich herangetragenen Beschwerden von Versicherten muss ich davon ausgehen, dass sich bei den Krankenkassen eine datenschutzgerechte Verfahrensweise in der Praxis nur sehr schleppend im Bewusstsein der Mitarbeiterinnen und Mitarbeiter niederschlägt. Ich halte es daher für außerordentlich wichtig, insbesondere auch die Regional- und Bezirksdirektionen und deren Personal immer wieder vollumfänglich auf das datenschutzkonforme Vorgehen hinzuweisen und dessen Umsetzung auch tatsächlich zu überprüfen. Denn nur so kann letztlich sichergestellt werden, dass die datenschutzkonforme Vorgehensweise auch dauerhaft angewandt wird. Die betroffenen Krankenkassen haben dies zugesagt. Eine Kasse beabsichtigt nunmehr, die Kontrolle in den Prüfplan ihres Referats Datenschutz aufzunehmen, um so sicherzustellen, dass regelmäßige Kontrollen im Unternehmen stattfinden.

Ich empfehle allen Krankenkassen, Kontrollmechanismen zu etablieren, die die ständige Überprüfung des Verfahrens zur Erhebung medizinischer Daten gewährleisten und der eigenständigen Erhebungskompetenz des Medizinischen Dienstes Rechnung tragen.

3. Einsicht in Versichertenunterlagen ehemaliger Fremd- und Zwangsarbeiter

Der Firmennachfolger eines in der NS-Zeit wichtigen Rüstungsbetriebes wollte nachforschen lassen, welche Rolle sein Betrieb in der NS-Zeit bei der Beschäftigung von Fremd- und Zwangsarbeitern gespielt hat. In diesem Zusammenhang bat der mit der Recherche Beauftragte unsere Dienststelle um Unterstützung bei seinem Anliegen, Auskunft bzw. Einsicht in bei der AOK Baden-Württemberg vorhandene Versichertenunterlagen zu erhalten, was die Krankenkasse mangels Rechtsgrundlage zunächst ablehnte.

Fremdarbeiter, die während der NS-Zeit zur Zwangsarbeit eingesetzt waren, waren unfreiwillig Mitglied in der gesetzlichen Krankenversicherung (vgl. hierzu auch 21. Tätigkeitsbericht für das Jahr 2000, LT-Drucksache 12/6020, und 28. Tätigkeitsbericht für das Jahr 2007, LT-Drucksache 14/2050). Diese Versicherungsunterlagen sind teilweise bis heute noch bei der AOK Baden-Württemberg vorhanden. Dabei handelt es sich um Sozialdaten, die als sog. sensitive Daten gemäß § 33 LDSG einem besonderen Schutz unterliegen und nur dann in zulässiger Weise genutzt werden dürfen, wenn eine besondere Rechtsvorschrift aus dem Fünften oder Zehnten Buch des Sozialgesetzbuchs dies ausdrücklich vorsieht. Auskunftsansprüche bzw. Einsichts-

rechte gibt es nach den einschlägigen Bestimmungen des Sozialgesetzbuchs jedoch nur für einen bestimmten Personenkreis (Betroffene), dem der Anfragende fraglos nicht angehörte.

Um dem nachvollziehbaren Interesse des Firmennachfolgers daran, welche Rolle sein Betrieb in der Zeit des Nationalsozialismus gespielt hat, Rechnung zu tragen, hat mein Amtsvorgänger im vergangenen Jahr nach einem gangbaren Weg gesucht, der gleichwohl die Belange des Datenschutzes wahrt. Ausgangspunkt der Überlegungen war, dass Auskunftsansprüche neben den unmittelbar betroffenen Fremd- und Zwangsarbeitern auch (betroffenen) juristischen Personen zustehen, da sich der Sozialdatenschutz über § 35 Abs. 4 des Ersten Buches des Sozialgesetzbuchs (SGB I) ebenfalls auf deren Betriebs- und Geschäftsgeheimnisse erstreckt. Die Frage, ob ein Betrieb in der NS-Zeit Fremd- und Zwangsarbeiter beschäftigt hat, ist eine Information, über die einem Betriebsinhaber Auskünfte auf der Grundlage von § 83 Abs. 1 SGB X erteilt werden dürfen. Es kann dabei aber nicht um die Nennung der Namen dieser Personen gehen, sondern lediglich um die Frage, ob und wenn ja, wie viele Personen seinerzeit in der Firma beschäftigt waren.

Nach intensiven Gesprächen mit der AOK wurde das folgende weitere Vorgehen vereinbart:

Bei der einen Antrag nach § 83 Abs. 1 SGB X stellenden juristischen Person (Unternehmensnachfolge) muss es sich eindeutig um einen Betrieb handeln, der in den 30-er und 40-er Jahren bereits bestanden hat. Dies muss durch entsprechende Nachweise dargelegt werden, aus denen hervorgeht, dass eine eindeutige Rechtsnachfolge erfolgt ist und das heutige Unternehmen in die Rechte und Pflichten des damaligen Unternehmens eingetreten ist.

Bei den Unterlagen der Fremd- und Zwangsarbeiter handelt es sich um Sozialdaten, die nicht in automatisierten Verfahren gespeichert sind. Das Auffinden der Daten wird daher regelmäßig schwieriger sein als das Auffinden von Sozialdaten in automatisierten Verfahren. Aus diesem Grund hält es die Krankenkasse zu Recht für ein zwingendes Verfahrenserfordernis, dass seitens des Betriebsinhabers bzw. von dessen Bevollmächtigtem noch nähere Angaben gemacht werden, die das Auffinden der Daten mit vertretbarem Verwaltungsaufwand ermöglichen.

4. Kundenwerbung mit Postwurfsendung

Ein Bürger schickte mir die Postwurfsendung einer Krankenkasse zur Gewinnung von Neukunden zu, die erhebliche datenschutzrechtliche Mängel aufwies.

Der Wettbewerb ist längst auch in der Welt der Krankenkassen angekommen. Doch nach wie vor tun sich die öffentlich-rechtlichen Kassen schwer damit, die datenschutzrechtlichen Belange bei der Kundenwerbung zu beachten. Ausführungen zur grundsätzlichen datenschutzrechtlichen Problematik im Zusammenhang mit der Gewinnung von Neukunden durch Krankenkassen waren bereits in den letzten Tätigkeitsberichten (vgl. 27. Tätigkeitsbericht für das Jahr 2006, LT-Drucksache 14/650, 28. Tätigkeitsbericht für das Jahr 2007, LT-Drucksache 14/2050) enthalten. Die damals geäußerte Hoffnung, dass die Krankenkassen nunmehr sicherstellen, dass in Zukunft Datenschutzverstöße bei Werbeaktionen zur Gewinnung von Neukunden nicht mehr auftreten, hat sich leider nur teilweise erfüllt. Denn nach wie vor erfahre ich von datenschutzrechtlich bedenklichen Werbeaktionen gerade auch einer Krankenkasse, die sich in der Vergangenheit einsichtig gezeigt hatte.

Diese Krankenkasse hatte meinem Amtsvorgänger versichert, die Ablaufprozesse künftig so zu gestalten, dass vor einer Produktionsfreigabe von Werbematerial an externe (Werbe-)Firmen immer erst eine Endabnahme durch ihren behördlichen Datenschutzbeauftragten zu erfolgen hat. Dass es hierbei nicht sehr sorgfältig zugegangen sein muss, konnten meine Mitarbeiter feststellen, als ein Bürger uns eine Postwurfsendung dieser Krankenkasse zuschickte, die in verschiedener Hinsicht datenschutzrechtliche Mängel aufwies: So enthielt sie keine Möglichkeit, der Speicherung und Nutzung der Daten zu widersprechen, sah keine Bestätigung des Einverständnisses mittels Unterschrift vor und es fehlte auch der Hinweis auf das Einverständnis durch Erziehungsberechtigte bei Minderjährigen.

Nach § 4 Abs. 3 LDSG bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Ein solcher Ausnahmetatbestand war für uns bei der konkreten Werbeaktion nicht erkennbar, sodass es beim Schriftformerfordernis blieb. Eine vergleichbare Regelung enthält auch § 67 b Abs. 2 Satz 3 des Zehnten Buches des Sozialgesetzbuchs (SGB X). Auch danach muss die Einwilligung schriftlich erklärt werden und den in § 126 des Bürgerlichen Gesetzbuchs näher geregelten Voraussetzungen entsprechen. Die Betroffenen müssen daher ihr Einverständnis nicht nur schriftlich festhalten, sondern auch eigenhändig unterzeichnen. Erfreulicherweise erklärte sich die Krankenkasse sofort bereit, das entsprechende Werbematerial zu ändern.

Kurze Zeit darauf machte allerdings dieselbe Krankenkasse im Zusammenhang mit einem Beachvolleyball-Turnier erneut auf sich aufmerksam. Dabei wurde auf dem Anmeldebogen sowohl bei der Spieler- als auch bei der Fananmeldung die komplette Adresse, das Geburtsdatum, die E-Mail-Adresse und sogar die Krankenkasse erhoben. Das Anmeldeformular enthielt jedoch keinerlei Hinweis auf die Freiwilligkeit beim Ausfüllen der einzelnen Datenfelder. Des Weiteren konnte weder dem dazu gehörenden Flyer noch dem Anmeldebogen entnommen werden, zu welchem Zweck die einzelnen Daten erhoben werden.

Auf die datenschutzrechtliche Problematik des Vorgehens angesprochen, teilte uns die Krankenkasse mit, es handle sich um eine Einzelmaßnahme einer Regionaldirektion. Das Feld „Geburtsdatum“ werde zur Einteilung der Altersklassen für die einzelnen Mannschaften benötigt. Künftig werde das Feld „Krankenkasse“ entfernt. Die Datenfelder „Telefon“ und „E-Mail-Adresse“ würden mit dem Hinweis auf die Freiwilligkeit der Angaben versehen. Bei den Personen, die sich aufgrund des Flyers zum Turnier angemeldet hatten, werde nachträglich die Einwilligung zur Speicherung der Daten eingeholt. Bei Nichterteilung der Einwilligung erfolge die Datenlöschung. Im Übrigen habe die Krankenkasse unsere früheren Hinweise zum Anlass genommen, intern die entsprechenden Verfahrensweisen und Medien zu überarbeiten. Aufgrund der Vielzahl der betroffenen Prozesse und Formulare dauere dieser Vorgang noch an. Unabhängig davon sei beabsichtigt, alle Regionaldirektionen im Rahmen einer Tagung über das Thema Neukundenwerbung zu informieren.

Nicht unerwähnt soll bleiben, dass leider auch andere gesetzliche Krankenkassen im Rahmen ihrer Mitgliederwerbung hinter dem zurückbleiben, was wir als den richtigen Maßstab betrachten. Es bleibt also einmal mehr zu hoffen, dass mein neuerlicher Vorstoß endlich bewirkt, dass die Krankenkasse einschließlich ihrer Untergliederungen die vorgesehene datenschutzkonforme Verfahrensweise auch tatsächlich umsetzt.

Meine Mitarbeiter und ich werden – soweit es die schmalen Ressourcen meiner Dienststelle erlauben – auch weiterhin allen bekannt werdenden Datenschutzverstößen bei Krankenkassen unter strikter Wahrung des Gleichbehandlungsgrundsatzes nachgehen.

5. Patientengewinnung für strukturierte Behandlungsprogramme

Mit der Einführung der strukturierten Behandlungsprogramme streben Krankenkassen an, ihren chronisch kranken Versicherten passgenaue Programme anzubieten. Diese durchaus sinnvollen und erwünschten Maßnahmen müssen aber hinsichtlich der Patientengewinnung datenschutzkonform ablaufen.

Fast 20 Prozent der Bundesbürger, so lauten Schätzungen, sind chronisch krank. Sie leiden z. B. an Diabetes mellitus, koronarer Herzkrankheit (KHK), Asthma bronchiale oder chronisch obstruktiven Lungenerkrankungen (COPD). Chronische Krankheiten erfordern eine gut abgestimmte kontinuierliche Behandlung und Betreuung. Experten haben immer wieder darauf hingewiesen, dass es gerade in diesem Bereich erhebliche Qualitätsmängel in der medizinischen Versorgung gibt. Darum wurden in der gesetzlichen Krankenversicherung mit dem am 1. Januar 2002 in Kraft getretenen Gesetz zur Reform des Risikostrukturausgleichs in der gesetzlichen Krankenversicherung (BGBl. I 2001, S. 3465) die gesetzlichen Grundlagen für spezielle

strukturierte Behandlungsprogramme (auch als Chronikerprogramme oder Disease Management Programme – DMP – bezeichnet) geschaffen und im Risikostrukturausgleich der Krankenkassen finanziell gefördert.

Ziel dieser Programme ist, die Versorgung von chronisch Kranken zu verbessern. Komplikationen und Folgeerkrankungen chronischer Krankheiten sollen durch eine gut abgestimmte, kontinuierliche Betreuung und Behandlung möglichst vermieden werden. Zu den Programmen gehören regelmäßige Arzttermine mit Beratungsgesprächen und Untersuchungen sowie die Vermittlung von Hintergrundinformationen zum Beispiel durch Schulungen. Ärzte, die an solchen Programmen teilnehmen, müssen bestimmte Voraussetzungen erfüllen und festgelegte Qualitätsanforderungen einhalten.

Eine Bezirksdirektion einer Krankenkasse hatte nun im Zusammenhang mit der Gewinnung von eingeschriebenen DMP-Patienten Ärzte angeschrieben und aufgefordert, bestimmte Angaben über ihre Patienten – und zwar ohne deren Kenntnis – gegenüber der Krankenkasse zu machen.

IHRE Krankenkasse

- ganz individuell und nur in Stuttgart!

Ihre Krankenkasse - PF 12 34 - 70000 Stuttgart

Herrn
Dr. Hermann S.....
Hauptstraße 4
70000 Stuttgart

Bearbeiter: Frau Musterle
Telefon: 0711/11111111111
Mail: gabriele.musterle@ihre-krankenkasse.de
Stuttgart, den 1.3.2009

Ihr DMP-Potential

Sehr geehrter Herr Dr. S.....,

unsere aktuelle Chronikerselektion weist für Ihre Praxis folgendes DMP-Potential aus:

Diabetes Typ I	Diabetes Typ II	KHK	Asthma	COPD
0	6	8	5	10

DMP-Teilnehmer profitieren nachweislich in mehrfacher Hinsicht von den Disease-Management-Programmen. Deshalb wollen wir unsere Versicherten aus dem oben bezifferten Potential anschreiben, informieren und zur Teilnahme motivieren. Jedoch nicht ohne Ihre Zustimmung.

Deshalb unsere Bitte: Wenn Sie mit der Aktion einverstanden sind, fordern Sie

die namentliche DMP-Potentialliste Ihrer Praxis

an. Sie können dann die Namen der Patienten streichen, die Ihrer Ansicht nach nicht angeschrieben werden sollen und uns die überarbeitete Liste wieder zukommen lassen.

Für die Zusammenarbeit besten Dank.

Mit freundlichen Grüßen
gez. G. Musterle

Ein Arzt, der ein vergleichbares Schreiben erhalten hatte, wandte sich mit der Bitte um Prüfung an meinen Amtsvorgänger, da er die praktizierte Vorgehensweise der Krankenkasse aus datenschutzrechtlicher Sicht für nicht in Ordnung hielt.

Die Krankenkasse teilte dazu mit, sie biete auf der Grundlage des § 137 f des Fünften Buches des Sozialgesetzbuchs (SGB V) strukturierte Behandlungsprogramme für chronische Krankheiten an. Um diese Behandlungsprogramme zielgerichtet anbieten zu können, ermittle sie auf der Grundlage von § 284 Abs. 3 Satz 1 in Verbindung mit Absatz 1 Nr. 14 SGB V die potenziellen Versicherten. Diese würden schriftlich über die Behandlungsprogramme informiert. Sofern die Versicherten teilnehmen wollen, müssten sie sich an ihren zuständigen Haus- oder Facharzt wenden, der dann nach einer ausführlichen Beratung entscheide, ob der Patient aufgrund seines Krankheitsbildes in das Behandlungsprogramm aufgenommen werden könne. Die sog. Potenzialliste enthalte die Datenbasis für ein persönliches Gespräch der Krankenkasse mit dem betreffenden Arzt. Daraus werde zur Vorbereitung der Gespräche erkennbar, in welchem Rahmen grundsätzlich die Möglichkeit bestehe, weitere Patienten für derartige Programme zu gewinnen. Die Bezirksdirektionen seien ausdrücklich darauf hingewiesen worden, dass diese Potenzialliste den Ärzten – auch auf deren Anforderung hin – nicht zugeschickt werden dürfe. Die betreffende Bezirksdirektion halte sich bedauerlicherweise nicht an diese Vorgaben.

Gemäß § 137 f Abs. 3 Satz 2 SGB V können Versicherte an strukturierten Behandlungsprogrammen auf freiwilliger Basis teilnehmen, wenn sie nach umfassender Information durch ihre Krankenkasse schriftlich eine Einwilligung zur Teilnahme an dem Programm und zur Erhebung, Verarbeitung und Nutzung der nach § 266 Abs. 7 SGB V festgelegten Daten erteilen.

Im Ergebnis teile ich die Auffassung der Hauptverwaltung der Krankenkasse, dass das Verfahren zur Gewinnung potenzieller DMP-Patienten für strukturierte Behandlungsprogramme nicht „an den Patienten vorbei“ erfolgen darf. Eine bilaterale Vorgehensweise (Kasse mit Arzt), wie durch die Bezirksdirektion geschehen, ist datenschutzrechtlich bereits deshalb nicht in Ordnung, weil die Krankenkasse auf diese Weise im Rücklauf aus den „bereinigten“ Listen (durch die vom Arzt vorgenommenen Streichungen) entnehmen könnte, welche ihrer Versicherten (allein) aus ärztlicher Sicht für die Aufnahme in DMP-Programme als ungeeignet erscheinen. Des Weiteren könnte die Krankenkasse durch eine entsprechende Auswertung dieser Informationen erkennen, welche ihrer Versicherten trotz einer aus Sicht des Arztes attestierten Eignung zur Teilnahme an bestimmten DMP-Programmen aus anderen Gründen nicht willens und bereit sind. Nachdem die Teilnahme freiwillig ist und eine „Einschreibung“ nur dann erfolgt, wenn sowohl der Arzt als auch der Patient die Teilnahmefähigkeit bzw. -bereitschaft jeweils durch ihre Unterschriften separat dokumentiert haben, verstößt die Vorgehensweise der Bezirksdirektion gegen den in § 67 a Abs. 1 des Zehnten Buches des Sozialgesetzbuchs (SGB X) normierten Erforderlichkeitsgrundsatz, wonach Leistungsträger nur diejenigen (Sozial-)Daten erheben dürfen, die zur Erfüllung ihrer Aufgaben auch tatsächlich erforderlich sind.

Die Krankenkasse hat zugesichert, sie habe die Bezirksdirektion aufgefordert, das Anschreiben an die Ärzte zukünftig nicht mehr einzusetzen. Darüber hinaus werde dieser Fall zum Anlass genommen, alle Mitarbeiter, die in diesem Bereich tätig sind, erneut über die datenschutzkonforme Vorgehensweise zu informieren.

3. Abschnitt: Soziales

1. Neuordnung der Grundsicherung für Arbeitsuchende

Das Bundesverfassungsgericht hat Ende 2007 die Hartz IV-Arbeitsgemeinschaften für mit der Verfassung unvereinbar erklärt. Eine Neuordnung ist bislang noch nicht zustande gekommen.

Kurz nach Erscheinen des letzten Tätigkeitsberichts meiner Dienststelle hat das Bundesverfassungsgericht entschieden, dass die Arbeitsgemeinschaften

als Gemeinschaftseinrichtung von Bundesagentur für Arbeit und kommunalen Trägern mit dem Grundgesetz nicht vereinbar sind[2]. Die Einrichtung der Arbeitsgemeinschaften verstoße unter anderem gegen den Grundsatz der Verantwortungsklarheit. Die organisatorische und personelle Verflechtung bei der Aufgabenwahrnehmung behindere eine klare Zurechnung staatlichen Handelns zu einem der beiden Träger. Ausdruck hiervon seien insbesondere Unsicherheiten hinsichtlich der Anwendbarkeit von Bundes- und Landesrecht, wie sie etwa beim Datenschutz aufgetreten seien.

Das Bundesverfassungsgericht hat entschieden, dass die Norm, die die Einrichtung der Arbeitsgemeinschaften regelt, längstens bis zum 31. Dezember 2010 anwendbar bleibt, da dem Gesetzgeber für eine Neuregelung „ein der Größe der Umstrukturierungsaufgabe angemessener Zeitraum“ belassen werden müsse.

Anfang des Jahres 2009 hat das Bundesministerium für Arbeit und Soziales einen Gesetzentwurf zur Neuorganisation erstellt. Danach sollten für Langzeitarbeitslose künftig sog. „Zentren für Arbeit und Grundsicherung“ (ZAG) zuständig sein. In diesen Einrichtungen sollten Bundesagentur und Kommunen weiterhin zusammenwirken. Hierfür war eine Änderung des Grundgesetzes vorgesehen. Die datenschutzrechtliche Kontrolle über die ZAG sollte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ausüben. Die Unionsfraktion stoppte das Vorhaben.

Infolgedessen gibt es fast zwei Jahre nach der Entscheidung des Bundesverfassungsgerichts und ein Jahr vor Ablauf der vom Gericht gesetzten Frist noch keine gesetzliche Neuregelung. Nach dem Koalitionsvertrag vom 26. Oktober 2009 wird nunmehr eine „verfassungsfeste Lösung“ ohne Änderung des Grundgesetzes und ohne Änderung der Finanzbeziehungen angestrebt.

Eine Neuregelung durch den Bundesgesetzgeber ist weiterhin dringend erforderlich. Dabei ist auch die datenschutzrechtliche Aufsichtszuständigkeit eindeutig zu regeln.

2. Kontrollbesuche bei zwei Arbeitsgemeinschaften

Meine Dienststelle kontrollierte auch im vergangenen Berichtszeitraum wieder Träger der Grundsicherung für Arbeitsuchende vor Ort. In diesem Zusammenhang befasste sie sich unter anderem mit folgenden Themenbereichen:

2.1 Anforderung von Kontoauszügen

Das Bundessozialgericht hat sich in zwei Urteilen zu der lange Zeit umstrittenen Frage der Zulässigkeit der Anforderung von Kontoauszügen geäußert.

Mit Urteil vom 19. September 2008 (B 14 AS 45/07 R)[3] und Urteil vom 19. Februar 2009 (B 4 AS 10/08 R)[4] hat das Bundessozialgericht zur Zulässigkeit der Anforderung von Kontoauszügen Stellung genommen. Danach ist die Anforderung der Kontoauszüge jedenfalls der letzten drei Monate bei der Beantragung von Leistungen nach dem Zweiten Buch des Sozialgesetzbuchs auch ohne konkreten Verdacht des Leistungsmissbrauchs zulässig. Die Obliegenheit, Kontoauszüge vorzulegen, gilt allerdings nicht in vollem Umfang für die Ausgabenseite, das heißt für die Frage, wofür der Leistungsbezieher seine Mittel verwendet. Eine Einschränkung ergibt sich hier für besondere Arten personenbezogener Daten. Dies sind Angaben über die rassische und ethnische

[2] Die Entscheidung kann im Internet nachgelesen werden unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20071220_2bvr243304.html

[3] Die Entscheidung kann im Internet nachgelesen werden unter http://juris.bundessozialgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bsg&Art=en&Datum=2008-9&nr=10776&pos=9&anz=24

[4] Die Entscheidung kann im Internet nachgelesen werden unter http://juris.bundessozialgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bsg&Art=en&Datum=2009-2&nr=10912&pos=4&anz=21

Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Geschützt ist die Geheimhaltung des Verwendungszwecks bzw. des Empfängers der Überweisung. Dementsprechend dürften etwa Angaben über Gewerkschaftsbeiträge, Spenden an Kirchen oder an politische Parteien hinsichtlich des Empfängers, nicht aber der Höhe, ohne Weiteres geschwärzt werden. Lediglich für den Fall, dass sich aus den insoweit geschwärzten Kontoauszügen eines Leistungsbeziehers ergibt, dass in auffälliger Häufung oder Höhe Beträge überwiesen werden, ist nach Auffassung des Bundessozialgerichts im Einzelfall zu entscheiden, inwieweit ausnahmsweise doch eine Offenlegung auch des bislang geschwärzten Adressaten gefordert werden kann.

Die in den Urteilen geäußerte Ansicht des Bundessozialgerichts bestätigt die langjährige Auffassung meiner Dienststelle (vgl. 20. Tätigkeitsbericht für das Jahr 1999, LT-Drucksache 12/4600).

Das Bundessozialgericht hat außerdem darauf hingewiesen, dass die Leistungsträger auf die Möglichkeiten der Schwärzung der Adressaten auf der Ausgabenseite bereits bei ihrem Mitwirkungsbegehren gesondert hinweisen müssen.

Ein solcher Hinweis wurde von einer durch meine Dienststelle kontrollierten Arbeitsgemeinschaft bisher nicht generell, sondern nur auf konkrete Nachfrage des Antragstellers erteilt. Die betroffene Arbeitsgemeinschaft hat die Mitarbeiter inzwischen in Teambesprechungen ausführlich auf die Auswirkungen der Urteile hingewiesen.

Leistungsträger haben die Antragsteller auf die Möglichkeit der Schwärzung besonderer Arten personenbezogener Daten, insbesondere von Adressaten auf der Ausgabenseite von Kontoauszügen, hinzuweisen.

2.2 Vorlage einer Mietbescheinigung

Zu den Leistungen zur Sicherung des Lebensunterhalts gehören auch Leistungen für Unterkunft und Heizung. In diesem Zusammenhang verlangen Träger der Grundsicherung für Arbeitsuchende teilweise die Vorlage einer vom Vermieter zu unterzeichnenden Mietbescheinigung.

Leistungsträger dürfen eine vom Vermieter auszufüllende Mietbescheinigung dann nicht verlangen, wenn ein Antragsteller die für die Aufgabenerfüllung erforderlichen Angaben in anderer Weise, z. B. mit Hilfe eines Mietvertrags, der Nebenkostenabrechnung oder anderer Unterlagen, belegen kann. Aus Sicht des Datenschutzes ist dies die schonendere und damit vorzugswürdige Vorgehensweise, wenn damit verhindert werden kann, dass der Antragsteller seinen Vermieter einbeziehen muss.

Soweit die betroffene Person ihrer Mitwirkungspflicht durch Beibringung einer Mietbescheinigung nachkommen möchte, sollte ein neutral gehaltenes Formular „Mietbescheinigung“ zum Einsatz kommen, aus dem weder der Zweck der Erhebung noch der Sozialleistungsträger erkennbar ist. Hiermit wird vermieden, dass dem Vermieter die Beantragung von Arbeitslosengeld II bzw. Sozialgeld offenbart wird.

Das von einer kontrollierten Arbeitsgemeinschaft verwendete Formular enthielt einen Hinweis auf den Zweck der Erhebung („... zur Beantragung von Arbeitslosengeld II/Sozialgeld“). Auf Aufforderung meiner Dienststelle hat die Arbeitsgemeinschaft den Hinweis entfernt. Ebenfalls auf Intervention meiner Dienststelle wurde ein Hinweis auf eine angebliche Verpflichtung des Vermieters, die Mietbescheinigung auszufüllen, beseitigt.

Die Vorlage einer Mietbescheinigung darf lediglich unter engen Voraussetzungen verlangt werden. Das Formular sollte weder den Zweck der Erhebung noch den Sozialleistungsträger erkennen lassen und darf keinesfalls falsche Hinweise enthalten.

2.3 Nichtzulassung einer Überprüfung durch unsere Dienststelle

Öffentliche Stellen sind gesetzlich verpflichtet, mich in meiner Arbeit zu unterstützen. Dies wird leider nicht immer beachtet.

Im Rahmen eines Kontrollbesuchs bei einer Arbeitsgemeinschaft war vorgesehen, Bildschirmarbeitsplätze stichprobenweise zu überprüfen. Im Vorfeld ist sowohl der Kontrollbesuch als auch der geplante Untersuchungsumfang schriftlich angekündigt worden. Im Einzelnen hatten meine Mitarbeiter vor, einen Arbeitsplatz mit Hilfe der IT-Berechtigungen eines beliebigen Mitarbeiters der Arbeitsgemeinschaft näher in Augenschein zu nehmen. Auf diese Weise sollte herausgefunden werden, ob die tatsächlich vorhandenen Berechtigungen innerhalb von verschiedenen automatisierten Verfahren, aber auch auf Dateisystemebene datenschutzkonform vergeben wurden. Eine solche Überprüfung wurde von der Arbeitsgemeinschaft mit der Begründung verweigert, dass eine Einzelfallüberprüfung nicht angekündigt gewesen sei und deshalb zum Schutz des Mitarbeiters, mit dessen Account die Prüfung durchgeführt worden sollte, nicht zugelassen werden könne. Meine Mitarbeiter mussten daher unverrichteter Dinge wieder abziehen. Keine Frage, dass dieser Verstoß gegen die vom Gesetz vorgeschriebene Pflicht zur Unterstützung nach § 29 LDSG eine förmliche Beanstandung gemäß § 30 LDSG nach sich zog.

§ 29 LDSG

Die öffentlichen Stellen sind verpflichtet, den Landesbeauftragten für den Datenschutz und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist im Rahmen der Kontrollbefugnis nach § 28 insbesondere

1. *Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,*
2. *jederzeit Zutritt zu den Diensträumen zu gewähren.*

Fairerweise ist nachzutragen, dass die Arbeitsgemeinschaft inzwischen mitteilte, sie rücke von ihrer bisherigen Rechtsauffassung ab und bedauere ihren Rechtsirrtum.

2.4 Technischer und organisatorischer Datenschutz in einer Arbeitsgemeinschaft (ARGE)

Gemäß dem Zehnten Buch des Sozialgesetzbuchs sind technisch-organisatorische Maßnahmen zur Einhaltung der Datenschutzbestimmungen zu realisieren. Eine wichtige Maßnahme zum Schutz personenbezogener Daten ist dabei eine effektive Zutritts- und Zugriffskontrolle. Das bedeutet, dass sicherzustellen ist, dass Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen und auch zu papiergebundenen Daten haben. Der Kreis derjenigen, die hierzu berechtigt sind, ist zudem möglichst klein zu halten.

In einer ARGE haben meine Mitarbeiter im Rahmen eines Besuches vor Ort festgestellt, dass der Zutritt zu allen Räumlichkeiten mittels eines einzigen Schlüssels möglich war. Somit hatte jeder Mitarbeiter Zutritt zu allen anderen Büros. In den einzelnen Büros dieser ARGE wurden aber Akten nicht nur in Schränken gelagert, sondern es lagen auch die jeweils aktuellen, in Arbeit befindlichen Vorgänge auf den Tischen der Mitarbeiter. Eine wirksame Zugriffskontrolle war somit nicht realisiert.

Was ist zu tun?

Grundsätzlich gilt, dass es Mitarbeitern nur möglich sein darf, auf diejenigen personenbezogenen Daten zuzugreifen, die sie im Rahmen der Erfüllung ihrer Dienstpflicht bearbeiten müssen. Zutritts- oder Zugriffs-

kontrollen müssen dementsprechend ausgestaltet sein. Wir empfehlen, dass Mitarbeitern nur ein Zutritt in diejenigen Räume möglich ist, die sie zur Erfüllung ihrer dienstlichen Aufgaben betreten müssen. Die Vergabe von Zugangsberechtigungen ist zudem mittels eines transparenten Genehmigungsprozesses abzubilden.

3. Datenerhebung einer Arbeitsgemeinschaft bei Dritten

Das Zweite Buch des Sozialgesetzbuchs (SGB II) sieht in § 60 Auskunftspflichten Dritter vor. Die Norm ist aber kein Freibrief für Leistungsträger.

In einem von meiner Dienststelle geprüften Fall hatte sich eine Arbeitsgemeinschaft an die ehemalige Bank einer Leistungsbezieherin gewandt und diese unter Hinweis auf „Ihre Auskunftspflicht gemäß § 60 Sozialgesetzbuch II“ nach dem Stand zweier Konten der Leistungsbezieherin am Tage der Auflösung gefragt. Die Bank erteilte diese Auskunft. Dies reichte der Arbeitsgemeinschaft aber nicht aus. In einem zweiten Anlauf wurde die Bank – wiederum unter Hinweis auf „Ihre Auskunftspflicht gemäß § 60 SGB II“ – aufgefordert, größere Ein- und Auszahlungen auf den Konten der Leistungsbezieherin über einen Zeitraum von zwei Jahren mitzuteilen.

§ 60 SGB II sieht Auskunftspflichten Dritter vor. Absatz 2 Satz 1 der Vorschrift lautet wie folgt:

> *Wer jemandem, der eine Leistung nach diesem Buch beantragt hat oder bezieht, zu Leistungen verpflichtet ist, die geeignet sind, Leistungen nach diesem Buch auszuschließen oder zu mindern, oder wer für ihn Guthaben führt oder Vermögensgegenstände verwahrt, hat der Agentur für Arbeit auf Verlangen hierüber sowie über damit im Zusammenhang stehendes Einkommen oder Vermögen Auskunft zu erteilen, soweit es zur Durchführung der Aufgaben nach diesem Buch erforderlich ist.*

Von der Regelung werden auch Banken und Sparkassen erfasst. Die Auskunftspflicht trifft aber nur denjenigen, der zum Zeitpunkt der Anfrage des Leistungsträgers noch ein Guthaben führt oder Vermögensgegenstände verwahrt. Dies war vorliegend nicht der Fall, da die Konten schon längst aufgelöst waren. Außerdem werden Auskünfte über Kontenbewegungen nicht von der Auskunftspflicht umfasst. Darüber hinaus muss die Anfrage des Leistungsträgers so beschränkt werden, dass keine Sollsalden mitgeteilt werden.

Die datenschutzrechtlichen Verstöße habe ich nach § 30 LDSG beanstandet. Die betroffene Arbeitsgemeinschaft hat mir zwischenzeitlich zugesichert, meine Ausführungen künftig zu beachten; dies soll durch Dienstbesprechungen und interne Kontrollmaßnahmen gewährleistet werden.

Die Leistungsträger haben, bevor sie Dritte auf eine Auskunftspflicht hinweisen, gewissenhaft zu prüfen, ob und inwieweit eine solche im konkreten Fall überhaupt besteht.

4. Auskunftserteilung an den Betroffenen

Zu den wesentlichen Bestandteilen des allgemeinen Persönlichkeitsrechts gehört das Auskunftsrecht des Betroffenen über die zu seiner Person gespeicherten Sozialdaten. Der Gesetzgeber hat hiervon aber Ausnahmen zugelassen.

§ 83 des Zehnten Buchs des Sozialgesetzbuchs (SGB X) regelt das Auskunftsrecht des Betroffenen im Sozialleistungsbereich. Absatz 4 enthält als Ausnahme von der Auskunftspflicht folgende Ausschlusstatbestände:

> *Die Auskunftserteilung unterbleibt, soweit*
>
> *1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,*

2. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder

3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen,

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

Bei der Prüfung, ob die Auskunftserteilung ausnahmsweise zu unterbleiben hat, ist Folgendes zu beachten:

– Die Auskunftserteilung unterbleibt nur, soweit die Voraussetzungen des Absatzes 4 vorliegen. Gegebenenfalls ist Auskunft über einen Teil der gespeicherten Daten zu erteilen.

– Das Vorliegen eines Ausnahmetatbestands nach Absatz 4 Nr. 1 bis 3 führt noch nicht zwangsläufig zur Auskunftsverweigerung. Erforderlich ist eine Abwägung zwischen dem Geheimhaltungsinteresse und dem Auskunftsinteresse.

– Soweit die Auskunftserteilung abgelehnt wird, bedarf die Ablehnung der Auskunftserteilung keiner Begründung, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an die für die Kontrolle des Datenschutzes zuständige Stelle wenden kann (§ 83 Abs. 5 SGB X).

Unsere Kontrolltätigkeit zeigt, dass Behörden, die eine Auskunftserteilung ablehnen, die Prüfung nicht immer wie gesetzlich vorgesehen durchführen.

Der Anspruch auf Auskunft umfasst grundsätzlich auch die Herkunft der gespeicherten Sozialdaten. Das Auskunftsrecht ist aber auch diesbezüglich nicht ohne Ausnahme. Im Sozialhilferecht kann ein überwiegendes Interesse des Leistungsempfängers, die Identität der Person, die der Behörde Daten über den Leistungsempfänger mitgeteilt hat (Informant), festzustellen, dann in Betracht kommen, wenn ausreichende Anhaltspunkte für die Annahme vorliegen, dass der Informant wider besseres Wissen und in der vorgefassten Absicht, den Ruf des Leistungsempfängers zu schädigen, gehandelt oder der Behörde leichtfertig falsche Daten übermittelt hat (Urteil des Bundesverwaltungsgerichts vom 4. September 2003, 5 C 48/02).

Demgegenüber ist die neuere Rechtsprechung zur Jugendhilfe strenger: Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Urteil vom 10. Dezember 2003, 12 E 453/02), das Verwaltungsgericht Göttingen (Urteil vom 9. Februar 2006, 2 A 199/05) und das Schleswig-Holsteinische Verwaltungsgericht (Urteil vom 11. Mai 2009, 15 A 160/08) gehen davon aus, dass es sich bei Tipps von Informanten regelmäßig um anvertraute Daten im Sinne des § 65 des Achten Buchs des Sozialgesetzbuchs handelt, die einem besonderen Vertrauensschutz unterliegen und nur weitergegeben werden dürfen,

– wenn der Datengeber einwilligt,

– wenn bestimmte Konstellationen vorliegen, bei denen eine Datenweitergabe zum Kindeswohl erforderlich ist, oder

– wenn die Personen, die gemäß § 203 Abs. 1 oder 3 des Strafgesetzbuchs der Schweigepflicht unterliegen, dazu befugt wären.

Die Ablehnung einer Auskunftserteilung setzt eine sorgfältige Prüfung aller einschlägigen Regelungen voraus.

5. Datensammelwut beim Sozialamt

Das Erheben von Sozialdaten ist zulässig, wenn ihre Kenntnis zur Aufgabenerfüllung erforderlich ist. Dies ist nicht immer der Fall.

– Ein Sozialhilfeträger hatte im Bereich der „Hilfe zur Pflege“ einen Fragebogen verwendet, in dem eine Vielzahl personenbezogener Daten erhoben wurde, „um die passende individuelle Hilfeleistung gewähren zu können“. So sollte der Betroffene nicht nur erläutern, wie er seine Freizeit gestaltet und welche Hobbys er hat, sondern auch gleich mitteilen, ob und gegebenenfalls in welchem Verein er Mitglied ist. Außerdem sollten alle gesundheitlichen Einschränkungen und Erkrankungen aufgezählt werden mitsamt der Angabe, ob jeweils eine Behandlung stattfindet oder nicht. Weiter sollte der Betroffene mitteilen, ob er Über- oder Untergewicht hat, und Angaben zu seinen Ernährungsgewohnheiten und sportlichen Aktivitäten machen.

  Auf unsere Aufforderung mitzuteilen, zu welchem Zweck und aufgrund welcher Rechtsgrundlage die einzelnen Sozialdaten erhoben werden, hat der betroffene Sozialleistungsträger mitgeteilt, den Fragebogen nicht mehr zu verwenden.

– Im Bereich der Sozialhilfe ist für Personen, die aufgrund einer Krankheit einer kostenaufwändigen Ernährung bedürfen, ein Mehrbedarf vorgesehen. Ein Sozialhilfeträger hatte sich nicht mit einem Attest des behandelnden Arztes zufriedengegeben, sondern standardmäßig eine Vielzahl detaillierter medizinischer Angaben verlangt. So sollte der Hausarzt des Betroffenen – je nach Krankheit – Laborbefunde der letzten sechs Monate, den letzten neurologischen Befund, den Endoskopiebefund etc. angeben und Ausführungen zur Medikation machen. An dieser Vorgehensweise hatte auch das von meiner Dienststelle beteiligte Ministerium für Arbeit und Soziales Zweifel. Der betroffene Sozialhilfeträger hat zwischenzeitlich mitgeteilt, den Fragebogen nicht mehr standardmäßig einsetzen zu wollen.

Die Sozialleistungsträger haben bei jedem einzelnen Datum zu prüfen, ob dessen Kenntnis für die Erfüllung ihrer Aufgaben erforderlich ist.

6. Perspektive 50plus

Mit dem Programm „Perspektive 50plus“ will das Bundesministerium für Arbeit ältere, über 50-jährige Arbeitslose in das Berufsleben wieder eingliedern. Das ist sicher ein löbliches Vorhaben, jedoch sollten auch hier die Belange des Datenschutzes ausreichend beachtet werden.

Im Rahmen des Programms „Perspektive 50plus“ ist vorgesehen, den Erfolg verschiedener Maßnahmen zu erheben. Hierfür sollen drei verschiedene, private Unternehmen personenbezogene Daten der betroffenen Personen erhalten. Da es sich hierbei um Sozialdaten handelt, die nach dem Gesetz einem besonderen Schutz unterliegen, musste deren Übermittlung durch die jeweiligen Sozialministerien der Länder genehmigt werden. Deshalb hatte sich das Ministerium für Arbeit und Soziales Baden-Württemberg an mein Amt mit der Bitte gewandt, eine datenschutzrechtliche Bewertung durchzuführen. Auch bei den anderen Landesbeauftragten für den Datenschutz waren vergleichbare Anfragen eingegangen, handelte es sich doch um ein bundesweites Verfahren. Meine Kollegen und ich sahen schon aufgrund der Datenarten im Zusammenhang mit der eingesetzten Infrastruktur und Technologie dieses Programm kritisch.

So war u. a. die Übermittlung sehr sensibler personenbezogener Daten, die Rückschlüsse auf Schulden und Suchtprobleme zuließen, vorgesehen. Ein weiteres Problem stellte die zunächst geplante Pseudonymisierung unter Verwendung der Kundennummer der Bundesagentur für Arbeit (BA-Kundennummer) dar, denn die BA-Kundennummer lässt sich einem einzelnen Betroffenen eindeutig zuordnen, sodass eine Re-Identifizierung möglich gewesen wäre. Ferner waren die einzelnen technischen Sicherheitsvorkehrungen der beteiligten Einrichtungen vollkommen unterschiedlich.

Diese und ähnliche Kritikpunkte wurden auch von einigen anderen Kollegen vorgebracht. Die von mir erbetene Zustimmung zur Genehmigung der Datenübermittlung an die privaten Stellen habe ich daher verweigert. In diesem Zusammenhang haben wir dem Ministerium für Arbeit und Soziales Baden-Württemberg konkrete Anregungen zu einer Verbesserung des Datenschutzes gegeben. Das Ministerium versagte daraufhin zunächst eine Genehmigung der Datenübermittlung. In einer Besprechung mit dem Antragsteller, verschiedenen Landes-Sozialministerien und dem Bundesministerium für Arbeit wurden dann zusammen mit den Datenschutzbeauftragten aus Bund und Ländern Alternativen für die Umsetzung des Programms erarbeitet. Dabei konnten die Sicherheitsmaßnahmen auf ein einheitliches, hohes Niveau gebracht und ein wirksames Pseudonymisierungsverfahren eingerichtet werden; damit waren die datenschutzrechtlichen Bedenken ausgeräumt.

Die hier praktizierte enge Zusammenarbeit, bei der das Ministerium und meine Dienststelle vertrauensvoll Hand in Hand im Interesse der Sache kooperiert haben, brachte auch aus datenschutzrechtlicher Sicht einen Erfolg.

6. Teil: Kommunales und anderes

1. Abschnitt: Kommunales

1. Haupt- oder Nebenwohnung? Diese Frage sorgt immer wieder für Nachfragen und Irritationen

Bereits im 28. Tätigkeitsbericht für das Jahr 2007 (vgl. LT-Drucksache 14/2050) tauchte das Thema „Haupt- oder Nebenwohnung“ auf. In dem dort dargestellten Einzelfall ging es im Kern darum, dass der bloße Verdacht oder gar die vage Möglichkeit einer rechtlich relevanten Änderung der Wohnungsbenutzungs- bzw. Aufenthaltszeiten der Meldebehörde nicht das Recht gibt, die früheren Angaben des Meldepflichtigen in Frage zu stellen und diesen unabhängig von einem melde- oder mitteilungspflichtigen Vorgang erneut zu befragen.

Inzwischen stellte sich heraus, dass die Stadt trotz unserer förmlichen Beanstandung weiter gegen den Petenten nach § 5 a Abs. 2 des Meldegesetzes (MG) ermittelte. Was war geschehen? Die Meldebehörde hatte im Internet über die Verhältnisse des Petenten recherchiert und sich so weitere Informationen beschafft. Selbstverständlich war die Internet-Recherche bei unveränderter Sach- und Rechtslage ebenfalls nicht zulässig und wurde deshalb von uns wiederum gemäß § 30 LDSG beanstandet.

Doch nun stellte sich die Frage, ob die Stadt auf der Grundlage der rechtswidrig erlangten Anhaltspunkte weiter gegen den Petenten ermitteln durfte oder ob diese im Ergebnis einem Verwertungsverbot unterlagen. Wir haben uns die Beantwortung dieser Frage nicht leicht gemacht. Im Hinblick auf die Zuverlässigkeit des Melderegisters ist es einerseits nicht befriedigend, wenn die Meldebehörde trotz Anhaltspunkten für dessen Unrichtigkeit nicht weiter ermitteln darf und man nicht ausschließen kann, dass der Datenschutz es Meldepflichtigen zumindest mittelbar ermöglicht, sich bestehenden melderechtlichen Vorschriften zu entziehen. Doch wenn man andererseits zulassen würde, dass in unzulässiger Weise gewonnene Informationen zu einem Ermittlungsverfahren führen, liefe die Regelung des § 5 a Abs. 2 MG ins Leere, da die Meldebehörde sich dann stets konkrete Anhaltspunkte durch Recherchen „ins Blaue hinein“ beschaffen könnte. Auch legten wir bei der Bewertung des Sachverhaltes den Rechtsgedanken des § 13 Abs. 1 Satz 2 MG zugrunde, nach dem die Meldebehörde verpflichtet ist, unzulässig gespeicherte Daten zu löschen. Im Rahmen einer Gesamtbetrachtung kam mein Vorgänger deshalb in Abstimmung mit dem Innenministerium Baden-Württemberg zu dem Ergebnis, dass die Stadt nicht berechtigt war, aufgrund der rechtswidrig erlangten Anhaltspunkte für eine Unrichtigkeit des Melderegisters hinsichtlich des Wohnungsstatus des Petenten von Amts wegen zu ermitteln. Allerdings blieb ein schaler Beigeschmack zurück, da man sich nicht des Eindrucks erwehren konnte, dass sich hier beide Seiten aus unterschiedlichen Gründen bewusst nicht regelkonform verhalten hatten.

§ 5 a Meldegesetz (MG)
Richtigkeit und Vollständigkeit des Melderegisters

(1) Ist das Melderegister unrichtig oder unvollständig, hat es die Meldebehörde von Amts wegen zu berichtigen oder zu ergänzen (Fortschreibung). Der Betroffene soll vorher gehört werden. Von der Fortschreibung des Melderegisters sind unverzüglich diejenigen Stellen zu unterrichten, denen im Rahmen regelmäßiger Datenübermittlungen unrichtige oder unvollständige Daten übermittelt worden sind.

(2) Liegen der Meldebehörde bezüglich einzelner oder einer Vielzahl namentlich bekannter Einwohner konkrete Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit des Melderegisters vor, hat sie den Sachverhalt von Amts wegen zu ermitteln.

(3) Die in Absatz 1 Satz 3 genannten Stellen haben, soweit sie nicht Aufgaben der amtlichen Statistik wahrnehmen oder öffentlich-rechtliche Re-

ligionsgesellschaften sind, die Meldebehörden unverzüglich zu unterrichten, wenn ihnen konkrete Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit übermittelter Daten vorliegen. Sonstige öffentliche Stellen, denen auf deren Ersuchen hin Meldedaten übermittelt worden sind, dürfen die Meldebehörden bei Vorliegen solcher Anhaltspunkte unterrichten. Absatz 2 bleibt unberührt. Gesetzliche Geheimhaltungspflichten, insbesondere das Steuergeheimnis nach § 30 der Abgabenordnung, und Berufs- oder besondere Amtsgeheimnisse stehen der Unterrichtung nach den Sätzen 1 und 2 nicht entgegen, soweit sie sich auf die Angabe beschränkt, dass konkrete Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit übermittelter Daten vorliegen.

(4) Absatz 1 Satz 3 sowie Absatz 3 sind bei der Weitergabe von Daten und Hinweisen nach § 29 Abs. 8 entsprechend anzuwenden.

Der dargestellte Einzelfall ist nur einer von vielen, die mich regelmäßig zu dieser Thematik erreichen. Deshalb ergänzend noch einige allgemeine Hinweise hierzu:

Nach dem Meldegesetz für Baden-Württemberg ist bei mehreren Wohnungen im Inland eine dieser Wohnungen die Hauptwohnung. Hauptwohnung ist nach § 17 MG die vorwiegend benutzte Wohnung. Dies führt – vor allem bei Betroffenen, die nicht verheiratet sind und sich in keiner Lebenspartnerschaft befinden – mitunter zu dem Ergebnis, dass die Hauptwohnung nicht in der Gemeinde ist, wo sie nach ihrem Empfinden den Lebensmittelpunkt haben. Häufig wird auch beklagt, dass die Meldebehörden zur Ermittlung des überwiegenden Aufenthalts taggenaue Vergleichsberechnungen verlangen bzw. anstellen und hierzu entsprechende Belege anfordern. Dies wird häufig als ein zu großer Eingriff in das Persönlichkeitsrecht empfunden. Verständlich, dass sich manche Betroffene dadurch in ihrem Recht auf Freizügigkeit und Selbstbestimmung eingeschränkt fühlen. Allerdings ist für die Prüfung der datenschutzrechtlichen Zulässigkeit maßgeblich, welche Regelungen der Gesetzgeber hierzu getroffen hat und ob diese von der Meldebehörde beachtet wurden. In einigen Fällen waren aber auch wir der Auffassung, dass die geübte Verwaltungspraxis nicht ganz unbedenklich war.

§ 17 Meldegesetz (MG)
Mehrere Wohnungen

(1) Hat ein Einwohner mehrere Wohnungen im Inland, so ist eine dieser Wohnungen seine Hauptwohnung.

(2) Hauptwohnung ist die vorwiegend benutzte Wohnung des Einwohners. Hauptwohnung eines verheirateten oder eine Lebenspartnerschaft führenden Einwohners, der nicht dauernd getrennt von seiner Familie oder seinem Lebenspartner lebt, ist die vorwiegend benutzte Wohnung der Familie oder der Lebenspartner. Hauptwohnung eines minderjährigen Einwohners ist die Wohnung der Personensorgeberechtigten; leben diese getrennt, ist Hauptwohnung die Wohnung des Personensorgeberechtigten, die von dem Minderjährigen vorwiegend benutzt wird. Auf Antrag eines Einwohners, der in einer Einrichtung für behinderte Menschen untergebracht ist, bleibt die Wohnung nach Satz 3 bis zur Vollendung des 27. Lebensjahres seine Hauptwohnung. In Zweifelsfällen ist die vorwiegend benutzte Wohnung dort, wo der Schwerpunkt der Lebensbeziehungen des Einwohners liegt. Kann der Wohnungsstatus eines verheirateten oder eine Lebenspartnerschaft führenden Einwohners nach den Sätzen 2 und 5 nicht zweifelsfrei bestimmt werden, ist Hauptwohnung die Wohnung nach Satz 1.

(3) Nebenwohnung ist jede weitere Wohnung des Einwohners im Inland.

(4) Der Meldepflichtige hat bei jeder An- oder Abmeldung zu erklären, welche weiteren Wohnungen nach Absatz 1 er hat und welche Wohnung seine Hauptwohnung ist. Er hat der Meldebehörde der neuen Hauptwohnung jeden Wechsel der Hauptwohnung innerhalb einer Woche schriftlich mitzuteilen.

Auch die Gerichte haben sich bereits vielfach mit der Festlegung der Hauptwohnung befasst. Bedeutsam sind hierzu u. a. folgende zwei Urteile:

- Nach einer Entscheidung des Verwaltungsgerichtshofes Baden-Württemberg vom 21. April 1992, 1 S 2186/91, ist der vorwiegende Aufenthalt bei mehreren genutzten Wohnungen durch einen rein rechnerischen Vergleich der jeweiligen Aufenthaltszeiten ohne Rückgriff auf prägende Vergleichszeiträume und Regelvermutungen zu bestimmen. Die Vergleichsberechnung kann erforderlichenfalls taggenau erfolgen.
- Nach einem Urteil des Verwaltungsgerichts Karlsruhe vom 22. Februar 2001, 6 K 3161/99, ist bei einem von vornherein begrenzten Zeitraum, in dem mehrere Wohnungen benutzt werden, für die Feststellung der Hauptwohnung eine Vergleichsberechnung zugrunde zu legen, sofern der Zeitraum zwei Monate überschreitet.

Soweit Meldebehörden bei mehreren Wohnungen im Inland, die zeitgleich länger als zwei Monate benutzt werden, zur Bestimmung des überwiegenden Aufenthalts bzw. der Hauptwohnung eine Vergleichsberechnung anstellen, der gegebenenfalls eine taggenaue Aufstellung (mit geeigneten Belegen) zugrunde liegt, ist dies unter Berücksichtigung der obigen Ausführungen aus Sicht des Datenschutzes grundsätzlich hinnehmbar. Die Neustrukturierung des Melderechts infolge der Föderalismusreform I könnte und sollte in diesem Punkt für eine Verwaltungsvereinfachung genutzt werden; ich vermute allerdings, dass die dahinterstehenden fiskalischen Interessen der Wohnsitzgemeinden eine bürgerfreundliche Lösung erschweren.

Bei einer Ablösung des Melderechtsrahmengesetzes und der Landesmeldegesetze durch ein Bundesmeldegesetz (siehe auch in diesem Tätigkeitsbericht 1. Teil, Nummer 3.5) wäre es wünschenswert, wenn der Gesetzgeber es den Meldepflichtigen bei mehreren Wohnungen im Inland überlassen würde, welche Wohnung sie als Hauptwohnung festlegen.

2. Willkürliche Änderung des Auszugstages durch eine Meldebehörde sowie Auskunftsanspruch des Betroffenen

Dürfen Meldebehörden ohne hinreichend konkrete Anhaltspunkte das von einem Einwohner angegebene Datum des Auszuges ändern, wenn sie hieran Zweifel haben? Und dürfen aus Gründen des „Informantenschutzes“ bei einem bestehenden Auskunftsanspruch des Auskunftsbegehrenden über die zu seiner Person gespeicherten Daten in Unterlagen einzelne Passagen geschwärzt werden?

Um die Antwort auf die beiden Fragen vorwegzunehmen: Nein, natürlich dürfen Meldebehörden nicht willkürlich das vom Meldepflichtigen angegebene Datum des Auszugs ändern. Sie benötigen auch bei vorhandenen Zweifeln an der Richtigkeit des mitgeteilten Datums konkrete Hinweise, um dieses zu ändern. Und was den „Informantenschutz“ angeht: Um Dritte zu schützen, kann es in Einzelfällen auch bei einem bestehenden Auskunftsanspruch durchaus zulässig sein, bestimmte Stellen in Unterlagen zu schwärzen.

Aber der Reihe nach: Eine ehemalige Einwohnerin einer Stadt in der Region Neckar-Alb wandte sich an uns, da die dortige Meldebehörde ihren Melderegistereintrag von Amts wegen berichtigt hatte. Auch machte die Petentin geltend, dass sie im Rahmen eines Auskunftsersuchens über die zu ihrer Person gespeicherten Daten nicht in vollem Umfang informiert worden sei. In den ihr zur Verfügung gestellten Unterlagen seien Schwärzungen vorgenommen worden, sodass teilweise nicht nachvollziehbar gewesen sei, von wem die aus ihrer Sicht nachteiligen Informationen stammten. Sie wollte zu beiden Punkten wissen, ob die Stadt korrekt gehandelt hatte.

Berichtigung des Melderegisters:

Die Berichtigung des Melderegisters von Amts wegen regelt § 5 a Abs. 1 Satz 1 des Meldegesetzes (MG). Danach ist die Meldebehörde verpflichtet, das Melderegister im Falle der Unrichtigkeit zu berichtigen. Ob Daten unrichtig sind, bestimmt sich dabei ausschließlich nach objektiven Kriterien.

Vermutungen oder bloße Hinweise, dass Daten unrichtig sein könnten, reichen hierfür nicht aus. Im vorliegenden Fall ging es um den Zeitpunkt, in dem die Petentin im Sinne des Melderechts aus ihrer Wohnung ausgezogen war. Ein Auszug im Sinne des Melderechts setzt voraus, dass die Wohnung endgültig mit der Absicht verlassen wurde, sie überhaupt oder jedenfalls in absehbarer Zeit nicht mehr zum Wohnen oder Schlafen zu benutzen. Vom endgültigen Verlassen einer Wohnung ist die nur vorübergehende Unterbrechung der Benutzung abzugrenzen. In der Regel wird der Tatbestand des Auszugs in Fällen von länger dauernden Unterbrechungen der tatsächlichen Nutzung einer Wohnung erst bei einer Unterbrechung von etwa drei Jahren als gegeben angesehen. Der städtischen Stellungnahme konnten keine konkreten Anhaltspunkte entnommen werden, dass die Petentin vor ihrer Abmeldung aus ihrer Wohnung im melderechtlichen Sinne ausgezogen war. Die Auffassung der Stadt, der Wohnsitz sei bereits vor Jahren auf unabsehbare Zeit ins Ausland verlegt worden, blieb unbelegt. Unmaßgeblich waren insofern auch einige Argumente, die die Stadt ins Feld geführt hatte:

- Die Nichtteilnahme eines Kindes am Unterricht während eines Schuljahrs ist kein geeignetes Kriterium, das auf einen (früheren) Auszug aus der Wohnung hindeutet, wenn in der Regel ein Drei-Jahres-Zeitraum zugrunde gelegt wird, um festzustellen, ob nur eine Unterbrechung oder ein endgültiger Auszug im melderechtlichen Sinne vorliegt.
- Das Schreiben einer dritten Person, das der Stadt zuging, enthielt keine objektiven Kriterien, dass die tatsächliche Nutzung der Wohnung nach dem berichtigten Datum nicht beabsichtigt war. Im Gegenteil, das Schreiben ließ völlig offen, wann die Wohnung zuletzt tatsächlich genutzt wurde, und ging auch nicht auf den entscheidenden Punkt ein, wie lange die Absicht bestand, diese auch weiterhin tatsächlich zu nutzen.
- Nach den Aussagen der Vermieter der Petentin stand die Wohnung der Familie der Petentin jederzeit zur Verfügung. Selbst wenn die Wohnung im genannten Zeitraum nicht mehr benutzt worden war, bedeutet dies nicht automatisch, dass die Petentin bereits zu diesem Zeitpunkt nicht mehr die Absicht hatte, die Wohnung weiter zu nutzen, wozu sie laut Auskunft ihrer Vermieter ja auch jederzeit die Möglichkeit gehabt hätte.
- Die Stadt legte es zu Lasten der Petentin aus, dass diese nicht persönlich beim Einwohnermeldeamt vorgesprochen habe. Das konnte jedoch nicht als Indiz für einen Auszug aus der Wohnung angesehen werden. Die Stadt hatte die Petentin schriftlich gemäß § 5 a Abs. 1 Satz 2 MG angehört und dabei aufgefordert, eine verbindliche, schriftliche Erklärung über die genauen Aufenthaltszeiten in einem bestimmten Zeitraum abzugeben. Ein persönliches Erscheinen nach § 20 MG wurde jedoch nicht verlangt und war somit auch nicht erforderlich. Das Nichterscheinen darf dann aber auch nicht zum Nachteil der Betroffenen ausgelegt werden. Welchen Beitrag die Petentin zur Aufklärung des Sachverhalts geleistet hat, ist für die Festlegung des Abmeldedatums bzw. des Auszugstages, die nach objektiven Kriterien zu erfolgen hat, nicht ausschlaggebend.

Im Ergebnis haben die Ermittlungen der Meldebehörde zum Sachverhalt zu keinen belegbaren Erkenntnissen geführt, die als objektive Kriterien gewertet werden konnten. Deshalb war es datenschutzrechtlich nicht zulässig, ein quasi „aus der Luft gegriffenes“ Abmeldedatum bzw. einen bestimmten Auszugstag festzulegen und das Melderegister entsprechend zu bereinigen. Ich habe die Änderung des Abmeldedatums durch die Meldebehörde gemäß § 30 LDSG förmlich beanstandet und deren Aufsichtsbehörde hierüber informiert.

Schwärzung von einzelnen Passagen:

Der Auskunftsanspruch des Betroffenen nach § 11 des Meldegesetzes (MG) erstreckt sich grundsätzlich auf alle von der Meldebehörde über ihn gespeicherten Daten. Dies schließt in der Regel auch Angaben über die Herkunft der Daten ein. Nach § 11 Abs. 3 Nr. 3 MG unterbleibt jedoch die Auskunft, soweit die Daten eines Dritten ihrem Wesen nach, insbesondere wegen der überwiegenden Interessen dieser Person, geheim gehalten wer-

den müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss. Die Auskunft unterbleibt somit, soweit eine Abwägung ergibt, dass dem entgegenstehenden Interesse des Dritten das größere Gewicht zukommt.

Bei personenbezogenen Daten mit Doppel- und Mehrfachbezug kann die Auskunft an den Betroffenen wegen überwiegender privater Interessen einer dritten Person auch unterbleiben. Die Stadt hatte eine entsprechende Interessenabwägung vorgenommen, deren Ergebnis nach dem uns bekannten Sachverhalt nicht zu beanstanden war.

§ 11 Meldegesetz (MG)
Auskunft an den Betroffenen

(1) Die Meldebehörde hat dem Betroffenen auf Antrag Auskunft zu erteilen über

1. *die zu seiner Person gespeicherten Daten und Hinweise, auch soweit sie sich auf deren Herkunft beziehen,*
2. *die Empfänger oder Kategorien von Empfängern von regelmäßigen Datenübermittlungen sowie die Arten der zu übermittelnden Daten,*
3. *die Zwecke und die Rechtsgrundlagen der Speicherung und von regelmäßigen Datenübermittlungen.*

(2) Die Auskunft kann auch im Wege des automatisierten Abrufs über das Internet erteilt werden. Dabei ist zu gewährleisten, dass nach den allgemein anerkannten Regeln der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden, die insbesondere die Vertraulichkeit und die Unversehrtheit der im Melderegister gespeicherten und an den Betroffenen übermittelten Daten gewährleisten. Der Nachweis der Urheberschaft des Antrags ist durch eine qualifizierte elektronische Signatur nach dem Signaturgesetz zu führen. § 32 a Abs. 1 Satz 1 gilt entsprechend.

(3) Die Auskunft unterbleibt, soweit

1. *sie die ordnungsgemäße Erfüllung der in der Zuständigkeit der Meldebehörde liegenden Aufgaben gefährden würde,*
2. *sie die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes, des Landes oder eines anderen Landes Nachteile bereiten würde,*
3. *die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen*

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(4) Die Auskunft unterbleibt ferner, soweit

1. *dem Betroffenen in den Fällen der Annahme als Kind sowie der Änderung des Vornamens des Ehegatten aufgrund der Vorschriften des Transsexuellengesetzes die Einsicht in einen Eintrag im Geburten- oder Familienbuch nach § 61 Abs. 2 und 3 des Personenstandsgesetzes nicht gestattet werden darf,*
2. *gegenüber dem Betroffenen im Falle der Anbahnung einer Annahme als Kind ein Offenbarungsverbot nach § 1758 Abs. 2 des Bürgerlichen Gesetzbuchs besteht.*

(5) Bezieht sich die Auskunftserteilung auf Daten, die der Meldebehörde von Verfassungsschutzbehörden, dem Bundesnachrichtendienst oder dem Militärischen Abschirmdienst übermittelt worden sind, ist sie nur mit Zustimmung dieser Stellen zulässig.

(6) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf

die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Landesbeauftragten für den Datenschutz wenden kann.

(7) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht das Innenministerium im Einzelfall feststellt, dass durch die Auskunft die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Landesbeauftragten für den Datenschutz an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

Auskünfte über gespeicherte Daten erteilt grundsätzlich die Daten speichernde Stelle selbst, da mein Amt keinen unmittelbaren Überblick über die von anderen Behörden gespeicherten Daten hat. Anträge auf Auskunftserteilung sollten deshalb – nach Möglichkeit schriftlich – direkt an die entsprechende Behörde oder sonstige öffentliche Stelle gerichtet werden. Von dort erhalten die Auskunftsbegehrenden dann unentgeltlich Auskunft über die zu ihrer Person gespeicherten Daten. Im Fall einer Auskunftsverweigerung können sich die betroffenen Bürgerinnen und Bürger gerne an meine Dienststelle wenden; wir gehen dann der Angelegenheit nach. Dabei sollten uns die betreffende Behörde sowie die Einzelheiten des Antrags auf Auskunft mitgeteilt werden, am besten samt einer Kopie des schriftlichen Antrags bzw. der ablehnenden Antwort der Behörde.

3. Die Weitergabe von Meldedaten

Im Bereich des Meldewesens ist die Frage, ob personenbezogene Daten von den Meldebehörden an andere Stellen weitergegeben werden dürfen und ob man als Betroffener die Weitergabe gegebenenfalls verhindern kann, ein echter „Dauerbrenner". Häufig erreichen mich Beschwerden von Bürgern, die sich ärgern bzw. ihr Unverständnis darüber äußern, dass Meldebehörden ihre Daten, ohne sie zuvor fragen oder auch nur unterrichten zu müssen, herausgeben.

Im Meldegesetz (MG) gibt es Übermittlungsvorschriften für die Meldebehörden zur Weitergabe von personenbezogenen Daten aus dem Melderegister an Empfänger aus dem öffentlichen und privaten Bereich. Für bestimmte Datenempfänger sieht das Meldegesetz Gruppenauskünfte aus dem Melderegister vor, die jeweils auf die Bedürfnisse dieser Datenempfänger zugeschnitten sind. In diesem Zusammenhang sind die Herausgabe von Einwohnerdaten an Parteien für Wahlwerbungszwecke, die Veröffentlichung von Jubiläumsdaten, die Herausgabe von Adressbüchern und die Übermittlung von Einwohnerdaten an den Südwestrundfunk (SWR) zu nennen.

Da mich immer wieder Eingaben zu diesen Themenkomplexen erreichen, nachfolgend hierzu eine kurze Übersicht:

– Gruppenauskünfte an Parteien

  Die Meldebehörde (Gemeinde) darf u. a. im Zusammenhang mit allgemeinen Wahlen zu parlamentarischen und kommunalen Vertretungskörperschaften in den sechs Monaten vor der Wahl den Parteien und anderen Trägern von Wahlvorschlägen, die sich an der Wahl beteiligen, auf Antrag die Vor- und Familiennamen, Doktorgrade und Anschriften von wahlberechtigten Personen bestimmter Altersgruppen mitteilen; die Geburtstage dürfen hierbei nicht mitgeteilt werden. Rechtsgrundlage hierfür ist § 34 Abs. 1 MG. Zu beachten ist dabei, dass es sich bei Bürgermeisterwahlen nicht um Wahlen im Sinne von § 34 Abs. 1 MG handelt. Deshalb dürfen hierfür keine personenbezogenen Daten nach dieser Vorschrift übermittelt werden.

  Die Daten sollen es den Parteien ermöglichen, mit potenziellen Wählern persönlichen Kontakt aufzunehmen, indem sie diesen persönlich adressierte Schreiben zukommen lassen. Die Datenempfänger dürfen die Adressen

der Wahlberechtigten nur für Zwecke der Werbung für die Wahl verwenden, für die sie die Adressen erhalten haben. Sie sind verpflichtet, die Daten spätestens einen Monat nach der Wahl zu löschen.

Aufgrund dieser Vorschrift ist es beispielsweise zulässig, wenn eine Meldebehörde an eine Partei die Adressen von Jung- oder Erstwählern oder von Senioren herausgibt. Auch eine Auskunft über die Angehörigen beider genannten Gruppen würde sich noch im Rahmen des § 34 Abs. 1 MG halten, wenn die Partei darlegt, dass sie die beiden Gruppen mit jeweils unterschiedlichen altersspezifischen Themen ansprechen möchte. Nachdem der Gesetzgeber die Auskunftserteilung aber bewusst auf „Gruppen von Wahlberechtigten" beschränkt hat, darf sich eine Gruppenauskunft nach § 34 Abs. 1 MG nicht auf alle Wahlberechtigten erstrecken, auch nicht durch eine schlichte „Addition" von Wählergruppen, denn das käme einer Umgehung der gesetzlichen Schranken gleich. Soweit alle Wahlberechtigten angesprochen werden sollen, ist auf anderweitige Möglichkeiten wie z. B. Postwurfsendungen zu verweisen.

Da vielen Betroffenen trotz der Hinweispflicht der Meldebehörden nicht bekannt ist, dass der Gesetzgeber hier ein Widerspruchsrecht vorgesehen hat, habe ich im Vorfeld der jüngsten Bundestagswahl eine Pressemitteilung unter der Überschrift „Schutz vor unerwünschter Wahlwerbung ist möglich" (abrufbar über die Internet-Seite meines Amts unter „Der LfD und seine Aufgaben" → „Pressemitteilungen") herausgegeben und folgenden Rat gegeben: „Jeder, der eine solche Wahlwerbung nicht wünscht, sollte möglichst bald von seinem Widerspruchsrecht gegenüber der Meldebehörde seines Wohnorts Gebrauch machen, am besten schriftlich." Außerdem habe ich darauf hingewiesen, dass das Einwohnermeldeamt den Widerspruch so lange beachten müsse, bis der Betroffene ihn gegebenenfalls wieder zurücknimmt. Der Bürger brauche deshalb nicht vor jeder Wahl erneut aktiv zu werden. Der Gesetzgeber könnte den Bürgern aber noch weiter entgegenkommen, denn eigentlich ist auch die Widerspruchslösung unbefriedigend. Es wäre besser, wenn die Bürger nicht von sich aus aktiv werden müssten. Leider hat die Landesregierung bzw. der Gesetzgeber der langjährigen Forderung meiner Dienststelle, die Nutzung der Einwohneradressen für Wahlwerbezwecke von der ausdrücklichen Einwilligung der Betroffenen abhängig zu machen und die geltende Widerspruchs- durch eine datenschutzfreundlichere Einwilligungslösung zu ersetzen, bisher nicht Rechnung getragen.

– Veröffentlichung von Jubiläumsdaten

Immer wieder fragen Bürger bei uns an, ob die Meldebehörde die Daten von Jubilaren – ohne vorab fragen zu müssen – selbst veröffentlichen und/oder zu diesem Zweck an die Medien weitergeben darf.

Ja, eine Meldebehörde darf dies grundsätzlich tun, wenn der Betroffene dem nicht zuvor widersprochen hat. Rechtsgrundlage hierfür ist § 34 Abs. 2 MG. Danach dürfen Namen, Doktorgrad und Anschriften von Altersjubilaren (ab 70. Geburtstag) und Ehejubilaren (ab goldener Hochzeit) sowie Tag und Art des Jubiläums veröffentlicht und an Presse und Rundfunk zum Zwecke der Veröffentlichung herausgegeben werden. Ob die Meldebehörde so verfährt oder nicht, steht aber in ihrem Ermessen; weder Bürger noch Presse oder Rundfunkanstalten haben einen Anspruch darauf, dass Jubiläumsdaten herausgegeben werden. Es besteht auch kein Anspruch auf eine fehlerfreie Ermessensausübung, da das Ermessen der Meldebehörde nicht im Interesse der Jubilare oder der Presse eingeräumt wurde, sondern zur Befriedigung des Informationsbedürfnisses der Allgemeinheit. Die Meldebehörde ist jedoch zur Gleichbehandlung aller Medien verpflichtet. Die Einstellung von Jubiläumsdaten in das Internet durch die Gemeinde bedarf hingegen aus Sicht des Datenschutzes wegen der globalen Zugänglichkeit der Daten der ausdrücklichen Einwilligung der Betroffenen.

– Übermittlung von Einwohnerdaten zum Zwecke der Veröffentlichung eines Einwohner- oder Adressbuches

Die Meldebehörde darf Vor- und Familiennamen, Doktorgrad und Anschriften der volljährigen Einwohner in Einwohnerbüchern und ähn-

lichen Nachschlagewerken sowie in elektronischen Adressverzeichnissen veröffentlichen und an andere zum Zweck der Herausgabe solcher Werke übermitteln (§ 34 Abs. 3 MG). Auch wenn der Gesetzgeber inzwischen den Gemeinden die Veröffentlichung von elektronischen Adressverzeichnissen erlaubt und damit auch eine Einstellung entsprechender Verzeichnisse in das Internet ermöglicht wird, ist dies – auch im Hinblick auf den örtlichen Wirkungskreis einer Gemeinde – aus Sicht des Datenschutzes nicht hinnehmbar. Datenschutzrechtlich hat dieser Eingriff nämlich eine völlig andere Qualität, da die Daten weltweit abgerufen werden können. Die Veröffentlichung im Internet erreicht einen viel größeren Personenkreis als jede andere Veröffentlichung. Außerdem eröffnet die Veröffentlichung im Internet vielfältige Auswertungs- und Verknüpfungsmöglichkeiten, durch die schutzwürdige Interessen der Betroffenen berührt sein können. Die Veröffentlichung von Adressdaten im Internet darf deshalb nur vorgenommen werden, wenn die Einwohner dazu ihr ausdrückliches Einverständnis gegeben haben. Dabei genügt es den datenschutzrechtlichen Anforderungen nicht, den Betroffenen lediglich das Recht einzuräumen, der beabsichtigten Datenweitergabe zu widersprechen.

– Übermittlung von Einwohnerdaten an den Südwestrundfunk (SWR)

Die Frage, ob und gegebenenfalls unter welchen Voraussetzungen die Meldebehörde berechtigt ist, Daten an den SWR bzw. an die Gebühreneinzugszentrale (GEZ) zu übermitteln, beschäftigt Betroffene immer wieder, wie aus der Vielzahl der mir zugehenden Eingaben deutlich wird. In der Tat ist die Meldebehörde aufgrund verschiedener Rechtsvorschriften befugt oder sogar verpflichtet, bestimmte Einwohnerdaten an den SWR weiterzugeben:

Nach § 35 Abs. 1 MG ist die Meldebehörde berechtigt, den SWR oder die von ihm mit dem Einzug der Rundfunkgebühr beauftragte GEZ über den Zuzug, den Wegzug und den Tod von volljährigen Einwohnern zu unterrichten. Dabei darf sie Familiennamen, Vornamen, frühere Namen, Geburtstag, Anschriften, Tag des Ein- und Auszugs, Familienstand und Sterbetag übermitteln. Diese Regelung wurde, obwohl wir uns damals nachdrücklich gegen sie gewandt hatten, im Jahre 1995 in das Meldegesetz eingefügt. Wir hatten dabei die Auffassung vertreten, dass diese Art von Meldedienst über das hinausgeht, was zur Ermittlung von „Schwarzsehern und -hörern“ verhältnismäßig wäre. Jedoch sind die vom Gesetzgeber hierzu erlassenen Rechtsvorschriften der Maßstab für eine datenschutzrechtliche Prüfung eines Einzelfalls.

Obwohl nahezu alle Gemeinden und Städte im Land dem SWR nach § 35 MG regelmäßig Veränderungen mitteilen, begnügt sich der SWR damit nicht immer. Zur Erleichterung der Arbeit der eingesetzten Gebührenbeauftragten bei der Ermittlung von „Schwarzsehern und -hörern“ versucht die GEZ darüber hinaus offenbar immer wieder, von Bürgermeisterämtern komplette Listen mit den Adressdaten aller volljährigen Einwohner zu erhalten (in Einzelfällen wurden auch Adressdaten von Einwohnern ab 16 Jahren angefordert). Regelmäßig wenden sich dann die von einem entsprechenden Auskunftsersuchen betroffenen Gemeinden an mich mit der Frage, ob sie dem SWR die erbetenen Listen übermitteln dürfen bzw. müssen.

Meine Vorgänger und auch ich haben die Herausgabe solcher Listen stets als unzulässig angesehen, weil ein solcher „Rundumschlag“ unverhältnismäßig ist, obwohl der Verwaltungsgerichtshof Baden-Württemberg in seinem Urteil vom 15. November 1994, 1 S 310/94, die Auffassung vertrat, eine solche Datenübermittlung an die Rundfunkanstalt sei aufgrund von § 29 MG möglich. Die Rundfunkanstalt hat jedoch nach der Auffassung des Verwaltungsgerichtshofs keinen absoluten Übermittlungsanspruch; vielmehr hat das Bürgermeisteramt eine Ermessensentscheidung zu treffen und dabei zu prüfen, ob die Rundfunkanstalt besondere Gesichtspunkte geltend macht, die über das grundsätzlich bestehende öffentliche Interesse an der Aufgabenwahrnehmung der Rundfunkanstalten hinausgehen. Ein solcher von der Rundfunkanstalt geltend zu machender Gesichtspunkt könnte nach Ansicht des Verwaltungsgerichtshofs sein,

dass eine bestimmte Gemeinde oder ein Stadtteil im Verhältnis zu vergleichbaren Gemeinden oder Stadtteilen und entgegen der statistisch belegten Aussage, dass nahezu alle Haushalte der Bundesrepublik über Rundfunkgeräte verfügen, nach dem der Rundfunkanstalt vorliegenden Bestandsverzeichnis zu wenig Anmeldungen von Rundfunkteilnehmern aufweist. Liegt diese Voraussetzung vor, können wir den Kommunen nicht empfehlen, entsprechende Übermittlungsersuchen der Rundfunkanstalt abzulehnen.

– Widerspruchsmöglichkeiten

Ein für die Bürger wichtiger Aspekt im Zusammenhang mit der Weitergabe von Einwohnerdaten ist, ob und gegebenenfalls wie der Einzelne die Weitergabe seiner Daten durch die Meldebehörde verhindern kann. Was die Weitergabe von Einwohnerdaten an den SWR betrifft, kann ich den Betroffenen nur sagen, dass es hier keine Möglichkeit gibt, die Datenweitergabe zu verhindern, da dies der Gesetzgeber nicht vorgesehen hat. Anders hingegen verhält es sich bei der Herausgabe von Einwohnerdaten für Wahlwerbungszwecke, der Veröffentlichung von Jubiläumsdaten und der Herausgabe von Adressbüchern. Hier haben die Betroffenen das Recht, der Weitergabe ihrer Daten zu widersprechen; die Meldebehörde ist verpflichtet, die Bürger auf ihr Widerspruchsrecht hinzuweisen (§ 34 MG). Ich halte diese Regelung für einen gerade noch vertretbaren Kompromiss zwischen dem Informationsinteresse der Parteien bzw. der Allgemeinheit und dem Interesse der einzelnen Bürger auf Wahrung ihrer Privatsphäre, weil sie ihnen wenigstens die Möglichkeit gibt, die Herausgabe ihrer Daten im Wege des Widerspruchs zu verhindern.

Da trotz der den Gemeinden obliegenden Hinweispflicht erfahrungsgemäß viele Einwohner über ihr Widerspruchsrecht nicht Bescheid wissen und dieses dann auch nicht in Anspruch nehmen, sollte der Gesetzgeber die geltende Widerspruchslösung durch eine datenschutzfreundlichere Einwilligungslösung ersetzen. Zumindest sollten die Meldebehörden ihre Einwohner regelmäßig in geeigneter Form – auch über die gesetzlichen Vorgaben hinaus – auf ihre Widerspruchsmöglichkeiten deutlich hinweisen.

2. Abschnitt: Bau- und Wohnungswesen, Vermessungswesen, Geodaten

1. Internet-Veröffentlichung von Bürgerstellungnahmen im Bauleitplanverfahren

Transparenz bei Verwaltungsverfahren ist in einem demokratischen Rechtsstaat von überragender Bedeutung. Dürfen jedoch schriftliche Anregungen und Stellungnahmen, die von Bürgern im Rahmen der Öffentlichkeitsbeteiligung im Bauleitplanverfahren eingebracht werden, auch im Internet veröffentlicht werden?

Eine Bürgerin einer größeren Stadt wandte sich mit folgendem Anliegen an meine Dienststelle: Die Stadt, in der sie wohnt, hatte ein Bebauungsplanänderungsverfahren eingeleitet, durch das die bauliche Nutzung eines in der Nachbarschaft der Petentin gelegenen öffentlichen Gebäudes neu festgelegt werden sollte. Ausweislich des Planentwurfs sollten die Räumlichkeiten dieses Anwesens künftig für gesellschaftliche und kulturelle Veranstaltungen örtlicher Vereine und Organisationen zur Verfügung stehen. Damit war die Petentin nicht einverstanden und machte dies in einem Schreiben an den Oberbürgermeister deutlich. Dabei war ihr, wie sie in ihrer Eingabe betonte, durchaus bewusst, dass ihr Einspruch im Gemeinderat diskutiert werden würde. Nicht gerechnet hatte die Petentin jedoch damit, dass ihre durchaus kritische Äußerung unverändert nicht nur als Anlage zu den Unterlagen der Gemeinderatssitzung, in der über die Auslegung des Bebauungsplans beschlossen wurde, sondern auch durch den Internet-Auftritt der Gemeinde veröffentlicht werden würde.

Zu Recht sah sich die Petentin durch dieses Vorgehen der Stadt in ihrem Recht auf informationelle Selbstbestimmung verletzt.

Meine Dienststelle vertritt seit jeher die Auffassung, dass weder das baden-württembergische Kommunalrecht noch das Landesdatenschutzgesetz (LDSG) eine Rechtsgrundlage dafür bieten, die Unterlagen, welche den Mitgliedern des Gemeinderats gemäß § 34 Abs. 1 der Gemeindeordnung (GemO) zur Vorbereitung einer Gemeinderatssitzung mitzuteilen sind, Dritten zugänglich zu machen, wenn und soweit diese Dokumente personenbezogene Daten, das heißt Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, enthalten. Ein datenschutzrechtlicher Erlaubnistatbestand, der eine andere Handhabung gestatten würde, lässt sich insbesondere auch nicht aus dem in § 35 Abs. 1 GemO statuierten Grundsatz der Öffentlichkeit der Sitzungen des Gemeindeparlaments ableiten, denn diese Vorschrift zielt auf die Zugänglichkeit der Sitzungen, nicht auch der Sitzungsunterlagen ab. Das soeben Gesagte gilt – wie mein Vorgänger im 23. Tätigkeitsbericht für das Jahr 2002 (LT-Drucksache 13/1500) ausführlicher dargelegt hat – erst recht, wenn das Internet als Plattform der Verbreitung der Sitzungsunterlagen genutzt werden soll; denn die weltweite Publikation im Netz überschreitet grundsätzlich den Aufgaben- und Wirkungskreis der Gemeinde und impliziert überdies entgegen § 20 Absätze 2 bis 5 LDSG eine Übermittlung der in den Unterlagen enthaltenen personenbezogenen Daten auch in solche Staaten außerhalb der Europäischen Union, in denen ein angemessenes Datenschutzniveau nicht gewährleistet ist.

Und das Baurecht? Die maßgeblichen Vorschriften des materiellen Bauplanungsrechts finden sich im ersten Teil des Baugesetzbuchs (BauGB). Tatsächlich stößt man hier mittlerweile auf eine Norm, welche es den Gemeinden ausdrücklich gestattet, im Bauleitplanverfahren auf das Internet zurückzugreifen: Gemäß § 4 a Abs. 4 BauGB können (müssen aber nicht) bei der Öffentlichkeits- und Behördenbeteiligung im Sinne der §§ 3 und 4 BauGB ergänzend elektronische Informationstechnologien genutzt werden. Die Gemeinde darf demnach etwa die nach Maßgabe des § 4 zu beteiligenden Behörden und sonstigen Träger öffentlicher Belange auf elektronischem Wege konsultieren und die nach § 3 Abs. 2 Satz 1 BauGB vorgeschriebene einmonatige Auslegung der Entwürfe der Bauleitpläne mit Begründung und den nach ihrer Einschätzung wesentlichen, bereits vorliegenden umweltbezogenen Stellungnahmen parallel (auch) per Internet vornehmen.

Die baurechtliche Kommentarliteratur räumt jedoch ein, dass Stellungnahmen mit personenbezogenen Informationen nach § 3 Abs. 2 Satz 1 BauGB aus Gründen des Datenschutzes nur offengelegt werden dürfen, wenn die geschützten Daten zuvor unkenntlich gemacht worden sind. Erst recht ist eine solche Anonymisierung – die dem informationellen Selbstbestimmungsrecht freilich nur dann wirklich Rechnung trägt, wenn sich der ursprüngliche Personenbezug der Eingabe hernach nicht mehr oder nur noch mit unverhältnismäßigem Aufwand wiederherstellen lässt – unabdingbar, soweit die Gemeinde von ihrer Option Gebrauch macht, die Öffentlichkeit nach Maßgabe des besagten § 4 a Abs. 4 BauGB auch über das Internet zu beteiligen. Denn aufgrund der unbeschränkten Reichweite, der vielfältigen Verknüpfungsmöglichkeiten und des bekanntlich nahezu unauslöschlichen Gedächtnisses dieses Mediums greift die Veröffentlichung im Netz besonders intensiv in das informationelle Selbstbestimmungsrecht des Betroffenen ein.

Da sich der Personenbezug von Bürgereingaben, die primär oder ausschließlich die von der Bauleitplanung berührten individuellen Belange eines Einwohners zum Gegenstand haben, indessen kaum je so vollständig wird tilgen lassen, dass sich die Person des Betroffenen aus dem Inhalt der Stellungnahme nicht mehr erschließen ließe, ist auf ihre Offenlegung im Internet, zu der das Baugesetzbuch die Gemeinde ja keinesfalls verpflichtet, regelmäßig zu verzichten.

Es gab daher unseres Erachtens auch unter baurechtlichen Gesichtspunkten keine hinreichende Rechtsgrundlage dafür, das Schreiben der Petentin an die Stadtverwaltung, zumal unter Verzicht auf jegliche Anonymisierung, im Internet zu veröffentlichen. Dies haben wir der Stadt mitgeteilt und diese gebeten, unsere Rechtsauffassung künftig zu beachten.

Anregungen und Stellungnahmen, die von Bürgern im Bauleitplanverfahren abgegeben worden sind, dürfen aus Gründen des Datenschutzes regelmäßig nicht im Internet veröffentlicht werden.

2. Landesgeodatenzugangsgesetz

Die europäische „INSPIRE"-Richtlinie soll in Baden-Württemberg durch ein Landesgeodatenzugangsgesetz (LGeoZG) umgesetzt werden, welches dem Aufbau einer baden-württembergischen Geodateninfrastruktur dient. Das Gesetz berührt auch Belange des Datenschutzes.

Der datenschutzgerechte Umgang mit sog. Geodaten, das heißt mit Daten, die einen direkten oder indirekten Bezug zu einem Standort oder einem geografischen Gebiet aufweisen, hat in der Vergangenheit in der datenschutzrechtlichen Diskussion eine eher untergeordnete Rolle gespielt. Doch seit einiger Zeit ist das Thema gleichsam aus seinem Dornröschenschlaf erwacht, denn Politik und Wirtschaft haben das wirtschaftliche Potenzial entdeckt, welches in den bei der Verwaltung in Bund und Ländern, bei Städten und Gemeinden vorliegenden Geodaten aller Art schlummert. Bestrebungen, diesen „Datenschatz" zu heben und landes- bzw. bundesweit in vernetzter und interoperabler Form zu erschließen, sind längst in vollem Gange.

Auch die Europäische Union ist vor einiger Zeit initiativ geworden und hat mit einer „Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE)" ein Instrument geschaffen, das den Zugang zu und die Nutzung von Geodaten für die Bürger, die Verwaltung und die Wirtschaft vereinfachen soll. Bei dieser Richtlinie handelt es sich um ein etwas zwiespältiges Regelwerk, das vordergründig umweltpolitische Ziele verfolgt, tatsächlich jedoch zahlreiche weitere Politikfelder berührt. INSPIRE hält die Mitgliedstaaten – vereinfacht dargestellt – dazu an, die bei ihren Behörden und anderen öffentlichen Stellen in elektronischer Form vorhandenen Geodaten in harmonisierter, standardisierter und interoperabler Form bereitzustellen und über öffentlich verfügbare und via Internet zugängliche Netzdienste zu erschließen.

Auf der Ebene des Bundes ist die INSPIRE-Richtlinie durch ein Geodatenzugangsgesetz vom 10. Februar 2009 (BGBl. I, S. 278) bereits umgesetzt worden; dieses gilt jedoch nur für Stellen des Bundes und bundesunmittelbare juristische Personen des öffentlichen Rechts, die Geodaten vorhalten. Um die Richtlinie vollständig in nationales Recht zu transformieren, ist daher ergänzend ein gesetzgeberisches Tätigwerden der Länder erforderlich.

In Baden-Württemberg ist das diesbezügliche Gesetzgebungsverfahren noch nicht abgeschlossen, doch ist der Entwurf eines künftigen „Gesetzes über den Zugang zu digitalen Geodaten für Baden-Württemberg", oder etwas kürzer: eines „Landesgeodatenzugangsgesetzes", bereits in die Anhörung gegangen. Das Landesgeodatenzugangsgesetz folgt eng dem bundesrechtlichen Vorbild und verschreibt sich dem Aufbau einer baden-württembergischen Geodateninfrastruktur, als deren Kernkomponente die amtlichen Daten des Liegenschaftskatasters und der Landesvermessung fungieren. In diese Geodateninfrastruktur sollen die öffentlichen Stellen in Baden-Württemberg die bei ihnen in digitaler Form vorhandenen geodätischen Informationen einbringen, sofern diese die richtlinienrelevanten Politikfelder betreffen. Geodaten, Metadaten, Geodaten- und Netzwerkdienste werden über ein elektronisches Netzwerk, das über ein „Geoportal Baden-Württemberg" zugänglich sein wird, miteinander verknüpft. Über das besagte Geoportal sollen im Übrigen auch natürliche und juristische Personen des Privatrechts Geodaten bereitstellen dürfen.

Und wo bleibt der Datenschutz? Viele Geodaten erlauben Rückschlüsse auf persönliche und sachliche Verhältnisse einer bestimmten oder über Wohnanschriften oder Eigentümer- bzw. Standortdaten doch bestimmbaren natürlichen Person, weisen also einen Personenbezug auf. Hierauf haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 6./7. November 2008 („Datenschutzgerechter Zugang zu Geoinformationen", vgl. Anhang 22) hingewiesen und dabei angemahnt, dass Geo-

datenzugangsgesetze einen differenzierenden Ausgleich zwischen Informations- und Schutzinteressen für die spezielle Problematik der Geobasis- und der Geofachdaten vornehmen müssen. Mit einer möglichen datenschutzrechtlichen Relevanz geodätischer Informationen rechnet auch die INSPIRE-Richtlinie und sieht daher vor, dass der Zugang der Öffentlichkeit zu Geodaten mit Personenbezug eingeschränkt werden kann.

Der Bundesgesetzgeber hat dementsprechend eine Regelung zum Schutz der Belange des informationellen Selbstbestimmungsrechts in seinem Geodatenzugangsgesetz vorgesehen, indem er die einschlägigen Zugangsbeschränkungen nach dem Umweltinformationsgesetz für entsprechend anwendbar erklärt. Im Prinzip folgt der Landesgesetzgeber auch insoweit der bundesgesetzlichen Vorlage: In Analogie zur entsprechenden Regelung im Umweltinformationsgesetz des Bundes ist der Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten nach der Entwurfsfassung zu beschränken, soweit anderenfalls personenbezogene Daten offenbart und dadurch Interessen der Betroffenen erheblich beeinträchtigt würden – es sei denn, die Betroffenen haben zugestimmt oder das öffentliche Interesse an Zugang überwiegt.

Erfreulicherweise hat das federführende Ministerium für Ernährung und Ländlichen Raum, das unsere Dienststelle frühzeitig in seine Überlegungen einbezogen hat, jedoch darüber hinaus nach bayerischem Vorbild eine Regelung in den Entwurf aufgenommen, nach der bereits bei der Bereitstellung der Geodaten und Geodatendienste für die Öffentlichkeit und für andere Geodaten haltende Stellen die Vorschriften des Landesdatenschutzgesetzes in ihrer jeweils geltenden Fassung entsprechend anzuwenden sind. Damit soll ausweislich der Entwurfsbegründung dem datenschutzrechtlichen Gefährdungspotenzial, das aufgrund der Vielzahl möglicher Datenabrufe zu erwarten ist, bereits bei der Entscheidung über die Verfügbarmachung von Geodatendiensten begegnet werden.

Der Ausgang des Gesetzgebungsverfahrens im Land bleibt abzuwarten. Wenn es bei dem zur Anhörung freigegebenen Entwurf bleibt, so wird den Belangen des Datenschutzes bei der Umsetzung der INSPIRE-Richtlinie letztlich besser Rechnung getragen als auf Bundesebene. Der technische Fortschritt und die vielseitige Nutzbarkeit von Geodaten werden weitere datenschutzrechtliche Herausforderungen mit sich bringen.

3. Google Street View

„Google Street View“ ist aus datenschutzrechtlicher Sicht ein „heißes Eisen“. Da sich die Zuständigkeit unserer Dienststelle jedoch sachlich auf die Kontrolle des Datenschutzes bei den öffentlichen Stellen und örtlich auf Baden-Württemberg beschränkt, sind wir für dieses Projekt nicht der richtige Ansprechpartner. Hierauf mussten wir besorgte Bürgerinnen und Bürger immer wieder hinweisen.

Wenige datenschutzrechtliche Themen dürften in der Berichterstattung der Medien in den vergangenen Monaten breiteren Raum eingenommen haben als das Projekt „Google Street View“. Worum es dabei geht, bedarf vermutlich kaum mehr einer Erläuterung: In Erweiterung seines bekannten Online-Dienstes „Google Maps“ lässt das in Kalifornien beheimatete, jedoch global agierende Unternehmen „Google Inc.“ den Straßenraum von Städten und auch anderen Orten in aller Welt mithilfe spezieller 3D-Kameras systematisch aus der Perspektive eines virtuellen Fußgängers fotografieren und stellt das gewonnene dreidimensionale und hochauflösende Bildmaterial in das Internet. Damit kann der Nutzer des Dienstes die erfassten Städte nicht mehr nur, wie schon bislang, aus der Vogelperspektive betrachten, sondern bequem vom heimischen PC aus kostenlose digitale Stadtrundgänge unternehmen. Seit einiger Zeit sind die charakteristischen Kamerafahrzeuge des Suchmaschinenriesen nunmehr auch in den deutschen Städten unterwegs und sorgen bei nicht wenigen Menschen für Unbehagen. Denn nicht jedermann ist damit einverstanden, dass gestochen scharfe Bilder seiner Wohnumgebung, seines Hauses, seines Gartens etc., die mühelos mit Satellitenfotos, Adressdatenbanken und anderen personenbezogenen Daten verknüpft werden können, mit einem simplen Mausklick von jedem beliebigen Internet-Nutzer abgerufen werden können.

Es verwundert daher nicht, dass sich viele besorgte Bürger, aber auch einige Gemeinden an unsere Dienststelle gewandt haben, um unseren Rat in Sachen „Google Street View“ einzuholen; denn verständlicherweise wird der Landesbeauftragte für den Datenschutz als der „natürliche“ Ansprechpartner in allen datenschutzrechtlichen Fragen wahrgenommen. Tatsächlich jedoch beschränkt sich die Zuständigkeit unserer Dienststelle nach gegenwärtiger Rechtslage sachlich auf die Kontrolle des Datenschutzes bei den Behörden und sonstigen öffentlichen Stellen; gegenüber einem Wirtschaftsunternehmen wie der Firma „Google“ können wir deswegen (derzeit noch) keinerlei Kontrollbefugnis in Anspruch nehmen. Hinzu kommt, dass die Google Germany GmbH, die inländische Tochter des amerikanischen Mutterkonzerns, ihren Unternehmenssitz in Hamburg und damit außerhalb unseres örtlichen Zuständigkeitsbereichs hat.

Wir müssen uns daher regelmäßig darauf beschränken, den Bürgern, die uns wegen „Google Street View“ um Rat gefragt haben, zu empfehlen, ihren etwaigen Widerspruch gegen die Veröffentlichung sie betreffender Abbildungen direkt bei der Google Germany GmbH einzureichen (entweder im Internet unter der Adresse *http://maps.google.de/intl/help/maps/streetview/faq.html#q7* oder schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg) und sich in Problemfällen an den zuständigen Hamburger Datenschutzbeauftragten zu wenden, dessen Dienststelle in Abstimmung mit den übrigen Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich mit der Google Germany GmbH über den Online-Dienst verhandelt und das Unternehmen zu einigen wichtigen datenschutzrechtlichen Zugeständnissen bewogen hat – so etwa zu der Zusage, alle Kamerafahrten im Voraus anzukündigen und in dem Falle, dass ein Betroffener Widerspruch einlegt, Abbildungen von Gesichtern, Gebäudeansichten und Kraftfahrzeugen auch in den erhobenen Rohdaten unkenntlich zu machen.

Wer mit der Veröffentlichung von Aufnahmen seiner Person, seines Fahrzeugs oder seines Grundstücks im Rahmen von „Google Street View“ nicht einverstanden ist, sollte direkt bei der „Google Germany GmbH“ Widerspruch einlegen. In Problemfällen empfehle ich, sich an meinen zuständigen Kollegen, den Hamburger Datenschutzbeauftragten, zu wenden.

3. Abschnitt: Landwirtschaft und Umwelt

1. Das Verfahren FIONA (Flächeninformation und Online-Antrag)

Praktisch, wenn Geodaten direkt für landwirtschaftliche Förderanträge verwendet werden können. Aber problematisch, wenn sich auch andere Verfahrensteilnehmer Informationen über die zustehenden Fördermittel verschaffen können.

Die Beantragung von Fördermitteln für die Bewirtschaftung von landwirtschaftlich genutzten Flächen muss mit dem sog. Gemeinsamen Antrag erfolgen. In dem Antragsformular sind umfangreiche Angaben zu machen, deren Erhebung und Zusammenstellung sich aufwändig gestaltet. Zur schnelleren Abwicklung des Antragsverfahrens hat das Ministerium für Ernährung und Ländlichen Raum (MLR) eine Software entwickeln lassen, mit der landwirtschaftliche Betriebe EDV-gestützt die Antragstellung über das Internet durchführen können. Dieses Verfahren mit Namen FIONA erlaubt es den landwirtschaftlichen Betrieben, über ein geografisches Informationssystem (GIS) auf Flächeninformationen, nach denen sich die Höhe der Fördermittel bemisst, zuzugreifen und diese Flächeninformationen in das sog. digitale Flurstücksverzeichnis (FSV) einzustellen, aus dem der Ausdruck des in Papierform zu stellenden Antrags generiert wird. Hierdurch sinkt nicht zuletzt der Aufwand für das Ministerium und die nachgeordneten Stellen spürbar.

Die Sache hat allerdings auch einen Haken, auf den mich ein Betroffener durch eine Eingabe hinwies: Mit FIONA falle es nicht nur ihm leicht, die Höhe der Fördermittel für ein von ihm bewirtschaftetes Grundstück zu berechnen, sondern dies könnten auch Dritte, die Zugriff auf FIONA haben. Dritte, die wüssten, welche landwirtschaftlichen Flächen er bewirtschafte, könnten nämlich ohne Weiteres durch Addition der Angaben über die ein-

zelnen Flurstücke die Höhe der ihm zustehenden Fördermittel insgesamt berechnen. Er bat uns, die Sache unter datenschutzrechtlichen Aspekten zu prüfen.

Mein Vorgänger nahm diese Eingabe zum Anlass, mit dem Ministerium für Ernährung und Ländlichen Raum eine Kontrolle der Anwendung FIONA zu vereinbaren, die schließlich im März 2008 stattfand und zu folgendem Ergebnis führte:

FIONA bedeutet einen Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Grundstückseigentümer, weil die Anwendung ihren Nutzern Zugriff auf personenbezogene Angaben Dritter eröffnet. Dies gilt namentlich für die GIS-Komponente der Anwendung, über die der Nutzer kartografisches Material und Luftfotografien des gesamten Landesgebiets einsehen und Informationen über die Lage, die Fläche und die Grenzen von Grundstücken und Parzellen, die Flurstücksnummern und die Bebauung bzw. Nutzung von Liegenschaften abrufen kann. Diese Angaben können mithilfe der Flurstücksnummer oder anderen Zusatzinformationen, über die der jeweilige Nutzer aus eigener Kenntnis verfügen mag, im Prinzip dem jeweiligen Eigentümer oder Pächter zugeordnet werden und lassen mithin in zahlreichen Fällen Rückschlüsse auf sachliche Verhältnisse bestimmter oder doch bestimmbarer natürlicher Personen zu.

Aus datenschutzrechtlicher Sicht werden diese personenbezogenen Daten an Stellen außerhalb des öffentlichen Bereichs übermittelt. Wie jede Datenverarbeitung im Sinne des Landesdatenschutzgesetzes, so ist auch diese Übermittlung nur zulässig, wenn das Landesdatenschutzgesetz selbst oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene – jeder Betroffene! – eingewilligt hat. Die Einwilligung sämtlicher Betroffener einzuholen, wäre im Falle von FIONA angesichts der Größe des insoweit in Rede stehenden Personenkreises allerdings wohl kaum praktikabel.

Als eine mögliche Rechtsgrundlage für die Datenverarbeitung in FIONA wurde uns von den Mitarbeitern des MLR § 14 des Vermessungsgesetzes für Baden-Württemberg (VermG) genannt. Hierzu muss man wissen, dass die vormals sehr strikten datenschutzrechtlichen Beschränkungen, welche das Vermessungsgesetz bis vor einigen Jahren im Hinblick auf die Übermittlung personenbezogener Daten des Liegenschaftskatasters aufwies, im Zuge einer Novellierung des Gesetzes erheblich gelockert worden sind, da der Landesgesetzgeber einen leichteren Zugang und eine umfassendere Verwendung dieser Informationen ermöglichen wollte. Nach der aktuellen Fassung des § 14 Abs. 2 VermG vom 1. Juli 2004 dürfen personenbezogene Geobasisinformationen übermittelt werden, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis dieser Informationen darlegt. Der Darlegung eines berechtigten Interesses bedarf es indessen nicht zur Übermittlung an öffentliche Stellen sowie zur Übermittlung von Basisinformationen der Landesvermessung, Angaben zur Bezeichnung, Gestalt, Größe, örtlichen Lage und Nutzung der Liegenschaften sowie von Informationen zu öffentlich-rechtlichen Festlegungen.

War mit dem Hinweis auf § 14 Abs. 2 VermG der gordische Knoten durchschlagen? Wir mussten dem Ministerium widersprechen: Dass ein berechtigtes Interesse nach Maßgabe des § 14 Abs. 2 VermG in vielen Fällen nicht mehr dargelegt werden muss, bedeutet nicht, dass es deshalb gänzlich verzichtbar wäre; die übermittelnde Stelle ist lediglich von der Verpflichtung entlastet, in jedem Einzelfall zu prüfen, ob es vorliegt. Weiß sie jedoch, dass der Adressat der Datenübermittlung kein berechtigtes Interesse nachweisen kann, so muss die Übermittlung dennoch unterbleiben. Auf FIONA übertragen bedeutet dies, dass Zugriffe auf personenbezogene Daten nach § 14 Abs. 2 VermG in Fällen der letztgenannten Art verweigert werden müssten. Nun kann die für FIONA verantwortliche Stelle im konkreten Einzelfall zwar schlechterdings nicht wissen, wie es um das berechtigte Interesse des Nutzers bestellt ist; da die Anwendung jedoch einem jeden bei der Landwirtschaftsverwaltung registrierten Antragsteller landwirtschaftlicher Flächenprämien ermöglicht, personenbezogene Daten der amtlichen Liegenschaftskarte über das ganze Landesgebiet hinweg einzusehen und jedes beliebige Grundstück in Baden-Württemberg zu vermessen, ist es offensichtlich, dass die dem Nutzer eingeräumten Zugriffsmöglichkeiten tatsäch-

lich jeweils nur zu einem geringen Bruchteil von einem berechtigten Interesse abgedeckt sein können. FIONA gestattet also Abrufe personenbezogener Daten, die auch unter den „entschärften“ Voraussetzungen des § 14 Abs. 2 VermG nicht gerechtfertigt sein dürften.

Auch andere Überlegungen des Ministeriums vermochten uns letztlich nicht zu überzeugen. Um es kurz zu machen: Eine Rechtsgrundlage, welche die Übermittlung der insbesondere aus der GIS-Komponente resultierenden personenbezogenen Daten zweifelsfrei gestatten würde, ist im Ergebnis nicht zu erkennen.

Damit ist aus datenschutzrechtlicher Sicht eigentlich der Stab über das Verfahren gebrochen. Ich will mich jedoch der Einsicht nicht verschließen, dass FIONA den Anwendern die nicht ganz unkomplizierte Beantragung landwirtschaftlicher Flächenprämien tatsächlich erheblich erleichtern kann. Was die Möglichkeit betrifft, dass dritte Nutzer durch Addition der einzelnen Grundstücke die ungefähre Höhe der dem Betroffenen zustehenden Fördermittel berechnen können, ist zudem zu bedenken, dass seit 2008 aufgrund europa- und bundesgesetzlicher Vorgaben Name und Wohnort der Empfänger von Beihilfen aus den großen europäischen Agrartöpfen „Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums“ (ELER) und „Europäischer Garantiefonds für Landwirtschaft“ (EGFL), deren Auszahlung über den Gemeinsamen Antrag abgewickelt wird, nebst der Gesamthöhe der jeweils bezogenen Mittel sogar frei zugänglich im Internet zu veröffentlichen sind.

Aus diesen Erwägungen wurde dem Ministerium für Ernährung und Ländlichen Raum mitgeteilt, dass unter Zurückstellung erheblicher datenschutzrechtlicher Bedenken davon abgesehen werde, die Anwendung FIONA wegen ihrer GIS-Komponente zu beanstanden. Hinsichtlich des technischen Datenschutzes waren noch mehrere Probleme vorhanden, wobei ich hier nur die drängendsten wiedergeben will:

Das Landesdatenschutzgesetz fordert, dass bei der Verarbeitung personenbezogener Daten die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Dies wird zumeist durch ein Zugriffsrechtesystem der betreffenden Anwendung gewährleistet, in dem ein Administrator festlegt, welcher Benutzer auf welche Daten zugreifen kann. Wie ein Zugriffsrechtesystem auf strukturierte Daten realisiert wird, ist seit längerem bekannt und in Datenbankmanagementsystemen, die häufig die Basis von Anwendungssystemen bilden, standardmäßig vorgesehen.

Bei geografischen Informationssystemen gestaltet sich die Realisierung eines Zugriffsschutzes jedoch schwieriger, weil Flurstücke durch eine beliebige Anzahl von Linien- und/oder Flächensegmenten dargestellt werden. Eine einheitliche Struktur ist nicht gegeben. Den Zugriff auf eine gewisse Anzahl von Flurstücken an Hand der Anzahl der Liniensegmente zu steuern, ist offensichtlich nicht zielführend. Genau das war eines der Probleme, auf das meine Mitarbeiter bei der Kontrolle von FIONA gestoßen sind. Hier kann jeder Benutzer auf alle Flurstücke und deren Flurstücksnummer in Baden-Württemberg zugreifen. Diese weitgehenden Zugriffsrechte wurden von mir in Frage gestellt. Immerhin ist die Wahrscheinlichkeit, dass z. B. ein landwirtschaftlicher Betrieb aus Schwetzingen Flurstücke bewirtschaftet, die in Isny liegen, äußerst gering. Weitere Probleme ergeben sich aus dem Wechsel der bewirtschafteten Grundstücke und deren Aufteilung. Zudem können die Benutzer die in das Flurstücksverzeichnis eingetragenen Daten per Download lokal speichern, also quasi ein „privates Katasteramt“ aufbauen. Dem Abgleich mit anderen geografischen Daten wären dadurch Tür und Tor geöffnet.

Meine Dienststelle hat folgende Empfehlungen gegeben und gebeten, deren Umsetzung (einzeln oder in Kombination) zu prüfen:

– Räumliche Eingrenzung

  Zu prüfen wäre zunächst, ob eine räumliche Eingrenzung des Zugriffs möglich ist. Ich vermag nicht nachzuvollziehen, warum jeder der möglichen ca. 52 000 Benutzer auf alle Flurstücke zugreifen können muss.

Eine Eingrenzung z. B. auf den Landkreis, in dem der Antragsteller seinen Wohnsitz hat, könnte ein erster Schritt zur Lösung des Problems sein. Ebenso darf der Zugriff nur auf die Flurstücke mit landwirtschaftlicher Nutzung eröffnet werden.

– Freischaltung

Die von einem landwirtschaftlichen Betrieb im letzten Jahr bewirtschafteten Flurstücke werden im Folgejahr automatisch in sein Flurstücksverzeichnis aufgenommen. Mit der automatischen Übernahme sollten diese Flurstücke für den Zugriff durch weitere Benutzer gesperrt werden.

– Anmeldung

Eine weitere Möglichkeit, den Zugriff nur auf die für die Antragstellung relevanten Flurstücke zu begrenzen, könnte darin bestehen, dass alle Flurstücke als „frei“ gekennzeichnet werden und der Antragsteller den alleinigen Zugriff auf ein Flurstück anmelden muss. Dadurch würde das Flurstück für andere Benutzer gesperrt.

– Protokollierung

Wenn schon nicht eingeschränkt werden kann, wer auf die Daten welcher Flurstücke zugreifen kann, dann sollte der Zugriff zumindest protokolliert werden. Auch die Protokollierung des Downloads wäre zu prüfen.

Bei der Kontrolle hat sich gezeigt, dass das Ministerium meinen Forderungen zwar nicht ablehnend gegenübersteht. Es sieht sich jedoch durch die Vorgaben der EU teilweise an einer Berücksichtigung gehindert. Die freizügige Informationspolitik der EU darf meines Erachtens aber nicht zur Folge haben, dass die hier beschriebene Verarbeitung personenbezogener Daten als zu vernachlässigender Eingriff in das Recht auf informationelle Selbstbestimmung abgetan wird.

Das Ministerium für Ernährung und Ländlichen Raum ist gefordert, für die Probleme des Zugriffschutzes auf personenbezogene geografische Daten bei FIONA eine technisch-organisatorisch befriedigende Lösung zu finden. Erfreulicherweise hat der auch für den Verbraucherschutz zuständige Landwirtschaftminister immer wieder betont, wie wichtig ihm der Datenschutz ist. Mein Anliegen ist also in guten Händen.

2. Agrarbeihilfen im Internet oder Landwirte am Subventionspranger?

Wer Beihilfen aus den europäischen Agrartöpfen EGFL und ELER bezieht, muss bis auf Weiteres akzeptieren, dass sein Name, sein Wohnort und die Höhe der empfangenen Mittel im Internet veröffentlicht werden. Die eindeutige, gemeinschaftsrechtlich vorgegebene Rechtslage lässt derzeit keine andere datenschutzrechtliche Bewertung zu.

Wie auf vielen anderen Rechtsgebieten, so ist auch im Datenschutzrecht zunehmend mit wichtigen gemeinschaftsrechtlichen Entwicklungen auf europäischer Ebene zu rechnen, die dem informationellen Selbstbestimmungsrecht des Bürgers nicht immer denselben Rang einräumen, den es innerhalb der deutschen Rechtsordnung genießt. Diese leidvolle Erfahrung machten die baden-württembergischen Landwirte, als sie Ende 2008 unverhofft Post vom Ministerium für Ernährung und Ländlichen Raum erhielten. In wohlgesetzten Worten eröffnete das Ministerium den Betroffenen, dass aufgrund gemeinschaftsrechtlicher Vorgaben ab Dezember 2008 bzw. ab April 2009 detaillierte personenbezogene Angaben über die Empfänger von Beihilfen aus den beiden großen europäischen Agrartöpfen ELER (Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums) und EGFL (Europäischer Garantiefonds für Landwirtschaft) unter der Internet-Adresse *www.agrar-fischerei-zahlungen.de* im Internet zu veröffentlichen seien.

Das Ministerium hatte die Betroffenen richtig informiert. Die im Detail recht komplexe, letztlich gemeinschaftsrechtlich vorgegebene Rechtslage sei an dieser Stelle nur kurz skizziert: Im Rahmen der sog. europäischen Transpa-

renzinitiative, mit der die Europäische Union politische Entscheidungsprozesse in der Union für den Bürger nachvollziehbarer gestalten möchte, ist in die grundlegende Verordnung (EG) Nr. 1290/2005 des Rates vom 21. Juni 2005 über die Finanzierung der Gemeinsamen Agrarpolitik durch eine Verordnung (EG) Nr. 1437/2007 im Jahr 2007 ein neuer Artikel 44 a eingefügt worden, welcher die Mitgliedstaaten der Europäischen Gemeinschaft verpflichtet, jedes Jahr nachträglich Informationen über die Empfänger von Mitteln aus den besagten beiden Landwirtschaftsfonds sowie über die Beträge, die jeder Begünstigte aus diesen Fonds erhalten hat, zu veröffentlichen. Eine weitere gemeinschaftsrechtliche Verordnung (EG) Nr. 259/2008 der Kommission vom 18. März 2008 hat diese Vorgaben dahingehend konkretisiert, dass die Veröffentlichung unter Angabe des Namens und des Wohnortes des Empfängers ausschließlich im Internet zu erfolgen hat. Der Bundesgesetzgeber hat ein Übriges getan und zwecks Durchführung des skizzierten EU-Rechts ein „Agrar- und Fischereifonds-Informationen-Gesetz“ (AFIG) sowie ergänzend eine „Agrar- und Fischereifonds-Informationen-Verordnung“ (AFIVO) erlassen, wobei sich diese letztgenannten bundesrechtlichen Normen allerdings strikt an den gemeinschaftsrechtlichen Vorgaben orientieren und insofern für die Betroffenen keine zusätzlichen Belastungen bedeuten.

Begreiflicherweise haben sich mehrere betroffene Landwirte, die wenig Verständnis dafür hatten, gleichsam an den „Subventionspranger“ gestellt zu werden, an meine Dienststelle gewandt und mich gebeten, gegen die Internet-Veröffentlichung ihrer Daten einzuschreiten. Leider musste ich den Beschwerdeführern jedoch mitteilen, dass mir letztlich die Hände gebunden sind, denn die Europäische Union und in deren Gefolge der Bundesgesetzgeber haben klare, wenn auch nicht unbedingt datenschutzfreundliche Fakten geschaffen. Gemäß § 4 Abs. 1 LDSG ist die Verarbeitung personenbezogener Daten ohne Einwilligung des Betroffenen zwar nur zulässig, wenn das Landesdatenschutzgesetz selbst oder eine andere Rechtsvorschrift sie erlaubt. Ist jedoch eine solche Rechtsgrundlage vorhanden (deren Verfassungskonformität hier unterstellt wird), lässt sich umgekehrt selbst gegen einen einschneidenden Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen, wie ihn die personenbezogene Veröffentlichung der empfangenen Agrarbeihilfen im Internet sicherlich darstellt, grundsätzlich nicht mehr ins Feld führen, er sei mit dem Datenschutzrecht nicht vereinbar.

Stattdessen musste ich mich – wie schon das Ministerium selbst – darauf beschränken, die Betroffenen auf ihr Recht hinzuweisen, gegen die an sich rechtmäßige Verarbeitung ihrer Daten gegebenenfalls ein schutzwürdiges, in ihrer persönlichen Situation begründetes Interesse einzuwenden. Ein solches individuelles Einwendungsrecht führt freilich nur zum Erfolg, wenn eine Abwägung ergibt, dass das öffentliche Interesse an der Datenverarbeitung nicht überwiegt.

Im Übrigen waren sowohl in Baden-Württemberg als auch in anderen Bundesländern bereits mehrere Gerichte mit der Frage der Rechtmäßigkeit der Veröffentlichungen befasst. Während das Verwaltungsgericht Wiesbaden in zwei vielbeachteten Vorabentscheidungsersuchen an den Gerichtshof der Europäischen Gemeinschaften dezidierte Zweifel daran geäußert hat, ob das einschlägige EG-Verordnungsrecht mit dem höherrangigen primären Gemeinschaftsrecht und der europäischen Datenschutzrichtlinie vereinbar ist, mochten ihm die meisten anderen mit der Veröffentlichung der „Agrarsubventionen“ befassten Gerichte, darunter auch der Verwaltungsgerichtshof Baden-Württemberg, in dieser Einschätzung bislang nicht folgen. Vielmehr zeichnet sich als „herrschende Meinung“ der deutschen Gerichtsbarkeit die Auffassung ab, dass das gemeinschaftsrechtliche Anliegen, eine größere Transparenz in Bezug auf die Verwendung der Haushaltsmittel und eine wirtschaftlichere Haushaltsführung zu gewährleisten, legitim und die Veröffentlichung der Informationen ein geeignetes und verhältnismäßiges Mittel sei, um dieses Ziel zu erreichen.

Damit dürfte einstweilen das „vorletzte“ Wort in der Sache gesprochen sein – bis zu einer etwaigen anderweitigen Entscheidung des Gerichtshofs der Europäischen Gemeinschaften.

Die Entscheidung des Gerichtshofs der Europäischen Gemeinschaften über die Vorabentscheidungsersuchen des Verwaltungsgerichts Wiesbaden

bleibt abzuwarten. Unbenommen bleibt es den Empfängern von Mitteln aus den Agrarfonds EGFL und ELER, gegen die Veröffentlichung ihrer Daten ein schutzwürdiges, in ihrer persönlichen Situation begründetes Interesse einzuwenden. Eine solche Einwendung wird allerdings nur im Einzelfall zum Erfolg führen können.

3. Veröffentlichung der Solareignung von Gebäudedächern im Internet

Dürfen Daten über die Eignung von Gebäuden für Photovoltaik- und Solar-Thermie-Anlagen im kommunalen Internet-Auftritt veröffentlicht werden?

Die Förderung regenerativer Energien gehört mittlerweile zum Standardprogramm auf allen politischen Ebenen. Doch auch dabei kann es datenschutzrechtliche Fallstricke geben. So wandte sich eine Stadt mit folgendem Anliegen im Jahr 2008 an meine Dienststelle: Sie plane auf der Grundlage eines Forschungsprojekts einer niedersächsischen Fachhochschule die Eignung aller Gebäudedächer, Anlagen und Freiflächen ihres Stadtgebiets für Photovoltaik- und Solar-Thermie-Anlagen errechnen zu lassen, um die gewonnenen Daten über das Energiepotenzial dieser Objekte mitsamt Angaben zur gegebenenfalls erforderlichen Investitionssumme alsdann im Rahmen ihres Internet-Auftritts gebäudescharf auf Karten und Luftbildaufnahmen zu veröffentlichen. Als Vorbild sollte ein bereits realisiertes ähnliches Projekt der Stadt Osnabrück dienen. Freilich gab es innerhalb der Stadtverwaltung unterschiedliche Auffassungen darüber, ob dem Vorhaben datenschutzrechtliche Bestimmungen entgegenstünden.

Tatsächlich gab es datenschutzrechtliche Bedenken: Denn bei dem Solarpotenzial von Gebäuden, die im Eigentum natürlicher Personen stehen, handelt es sich um Angaben über deren sachliche Verhältnisse, mithin um personenbezogene Daten im Sinne des Landesdatenschutzgesetzes. Die Veröffentlichung dieser Daten im Internet bedeutet aus datenschutzrechtlicher Sicht eine massenweise Übermittlung außerhalb des öffentlichen Bereichs im Sinne des § 18 LDSG, für die weder das Landesdatenschutzgesetz selbst noch die baden-württembergische Gemeindeordnung eine hinreichende Rechtsgrundlage bieten.

Die weitere Diskussion, in die mein Vorgänger wegen der bald absehbaren überörtlichen Relevanz des Vorgangs auch das Umweltministerium sowie die Landesanstalt für Umwelt, Messungen und Naturschutz (LUBW) einband, fokussierte sich auf das Landesumweltinformationsgesetz (LUIG). Dieses Landesgesetz bzw. das Umweltinformationsgesetz des Bundes (UIG), auf welches das Landesumweltinformationsgesetz in weiten Teilen verweist, gibt den nach Maßgabe des § 2 Abs. 1 LUIG informationspflichtigen Stellen in der Tat auf, die Öffentlichkeit auch unter Nutzung des Internets in angemessenem Umfang aktiv und systematisch über die Umwelt zu informieren. Soweit dabei allerdings personenbezogene Daten offenbart und dadurch Interessen der Betroffenen erheblich beeinträchtigt werden, muss – wie sich aus § 10 Abs. 6 in Verbindung mit § 9 Abs. 1 UIG und § 3 Abs. 1 LUIG ergibt – die Veröffentlichung unterbleiben, es sei denn, die Betroffenen hätten zugestimmt oder das öffentliche Interesse an der Bekanntgabe würde überwiegen.

Dass es sich bei der Information über das Solarenergie-Potenzial eines Gebäudedachs um eine einschlägige Umweltinformation handelt, ist sicher nachvollziehbar. Hingegen erschien uns durchaus zweifelhaft, ob auch die übrigen Voraussetzungen für eine aktive Verbreitung dieser Daten via Internet erfüllt sind. Sind die Interessen der Betroffenen denn nicht erheblich beeinträchtigt, wenn sie von wohlmeinenden Nachbarn zu ökologisch korrektem Verhalten angehalten, mit womöglich unwillkommenem Werbematerial einschlägiger Hersteller überflutet und eventuell auch mit offensiveren Verkaufsstrategien konfrontiert werden? Aus datenschutzrechtlicher Sicht zögert man, diese Fragen zu Ungunsten der Betroffenen zu beantworten. Überdies sieht § 9 Abs. 1 Satz 3 UIG eigentlich vor, dass die Betroffenen vor der Entscheidung über die Offenbarung ihrer personenbezogenen Informationen anzuhören sind.

Dennoch wollten wir uns dem Projekt nach dem Modell der Stadt Osnabrück, an dem außer der Stadt, die sich an uns gewandt hatte, zahlreiche

weitere Kommunen in Baden-Württemberg Interesse zeigten, nicht grundsätzlich in den Weg stellen. Mein Vorgänger erklärte sich deshalb letztlich bereit, datenschutzrechtliche Bedenken zurückzustellen, wenn die betroffenen Grundstückseigentümer zumindest Gelegenheit erhalten, gegen die Veröffentlichung des Solarpotenzials „ihres“ Gebäudedachs auf unbürokratischem Wege Widerspruch einzulegen. Auf diese Widerspruchsmöglichkeit müsse selbstverständlich in angemessener Weise hingewiesen werden, namentlich in den entsprechenden gemeindlichen Publikationsorganen (z. B. Amtsblätter) und in Tageszeitungen, bei der Werbung für das Vorhaben sowie nicht zuletzt an prominenter Stelle im Internet-Auftritt der Gemeinde selbst. Unter dieser Bedingung gaben wir der Stadt schließlich „grünes Licht“.

Unter Zurückstellung von Bedenken kann die Veröffentlichung des Solarpotenzials von Gebäuden im Internet-Auftritt der Gemeinde akzeptiert werden, wenn den betroffenen privaten Grundstückseigentümern ein Widerspruchsrecht eingeräumt wird. Auf dieses ist von der Kommune in geeigneter Weise hinzuweisen.

4. Nicht jede „Amtshilfe“ ist datenschutzrechtlich zulässig

Häufig werden personenbezogene Daten zwischen öffentlichen Stellen unter vermeintlichen Amtshilfegesichtspunkten ausgetauscht, ohne dass hierfür eine tragfähige Rechtsgrundlage besteht.

Es gibt bekanntlich Zeitgenossen, die es den Kommunalverwaltungen aus den verschiedensten Gründen nicht immer leicht machen. Manche Mitbürger profilieren sich als kritische und meinungsfreudige Beobachter der lokalen Politik, andere als kämpferische und beharrliche Widersacher eines womöglich längst genehmigten Vorhabens. Sind mehrere öffentliche Stellen betroffen, so neigen diese mitunter dazu, sich im Schulterschluss gegen den unbequemen „Kunden“ – gegebenenfalls auf dem „kurzen Dienstweg“ – bereitwillig mit Informationen auszuhelfen. Doch auch ein kritischer Bürger hat ein Recht auf informationelle Selbstbestimmung und darf erwarten, dass seine persönlichen Daten nur mit seiner Einwilligung oder auf einer eindeutigen Rechtsgrundlage verarbeitet werden. Dies wird in den Kommunalverwaltungen leider nicht immer beachtet.

Zwei Beispielsfälle aus unserer Praxis mögen dies illustrieren:

– Ein Bürger wandte sich an meine Dienststelle, weil das zuständige Landratsamt, bei dem er sich nach der Reichweite der Betriebsgenehmigung eines Unternehmens in seiner Nachbarschaft erkundigt hatte, seine Wohngemeinde gegen seinen erklärten Willen nachrichtlich an dem mit ihm geführten elektronischen Schriftwechsel beteiligt hatte. Von uns um eine Stellungnahme gebeten, legte mir das Landratsamt sinngemäß dar, dass der Petent sich bereits in dem immissionsschutzrechtlichen Genehmigungsverfahren, das dem Bau und Betrieb der fraglichen Industrieanlage vorangegangen war, als Vorkämpfer gegen dieses Vorhaben hervorgetan und angedroht habe, eine von ihm angeführte Bürgerinitiative zu reaktivieren. Es sei deshalb damit zu rechnen gewesen, dass die Gemeinde, auf deren Gemarkung die Industrieanlage lag, mit Bürgeranfragen zur Reichweite der Betriebsgenehmigung konfrontiert wird; darauf habe man die Gemeinde vorbereiten wollen.

  Dieses Vorbringen vermochte mich nicht zu überzeugen. Zwar war es denkbar, dass die vom Petenten aufgeworfene Frage auch kommunale Belange berührt. Jedoch hätte das Landratsamt die Gemeinde in dieser Angelegenheit konsultieren können, ohne die Person des Petenten ins Spiel zu bringen – auch wenn es wegen dessen bekannten Engagements weiteres „Ungemach“ wittern mochte. Die Übermittlung der personenbezogenen Information, dass (gerade) der Petent sich an das Landratsamt gewandt hatte, war daher meines Erachtens für die Erfüllung der Aufgaben des Landratsamtes nicht erforderlich und verstieß deshalb gegen das Datenschutzrecht. Ich bat das Landratsamt, meine Rechtsauffassung künftig zu beachten.

– Demgegenüber zeigte sich in einem anderen Fall eine Gemeinde übereifrig: Nach jahrelangen Auseinandersetzungen mit dem Betreiber eines örtlichen Gewerbebetriebs hielt sie es für an der Zeit, beim zuständigen Landratsamt ein Gewerbeuntersagungsverfahren anzuregen. Um den aus ihrer Sicht bestehenden Handlungsbedarf zu veranschaulichen, berichtete sie von wasser-, bau- und naturschutzrechtlichen Verstößen, aber auch von nicht geleisteten Sozialversicherungsbeiträgen, von anhängigen Zwangsvollstreckungsverfahren und von einschlägigen Eintragungen in den Führungszeugnissen zweier leitender Mitarbeiter des betreffenden Gewerbebetriebs.

  Woher hatte die Gemeinde alle diese Informationen? Unsere auf die Eingabe eines der Betroffenen eingeleiteten Nachforschungen ergaben, dass sie viele ihrer Erkenntnisse über die Jahre hinweg tatsächlich im Zuge der Wahrnehmung eigener Aufgaben gewonnen hatte. Hingegen hatte sie die mitgeteilten Auszüge aus dem Bundeszentralregister ebenso wie die Auskünfte des zuständigen Sozialversicherungsträgers sowie eines Gerichtsvollziehers eigens im Hinblick auf die von ihr befürwortete Gewerbeuntersagung erhoben.

  Wir wiesen die Gemeinde darauf hin, dass es Sache des nach der Gewerbeordnung zuständigen Landratsamts gewesen wäre zu entscheiden, welche personenbezogenen Daten für das von der Gemeinde angeregte Gewerbeuntersagungsverfahren benötigt werden. Für die vorauseilende „Amtshilfe“, mit dem die Gemeinde dem Landratsamt meinte vorgreifen zu müssen, sah ich deshalb keine datenschutzrechtliche Rechtsgrundlage.

Auch für die Informationsweitergabe zwischen Behörden gilt die datenschutzrechtliche Grundregel, dass personenbezogene Daten nur mit der Einwilligung des Betroffenen oder aufgrund einer einschlägigen datenschutzrechtlichen Erlaubnisnorm erhoben und übermittelt werden dürfen.

4. Abschnitt: Verkehr

1. Webcams an Bundesautobahnen und Videoüberwachung an Lichtsignalanlagen

Wann haben Daten über das Verkehrsgeschehen, die über eine Webcam oder per Videoüberwachung erhoben werden, einen Personenbezug?

Aktuelle Verkehrsmeldungen sind wichtig und für die meisten Verkehrsteilnehmer hilfreich. Kein Wunder, dass auch die Rundfunkanstalten, die die Autofahrer mit aktuellen Meldungen versorgen, am liebsten in „Echtzeit“ über das reale Verkehrsgeschehen „im Bilde“ sein wollen. Das Innenministerium wollte hierfür einen besonderen Service bieten und nahm das Projekt „Erfassung der Verkehrslage an relevanten Straßenabschnitten in Baden-Württemberg mittels Webcams“ in Angriff. Erfreulicherweise wurden wir von Beginn an beteiligt. Bei dem Vorhaben sollten aktuelle Bilder vom Verkehrszustand auf bestimmten Autobahnabschnitten ins Internet übertragen werden. Das Innenministerium hielt dies für datenschutzrechtlich nicht sonderlich relevant, da hierbei keine personenbezogenen Daten verarbeitet würden, denn aufgrund der eingeschränkten Bildauflösung und der entsprechenden Aufstellung der Webcams sei eine Identifizierung individueller Personen nicht möglich. Diese Einschätzung konnten wir zunächst nicht teilen, da auf einem übersandten Beispielbild – allerdings aus Rheinland-Pfalz – das amtliche Kennzeichen eines erfassten Fahrzeugs zu erkennen war. Ein mittelbarer Personenbezug konnte unseres Erachtens im Einzelfall auch durch individuelle Schriftzüge auf Lastkraftwagen hergestellt werden. Ich empfahl daher dem Innenministerium, sich vor einer Umsetzung der Gesamtkonzeption inhaltlich näher mit den datenschutzrechtlichen Aspekten zu befassen.

Später war einer Pressemitteilung zu entnehmen, dass in einer ersten Ausbaustufe 14 Webcams an sechs Standorten entlang der Autobahnen A 8 und A 81 aktuelle Bilder von der Strecke ins Internet übertragen und die Bilder von jedermann im Internet auf den Seiten der Straßenverkehrszentrale

Baden-Württemberg eingesehen werden können *(www.svz-bw.de)*. Dass wir daraufhin nochmals nachfassten, war selbstverständlich. Die pauschale Feststellung des Innenministeriums, aufgrund der eingeschränkten Bildauflösung und der Positionierung der Webcams sei eine Identifizierung individueller Personen generell nicht möglich, konnten wir – ungeachtet des unstreitig wichtigen Ziels aktueller Berichterstattung über das Verkehrsgeschehen – nicht ohne Weiteres teilen.

Einen Personenbezug haben Daten, die ihre Bezugsperson selbst ausweisen. Hierunter fallen Angaben, die üblicherweise zur Identifizierung einer Person benutzt werden, wie Name, Anschrift oder Geburtstag. Ein Personenbezug kann jedoch auch dann bestehen, wenn der jeweilige Betroffene durch zusätzliche Informationen identifiziert werden kann. Somit können auch anonymisierte, pseudonymisierte oder aggregierte Daten, sofern ihr ursprünglicher Personenbezug nicht unwiederbringlich „verloren“ ist, durchaus Gegenstand des informationellen Selbstbestimmungsrechts sein.

Wenn beispielsweise auf einem Bild, das eine an einer Autobahn aufgestellte Webcam aufgenommen hat, das Kennzeichen eines Fahrzeuges erkennbar ist, werden personenbezogene Daten verarbeitet. Aus Sicht des Datenschutzes kommt im vorliegenden Fall erschwerend hinzu, dass die durch die Webcams aufgenommenen Bilder in das Internet eingestellt werden und damit grundsätzlich weltweit ohne jegliche Einschränkungen zur Verfügung stehen. Auch deshalb sind an die Verarbeitung von personenbezogenen Daten im Internet stets besonders hohe datenschutzrechtliche Anforderungen zu stellen. Soweit die auf Veranlassung des Innenministeriums bzw. der Straßenbauverwaltung montierten Webcams Bilder mit Kfz-Kennzeichen oder anderen individuellen Merkmalen mit Bezug zu einer Personen liefern, ist hierfür eine Rechtsgrundlage nicht ersichtlich. Ich bat das Innenministerium daher, Maßnahmen zu prüfen und zu realisieren, die einen Personenbezug der Bilddaten zuverlässig ausschließen. In Betracht kommt hierbei beispielsweise, dass durch eine rechnerische Reduktion der Auflösung der Bilddaten die Erkennbarkeit von optischen Merkmalen erschwert wird, ohne dass die Aussagekraft der Bilder hinsichtlich des Verkehrsaufkommens eingeschränkt wird. Auch könnte gegebenenfalls durch eine Grauwertbilddarstellung die Erkennbarkeit von Fahrzeugen gegenüber einer Farbbilddarstellung reduziert werden. Das Innenministerium hat die Anregungen mittlerweile zurückgewiesen: Eine Reduzierung der Auflösung oder eine Grauwertbilddarstellung würden dazu führen, dass das Informationsgebot für die Verkehrsteilnehmer „nicht mehr attraktiv“ wäre; die erheblichen Investitionen in das System wären dann nicht mehr zu rechtfertigen.

Vor kurzem habe ich einer weiteren Pressemitteilung entnommen, dass in einer zweiten Ausbaustufe 67 zusätzliche Webcams bis Frühjahr 2010 an Autobahnen in Baden-Württemberg installiert werden sollen. In einer dritten Ausbaustufe sollen im Laufe des Jahres 2010 nochmals 32 Webcams in Betrieb gehen. Es bleibt zu hoffen, dass bei diesem Massenauftritt von Webcams an den Autobahnen der Datenschutz nicht „unter die Räder“ gerät. Der Hinweis auf einen drohenden „Attraktivitätsverlust“ kann sicher nicht das letzte Wort sein. Die „Attraktivität“ für Medien und Verkehrsteilnehmer ist kein geeigneter datenschutzrechtlicher Maßstab. Die rasante technische Entwicklung lässt erwarten, dass in einigen Jahren auch gestochen scharfe Bewegtbilder von Webcams problemlos übertragen werden können, die sicher für den Betrachter noch „attraktiver“ wären. Dass es auch anders geht, zeigt in diesem Zusammenhang das ansonsten eher zweifelhafte „Vorbild“ der Firma Google, die in ihrem neuen Dienst „Google Street View“ (vgl. 6. Teil, 2. Abschnitt, Nr. 3) für eine technische Unkenntlichmachung von Autokennzeichen sorgen will. Wir werden die weitere Entwicklung im wahrsten Sinne des Wortes jedenfalls aufmerksam beobachten.

Ein anderes Einsatzgebiet der Videotechnik im Verkehr ist die Videoüberwachung an Lichtsignalanlagen. Hier dient die Videotechnik der Verkehrssteuerung an Kreuzungen und bei mobilen Ampelanlagen in Baustellenbereichen. Starr ausgerichtete, brennweitenfixierte Videodetektoren erfassen dabei das Verkehrsaufkommen in Einzelbildaufnahmen und steuern nach Verarbeitung der Bilddaten die Ampeln entsprechend. Zwar kann auch bei den so gewonnenen Ablichtungen nicht völlig ausgeschlossen werden, dass

unter bestimmten Umständen ein Personenbezug hergestellt werden kann. Selbst bei der derzeitigen Auflösung der Videodetektoren könnte beispielsweise ein besonders seltenes Fahrzeug optisch erkannt und seinem Eigentümer, der häufig auch der Fahrer ist, zugeordnet werden. Ebenso könnten gegebenenfalls einzelne Fahrzeuge anhand angebrachter Schriftzüge erkannt werden. Bei Würdigung der Gesamtumstände konnten diese Bedenken jedoch vor allem deshalb zurückgestellt werden, weil die Bilddaten lediglich während der Verarbeitung zum Zweck der Detektion von Fahrzeugumrissen und der Anzahl der auf den Fahrspuren stehenden Kraftfahrzeuge im Arbeitsspeicher des Videodetektors gespeichert und danach umgehend gelöscht werden. Es handelt sich insofern um eine Verarbeitung in einem geschlossenen technischen System, bei der Personen keine Kenntnis der Bilddaten oder der Verarbeitungsergebnisse erlangen. Damit ist die Interpretation eines Personenbezugs aus den Bilddaten nicht möglich und mithin die Verarbeitung zulässig.

Von den Behörden und öffentlichen Stellen in Baden-Württemberg ist bei der Verarbeitung von Daten stets sorgfältig zu prüfen, ob diese einen Personenbezug haben und gegebenenfalls welche datenschutzrechtlichen Vorschriften dabei zu beachten sind. An die Veröffentlichung von personenbezogenen Daten im Internet sind wegen der weltweiten Verfügbarkeit und der bestehenden Verknüpfungsmöglichkeiten besonders hohe datenschutzrechtliche Anforderungen bei der Konzeption und Umsetzung zu stellen.

2. Zuverlässigkeitsüberprüfung für Fahrlehrbewerber

Darf die für die Fahrlehrerlaubnis zuständige Behörde hinsichtlich Fahrlehrbewerbern regelmäßig die Polizei fragen?

Fahrlehrer üben einen verantwortungsvollen Beruf aus. Vielleicht hing es damit zusammen, dass einige Behörden offenbar regelmäßig Erkundigungen bei der Polizei über die Zuverlässigkeit von Bewerbern für die Fahrlehrerlaubnis eingeholt haben. Als wir davon erfuhren, gingen wir der Sache nach. Wie sich herausstellte, erkundigten sich einige Behörden in jedem Fall bei der Polizei, und zwar unabhängig von Hinweisen auf eine Unzuverlässigkeit. Ein Landratsamt berief sich u. a. darauf, dass es von laufenden Ermittlungsverfahren, deren Sachverhalt unter Umständen gegen die Erteilung einer Fahrlehrerlaubnis sprechen würde, nur über eine Anfrage bei der Polizei erfahren könne.

Datenschutzrechtlich stellt sich die Angelegenheit wie folgt dar:

– Um personenbezogene Daten verarbeiten zu dürfen, wozu auch das Beschaffen und Nutzen solcher Daten zählt, bedarf es entweder einer normenklaren Rechtsvorschrift oder einer Einwilligung des Betroffenen (vgl. § 4 Abs. 1 LDSG).

  Zwar hat die zuständige Behörde die Zuverlässigkeit bzw. Unzuverlässigkeit des Antragstellers zu würdigen. Zu den Voraussetzungen der Fahrlehrerlaubnis gehört unter anderem, dass der Bewerber geistig, körperlich und fachlich geeignet ist und keine Tatsachen vorliegen, die ihn für den Fahrlehrerberuf als unzuverlässig erscheinen lassen (vgl. § 2 Abs. 1 Satz 1 Nr. 2 Fahrlehrergesetz – FahrlG –). Das Fahrlehrergesetz nennt aber als Unterlagen, welche für die Zuverlässigkeit bzw. Unzuverlässigkeit von Bedeutung sind, lediglich das Führungszeugnis nach dem Bundeszentralregistergesetz, das der Betroffene jedoch selbst zu beantragen hat (vgl. § 3 Satz 4 FahrlG).

– Auch bei einer Erteilung der Fahrerlaubnis für Pkw und Krafträder (A und B) führt die Fahrerlaubnisbehörde regelmäßig keine Ermittlungen zur Eignungsfrage im Sinne polizeirechtlicher Zuverlässigkeitskriterien durch. Bei diesen Klassen kommt gemäß § 11 Abs. 2 der Fahrerlaubnisverordnung nur eine anlassbezogene Eignungsprüfung in Frage, wenn aufgrund bekannt gewordener Tatsachen Zweifel begründet sind.

Meines Erachtens müssen die entscheidungserheblichen Tatsachen der entscheidenden Behörde selbst und nicht etwa irgendwelchen anderen Stellen vorliegen.

Eine vom Innenministerium Baden-Württemberg durchgeführte Behördenumfrage ergab, dass nur einige wenige Erlaubnisbehörden im Land generell bei der Polizei anfragen. Die aus dieser polizeilichen Auskunft gewonnenen Erkenntnisse waren wiederum so selten Grundlage für die Versagung der Fahrlehrerlaubnis, dass für eine generelle Anfrage bei der Polizei bei Fahrerlaubnisbewerbern die tatsächliche und rechtliche Grundlage fehlt.

Die Erlaubnisbehörde darf bei einem Antrag auf Erteilung der Fahrlehrerlaubnis nicht generell, sondern nur aus besonderem Anlass eine Anfrage nach der Zuverlässigkeit des Antragstellers an die Polizei richten.

3. Datenschutz hat grundsätzlich Vorrang im Verwaltungsverfahren

Ein (erwachsener) Bürger beschwerte sich zu Recht, dass seine personenbezogenen Daten von einem Kassen- und Steueramt ohne seine Einwilligung an seine Mutter übermittelt wurden.

Ein Einwohner eines Stadtkreises wandte sich mit folgendem Anliegen an meine Dienststelle: Ein Kassen- und Steueramt habe von ihm personenbezogene Daten wie Anschrift, Geburtsdatum, Aktenzeichen und Höhe von diversen Bußgeld- und Kostenbescheiden ohne seine Einwilligung an Dritte weitergegeben. Im Verlauf der Ermittlungen stellte sich heraus, dass es sich bei dem Datenempfänger um die Mutter des (erwachsenen) Petenten handelte. Das Kassen- und Steueramt hatte ihr eine umfassende Rückstandsdarstellung über offene Forderungen aus Bußgeldverfahren gegen ihren Sohn zukommen lassen.

Die von mir hierzu angehörte Stadt begründete die Weitergabe der personenbezogenen Daten des Petenten u. a. damit, dass die Mutter teilweise Kenntnis von den Rückständen gehabt habe und auch bereit gewesen sei, ausstehende Forderungen zu begleichen. Zudem sei sie davon ausgegangen, dass die Mutter mit Erlaubnis des Betroffenen gehandelt habe, da sie die Aktenzeichen der Vorgänge gekannt habe. Deshalb sei man auch von einer Ermächtigung der Mutter zu weiteren Vereinbarungen ausgegangen und habe ihr im weiteren Verlauf neue Vorgänge ihren Sohn betreffend offenbart, von denen sie bislang keine Kenntnis gehabt habe. Zudem liege das Begleichen der Forderungen im Interesse des Betroffenen.

So „pragmatisch“ wie hier die Stadt vorging, geht es natürlich nicht. Es ist nämlich u. a. Folgendes zu beachten:

Bei den weitergegebenen Daten des Sohnes handelt es sich um seine personenbezogenen Daten. Seine Mutter ist eine dritte Person im Sinne des Landesdatenschutzgesetzes. Das verwandtschaftliche Verhältnis ist hier nicht von Bedeutung. Eine Übermittlung personenbezogener Daten ist datenschutzrechtlich zulässig, wenn der Sohn als Betroffener hierin eingewilligt hat oder das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift die Datenübermittlung erlaubt.

Zur Einwilligung:

Eine wirksame Einwilligung des Betroffenen zur Datenverarbeitung setzt voraus, dass dieser vorab über die beabsichtigte Datenverarbeitung und deren Zweck aufgeklärt wird. Das informationelle Selbstbestimmungsrecht erfordert, dass der Betroffene mehr als nur die bloße Kenntnis der Datenverarbeitung hat, er muss auch tatsächlich die Möglichkeit haben, selbst darüber zu befinden. Grundsätzlich ist bei einer Einwilligung die Schriftform erforderlich. Auch ist die Einwilligung höchstpersönlich abzugeben. Die Abgabe der Einwilligung durch einen Bevollmächtigten scheidet daher aus. Zudem erfüllen mutmaßliche, stillschweigende oder auch konkludente Erklärungen nicht die Anforderungen des Landesdatenschutzgesetzes an eine Einwilligung des Betroffenen zur Datenverarbeitung. Darüber hinaus ist eine Erklärung, die nicht diesen Anforderungen entspricht, nichtig. Im vorliegenden Fall ersetzten die bloße Kenntnis der Mutter von personenbezogenen Daten ihres Sohnes und deren Absicht, offene Forderungen zu begleichen, aus Sicht des Datenschutzes die erforderliche, höchstpersönliche Einwilligung

des Petenten zur Weitergabe seiner personenbezogenen Daten nicht. Zumal die Möglichkeit, dass die Mutter auch ohne den Willen des Petenten von den Daten Kenntnis erlangt haben könnte, nicht der allgemeinen Lebenserfahrung widerspricht. Die Argumentation der Stadt, dass die bloße Kenntnis von personenbezogenen Daten einer Ermächtigung zu weiteren Handlungen gleichkomme, überzeugt ebenfalls nicht. Wenn die Sachkenntnis der Mutter des Petenten für eine „konkludente“ Erklärung ausreichen würde, könnten viele Personen, die Betroffenen nahe stehen, Entsprechendes für sich geltend machen, da solche Daten diesem Personenkreis durchaus bekannt sein können, ohne dass der Betroffene damit eine (aus datenschutzrechtlicher Sicht erforderliche) Einwilligung verbunden hat.

Zur Rechtsvorschrift:

Das Landesdatenschutzgesetz berücksichtigt zwar durchaus das Eigeninteresse des Betroffenen an der Datenverarbeitung. Wenn keine Einwilligung vorliegt und die Datenverarbeitung offensichtlich im Interesse des Betroffenen ist, könnte sie zulässig sein. Es darf hierbei jedoch kein Grund zur Annahme bestehen, dass der Betroffene seine Einwilligung zur Verarbeitung seiner Daten verweigern würde. Doch gerade dies war ja hier nicht der Fall. So konnte beispielsweise nicht ausgeschlossen werden, dass der Petent schlichtweg nicht wollte, dass seine Mutter Kenntnis davon erlangt, wie viele offene Forderungen in welcher Höhe die Stadt ihm gegenüber hat. Selbst wenn man annimmt, dass sowohl die Stadt als auch die Mutter für den Betroffenen etwas Gutes tun wollten, reicht diese Intention – so lobenswert sie auch sein mag – nicht aus, um das im Grundgesetz verankerte informationelle Selbstbestimmungsrecht des Petenten einzuschränken. Auch ist zu beachten, dass der Verzicht auf eine Einwilligung ausnahmsweise und nur in bestimmten Einzelfällen in Betracht kommt, in denen der Betroffene nur unter sehr erschwerten Bedingungen um seine persönliche Entscheidung gebeten werden kann (wie beispielsweise eine lange, schwere Krankheit oder ein langer Aufenthalt im Ausland). Da diese Regelung einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen darstellt, ist ein restriktiver Beurteilungsmaßstab anzulegen. Im vorliegenden Fall war jedoch nicht ersichtlich, weshalb der Petent nicht um Einwilligung in die Datenverarbeitung gebeten werden konnte. Er hätte schlichtweg gefragt werden können, ob es in seinem Interesse ist, wenn die Stadt mit seiner Mutter eine Absprache zur Schuldentilgung trifft und ihr hierfür die notwendigen Angaben übermittelt.

Nachdem wir der Stadt unsere Rechtsauffassung mitgeteilt und sie gebeten hatten, die datenschutzrechtlichen Vorschriften künftig zu beachten, wandte sich der Oberbürgermeister an uns und vertrat unter anderem die Auffassung, die Mutter des Petenten sei dessen Bevollmächtigte im Sinne des Verwaltungsverfahrensgesetzes gewesen und aus Sicht der Stadtverwaltung habe sich wegen der Vertretungsrechte sogar eine Pflicht zur Kooperation mit der Mutter ergeben. Damit stellte sich die Frage des Verhältnisses des Landesdatenschutzgesetzes zum Verwaltungsverfahrensgesetz des Landes. Nach meiner Auffassung hat das Landesdatenschutzgesetz bei der Verarbeitung von personenbezogenen Daten grundsätzlich Vorrang im gesamten Verwaltungsverfahren. Anders wäre es, wenn die fragliche Vorschrift einen speziellen datenschutzrechtlichen Regelungsgehalt hätte, der den allgemeinen datenschutzrechtlichen Regelungen des Landesdatenschutzgesetzes vorgeht. Das war hier jedoch nicht der Fall. Dies führte zu der vom Gesetzgeber gewollten Konsequenz, dass bei der Verarbeitung personenbezogener Daten im Rahmen von Verwaltungsverfahren der Handlungsspielraum der Behörde seine Schranken im Schutz des informationellen Selbstbestimmungsrechts des Einzelnen findet. Die Zulässigkeitsvoraussetzungen des Landesdatenschutzgesetzes sind danach zu beachten, wenn zur Abwicklung eines Verfahrens personenbezogene Daten übermittelt werden. Insofern konnte offen bleiben, ob im vorliegenden Fall – wie von der Stadt vorgetragen – im rein verwaltungsrechtlichen Sinne überhaupt eine „konkludente“ Bevollmächtigung vorlag.

Behörden und sonstige öffentliche Stellen in Baden-Württemberg haben sich bei der Verarbeitung von personenbezogenen Daten stets zu fragen, auf welcher Rechtsgrundlage die Verarbeitung erfolgt, und diese Vorschriften zu beachten, wenn keine Einwilligung des Betroffenen oder keine ausdrückliche Bevollmächtigung vorliegt.

7. Teil: Informations- und Kommunikationstechnik (IuK)

1. Der datenschutzrechtliche „GAU“

Es wäre schon schlimm genug, wenn man seinen USB-Stick in der Straßenbahn liegen lässt. Wenn eine Kommune aber eine umfangreiche Datensicherung „verliert“, ist das kaum zu übertreffen.

Bereits kurz nach meinem Amtsantritt musste ich die betrübliche Bekanntschaft mit einem „größten anzunehmenden Unfall“ (GAU) im Datenschutz machen: Im April 2009 erreichte uns der Anruf eines Mitarbeiters einer auf Sicherheit in der EDV spezialisierten Unternehmensberatung aus Nordrhein-Westfalen, wonach dort ein Rechner mit der auf den Festplatten gespeicherten Datensicherung einer Stadt aus dem Kraichgau aufgetaucht sei. Seiner Ansicht nach seien das brisante Daten. Da er nächste Woche ohnehin in Stuttgart zu tun habe, wolle er mich aufsuchen und mir eine Kopie der Datensicherung überlassen. Bei der Durchsicht durch meine Mitarbeiter stellte sich heraus, dass die Datensicherung im März 2007 angefertigt worden war. Sie umfasste ca. 180 GByte Daten in über 400 000 Dateien. Die Dateien stammten von einem Datei-Server, den Datenbanken eines sog. Exchange-Servers, aus fachspezifischen Anwendungen und von einem Rechner der städtischen Bibliothek. Der Rechner selbst war offenbar im Zuge einer Verwertung von gebrauchten Computern zu der Beratungsfirma gelangt.

In mehreren Anläufen versuchten meine Mitarbeiter bei der Stadt eine fundierte Stellungnahme einzuholen, wobei sie den Ernst der Lage durch beispielhafte Ausdrucke von Dokumenten – darunter „zur Illustration“ auch private Korrespondenz des Bürgermeisters selbst – untermauerten. Das vorläufige Ergebnis der Recherchen sieht so aus, dass die Stadt seinerzeit die Beschaffung eines neuen Serversystems geplant hatte. Vor dem Kauf wollte sie prüfen, ob der neue Rechner die erforderliche Leistung aufweist. Dazu ließ sie den neuen Rechner, auf dem sie Leistungstests durchführen wollte, testweise bei sich aufstellen. Zu Zwecken der Leistungsbeurteilung wurden auf dem neuen Server personenbezogene Echtdaten – vermutlich des alten Serversystems – gespeichert. Die Leistungstests verliefen nicht wie erhofft, die Stadt ließ den neuen Rechner von einem Unternehmen im Auftrag abbauen und gab ihn an den Hersteller zurück. Dabei unterblieb die Löschung der auf dem neuen Rechner gespeicherten personenbezogenen Daten. Auf diese Weise hatte die Stadt es quasi jedermann, der Zugang zu dem vorübergehend eingesetzten Server hatte, ermöglicht, auf personenbezogene Daten der Bürger der Stadt zuzugreifen. Nur dem umsichtigen Vorgehen der Mitarbeiter des eingangs erwähnten EDV-Beratungsunternehmens ist es zu verdanken, dass sich der Schaden in Grenzen hielt. Solch ein Glück war im Berichtszeitraum nicht allen vergönnt.

Mit ihrer Vorgehensweise hat die Stadt folgende datenschutzrechtliche Verstöße begangen:

– Sie hat für Tests von Hard- und/oder Software echte personenbezogene Daten genutzt, obwohl § 9 Abs. 1 LDSG klar regelt, dass bei derartigen Systemtests keine oder so wenige personenbezogene Daten wie möglich herangezogen werden dürfen. Da es für Zwecke der Leistungsmessung und -bewertung zuverlässige Verfahren gibt, bei denen keine personenbezogenen Daten verarbeitet werden müssen, war die geschilderte Vorgehensweise nicht erforderlich.

– Nach § 9 Abs. 3 Nr. 3 LDSG muss derjenige, der personenbezogene Daten verarbeitet, Maßnahmen ergreifen, die geeignet sind, die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern. Ein probates Mittel hierfür wäre im vorliegenden Fall natürlich gewesen, die Daten auf dem Rechner vor dessen Rückgabe zu löschen. Für die datenschutzrechtliche Beurteilung ist dabei unerheblich, ob die Stadt oder das seinerzeit beauftragte Unternehmen als Auftragnehmer die Daten hätte löschen müssen.

– Ob und in welchem Umfang die Stadt ein externes Unternehmen mit der Verarbeitung ihrer Daten beauftragt hatte, blieb zunächst offen. Erforderlich wäre jedenfalls ein präziser schriftlicher Vertrag und eine wirksame Kontrolle durch die Stadt als Auftraggeber gewesen.

Im Ergebnis trägt die Stadt die datenschutzrechtliche Letztverantwortung. Angesichts der Schwere des Verstoßes bedurfte es keiner langen Abwägung. Für öffentliche Stellen, die so leichtsinnig mit den personenbezogenen Daten ihrer Bürger umgehen, sieht das Landesdatenschutzgesetz die (förmliche) Beanstandung nach § 30 vor. Dass der Datenschutzverstoß nicht böswillig erfolgte, ändert daran nichts.

Einen Tag vor Fertigstellung dieses Tätigkeitsberichts erreichte mich die von mir gemäß § 30 Abs. 4 LDSG eingeforderte Stellungnahme der Stadt. Darin räumt sie ein, dass man das System beschaffen wollte, um damit Datensicherungen anzufertigen. Wie von mir befürchtet, hatte die Stadt keinen schriftlichen Vertrag zur Datenverarbeitung im Auftrag gemäß § 7 LDSG mit den beauftragten Unternehmen geschlossen; vielmehr berief sie sich auf eine mündliche Zusicherung, dass das System nach der Rückgabe neu formatiert und konfiguriert werde. Die Stadt selbst habe ein neues Betriebssystem über das alte System installiert. Dabei wurden die Festplatten jedoch nicht neu formatiert, sodass alle nicht zum Betriebssystem gehörenden Dateien vollständig erhalten blieben.

Immerhin will die Stadt nun endlich die Konsequenzen aus dem Vorfall ziehen und ein Sicherheitshandbuch erstellen sowie Richtlinien für die Handhabung von mobilen Datenträgern und das sichere Löschen von magnetischen Datenträgern erlassen. Dazu will man sich vom Datenschutzbeauftragten des zuständigen Kommunalen Rechenzentrums beraten lassen bzw. mit diesem eng zusammenarbeiten.

Es ist zu begrüßen, dass die Stadt den leichtfertigen Umgang mit personenbezogenen Daten abstellen will. Ob eine punktuelle Beratung durch den Datenschutzbeauftragten des Kommunalen Rechenzentrums ausreicht, bleibt abzuwarten. Besser wäre es, wenn die Stadt einen eigenen behördlichen Datenschutzbeauftragten gemäß § 10 LDSG bestellt.

2. Das Verfahrensverzeichnis nach § 11 LDSG

2.1 Grundlegende Anforderungen

Nach § 11 LDSG hat jede öffentliche Stelle – oder eine von ihr beauftragte Stelle – ein Verzeichnis der automatisierten Verfahren, mit denen bei ihr personenbezogene Daten verarbeitet werden, zu führen. Daraus müssen die wesentlichen Strukturen des Verfahrens und die Rechtsgrundlage hervorgehen. In der Praxis stoße ich oft auf Unkenntnis oder Gleichgültigkeit hinsichtlich dieser Rechtspflicht.

Bei meiner Beratungs- und Kontrolltätigkeit muss ich leider immer wieder feststellen, dass die nach § 11 LDSG gesetzlich vorgeschriebenen Verfahrensverzeichnisse entweder überhaupt nicht oder nur in mangelhafter Weise vorhanden sind. Oftmals ist zudem unbekannt, was Verfahrensverzeichnisse eigentlich sind und dass sie unter bestimmten Umständen meinem Amt vorgelegt werden müssen. Ich möchte daher einige Erläuterungen und Hinweise zu diesem Thema geben.

– Was ist der Zweck eines Verfahrensverzeichnisses?

Schon während der Einführung eines automatisierten Verfahrens – dies geschieht oftmals in Form eines Projektes – muss sich die verantwortliche Stelle Gedanken zum Thema Datenschutz machen. In diesem Zusammenhang ist sowohl die Rechtmäßigkeit der Datenverarbeitung zu prüfen als auch ein Datenschutz- und Sicherheitskonzept zu erstellen, aus dem die zu ergreifenden technischen und organisatorischen Maßnahmen abgeleitet werden können. In einem Verfahrensverzeichnis werden nun alle für eine datenschutzrechtliche Prüfung erforderlichen Informationen zusammengestellt: Die Daten verarbeitende Stelle muss z. B. dokumentieren, welche personenbe-

zogenen Daten sie mit Hilfe welcher automatisierter Verfahren auf welche Weise verarbeitet und welche technischen und organisatorischen Datenschutzmaßnahmen sie dabei getroffen hat. Hierdurch kann sie einen Überblick über ihre Datenverarbeitung behalten. Das Verfahrensverzeichnis, dessen Struktur im Grunde durch den in § 11 Abs. 2 LDSG genannten Katalog vom Gesetzgeber vorgegeben wurde, ist somit unverzichtbar für eine effektive Eigenkontrolle, um zunächst für sich selbst die getroffenen technischen und organisatorischen Maßnahmen zu überprüfen. Zudem ist es eine wichtige Informationsquelle für Fremdkontrollen, etwa datenschutzrechtliche Kontrollen durch meine Dienststelle.

Ein Teil der Informationen, die in einem Verfahrensverzeichnis eingetragen sind, dienen zudem dazu, die Öffentlichkeit bei Bedarf über wesentliche Inhalte des automatisierten Verfahrens zu informieren. Diese Pflicht einer öffentlichen Stelle ergibt sich aus § 11 Abs. 4 LDSG.

– Welchen Inhalt hat ein Verfahrensverzeichnis?

Über den Inhalt eines Verfahrensverzeichnisses gibt § 11 Abs. 2 LDSG Auskunft. Folgende Informationen sind einzutragen und detailliert zu beschreiben:

- Name und Anschrift der verantwortlichen Stelle,
- die Bezeichnung des Verfahrens,
- die Zweckbestimmung und die Rechtsgrundlage der Verarbeitung,
- die Art der gespeicherten Daten,
- der Kreis der Betroffenen,
- die Empfänger der Daten oder Gruppen von Empfängern sowie die jeweiligen Datenarten, wenn vorgesehen ist, die Daten zu übermitteln, sie innerhalb der öffentlichen Stelle für einen weiteren Zweck zu nutzen oder sie im Auftrag verarbeiten zu lassen,
- die Fristen für die Prüfung der Sperrung und Löschung der Daten oder für die Sperrung und Löschung,
- die zugriffsberechtigten Personengruppen oder Personen, die allein zugriffsberechtigt sind,
- eine allgemeine Beschreibung der eingesetzten Hardware, der Vernetzung und der Software und
- die technischen und organisatorischen Maßnahmen nach § 9 LDSG.

– Was ist sonst noch zu beachten?

Bei der Erstellung eines Verfahrensverzeichnisses ist es wichtig, alle vom Gesetz geforderten Angaben vollständig und detailliert zu machen. So genügt es beispielsweise bei der Angabe der Rechtsgrundlage nicht, „nur“ ein Gesetz zu benennen. Es ist vielmehr der einschlägige Paragraph anzuführen. Da in aller Regel eine Vielzahl von Sicherheitsmaßnahmen nicht vom eingesetzten automatisierten Verfahren, sondern von der zugrunde liegenden technischen Infrastruktur abhängen (z. B. Sicherheitsmaßnahmen, die im lokalen Computernetzwerk getroffen sind), empfiehlt es sich, die verfahrensunabhängig getroffenen Sicherheitsmaßnahmen in einem Datenschutz- und Datensicherheitskonzept gebündelt zu beschreiben. Im Verfahrensverzeichnis kann dann auf dieses Konzept verwiesen werden. Auf jeden Fall ist es unerlässlich, die realisierten Maßnahmen vollständig und detailliert zu beschreiben.

Wichtig ist zudem, dass die jeweilige verantwortliche Stelle, wenn kein behördlicher Datenschutzbeauftragter bestellt wurde, meinem Amt, so schreibt es der Gesetzgeber vor, spätestens mit der ersten Einspeicherung von personenbezogenen Daten die Eintragungen des Verfahrensverzeichnisses vorlegen muss.

Zur Arbeitserleichterung hat mein Amt ein Merkblatt mit verschiedenen praktischen Tipps und Hinweisen zur Erstellung eines Verfahrensverzeichnisses entworfen. Dieses steht zum Download auf der Internet-Seite meiner Dienststelle bereit: www.baden-wuerttemberg.datenschutz.de.

2.2 Datenabgleich von Personaldaten durch Rechnungsprüfungsämter – Mängel auch bei den Verfahrensverzeichnissen

Wie schon im 4. Teil, Nummer 1, berichtet, habe ich mich intensiv mit den bei zwei kommunalen Stellen durchgeführten Verfahren des Datenabgleichs von Personaldaten durch Rechnungsprüfungsämter beschäftigt. Dabei wurden mir auch die Verfahrensverzeichnisse zugeleitet. Die Lektüre dieser Dokumente konnte mich nicht davon überzeugen, dass die Verfahren in datenschutzrechtlich zulässiger Weise abliefen.

Im Einzelnen gab es an den Verfahrensverzeichniseinträgen Folgendes zu bemängeln:

– Eine Stelle meinte es ganz besonders gut und ließ mir gleich drei Verfahrensverzeichniseinträge zukommen, die sich teilweise deutlich unterschieden. Grundsätzlich bin ich nur an einem Verfahrensverzeichniseintrag interessiert, nämlich dem, mit dem die Stelle ihren gesetzlichen Verpflichtungen nachzukommen gedenkt. Warum eine Stelle über mehrere, teilweise unterschiedliche Verfahrensverzeichniseinträge zu einem Verfahren verfügt, erschließt sich mir nicht. Die Vermutung, dass ein Verfahrensverzeichniseintrag eigens für die Stellungnahme erstellt wurde, ließ sich damit jedenfalls nicht entkräften.

– Bei der Angabe der „Art der gespeicherten Daten“ teilte mir eine Stelle mit, es handle sich um „alle finanzrelevanten Daten der Stadtverwaltung und ihrer Eigenbetriebe“. Ich erwarte in einem Verfahrensverzeichniseintrag keine Beschreibung jedes einzelnen Datenfeldes detailliert bis auf „bits“ und „bytes“. Aber dass die genannte Beschreibung wenig zum Verständnis beiträgt, welche personenbezogenen Daten verarbeitet werden, dürfte nachvollziehbar sein.

– Beide Stellen nutzten für die Verfahrensverzeichniseinträge ein soweit ersichtlich selbst entworfenes Formular. Dagegen ist zunächst nichts einzuwenden. Fragwürdig ist das Vorgehen dann, wenn beispielsweise eine Rubrik „Rechtsvorschrift“ zwar vorgesehen ist, aber keinen Eintrag enthält. Das schönste Formular nützt bei den Bemühungen, eine datenschutzrechtlich zulässige Verarbeitung durchzuführen, nichts, wenn die gesetzlich vorgeschriebenen Angaben im Verfahrensverzeichniseintrag nicht gemacht werden.

– In einem Eintrag war die Rede davon, dass das Verfahren an einem sog. Stand-alone-Arbeitsplatz-PC durchgeführt worden sei. In diesem Fall beschränken sich die Maßnahmen der Transportkontrolle auf den Umgang mit Datenträgern, weil definitionsgemäß („stand alone“) der Rechner keinen Zugang zu einem Netzwerk hat. Leider erklärte die Stelle in einem anderen Dokument, dass man für die Nutzung des Programms zum Datenabgleich eine Netzwerklizenz beschafft habe, was die Frage aufwirft, warum eine Netzwerklizenz beschafft worden ist, wenn der (oder die?) Rechner nicht mit einem Netzwerk verbunden war(en).

– Von ähnlicher „Güte“ waren Angaben zur Vernetzung, wenn in der Nummer 9 eines Verfahrensverzeichniseintrags einerseits durch Ankreuzen im Formular erklärt wird, „es gehe um nicht vernetzte PCs“, und andererseits im gleichen Absatz auch „Netz innerhalb der Stelle (Intranet)“ angekreuzt ist. In der Gewissheit, dass irgendetwas schon passen wird, könnte man hier natürlich auch die gesamte EDV-Infrastruktur der betreffenden Verwaltung aufzählen. Auf diese Weise wird aber der Vorschrift, wonach die bei dem konkreten Verfahren eingesetzte Hard- und Software und deren Vernetzung zu beschreiben ist, nicht Genüge getan.

– Wenn aber die PCs, mit denen der Abgleich durchgeführt wurde, in die Rechnernetzwerke der Stellen eingebunden waren, wovon ich ausgehe, hätte man bei der Verarbeitung die Erforderlichkeit von Maßnahmen der Transportkontrolle prüfen müssen. Ob man das getan hat, war aus den mir vorgelegten Unterlagen nicht ersichtlich. In beiden Fällen war die Rubrik Transportkontrolle mit „trifft nicht zu“ ausgefüllt worden. Maßnahmen der Transportkontrolle vorzusehen wäre richtig gewesen, solche nicht zu treffen wäre sachlich falsch gewesen, aber die Angabe „trifft nicht zu“ war in jedem Fall völlig verfehlt.

– Zur allgemeinen Beschreibung der eingesetzten Hardware, der Vernetzung und der Software gehört essentiell, dass im Verfahrensverzeichnis die Betriebssysteme genannt werden, unter denen die Anwendung läuft. Wenn das Betriebssystem von Client und gegebenenfalls Server nicht benannt wird, ist es kaum möglich, sich einen Eindruck von der Ablaufumgebung des Verfahrens zu verschaffen.

– Ebenso ist die bloße Nennung von Begriffen wie „Passwortvergabe“ oder „Passwortschutz“ so pauschal, dass sie wenig zur Erhellung des Umfangs einer Authentisierung beitragen kann. Wofür war das Passwort? Zur Anmeldung an einer Domäne, zur Anmeldung an dem lokalen PC oder zur Authentisierung gegenüber dem Verfahren? Das Verfahrensverzeichnis soll eigentlich dazu dienen, derartige Fragen zu beantworten.

– Häufig werden die Daten einer Anwendung in einem anwendungsspezifischen Format gespeichert. Daraus schließen manche Stellen, dass damit bereits ein Zugriffsschutz realisiert wird, da nur mit der jeweiligen Anwendung auf die Daten zugegriffen werden kann. Diese Aussage ist nur teilweise richtig. Dateien, deren Daten in einem anwendungsspezifischen Datenformat geschrieben wurden, können sehr wohl mit anderen Programmen gelesen werden und enthalten häufig personenbezogene Daten. Maßnahmen des Zugriffsschutzes im Rahmen des Dateisystems oder der verschlüsselten Speicherung sind in diesem Fall zur Sicherung der Vertraulichkeit der Daten unerlässlich.

An dieser Stelle will ich mit der Aufzählung enden und nur darauf hinweisen, dass sie hinsichtlich der Mängel nicht erschöpfend ist. Der Verdacht, dass auf meine Anforderung hin in beiden Fällen ein Verfahrensverzeichniseintrag „mit heißer Nadel gestrickt“ wurde, drängte sich bei der Lektüre förmlich auf.

Was ist zu tun: Ein Verfahrensverzeichnis muss den tatsächlichen Gegebenheiten des Verfahrens entsprechen und diese beschreiben, was unstreitig einen gewissen Aufwand und ausreichenden Sachverstand erfordert. Auf den vorangehenden Abschnitt weise ich nochmals hin.

Eine qualitative Verbesserung der Verfahrensverzeichniseinträge ist vor allem dann zu erwarten, wenn sie unter Einbeziehung eines behördlichen Datenschutzbeauftragten, der das Verfahrensverzeichnis der Stelle zu führen hat, erstellt werden. Alle öffentlichen Stellen sollten daher auch aus diesem Grund die Bestellung eines behördlichen Datenschutzbeauftragten ernsthaft ins Auge fassen.

3. Datenschutz bedeutet auch, Verantwortung zu übernehmen

Öffentliche Stellen, die personenbezogene Daten für sich selbst verarbeiten oder durch andere im Auftrag verarbeiten lassen, sind für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Dies ist vielen nicht bewusst.

„Dafür sind wir nicht verantwortlich, der Einsatz dieses automatisierten Verfahrens wurde uns vorgeschrieben.“ Auf solche und ähnliche Äußerungen treffe ich besonders im Umgang mit Schulen, sei es bei Kontrollbesuchen, sei es bei Beratungen oder bei der Bearbeitung von Bürgeranfragen. Die Zuständigkeit wird dann häufig gerne auf vorgesetzte Dienststellen

oder auf kommunale Schulträger abzuwälzen versucht; die stereotype Ausrede lautet zumeist: Datenschutzrechtlich verantwortlich ist das Kultusministerium (z. B. weil von dort ein landesweites EDV-Verfahren vorgegeben wurde) oder die Stadt XY als Schulträger (z. B. weil die Stadt die EDV-Ausrüstung der Schule zur Verfügung gestellt hat). Dieses Verhalten macht deutlich, dass elementare datenschutzrechtliche Grundbegriffe vielfach leider nicht bekannt sind oder ignoriert werden. Doch gerade die Frage nach der datenschutzrechtlichen Verantwortlichkeit ist aus meiner Sicht von zentraler Bedeutung. Diese bezieht sich nicht nur auf die gesetzliche Zulässigkeit und die ordnungsgemäße Verarbeitung, sondern auch auf die Realisierung der notwendigen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten.

Der Begriff der „verantwortlichen Stelle“ ist im Landesdatenschutzgesetz klar geregelt: Verantwortliche Stelle ist jede Stelle, die personenbezogene Daten für sich selbst verarbeitet oder durch andere im Auftrag verarbeiten lässt (§ 3 Abs. 3 LDSG).

Jede öffentliche Stelle, die personenbezogene Daten verarbeitet, ist gut beraten, wenn sie die Verantwortlichkeitsfrage genau prüft und dabei den Zweck der Datenverarbeitung im Auge behält. Wird sie lediglich als „Datenerfassungsstelle“ für Dritte tätig oder nutzt sie die verarbeiteten Daten zur Erfüllung eigener Aufgaben weiter? Die genaue Prüfung der Verantwortlichkeiten ist auch dann geboten, wenn eine solche Stelle ihre personenbezogenen Daten durch andere im Auftrag verarbeiten lässt, das heißt beispielsweise ein zentrales Rechenzentrum mit der Durchführung beauftragt (sog. Auftragsdatenverarbeitung). Entscheidet sich eine verantwortliche Stelle für eine Auftragsdatenverarbeitung, so bleibt sie dennoch weiterhin für die Einhaltung der Vorschriften des Datenschutzes und damit insbesondere für die notwendigen technischen und organisatorischen Schutzmaßnahmen in der Pflicht. Sie hat in dem Vertrag zur Auftragsdatenverarbeitung entsprechende Verpflichtungen des Auftragnehmers vorzusehen und deren Einhaltung konsequent zu überwachen.

4. EDV in der Praxis: Probleme bei Datei-Zugriffsberechtigungsstrukturen und die Tücken gekaufter Software

In einem Gesundheitsamt werden in großem Umfang sensible medizinische Daten von Bürgern verarbeitet. Wenn solche Daten in falsche Hände geraten, können sich daraus erhebliche Nachteile für die Betroffenen ergeben.

Ein Kontrollbesuch in einem Gesundheitsamt zeigte im technisch-organisatorischen Umfeld schwerwiegende Mängel auf, auf die ich hier näher eingehen will:

Ein Gesundheitsamt besteht aus mehreren Abteilungen, denen unterschiedliche Aufgaben zugewiesen sind. Im Rahmen eines Kontrollbesuches stellten meine Mitarbeiter nun fest, dass Dateien mit sensiblen personenbezogenen Daten von Mitarbeitern aus einer anderen Abteilung des Amtes zu lesen waren. Es handelte sich hierbei um Meldungen nach dem Infektionsschutzgesetz, in welchen im Klartext die Betroffenen mit ihren infektiösen Erkrankungen genannt wurden. Diese Daten waren beispielsweise von Mitarbeitern aus der Abteilung „Jugend- und Zahngesundheit“ zu lesen und sogar abzuändern. Nur der Vollständigkeit halber sei gesagt, dass die Betroffenen, um deren Daten es geht, weder Jugendliche noch zahnbehandlungspflichtige Patienten waren. Als der Leiter des Gesundheitsamts während des Kontrollbesuchs darauf angesprochen wurde, konnte keine Erklärung für die Möglichkeit des abteilungsübergreifenden Dateizugriffs gegeben werden. Eine Erforderlichkeit hierfür war nicht zu erkennen, weil die Abteilung „Jugend- und Zahngesundheit“ die fraglichen Daten für die Erfüllung ihrer eigenen Aufgaben nicht benötigte und daher auch nicht verarbeitete. Ich habe deshalb dem Amt gegenüber eine Beanstandung ausgesprochen.

Der Fall hat erneut gezeigt, dass Zugriffsberechtigungen sehr sorgfältig und umsichtig vergeben werden müssen. Weil sich außerdem die Berechtigungen aufgrund des üblichen Personalwechsels häufig ändern, ist auch deren regelmäßige Überprüfung und Aktualisierung unbedingt erforderlich. Die

Beschreibung transparenter, allen Beteiligten bekannter Prozesse, die insbesondere die Genehmigung zur Vergabe von Zugriffsrechten einschließt, ist hierbei hilfreich.

Gekaufte Software ist nicht immer dazu geeignet, die datenschutzrechtlichen Anforderungen zu erfüllen. Denn oftmals erfüllt zwar diese Software die fachlich-funktionalen Anforderungen; jedoch sind die datenschutzrechtlich vorgeschriebenen technischen Maßnahmen oft nicht umzusetzen, weil die Software nicht über die entsprechende Funktionalität verfügt. Dies sei an einem Beispiel aus unserer Kontrollpraxis dargestellt:

In Gesundheitsämtern ist häufig das automatisierte Verfahren Octoware anzutreffen. Es handelt sich hierbei um ein Produkt „von der Stange“. Bereits im Jahr 2006 wurde diese Software bei einem Kontrollbesuch in einem anderen Gesundheitsamt beanstandet (vgl. 27. Tätigkeitsbericht für das Jahr 2006, LT-Drucksache 14/650). Die von uns festgestellten Mängel waren damals insbesondere:

- keine technische Sicherstellung einer Mindestlänge des Passwortes,
- kein automatischer Verfall der Passwörter nach einer bestimmten Zeit,
- keine automatische Sperre nach einer gewissen Anzahl von Fehlanmeldungen,
- keine Passworthistorie, mit der verhindert wird, dass eines der letzten Passwörter erneut genutzt wird.

Zudem erfolgte – wie unsere Prüfung ergab – keine Eingabekontrolle innerhalb der Anwendung. Es wurde zwar erfasst, welcher Mitarbeiter die letzte Änderung an einem Datensatz durchgeführt hatte. Das Landesdatenschutzgesetz fordert von einer Eingabekontrolle jedoch, dass nachträglich überprüft werden kann, welche Daten zu welcher Zeit von wem in dem betreffenden Datenverarbeitungssystem eingegeben worden sind. In der Software Octoware war diese Funktionalität jedoch nicht vorhanden. In der verantwortlichen Stelle war zudem niemandem bekannt, ob eine Eingabekontrolle auf eine andere Weise durchgeführt oder einfach „von Hand“, das heißt durch simples Aufschreiben, realisiert wird. Somit wurde in diesem Amt nicht einmal versucht, die nicht vorhandene Funktionalität der Software durch eine organisatorische Regelung auszugleichen.

All diese festgestellten Mängel waren – wie gesagt – bereits im Jahre 2006 in einem anderen Gesundheitsamt vorhanden. Trotz unserer Aufforderung, die Mängel abstellen zu lassen, wurde offenbar vom Hersteller nichts unternommen.

Bereits vor der Beschaffung von Software „von der Stange“ – also am besten in der Projektphase – ist darauf zu achten, dass durch die zu beschaffende Software auch die datenschutzrechtlichen Anforderungen erfüllt werden. Erst hinterher das Fehlen von Funktionen mit datenschutzrechtlicher Relevanz festzustellen, ist nicht im Sinne des Datenschutzes; dieses Versäumnis ist aber leider in der Praxis immer wieder anzutreffen.

5. Orientierungshilfen zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

Im Berichtszeitraum wurden die Orientierungshilfen zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet von einer Arbeitsgruppe des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder überarbeitet. Neben vielen redaktionellen Änderungen wurden folgende inhaltliche Erweiterungen vorgenommen:

- Das Urteil des Amtsgerichts Berlin Mitte (Urteil von 27. März 2007, 5 C 314/06), wonach das Verfolgen von User-Bewegungen auf Homepages (Webservern) mittels Speicherung der IP-Adressen über den Nutzungsvorgang hinaus unzulässig ist, wurde berücksichtigt.
- Die Techniken „Sender Policy Framework/DomainKeys Identified Mail“ (SPF/DKIM), die zur Bekämpfung der SPAM-Flut entwickelt wurden,

wurden von der Arbeitsgruppe untersucht und aufgrund der datenschutzrechtlichen Unbedenklichkeit in die Orientierungshilfen aufgenommen. Verwaltungsnetze müssen über ein Firewallsystem an das Internet angebunden werden. Häufig werden parallel ein zentraler Spamfilter und ein Virenscanner betrieben. In beiden Systemen fallen bei der Internet-Nutzung personenbezogene Daten in Form von Protokolldaten und Inhaltsdaten an. Es ist daher zu klären, unter welchen Bedingungen auf die Daten zugegriffen werden darf. Unter Zuarbeit des Arbeitskreises Medien wurden die Bedingungen präzisiert, unter denen auf die Inhaltsdaten von E-Mails zugegriffen werden darf. Die Arbeitsgruppe vertritt weiterhin die Auffassung, dass die Protokolldaten nach sieben Tagen zu löschen sind.

Bedingt durch den technischen Wandel wird auch zukünftig eine Anpassung der Orientierungshilfen von Zeit zu Zeit erforderlich sein. Die öffentlichen Stellen sollten die nunmehr vorgenommenen Aktualisierungen in ihrem EDV-Betrieb bei Bedarf umsetzen. Die Orientierungshilfen können auf der Homepage meiner Dienststelle unter www.baden-wuerttemberg.datenschutz.de abgerufen werden.

6. Polizeiliche Datenverarbeitung

Polizeiarbeit ist zu einem nicht unerheblichen Teil Beschaffung von Information und deren Auswertung. Dazu bedient sich die Polizei Baden-Württembergs der elektronischen Datenverarbeitung. Daher ist die Kontrolle der polizeilichen Informationssysteme ein immer wiederkehrendes Thema auf meiner Agenda.

Im Berichtszeitraum wurden ein neues Vorgangsbearbeitungssystem der Polizei Baden-Württemberg namens ComVor („Computergestützte Vorgangsbearbeitung“) und die EDV-technische Bewältigung der Großlage NATO-Gipfel kontrolliert. Zusammenfassend lässt sich formulieren: Licht und Schatten.

6.1 Die polizeiliche Vorgangsbearbeitung ComVor

Das alte, großrechnerbasierte System zur Erfassung, Be- und Verarbeitung von polizeilichen Vorgängen in Baden-Württemberg stammt aus den achtziger Jahren des vorigen Jahrhunderts und war noch nicht für die aktuell erforderliche Vorgangsbearbeitung auf Sachbearbeiterebene konzipiert. Ein neues Vorgangsbearbeitungssystem war daher von Nöten und wurde in Kooperation mit zwei weiteren Bundesländern entwickelt. Das Ergebnis ist ein datenbankbasiertes Vorgangsbearbeitungssystem, bestehend aus der Vorgangsbearbeitung CV, einer Vorgangsverwaltungsanwendung namens ComVor Index und dem sog. Elektronischen Tagebuch ETB. Schon im Jahr 2008 wurden mehrere Polizeidirektionen auf das neue Vorgangsbearbeitungssystem ComVor umgestellt. Deshalb lag es nahe, die Pilotdienststelle einer Kontrolle zu unterziehen, die zu folgenden Ergebnissen führte:

– Verarbeitung personenbezogener Daten

Die Vorgangsbearbeitung CV dient zur Erfassung polizeilicher Vorgänge in Dokumenten. Sie unterscheidet zwischen den Objektrollen (Beschuldigter, Zeuge, Geschädigter etc.) und ihren Rolleninhalten (Name, Vorname, Geburtsdatum etc.) einerseits und ihrem Auftreten in polizeilichen Vorgängen andererseits, die über Formulare abgebildet werden. Dadurch wird prinzipiell eine effektive Trennung von personenbezogenen Daten und Vorgängen sowie bei Bedarf eine flexible Erweiterbarkeit über Formulare erreicht. Ein personenbezogenes Datum wird in der Vorgangsbearbeitung an genau einer Stelle in einer Datenbank gespeichert. Treten personenbezogene Daten in Formularen auf, werden diese daher lediglich als Verweise auf die Objektdaten in der Datenbank realisiert.

Die Teilkomponente ComVor Index dient zur Verwaltung von Vorgängen, indem gegebenenfalls eine Suche über die Vorgangsdatenbank durchgeführt wird. Es kann dabei über Objektrollen bzw. den

dazugehörigen Daten gesucht werden. Überwiegend dürfte ComVor Index dazu genutzt werden, an Hand der Vorgangsnummer Vorgänge zu suchen bzw. zu finden. Ich bin mir bewusst, dass die Suchfunktion die Gefahr birgt, ComVor als weiteres polizeiliches Auskunftssystem zu nutzen. Deshalb habe ich empfohlen, weitergehende Suchfunktionalitäten an bestimmte Berechtigungsstufen zu binden und diese nur restriktiv zu vergeben.

Das elektronische Tagebuch ETB ist in erster Linie ein reines Informationsmedium für den polizeilichen Sachbearbeiter, um sich einen Lageüberblick zu verschaffen. Soweit bei der Kontrolle ersichtlich, werden personenbezogene Daten in das ETB eingestellt. Ich habe darauf hingewiesen, dass sich der Umfang der Verarbeitung personenbezogener Daten an anderen Lagebildinformationssystemen orientieren muss. Ich kann nachvollziehen, dass die Gewinnung eines lokal begrenzten Lagebildes für die polizeiliche Arbeit erforderlich ist. Dazu ist die Kenntnis von personenbezogenen Daten meiner Ansicht nach aber nicht notwendig. Insbesondere ist darauf zu achten, dass in einer ersten Stufe keine personenbezogenen Daten angezeigt werden. Ich gehe davon aus, dass im ETB im Gegensatz zu anderen Lagebildinformationssystemen nur polizeilich geprüfte Vorgänge gespeichert werden, woraus sich zumindest eine Erhöhung der Datenqualität ergeben sollte.

– Berechtigungsverwaltung

Dem Grundsatz, dass der Nutzer nur Kenntnis derjenigen personenbezogenen Daten haben soll, die er für seine Aufgabenerfüllung braucht, wird in ComVor durch ein umfangreiches Berechtigungskonzept Rechnung getragen. Es erstreckt sich auf alle drei Komponenten. Die Berechtigungen werden an Funktionsrollen und an Organisationseinheiten ausgerichtet. Die Berechtigungsverwaltung ist dezentral organisiert. Die Berechtigungen werden lokal durch Personal in der jeweiligen Organisationseinheit vergeben.

– Löschung

Durch die Trennung der Vorgangsbeschreibung in Formular und Objektdaten wird erreicht, dass bei Löschung des Objekts dieses aus allen zum Sachverhalt gehörenden Formularen, in denen es in einer bestimmten Rolle aufgetreten ist, eliminiert wird. Diese Lösung ist datenschutzrechtlich zu begrüßen, weil sie sicherstellt, dass die Speicherdauer von personenbezogenen Daten effektiv kontrolliert werden kann. Damit sollten Dokumente, in denen personenbezogene Daten festgehalten werden und die in den Tiefen eines Dateisystems gespeichert sind und von keiner Löschroutine erfasst werden, eigentlich der Vergangenheit angehören.

Die bei der polizeilichen Vorgangsbearbeitung zu beachtenden Löschfristen ergeben sich nicht direkt aus gesetzlichen Vorschriften. Auffallend ist, dass die Löschfristen in dem neuen System mit generell fünf Jahren deutlich länger waren als im alten System, in dem Daten je nach Einzelfall zwischen einem und fünf Jahre gespeichert wurden. Ich habe gegenüber der Polizei die Auffassung vertreten, dass hinsichtlich der Speicherdauer nachgearbeitet werden muss.

– Schnittstellen

Da die Vorgangsbearbeitung die zentrale Anwendung der Polizei ist, bestehen Schnittstellen zu weiteren Polizeiverfahren, die nicht notwendigerweise von der gleichen datenschutzrechtlich verantwortlichen Stelle betrieben werden. Teilweise befanden sich die Entwicklungen noch im Planungsstadium. Wir haben darauf hingewiesen, dass wir eine effektive Übermittlungskontrolle in ComVor für erforderlich halten, falls Daten an eine andere Stelle, die verantwortliche Stelle im Sinne des Landesdatenschutzgesetzes ist, übermittelt werden sollen.

Insgesamt hat die Kontrolle ergeben, dass die Polizei mit der neuen Vorgangsbearbeitung ein leistungsfähiges System entwickelt hat, das datenschutzrechtliche Anforderungen grundsätzlich umsetzen kann. Jetzt gilt es, letzte Schwächen auszumerzen und bei der Weiterentwicklung den Datenschutz im Auge zu behalten.

6.2 Der NATO-Gipfel

Im Frühjahr 2009 fand in Baden-Baden, Kehl und Straßburg anlässlich des 60. Jahrestages des Bestehens der NATO ein zweitägiger NATO-Gipfel statt. Um die Sicherheit der teilnehmenden Delegationen zu gewährleisten, wurde zumindest aus meiner Sicht ein bis dahin im Land nicht gekannter polizeilicher Aufwand betrieben. Damit einher ging eine intensive EDV-technische Unterstützung, bei der personenbezogene Daten von Bürgern erhoben und verarbeitet wurden, die sich vermutlich nie hätten träumen lassen, dass sie eines Tages in einem Polizeicomputer durchleuchtet würden. Insgesamt waren ca. 650 PCs in Betrieb. Die Anzahl entspricht damit der Ausstattung von ungefähr zwei mittelgroßen Polizeidirektionen. Die Vielzahl der Betroffenen und die Eingriffstiefe in das Recht auf informationelle Selbstbestimmung veranlassten mich, die „Besondere Aufbauorganisation Atlantik“ (BAO Atlantik), die mit der Sicherung des Ereignisses beauftragt war, einer Kontrolle zu unterziehen. Dabei ergaben sich folgende Erkenntnisse:

– Dateien

Zu meinem Bedauern ist es der Polizei nicht gelungen, für die BAO Atlantik eine spezielle EDV-Anwendung zur Lagebearbeitung, in der alle die Lage betreffenden personenbezogenen Daten gespeichert worden wären, aufzubauen. Stattdessen mussten meine Mitarbeiter vor Ort feststellen, dass anscheinend Excel-Dateien die bevorzugte Speicher- und Verarbeitungslösung waren. Exemplarisch standen hierfür die Dateien der Einwohner der Sicherheitszonen der verschiedenen Örtlichkeiten, Dateien aller im Stadtgebiet Baden-Baden bzw. den entsprechenden Sicherheitszonen in Kehl und am Flugplatz Lahr registrierten Inhaber waffenrechtlicher Erlaubnisse, eine Datei aller Personen in räumlicher Nähe zu Aufenthaltsräumlichkeiten gefährdeter Staats- und Regierungschefs, Dateien mit Firmen und deren Mitarbeitern in diversen Sicherheitszonen bzw. zutrittsberechtigte Personen zu Sicherheitsbereichen, eine Liste der für Gefangenensammelstellen vorgesehenen Ärzte und die hoffentlich leer gebliebene Liste verletzter und einsatzunabhängig erkrankter und verletzter Beamtinnen und Beamten, die mit einer Anwendung namens Xenios auf einem Stand-alone-PC verwaltet wurden.

Die Dateien waren auf verschiedenen Servern bei der Polizeidirektion Offenburg, dem Einsatzlagezentrum bzw. dem Regierungspräsidium in Freiburg, der Polizeidirektion Rastatt/Baden-Baden, in einem landesweit verfügbaren Informationssystem (MOSS) oder auf Stand-alone-PCs gespeichert. Wie bei Dateien nicht unüblich, dürften sie daneben auch per polizeilicher E-Mail in diversen Postfächern und in sonstigen Ablagen gelandet sein. Wenn schon die Speicherorte über die Landkarte verstreut liegen, wollte man bei der datenschutzrechtlichen Verantwortlichkeit nicht nachstehen. Auch diese war auf mehrere Stellen verteilt. Die Konsequenzen, die ein derartiges Sammelsurium an Dateien für das Auskunftsrecht gemäß §§ 5 und 21 LDSG hat, sind klar. Der Betroffene weiß nicht nur nicht, wer wo welche personenbezogenen Daten über ihn speichert, sondern angesichts der Vielzahl von Dateien kann er auch nicht wissen, an welche verantwortliche Stelle er sich wenden muss, wenn er seinen Auskunftsanspruch geltend machen will. Auch die Löschung der Daten war für den Betroffenen bei dieser Ausgangslage alles andere als transparent, denn als Löschdatum, sofern man das als Datum bezeichnen mag, wurden „nach dem Nato-Gipfel“, „nach endgültiger Beendigung der Einsatzmaßnahmen“, „spätestens zum 31. Dezember 2009“ und weitere nicht ganz einfach einzugrenzende Zeiträume genannt. Bei den Verfahrensverzeichniseinträgen der auf einer Excel-

Datei basierenden „Vorgangsbearbeitung im Unterabschnitt 4.1-Ermittlungen“ und der „Befristeten Speicherung und Auswertung von Bild- und Videodaten sowie Daten von sichergestellten Laptops und Mobiltelefonen“ wurde gar erklärt, Fristen für die Prüfung der Löschung oder Sperrung könnten entfallen.

– Anwendungen

Neben den Excel-Dateien wurden noch weitere Verfahren, mit denen personenbezogene Daten gespeichert und verarbeitet werden, namens LaDok (Lagedokumentation), Arbeitsdatei RTF (Dokumentation der Anfragen in polizeilichen Auskunftssystemen), GeSa (Verwaltung und Dokumentation der in Gefangenensammelstellen aufgenommenen Personen) oder EPS-Web (Einsatzprotokollsystem) und das schon erwähnte Verfahren MOSS (Microsoft Office Sharepoint Server) eingesetzt. Eine Organisationseinheit hatte mit LaDok und MOSS sogar zwei Systeme im Einsatz.

Innerhalb MOSS, das auch als Plattform für die Anwendung Polizei Online dient, auf die alle Polizeibeamte des Landes zugreifen können, wurde der BAO Atlantik ein eigener Speicherbereich zugewiesen. Über die Berechtigungsverwaltung von MOSS wurde geregelt, wer auf die personenbezogenen Daten zugreifen kann. Die Gefahr bei derartig „kombinierten“ Systemen besteht erfahrungsgemäß darin, dass Zugriffsberechtigungen zu weitgehend vergeben werden. Bei einer stichprobenweisen Prüfung stellten meine Mitarbeiter beispielsweise fest, dass nicht mit Vollzugsaufgaben betraute Mitarbeiter des Landeskriminalamts auf die Liste der Waffenbesitzer (Name, Anschrift und Aufzählung der gemeldeten Waffen von Offenburg) zugreifen konnten. In einem anderen Fall hatten alle Benutzer einer Domäne namens LPDFR19 – also der Abteilung 6 des Regierungspräsidiums – lesenden und schreibenden Zugriff auf eine Datei, in der Waffeninhaber im Bereich der Polizeidirektion Rastatt/Baden-Baden gespeichert waren.

Hinsichtlich des technischen Datenschutzes äußerst fragwürdig war auch die Anwendung ITB/Videoauswertung des Einsatzabschnitts Folgemaßnahmen. Die Beamten brachten nämlich ihre EDV-Ausrüstung von ihrer Heimatdienststelle mit, wobei alle Einstellungen der Heimatdienststelle übernommen wurden. Alle Benutzer mussten mit der einheitlichen Kennung „users“ arbeiten und hatten Zugriff auf alle Daten. Ob dieses Vorgehen in der Heimatdienststelle datenschutzrechtlich zulässig ist, erscheint fraglich. Bei der BAO Atlantik hätte es Maßnahmen der Benutzer- und Zugriffskontrolle bedurft, wie sie nicht dadurch zu erreichen sind, dass alle Benutzer unter derselben Benutzerkennung in einem Netzwerk arbeiten.

Nur der Vollständigkeit halber sei erwähnt, dass nicht wenige der oben genannten Anwendungen die Gelegenheit eröffneten, in Freitextfeldern Daten einzugeben und abzuspeichern. Regelungen, was in die Freitextfelder einzugeben war, waren nicht erkennbar.

In einer Stellungnahme zu meinem Kontrollbericht hat das Innenministerium erklärt, die IT-Konzeption sei darauf ausgerichtet gewesen, auf der Grundlage einer einheitlichen technischen Plattform zu arbeiten. Hierunter versteht das Innenministerium offenbar, dass das Arbeiten auf Servern in mindestens vier sog. Domänen (Landespolizeidirektion Freiburg, Polizeidirektion Offenburg, Polizeidirektion Rastatt/Baden-Baden und Landeskriminalamt Baden-Württemberg) von Benutzern aus fünf Domänen (zusätzlich polizei-bw.net) und die gegenseitige Öffnung der Domänen (durch die Schaltung von sog. Vertrauensstellungen) mit mindestens sieben Anwendungen eine „einheitliche Plattform“ sei. Diese Auffassung teile ich nicht. Weiterhin vertrat das Innenministerium die Auffassung, die Verwendung unterschiedlicher Anwendungssysteme sei nicht zu vermeiden und deshalb zur sachgerechten Bewältigung erforderlich gewesen. Auch das ist nicht nachvollziehbar: LaDok, EPS-Web, Recherchetool-Funkbuch waren Anwendungen, die dazu

dienten, polizeiliches Handeln zu dokumentieren. Dass die Dokumentation polizeilichen Handelns so komplex ist, dass es dazu drei unterschiedlicher Anwendungen bedarf, ist nicht nachvollziehbar. Zur Speicherung erklärte das Innenministerium, entsprechend der IT-Konzeption sei weitgehend eine zentrale Speicherung von Daten erfolgt. Diese Behauptung deckt sich nicht mit den Beobachtungen meiner Mitarbeiter, wonach personenbezogene Daten auf diversen Servern und Laufwerken gespeichert wurden. Insgesamt hätte man dem Datenschutz sicher besser dadurch Genüge getan, wenn man eine eigenständige Domäne nur für die BOA Atlantik eingerichtet hätte. Meiner Schlussfolgerung, angesichts der „verteilten Speicherung" personenbezogener Daten sei deren termingerechte Löschung alles andere als gesichert, wollte sich das Innenministerium nicht anschließen. Immerhin hat es zugestanden, dass man als Prüffrist – nicht Löschfrist – für die Einsatzdokumentation nunmehr den April 2010 vorgemerkt hat.

Insgesamt hat die Datenverarbeitung beim NATO-Gipfel den Eindruck erweckt, als sei die IT-Strategie der BAO Atlantik „EDV by patchwork" gewesen. Dabei bleibt der Datenschutz erfahrungsgemäß auf der Strecke. Ich hoffe, dass die neue Vorgangsbearbeitung und die sich derzeit in Entwicklung befindlichen neuen polizeilichen Informationssysteme so flexibel sein werden, dass damit zukünftige Großlagen EDV-technisch in geordneten datenschutzrechtlichen Bahnen verlaufen und von mir begleitet werden können.

7. Kontrolle eines Personalrats

Auch der Personalrat einer Dienststelle ist Teil der meiner Kontrolle nach § 28 LDSG unterliegenden öffentlichen Stelle und hat wegen der hohen Vertraulichkeit der von ihm verarbeiteten Daten besondere datenschutzrechtliche Sorgfalt walten zu lassen.

Aufgrund der Eingabe eines Beschäftigten einer Stadt hat meine Dienststelle den Personalrat dieser Stadtverwaltung einer Kontrolle unterzogen. Besonders zu erwähnen ist, dass das Ergebnis der Kontrolle ausschließlich dem Personalrat mitgeteilt wurde, weil er seine Aufgaben im Verhältnis zu seiner Dienststelle unabhängig und eigenverantwortlich wahrnimmt. Im Einzelnen wurde von meinen Mitarbeitern Folgendes festgestellt bzw. empfohlen:

- Einer der Angehörigen des Personalrats nahm seine Aufgaben im Rahmen einer Freistellung im Umfang von fünfzig Prozent wahr. Für das städtische Sozialamt war er ebenfalls im Umfang von fünfzig Prozent tätig. Im EDV-System hatte dieses Personalratsmitglied nun eine Benutzerkennung, unter der er vom Personalratsbüro aus sowohl auf personenbezogene Daten, die der Personalratstätigkeit zuzuordnen waren, als auch auf personenbezogene Daten in seiner städtischen Tätigkeit zugreifen konnte. Diese Vorgehensweise entsprach nicht dem Gebot einer funktionsbezogenen Trennung innerhalb des EDV-Systems. Der Personalrat teilte mit, dass er die Problematik gegenüber der EDV-Abteilung angesprochen habe. Eine Lösung würde kurzfristig angestrebt.
- Mit dem Rechner erstellten die einzelnen Personalräte hauptsächlich Dokumente, die im Dateisystem des lokalen Rechners oder auf einem Server abgelegt wurden. Auch für den Personalrat gilt bei der Verarbeitung personenbezogener Daten, dass diese zu löschen sind, wenn ihre Kenntnis nicht mehr für die Aufgabenerfüllung erforderlich ist. Hierzu muss gegebenenfalls manuell das Dateisystem nach zu löschenden Dateien durchsucht werden.
- Zur Gewährleistung der Vertraulichkeit empfiehlt es sich, dass die von einem Personalrat erstellten Dateien verschlüsselt gespeichert werden. In Frage kommt auch, dass jedes Personalratsmitglied die Daten auf einem eigens beschafften USB-Stick verschlüsselt abspeichert und diesen in der Dienststelle verschlossen aufbewahrt.
- Bei der kursorischen Durchsicht des E-Mail-Postfachs wurden Nachrichten gefunden, deren Anhänge aus Dokumenten bestanden, in denen per-

sonenbezogene Daten gespeichert wurden. Auch für E-Mails müssen die Löschfristen eingehalten werden.

– Bei der Kontrolle fielen meinen Mitarbeitern Mängel der Benutzerkontrolle auf, die insbesondere für die von den einzelnen Personalratsmitgliedern genutzten PCs von besonderer Tragweite sein können:

  • Das Passwort war nur fünf Zeichen lang. Wir haben den Personalrat darauf hingewiesen, dass jedes seiner Mitglieder ein Kennwort mit einer Mindestlänge von acht Zeichen wählen solle, die aus Groß- und Kleinbuchstaben sowie Zahlen bestehen sollten.

  • Bildschirmsperren waren nicht aktiviert. Wir haben empfohlen, dies nachzuholen, damit ein PC bei vorübergehender Abwesenheit des Nutzers nicht von Dritten genutzt werden kann. Der Zeitraum bis zur Aktivierung der Bildschirmsperre sollte zehn Minuten nicht überschreiten.

  • Es fand keine Sperre bei erfolglosen Anmeldeversuchen statt. Wir halten es für erforderlich, dass nach einer von den Administratoren zu bestimmenden Anzahl von erfolglosen Anmeldungen die Benutzerkennung gesperrt wird. Diese Maßnahme ist deshalb angeraten, weil sonst von Unbefugten über das Netzwerk unbemerkt automatisiert Anmeldeversuche durchgeführt werden können, die insbesondere aufgrund eines zu kurzen Passworts mit hoher Wahrscheinlichkeit erfolgreich sind und damit den Schutz durch das Passwort unterlaufen.

Die Arbeit eines Personalrats bedingt den Umgang mit personenbezogenen Daten, deren Vertraulichkeit besonders hoch einzuordnen ist. Dies erfordert eine spezielle Konfiguration der Personalrats-PCs. Personalräte müssen regelmäßig prüfen, ob die Kenntnis aller von ihnen verarbeiteten personenbezogenen Daten zur Aufgabenerfüllung weiterhin erforderlich ist, und die Daten gegebenenfalls und nicht zuletzt im Interesse der Betroffenen löschen.

8. Die Neuregelung der informationstechnischen Zusammenarbeit zwischen Bund und Ländern – wo bleibt der Datenschutz?

Die Föderalismuskommission II hat auch die informationstechnische Zusammenarbeit zwischen Bund und Ländern auf eine neue verfassungsrechtliche Grundlage gestellt. Zur Umsetzung wurde ein IT-Staatsvertrag erarbeitet, der einen IT-Planungsrat mit weitreichenden Befugnissen vorsieht. Weder im Staatsvertrag noch im entsprechenden Ausführungsgesetz des Landes ist von Datenschutz die Rede.

Die Beschlüsse der Kommission von Bundestag und Bundesrat zur Modernisierung der Bund-Länder-Finanzbeziehungen (Föderalismuskommission II) haben u. a. zu einer Änderung des Grundgesetzes in Bezug auf die informationstechnische Zusammenarbeit geführt; danach können Bund und Länder aufgrund von Vereinbarungen die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen (gegebenenfalls auch mit qualifizierter Mehrheit) festlegen (Artikel 91 c Abs. 2 des Grundgesetzes – GG –). Zur weiteren Umsetzung wurde ein „Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag über die Ausführung von Artikel 91 c GG“ erarbeitet (vgl. LT-Drucksache 14/4908), der am 1. April 2010 in Kraft treten soll. Der darin vorgesehene IT-Planungsrat wird dann zum zentralen Gremium der IT-Steuerung von Bund und Ländern, das deren Zusammenarbeit in Fragen der Informationstechnik koordinieren, fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards beschließen und eGovernment-Projekte steuern soll. Dabei kann der IT-Planungsrat Beschlüsse, z. B. zu IT-Standards, auch mit Mehrheitsentscheidung fassen. Der Ratifizierungsprozess läuft. Bund und Länder haben außerdem jeweils eigene Ausführungsgesetze auf den Weg gebracht.

Im September 2009 unterrichtete das Innenministerium die Ministerien und mich über den Entwurf des Ausführungsgesetzes, verwies darauf, dass der Ministerrat dem Staatsvertrag bereits am 22. Juli 2009 zugestimmt habe,

und kündigte die Verabschiedung des Gesetzes durch den Landtag bis Ende des Jahres an. Leider musste ich nach der Lektüre des Ausführungsgesetzes, aber auch des Staatsvertrages selbst, feststellen, dass darin zwar Ausführungen zur Festlegung von „IT-Interoperabilitäts- und IT-Sicherheitsstandards“, aber nicht zur datenschutzrechtlichen Verträglichkeit von Standards enthalten sind. Weiter fiel auf, dass vorrangig auf „bestehende Marktstandards“ abgestellt werden soll (§ 3 Abs. 1 Satz 2 des Staatsvertrags). Vor einer Beschlussfassung über derartige „verbindliche Standards“ soll auf Antrag des Bundes oder dreier Länder grundsätzlich der Bedarf sowie die IT-fachliche Qualität und Widerspruchsfreiheit des vorgesehenen Standards durch eine vom IT-Planungsrat bestimmte, unabhängige Einrichtung geprüft werden (§ 3 Abs. 3 Satz 1).

Die Ausblendung des Datenschutzes in der Standardsetzung durch den IT-Planungsrat bedeutet aus meiner Sicht insbesondere im Hinblick auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (vgl. Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, siehe hierzu 1. Teil, Nr. 1) ein erhebliches, in Anbetracht der aktuellen Rechtsprechung des Bundesverfassungsgerichts eigentlich unverständliches Defizit. Ich schlug daher dem Innenministerium unter dem Vorbehalt, dass noch Änderungen am Staatsvertragsentwurf zu erreichen sind, vor, den Datenschutz als Standardisierungsmaßstab explizit aufzunehmen sowie vorzusehen, dass datenschutzrelevante neue IT-Standards auch auf Antrag des Bundesbeauftragten für den Datenschutz durch die besagte unabhängige Einrichtung zu überprüfen sind. Nicht unerwartet antwortete mir das Innenministerium kurz darauf, dass der Staatsvertrag bereits im Rahmen der Föderalismuskommission ausverhandelt worden sei; Änderungen seien nicht mehr möglich. Unter den Vertragspartnern bestehe jedoch Einigkeit, dass auch Datenschutzstandards einzuhalten sind. Das mag aufgrund des geltenden Rechts so sein. Dennoch meine ich, dass im Staatsvertrag eine Chance vertan wurde, den Datenschutz auch „offiziell“ zum Maßstab für die Standardisierungsarbeit des IT-Planungsrats zu machen und außerdem dafür zu sorgen, dass datenschutzoptimierte IT-Standards durch entsprechende Festlegungen marktfähig werden können. Ähnlich haben dies auch die Datenschutzbeauftragten von Bund und Ländern gesehen (vgl. Entschließung vom 8./9. Oktober 2009, Anhang 26). Dass es auch verfassungsrechtliche Zweifel an dem Konstrukt des IT-Planungsrats gibt, sei nur am Rande erwähnt. Immerhin wird auf dieses Bund-Länder-Gremium eine relativ unbestimmte, generelle Steuerungskompetenz übertragen, die nicht nur zu Lasten überstimmter Länder gehen, sondern im Einzelfall durchaus auch grundrechtssensible Bereiche erfassen kann.

Inhaltsverzeichnis des Anhangs

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder:

Anhang 1

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. April 2008

Berliner Erklärung:
Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts

Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste Quantensprung der Informationstechnik steht unmittelbar bevor: Die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nichtöffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoringverfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zu Schulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, 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.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und -sparsamkeit Rechnung getragen werden.

Anhang 2

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. März 2009

Defizite beim Datenschutz jetzt beseitigen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Deutschland auf, endlich die nötigen Konsequenzen aus den nicht mehr abreißenden Datenskandalen zu ziehen. Dazu sind mindestens folgende Schritte geboten:

1. Der Deutsche Bundestag wird aufgefordert, noch in dieser Legislaturperiode die von der Bundesregierung vorgelegten Gesetzentwürfe für erste notwendige Korrekturen des Bundesdatenschutzgesetzes im Bereich der Auskunfteien und des Adresshandels zu verabschieden. Ansonsten verlieren die Bürgerinnen und Bürger das Vertrauen in die Zusagen der Bundesregierung nach den Skandalen des Jahres 2008. Insbesondere mit Adressen darf nur noch mit ausdrücklicher Einwilligung der Betroffenen Handel getrieben werden. Der Entwurf für ein Datenschutzauditgesetz muss gründlich überarbeitet werden, damit dieser notwendige Schritt hin zu einem modernen Datenschutzrecht von der Praxis auch umgesetzt werden kann.

2. Mit Beginn der nächsten Legislaturperiode muss endlich eine grundlegende Modernisierung des Datenschutzrechts in Angriff genommen werden, die bereits zu lange aufgeschoben wurde. Nur so kann das Datenschutzrecht den Herausforderungen der Informationsgesellschaft zu Beginn des 21. Jahrhunderts gerecht werden.

3. Der Einsatz datenschutzfreundlicher Technik muss vorangetrieben und rechtlich verpflichtend vorgeschrieben werden. Darin liegt auch eine Chance für den Wirtschaftsstandort Deutschland in Zeiten der Krise.

Anhang 3

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. Oktober 2009

Aktueller Handlungsbedarf beim Datenschutz
– Förderung der Datenschutzkultur

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er-Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

- Das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z. B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;
- die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;
- ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;
- die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;
- die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;
- auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z. B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;
- im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;
- die Videoüberwachung in Staat und Gesellschaft einzuschränken;
- den Schutz der Meldedaten zu verbessern;
- ein praktikables Datenschutzaudit zu schaffen;
- die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

Anhang 4

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. April 2008

Mehr Augenmaß bei der Novellierung des BKA-Gesetzes

Der vom Bundesministerium des Innern erarbeitete Referentenentwurf eines Gesetzes zur Abwehr des internationalen Terrorismus durch das Bundeskriminalamt hat zum Ziel, das Bundeskriminalamt mit umfassenden polizeilichen Befugnissen zur Verhütung von terroristischen Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit in diesem Zusammenhang auszustatten. Insbesondere sind Befugnisse zur Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung vorgesehen. Außerdem will das Bundesinnenministerium eine Befugnis zum heimlichen Zugriff auf informationstechnische Systeme („Online-Durchsuchung“) in das BKA-Gesetz aufnehmen.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d. h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits, zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.

Dem Referentenentwurf zufolge soll die Aufgabenwahrnehmung durch das Bundeskriminalamt die Zuständigkeit der Landespolizeibehörden auf dem Gebiet der Gefahrenabwehr unberührt lassen. Dies führt zu erheblichen datenschutzrechtlichen Problemen, da nach geltendem Recht auch die Länder bei Abwehr einer durch den internationalen Terrorismus begründeten Gefahr parallele Abwehrmaßnahmen ergreifen können. Angesichts der Weite der für das Bundeskriminalamt vorgesehenen und den Landespolizeibehörden bereits eingeräumten Datenerhebungs- und Datenverarbeitungsbefugnisse steht zu befürchten, dass es zu sich überlappenden und in der Summe schwerwiegenderen Eingriffen in das informationelle Selbstbestimmungsrecht Betroffener durch das Bundeskriminalamt und die Landespolizeibehörden kommen wird.

Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z. B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes.

Das Bundesverfassungsgericht hat in seinem Urteil zur „Online-Durchsuchung“ vom 27. Februar 2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur „Online-Durchsuchung“, sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln.

Anhang 5

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. April 2008

Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet mit Sorge, dass die Datenschutzrechte der Bürgerinnen und Bürger im Rahmen der internationalen Zusammenarbeit der Sicherheitsbehörden immer häufiger auf der Strecke bleiben. Aktuelles Beispiel ist das am 11. März 2008 paraphierte deutsch-amerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität. Die Konferenz fordert Bundestag und Bundesrat auf, dem Abkommen so lange nicht zuzustimmen, bis ein angemessener Datenschutz gewährleistet ist.

Mit dem Abkommen wurde ein gegenseitiger Online-Zugriff auf Fundstellendatensätze von daktyloskopischen Daten und DNA-Profilen im hit/no-hit-Verfahren nach dem Muster des Prümer Vertrages vereinbart. Zudem wurden dessen Regelungen über den Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten weitgehend übernommen. Eine Übertragung des als Bedingung für diese umfangreichen Zugriffs- und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregimes erfolgte jedoch nicht.

Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terrorismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind, wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Datenübermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hintergrund sind die im Abkommen enthaltenen weiten Öffnungsklauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.

Anhang 6

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. April 2008

Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten

1. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.

2. Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer „elektronischen Ausforschung“ schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hiermit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government- und E-Commerce-Verfahren herzustellen.

3. Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.

4. Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste aus.

5. Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.

6. Auch wenn Online-Durchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Online-Durchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenüber steht.

7. Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:

   – Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Artikel 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.

- Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.
- Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.
- Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.
- Für die Durchführung von „Quellen-Telekommunikationsüberwachungen“, die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.

8. Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstechnische Systeme, z. B. bei der Überwachung der Telekommunikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.

Anhang 7

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. April 2008

Keine Vorratsspeicherung von Flugpassagierdaten

Die EU-Kommission hat den Entwurf eines Rahmenbeschlusses des Rates zur Speicherung von Flugpassagierdaten und zu deren Weitergabe an Drittstaaten vorgelegt. Künftig sollen die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast insgesamt 19 Datenelemente, bei unbegleiteten Minderjährigen sechs weitere Datenelemente, an eine von dem jeweiligen Mitgliedstaat bestimmte „Zentralstelle“ übermitteln. Die Daten sollen bei den Zentralstellen anlass- und verdachtsunabhängig insgesamt 13 Jahre lang personenbezogen gespeichert werden und zur Durchführung von Risikoanalysen dienen. Unter im Einzelnen noch unklaren Voraussetzungen sollen die Daten an Strafverfolgungsbehörden von Nicht-EU-Staaten (z. B. die USA) übermittelt werden dürfen. Neben Grunddaten zur Person, über Reiseverlauf, Buchungs- oder Zahlungsmodalitäten und Sitzplatzinformationen sollen auch andere persönliche Angaben gespeichert werden. Unklar ist, welche Daten unter „allgemeine Hinweise“ gespeichert werden dürfen. Denkbar wäre, dass beispielsweise besondere Essenswünsche erfasst werden.

Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und -Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Artikel 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe „ins Blaue hinein“, also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr, sind unzulässig.

Der Vorschlag für den Rahmenbeschluss erfolgte, ohne den Nutzen der erst jüngst in nationales Recht umgesetzten Richtlinie 2004/82/EG[5], die bereits alle Beförderungsunternehmen verpflichtet, die Daten von Reisenden an die Grenzkontrollbehörden zu übermitteln, auszuwerten. Hinzu kommt, dass der Vorschlag kaum datenschutzrechtliche Sicherungen enthält. Er bezieht sich nur auf eine bisher nicht bestehende und im Entwurf mit Mängeln behaftete EU-Datenschutzregelung. Diese Mängel wirken sich dadurch besonders schwerwiegend aus, dass in den Drittstaaten ein angemessenes Datenschutzniveau nicht immer gewährleistet ist und eine Änderung dieser Situation auch in Zukunft nicht zu erwarten ist.

Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen und des Europäischen Datenschutzbeauftragten sowie der Artikel 29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.

[5] RL 2004/82 EG v. 29. April 2004 Amtsbl. L 261 (2004) S. 24 ff., Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die Beförderten zu übermitteln.

Anhang 8

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 6./7. November 2008

Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. „Schwedische Initiative“) vom 18. Dezember 2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der „Schwedischen Initiative“ verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

- Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln,
- eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,
- Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,
- Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,
- normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,
- vollständige Umsetzung der Datenschutzbestimmungen in Artikel 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,
- normenklare Bestimmung, welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,
- normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.

Anhang 9

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 6./7. November 2008

Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich

Auf europäischer Ebene ist eine Vielzahl von Vorhaben beschlossen bzw. initiiert worden, die in ihrer Gesamtheit zu erheblichen Eingriffen in die Persönlichkeitsrechte führt:

- Die Telekommunikationsunternehmen in den Mitgliedstaaten der EU sind verpflichtet, die bei der Nutzung öffentlich zugänglicher Telekommunikationsdienste anfallenden Verkehrsdaten über das Kommunikationsverhalten der Einzelnen für die Sicherheitsbehörden ohne konkreten Anlass auf Vorrat zu speichern.
- Die Pässe der Bürgerinnen und Bürger der EU-Mitgliedstaaten werden mit biometrischen Merkmalen ausgestattet.
- Fluggastdaten (PNR) werden in die USA übermittelt, um sie den dortigen Behörden zur Verfügung zu stellen. Die Nutzung von Fluggastdaten zu Strafverfolgungszwecken wird auch in der Europäischen Union vorbereitet.
- Der Vertrag von Prüm, der in den Rechtsrahmen der Union überführt wird, ermöglicht den Polizei- und Strafverfolgungsbehörden der Mitgliedstaaten einen gegenseitigen Zugriff auf Fingerabdruck-, DNA- und Kfz-Daten.
- Es soll ein Europäisches Strafregisterinformationssystem geschaffen werden, mit dem Informationen über strafrechtliche Verurteilungen zwischen den Mitgliedstaaten ausgetauscht werden können.
- Das Schengener Informationssystem wird weiter ausgebaut, u. a. durch die Speicherung von biometrischen Merkmalen. Zudem wird der Kreis der Nutzer erweitert um das Europäische Polizeiamt EUROPOL und die Einheit für justizielle Zusammenarbeit in der EU (EUROJUST).
- Ein Europäisches Visa-Informationssystem (VIS) wird eingeführt, um den Austausch von Visa-Daten zwischen den Mitgliedstaaten zu erleichtern. Auch für EUROPOL, die Sicherheitsbehörden und die Nachrichtendienste soll dieser Datenbestand zugänglich sein.
- Das europäische Verfahren EURODAC, in dem die Fingerabdrücke von Asylbewerberinnen und Asylbewerbern gespeichert sind, soll auch von der Polizei und den Strafverfolgungsbehörden genutzt werden können.
- Der Aufgabenbereich von EUROPOL soll über die Bekämpfung der Organisierten Kriminalität hinaus auch auf andere Formen der schweren Kriminalität erweitert werden. Außerdem soll EUROPOL erstmals die Befugnis erhalten, Daten auch von privaten Stellen entgegenzunehmen und Zugriff auf alle polizeilich relevanten Datenbanken in der EU bekommen.
- Der Informationsaustausch zwischen den Strafverfolgungsbehörden der EU wird entsprechend dem Rahmenbeschluss des Rates vom 18. Dezember 2006 („Schwedische Initiative“) ausgebaut. Danach soll der Austausch verfügbarer Daten innerhalb der EU zu den gleichen Bedingungen erfolgen wie nach nationalem Recht.

Neben diesen Vorhaben gibt es zudem Abkommen auf bilateraler Ebene zwischen EU-Mitgliedstaaten und Drittstaaten, wie z. B. das Abkommen der Bundesrepublik Deutschland mit den Vereinigten Staaten für einen erweiterten Informationsaustausch zwischen den Sicherheitsbehörden.

Der Aufbau zentraler Datenbestände und der Ausbau der grenzüberschreitenden Datenübermittlung greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung ein und führen dadurch zu Gefahren für jede Einzelne und jeden Einzelnen. Diese werden noch gesteigert durch die angestrebte Verknüpfbarkeit der bestehenden und geplanten Datenbanken.

Umso wichtiger ist deshalb ein hoher und gleichwertiger Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Europa. Dies wurde von den Datenschutzbeauftragten auf nationaler und europäischer Ebene mehrfach angemahnt. Der hierzu im Oktober 2005 vorgelegte Rahmenbeschluss-Vorschlag genügt diesen Anforderungen nicht (siehe dazu die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 „Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen“). Zur Wahrung des erforderlichen Gleichgewichts zwischen Freiheit und Sicherheit sollten die Parlamente und Regierungen ihre Einflussmöglichkeiten bei europäischen Vorhaben stärker nutzen und dabei auch datenschutzrechtliche Aspekte einbringen. Wie notwendig ein angemessener Datenschutz ist, hat sich beim Verfahren der Aufnahme Verdächtiger in die so genannte EU-Terrorliste gezeigt, das durch den Europäischen Gerichtshof für rechtswidrig erklärt wurde.

Die Datenschutzbeauftragten fordern deshalb:

– Bei jeder neuen Initiative ist das Verhältnismäßigkeitsprinzip zu wahren und deren Auswirkung auf das bestehende System von Eingriffsmaßnahmen zu berücksichtigen.

– Im Hinblick auf den Kumulationseffekt sind die verschiedenen europäischen Initiativen zudem grundrechtskonform aufeinander abzustimmen. Redundanzen und Überschneidungen müssen verhindert werden.

– Ein Rechtsakt muss unverzüglich beschlossen werden, der über den Rahmenbeschlussvorschlag hinaus einen hohen und gleichwertigen Datenschutzstandard bei der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit verbindlich vorschreibt. Die gesamte nationale und grenzüberschreitende Informationsverarbeitung in diesem Bereich muss davon erfasst sein, um ein einheitliches Datenschutzniveau in den EU-Mitgliedstaaten zu gewährleisten.

– Ein unabhängiges, beratendes Datenschutzgremium sowie eine unabhängige und umfassende datenschutzrechtliche Kontrolle müssen für die polizeiliche und justizielle Zusammenarbeit eingerichtet bzw. gewährleistet werden.

Anhang 10

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 6./7. November 2008

Abfrage von Telekommunikationsverkehrsdaten einschränken:
Gesetzgeber und Praxis müssen aus
wissenschaftlichen Erkenntnissen Konsequenzen ziehen

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100 g, 100 h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotenzial in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10.200 (2002) auf 40.000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.

Das Bundesministerium der Justiz hat die Studie erst im Februar dieses Jahres und somit nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung im Gesetz vom 21. Dezember 2007 erforderlich gewesen wäre. Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch die Studie in ihrer schon früher geäußerten Kritik (vgl. ihre Entschließung vom 8./9. März 2007) bestätigt. Sie fordern den Gesetzgeber auf, die gesetzliche Regelung unter folgenden Aspekten nun zügig nachzubessern:

- Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.
- Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.
- Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der Strafprozessordnung vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z. B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.
- Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.
- Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 % der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und

Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substantiierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grundrechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen – trotz hoher Belastungen in der Praxis – unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können. Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen.

Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage ist – unter den neuen rechtlichen Rahmenbedingungen und aufgrund der Weiterentwicklung der Technik – unerlässlich. Insbesondere sollten dabei Notwendigkeit und Nutzen der Verkehrsdatenabfrage – auch im Vergleich zu anderen möglichen Maßnahmen – mit Blick auf den Verhältnismäßigkeitsgrundsatz auf den Prüfstand gestellt werden.

Anhang 11

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. März 2009

Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage

Die Speicherung von Daten im polizeilichen Informationssystem INPOL durch die Polizeien des Bundes und der Länder ist nur dann rechtmäßig, wenn eine Rechtsverordnung gemäß § 7 Abs. 6 Bundeskriminalamtsgesetz das Nähere über die Art der Daten bestimmt, die in dieser Datei gespeichert werden dürfen. Eine solche Rechtsverordnung existiert nicht. Mit Urteil vom 16. Dezember 2008 (Az. 11 LC 229/08) hat das Niedersächsische Oberverwaltungsgericht dies in Bezug auf die Verbunddatei „Gewalttäter Sport“ bekräftigt. Das Urteil ist nicht nur für die Rechtmäßigkeit der Hooligan-Datei bedeutsam, sondern hat Auswirkung auf alle im Rahmen von INPOL geführten Verbunddateien.

Mit der Entscheidung des Gerichts wird die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt. Die vom Bundesministerium des Innern bisher vertretene Auffassung, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, wird durch die einschlägigen Regelungen nicht gestützt.

Ohne eine derartige Rechtsverordnung ist die Gesamtheit der in Verbunddateien stattfindenden polizeilichen Datenverarbeitungen rechtswidrig. Die Datenschutzbeauftragten von Bund und Länder fordern das Bundesministerium des Innern und die Landesregierungen auf, unverzüglich daraus Konsequenzen zu ziehen und die polizeiliche Datenverarbeitung auf den Prüfstand zu stellen.

Anhang 12

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. Oktober 2009

Kein Ausverkauf von europäischen Finanzdaten an die USA!

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglichkeiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungs wegen verwehrt sind.

Ein derartiger weit reichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachtes wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig. Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängige Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

Im Übrigen bestehen bereits an der Notwendigkeit eines so weit reichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebliche Zweifel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

Anhang 13

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. Oktober 2009

Datenschutzdefizite in Europa auch nach Stockholmer Programm

Die Europäische Union will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem „Europa der Bürger". Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von zum Teil äußerst eingriffsintensiven Maßnahmen, wie z. B. ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

- Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.
- Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.
- Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.
- Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.
- Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen – auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL und EUROJUST – im weiteren Verfahren einzusetzen.

Anhang 14

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 6./7. November 2008

Elektronische Steuererklärung sicher und datenschutzgerecht gestalten

Mit dem Steuerbürokratieabbaugesetz (BR-Drs. 547/08) sollen u. a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Abs. 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Abs. 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens anstelle der qualifizierten elektronischen Signatur ein so genanntes anderes sicheres Verfahren im Benehmen mit dem Bundesinnenministerium zuzulassen oder sogar auf beide Verfahren vollständig zu verzichten. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalausweises möglich sein soll.

Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der Abgabenordnung zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronisch übermittelten Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1. Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit alternativlos.

2. Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.

3. Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

Anhang 15

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. März 2009

Auskunftsanspruch der Steuerpflichtigen
im Besteuerungsverfahren gewährleisten!

Das Bundesministerium der Finanzen (BMF) hat mit einer einfachen Verwaltungsanweisung den Auskunftsanspruch der Bürgerinnen und Bürger im Besteuerungsverfahren weitgehend eingeschränkt. Es macht die Auskunftserteilung von einem „berechtigten Interesse“ abhängig, was zu einer Einschränkung des Auskunftsrechts führt.

Die Vorgehensweise des BMF steht im krassen Widerspruch zum Beschluss des Bundesverfassungsgerichts vom 10. März 2008 (1 BvR 2388/03). Danach sind auch von der Finanzverwaltung die Grundrechte auf informationelle Selbstbestimmung und auf effektiven Rechtsschutz zu gewährleisten. Der in § 19 Bundesdatenschutzgesetz (BDSG) verankerte umfassende Auskunftsanspruch findet auch im Besteuerungsverfahren unmittelbare Anwendung.

Es ist inakzeptabel, dass verfassungsrechtlich garantierte Auskunftsrechte der Steuerpflichtigen ausgehebelt werden. Auch die Finanzverwaltung ist an Recht und Gesetz gebunden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

Anhang 16

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. April 2008

Keine Daten der Sicherheitsbehörden an Arbeitgeber
zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Übermittlung polizeilicher und nachrichtendienstlicher Erkenntnisse an Arbeitgeber zur Überprüfung von Bewerberinnen und Bewerbern, Beschäftigten und Fremdpersonal (z. B. Reinigungskräfte) außerhalb gesetzlicher Grundlagen. In zunehmendem Maß bitten Arbeitgeber die Betroffenen, in eine Anfrage des Arbeitgebers bei der Polizei oder dem Verfassungsschutz zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft („fremdbestimmte Selbstauskunft") selbst einholen und ihrem Arbeitgeber vorlegen. Eine solche „Einwilligung des Betroffenen" ist regelmäßig keine wirksame Einwilligung. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes ausgesetzt.

Die gesetzliche Grundentscheidung, in einem „Führungszeugnis" dem Arbeitgeber nur ganz bestimmte justizielle Informationen zu einer Person verfügbar zu machen, wird dadurch unterlaufen. Es stellt einen Dammbruch dar, wenn jeder Arbeitgeber durch weitere Informationen direkt oder indirekt an dem Wissen der Sicherheitsbehörden und Nachrichtendienste teilhaben kann. Die Übermittlung dieser Informationen an Arbeitgeber kann auch den vom Bundesarbeitsgericht zum „Fragerecht des Arbeitgebers" getroffenen Wertentscheidungen widersprechen. Danach darf der Arbeitgeber die Arbeitnehmerinnen und Arbeitnehmer bei der Einstellung nach Vorstrafen und laufenden Ermittlungsverfahren fragen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert.

Polizei und Nachrichtendienste speichern – neben den in ein „Führungszeugnis" aufzunehmenden Daten – auch personenbezogene Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden oder Arbeitgebern in einem „Führungszeugnis" nicht übermittelt werden dürfen. Es stellt eine grundsätzlich unzulässige Durchbrechung des Zweckbindungsgrundsatzes dar, wenn ein Arbeitgeber diese Daten – über den Umweg über die Polizei oder einen Nachrichtendienst – für Zwecke der Personalverwaltung erhält. Dabei ist besonders zu beachten, dass polizeiliche oder nachrichtendienstliche Daten nicht zwingend gesicherte Erkenntnisse sein müssen, sondern oftmals lediglich Verdachtsmomente sind. Die Folgen von Missdeutungen liegen auf der Hand.

Anhang 17

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. April 2008

Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft“ gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z. B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle

Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.

Anhang 18

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 6./7. November 2008

Adress- und Datenhandel nur mit Einwilligung der Betroffenen

Der auf dem „Datenschutzgipfel“ im September 2008 gefundene Konsens, den Adress- und Datenhandel zukünftig nur auf der Grundlage einer Einwilligung zuzulassen, ist in Politik und Gesellschaft auf breite Zustimmung gestoßen. Nur eine solche Lösung respektiert das informationelle Selbstbestimmungsrecht und damit die Wahlfreiheit der Verbraucherinnen und Verbraucher. Wer davon jetzt abrücken will, verkennt die aufgrund der jüngsten Datenskandale ans Licht gekommenen Missstände, deren Ursache nicht nur in der kriminellen Energie Einzelner zu suchen ist. Um die Daten der Betroffenen tatsächlich wirksam schützen zu können, muss die Wahlmöglichkeit der Menschen von Maßnahmen flankiert werden, die die Herkunft der Daten jederzeit nachvollziehbar macht.

Die von der Werbewirtschaft gegen die Einwilligungslösung ins Feld geführten Argumente sind nicht überzeugend. Die behaupteten negativen Folgen für den Wirtschaftsstandort sind nicht zu belegen. Unabhängig davon gilt: Es gibt keine schutzwürdigen Interessen für die Beibehaltung von Geschäftsmodellen, die darauf beruhen, hinter dem Rücken und ohne Information der Betroffenen mit deren Daten Handel zu treiben. Die Einführung des Einwilligungsprinzips würde im Gegenteil zielgenaueres und wirksameres Direktmarketing erlauben. Die Bundesregierung sollte sich deshalb nicht von ihrer Absicht abbringen lassen, die beim „Datenschutzgipfel“ gegebenen Zusagen zur schnellen Verbesserung des Datenschutzes einzulösen. Sie würde es sonst versäumen, die notwendigen Lehren aus den jüngsten Skandalen zu ziehen. Der Referentenentwurf des Bundesinnenministeriums zur Änderung des Bundesdatenschutzgesetzes im Bereich des Adress- und Datenhandels (Stand: 22. Oktober 2008) zieht mit der Einwilligungslösung – bei aller Verbesserungswürdigkeit im Detail – die einzig richtige und notwendige Konsequenz aus den zahlreichen Datenskandalen und darf nicht verwässert werden.

Anhang 19

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. März 2009

Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz

Datenskandale der letzten Zeit haben deutlich gemacht, dass bei der Verarbeitung von Beschäftigtendaten weder Transparenz noch Rechtssicherheit besteht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, nach jahrelanger Untätigkeit jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen.

Ziel des neuen Beschäftigtendatenschutzgesetzes muss sein, Rechtssicherheit herzustellen, Regelungslücken zu schließen und bereits vorhandene Regelungsaspekte sowie Vorgaben der Rechtsprechung in einem Spezialgesetz zusammenzufassen. Die Konferenz der Datenschutzbeauftragten hält deshalb vor allem folgende Eckpunkte für unverzichtbar:

- Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.
- Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festlegungen im Hinblick auf Gesundheitsdaten (u. a. zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen, etc.).
- Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z. B. der Innenrevision auf erhobene Personaldaten bedarf enger gesetzlicher Vorgaben.
- Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da die Nutzung von Telefon, Internet und E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kommunikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand ggf. Dritte (z. B. Mitarbeitervertretungen oder Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.
- Der Einsatz von Überwachungssystemen, wie z. B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.
- Es bedarf der Festlegung der Rechte der Beschäftigten, z. B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.
- Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.
- Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.
- Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch gewonnenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

Anhang 20

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. April 2008

Medienkompetenz und Datenschutzbewusstsein
in der jungen „online-Generation“

1. Die Nutzung moderner Informationssysteme ist auch mit Risiken verbunden. Diese begründen ein besonderes Schutzbedürfnis der Bürgerinnen und Bürger. Dieses verlangt aber nicht nur rechtliche Vorkehrungen und Sicherungen, sondern auch Aufklärung und Information darüber, mit welchen Risiken die Nutzung dieser Informationssysteme verbunden sind. Dies gilt vor allem für die junge „online-Generation“, die in der Altersgruppe der 14- bis 19-Jährigen zu 96 % regelmäßig das Internet nutzt, und zwar im Durchschnitt länger als zweieinhalb Stunden täglich.

2. Die Datenschutzbeauftragten des Bundes und der Länder sehen es daher als wichtige Aufgabe an, Kinder und Jugendliche für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den Daten anderer zu sensibilisieren. Diese Aufgabe obliegt gesellschaftlichen Einrichtungen ebenso wie staatlichen Organen.

   Die Erfahrungen, die anlässlich des 2. Europäischen Datenschutztages am 28. Januar 2008 gemacht wurden, stützen dies. Zu dem Motto „Datenschutz macht Schule“ wurde von den Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl von Veranstaltungen und Schulbesuchen organisiert. Eltern, Lehrkräfte, Schülerinnen und Schüler, aber auch Studierende hatten dabei die Möglichkeit, sich z. B. bei Podiumsdiskussionen, Rollenspielen und Workshops über datenschutzrelevante Fragen bei der Nutzung moderner Medien zu informieren. Die dabei gewonnenen Erfahrungen lassen nicht nur einen enormen Informationsbedarf, sondern auch ein großes Informationsinteresse erkennen, und zwar bei allen Beteiligten, bei den Jugendlichen ebenso wie bei ihren Eltern und den Lehrkräften.

   Bei den Informationsangeboten, die derzeit den Schulen angeboten werden, um die Medienkompetenz junger Menschen zu verbessern, spielt das Thema „Datenschutz“ aber nur eine untergeordnete Rolle. Es beschränkt sich überwiegend auf Fragen der Datensicherheit und wird zudem häufig von Fragen des Jugendmedienschutzes und des Verbraucherschutzes überlagert.

3. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für notwendig, dass die für die schulische Bildung zuständigen Ministerinnen und Minister der Landesregierungen bei der Förderung der Medienkompetenz von Kindern und Jugendlichen – schon im Grundschulalter – deren Datenschutzbewusstsein stärken. Der Datenschutz muss bei den Angeboten und Projekten zur Förderung der Medienkompetenz eine größere Rolle spielen. Die bisherigen Ansätze reichen bei weitem nicht aus. Gerade bei jungen Menschen muss das Bewusstsein über den Datenschutz als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker gefördert werden.

Anhang 21

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 6./7. November 2008

Mehr Transparenz durch Informationspflichten bei Datenschutzpannen

In den letzten Monaten hat eine Reihe von gravierenden Datenschutzverstößen die Aufmerksamkeit der Öffentlichkeit und der Medien gefunden. In vielen dieser Fälle lag der Verlust oder Missbrauch personenbezogener Daten längere Zeit zurück und war der verantwortlichen Stelle bekannt, ohne dass die Betroffenen oder die zuständige Datenschutzaufsichtsbehörde hierüber informiert worden wären. Dadurch wurde ihnen die Möglichkeit genommen, Sicherheitsmaßnahmen zu ergreifen und mögliche Schäden zu begrenzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt deswegen die Forderung, alle verantwortlichen Stellen – grundsätzlich auch alle öffentlichen Stellen – gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen. Hinter diesem Interesse hat der Wunsch der entsprechenden Stellen zurückzustehen, solche Vorkommnisse geheim zu halten, um keinen Imageschaden oder keine wirtschaftlichen Nachteile zu erleiden.

Etliche Staaten haben bereits entsprechende Regelungen. Eine solche Informationspflicht würde die Transparenz erhöhen und das Vertrauen der Betroffenen in eine korrekte Datenverarbeitung stärken. Darüber hinaus würde sie einen wichtigen Anstoß geben, mehr für Datenschutz und Datensicherheit zu tun.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, entsprechende umfassende Informationspflichten für Unternehmen und öffentliche Stellen im Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zu schaffen. Die übrigen aus Anlass der Datenschutzskandale in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008 erläuterten Forderungen zur Novellierung des Bundesdatenschutzgesetzes werden bekräftigt.

Anhang 22

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 6./7. November 2008

Datenschutzgerechter Zugang zu Geoinformationen

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potenzial an volkswirtschaftlichem Nutzen und ist geeignet, vielen E-Government- und E-Commerce-Anwendungen die erforderliche Infrastruktur zur Verfügung zu stellen. Als einen ersten Schritt regelt das europäische Recht mit der so genannten INSPIRE-Richtlinie, die bis Mai 2009 in nationales Recht umgesetzt werden muss, die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben aufgrund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer bzw. Standortdaten als personenbezogene Daten zur Verfügung gestellt. Diesem Umstand müssen die gesetzlichen Regelungen gerecht werden und angemessene Datenschutzregelungen enthalten.

Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (BT-Drs. 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das Umweltinformationsgesetz ist nach Ansicht der Konferenzen der Datenschutz- und der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb nicht interessengerecht. Ein Geodatenzugangsgesetz muss einen differenzierenden Ausgleich zwischen Informations- und Schutzinteressen für die spezielle Problematik der Geobasis- und der Geofachdaten vornehmen. Es ist insbesondere zu berücksichtigen, dass nach der INSPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

Anhang 23

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 6./7. November 2008

Gegen Blankettbefugnisse für die Software-Industrie

Gegenwärtig wird auf europäischer Ebene über Änderungen der Richtlinie zum Datenschutz in der elektronischen Kommunikation (2002/58/EG) beraten. Dabei geht es auch um die Frage, ob in Zukunft einzelfallunabhängig Verkehrsdaten zur Gewährleistung der Netz- und Informationssicherheit, also etwa zur Verfolgung von Hackerangriffen, verarbeitet werden dürfen.

Bereits auf der Grundlage der geltenden Richtlinie erlaubt § 100 Telekommunikationsgesetz den Telekommunikationsdiensteanbietern eine zielgerichtete, einzelfallbezogene Datenverarbeitung zur Fehlerbeseitigung und Missbrauchsbekämpfung. Diese Regelung hat sich in der Praxis bewährt. Es ist daher nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.

Obwohl die Europäische Kommission eine Änderung der bisherigen Rechtslage nicht für erforderlich hält, schlagen mehrere Mitgliedstaaten bei den gegenwärtigen Beratungen im Rat vor, entsprechend den Vorstellungen der Software-Industrie (Business Software Alliance) eine generelle Ermächtigung in die Richtlinie aufzunehmen, wonach *„jede natürliche oder juristische Person mit einem berechtigten Interesse“* berechtigt sein soll, Verkehrsdaten zu verarbeiten, um „technische Maßnahmen zur Gewährleistung der Sicherheit eines öffentlichen Telekommunikationsdienstes, eines öffentlichen oder privaten Telekommunikationsnetzes, eines Dienstes der Informationsgesellschaft oder von Endgeräten zu deren Nutzung“ zu ergreifen. Damit wäre nicht nur der jeweilige Diensteanbieter, der Maßnahmen zum Schutz des eigenen Angebots treffen will, zur einzelfallunabhängigen Speicherung von Verkehrsdaten berechtigt, sondern praktisch jeder mit einem wirtschaftlichen Verarbeitungsinteresse, insbesondere auch die Hersteller von Sicherheitssoftware.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt eine solche zeitlich unbegrenzte und inhaltlich unbestimmte Blankett-Ermächtigung als inakzeptabel ab. Der Hinweis auf die „Informationssicherheit“ rechtfertigt es nicht, dass Verkehrsdaten nahezu uferlos auch von Dritten verarbeitet werden. Die Bundesregierung wird aufgefordert, einer derartigen Aufweichung des Telekommunikationsgeheimnisses im Rat ihre Zustimmung zu verweigern.

Anhang 24

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 6./7. November 2008

Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten

Mit der Gesundheitsreform soll über die Einführung von Wettbewerbsmechanismen die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert werden. Die Kassen sind daher bemüht und auch vom Gesetzgeber gehalten, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und strukturierte Behandlungsprogramme für chronisch kranke Versicherte, die jedoch lediglich Angebotscharakter haben dürfen. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Diese Vorgaben werden von einzelnen Krankenkassen nicht beachtet, wenn sie versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen.

Um Teilnehmerinnen und Teilnehmer zu gewinnen und um Maßnahmen durchzuführen, bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutzrechtlich nach dem Sozialgesetzbuch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält die Einhaltung insbesondere der folgenden Eckpunkte bei gesundheitlichen Steuerungsprogrammen der Krankenkassen für unerlässlich:

- Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.
- Die erstmalige Kontaktaufnahme mit potenziell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.
- Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.
- Wenn Versicherte – zu welchem Zeitpunkt auch immer – eindeutig zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.

Anhang 25

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 6./7. November 2008

Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren

Die Bundesregierung hat am 25. Juni 2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492). Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an die Zentrale Speicherstelle zu dulden, obwohl zurzeit nicht verlässlich abgeschätzt werden kann, in welchem Umfang die Speicherung der Daten tatsächlich erforderlich ist. Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substantiierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.

Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des technisch-organisatorischen Datenschutzes noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

- Es muss sichergestellt werden (z. B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauftragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.
- Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.
- Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver- und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.
- Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.
- Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Löschungskonzept muss weiterentwickelt und umgesetzt werden.
- Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen.
- Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

Anhang 26

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. Oktober 2009

Staatsvertrag zum IT-Planungsrat –
Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die informationstechnische Kooperation von Bundes- und Landesbehörden zunehmend die Verarbeitung von personenbezogenen Daten betrifft, die durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen sind, etwa durch wirksame Verschlüsselungsverfahren.

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen.

Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrats teilnehmen soll. Sie hält es für geboten, auch die Landesdatenschutzbeauftragten einzubeziehen.

Anhang 27

Entschließung
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 seiner 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.

Anhang 28

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 8./9. Oktober 2009

Krankenhausinformationssysteme datenschutzgerecht gestalten!

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.

Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Artikel 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.

Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechende Systeme anzubieten.

Anhang 29

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 16. September 2008

Entschlossenes Handeln ist das Gebot der Stunde

Nie haben sich in der jüngeren Geschichte die Skandale um den Missbrauch privater Daten in der Wirtschaft so gehäuft wie heute und damit deutlich gemacht, dass nicht nur im Verhältnis Bürger-Staat das Grundrecht auf informationelle Selbstbestimmung bedroht ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt – zuletzt in ihrer Berliner Erklärung vom 4. April dieses Jahres – auf diese Gefahren hingewiesen, die von massenhaften Datensammlungen privater Unternehmen und ihrer unkontrollierten Nutzung ausgehen. Sie hat auch deshalb den Gesetzgeber zu einer grundlegenden Modernisierung und Verbesserung des Datenschutzrechts aufgefordert und eine neue Datenschutzkultur angemahnt.

Dass jetzt endlich im politischen und gesellschaftlichen Raum die Problematik erkannt und diskutiert wird, ist zu begrüßen. Dabei kann und darf es aber nicht bleiben, nur entschlossenes Handeln kann die Bürgerinnen und Bürger vor weiterem Missbrauch ihrer persönlichen Daten schützen und das verlorene Vertrauen wiederherstellen.

Das vom Grundgesetz garantierte Recht eines Jeden, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden, muss endlich die ihm gebührende Beachtung finden. Die Weitergabe von persönlichen Angaben zu Werbezwecken darf nur mit ausdrücklicher Einwilligung der Betroffenen zulässig sein. Daten sind mit einem Vermerk über ihre Quelle zu kennzeichnen. Der Abschluss von Verträgen darf nicht von der Einwilligung in die Datenübermittlung zu Werbezwecken abhängig gemacht werden. Verstöße gegen den Datenschutz dürfen nicht ohne Konsequenzen bleiben, sondern müssen strikt geahndet werden. Deshalb müssen die bestehenden Lücken in den Bußgeld- und Strafbestimmungen geschlossen und der Bußgeld- und Strafrahmen für Datenschutzverstöße deutlich erhöht werden. Diese Sofortmaßnahmen, die bereits Gegenstand des Spitzentreffens im Bundesministerium des Innern am 4. September 2008 waren, können vom Deutschen Bundestag noch in den bereits vorliegenden Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes aufgenommen werden.

Gesetzgeberische Maßnahmen allein helfen aber nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht sanktioniert werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, die Datenschutzaufsichtsbehörden endlich organisatorisch, personell und finanziell in die Lage zu versetzen, ihren Beratungs- und Kontrollaufgaben flächendeckend, unabhängig und wirkungsvoll nachkommen zu können, und entsprechend der EU-Datenschutzrichtlinie mit wirksamen Einwirkungsbefugnissen auszustatten, die sie bisher nicht haben.

Außerdem müssen Konzepte zur grundlegenden Modernisierung des Datenschutzes entwickelt und umgesetzt werden. Wichtige Themen sollten dabei noch in dieser Legislaturperiode angegangen werden:

- Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren
- Stärkung der datenschutzrechtlichen Auskunftsrechte
- Pflicht zur Information der betroffenen Personen und der Aufsichtsbehörden bei Datenpannen und missbräuchlicher Datennutzung
- Gewinnabschöpfung aus unbefugtem Datenhandel
- Einführung eines gesetzlich geregelten Datenschutzaudits, mit dem unabhängig und qualifiziert die Datenschutzkonformität von Verfahren und Produkten bestätigt wird
- Stärkung der betrieblichen Datenschutzbeauftragten als Organ der Selbstkontrolle

– Spezialisierung der Strafverfolgungsbehörden

– Anerkennung von Datenschutzbestimmungen als verbraucherschützende Normen

Nur wenn jetzt den Ankündigungen Taten folgen und entschlossen gehandelt wird, können die Bürgerinnen und Bürger künftig vor Datenmissbrauch und Verletzung ihres Grundrechts auf informationelle Selbstbestimmung besser als in der Vergangenheit geschützt werden.

Anhang 30

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 16. April 2009

Datenschutz beim vorgesehenen Bürgerportal unzureichend

Der Gesetzentwurf zur Regelung von Bürgerportalen (BR-Drs. 174/09) soll rechtliche Rahmenbedingungen für eine sichere und vertrauenswürdige elektronische Kommunikation zwischen Bürgerinnen und Bürgern und der Wirtschaft und Verwaltung im Internet schaffen. Private Anbieter sollen die Portale betreiben, über die der sichere E-Mail-Verkehr De-Mail, eine sichere Dokumentenablage De-Safe und ein Identitätsbescheinigungsdienst abgewickelt werden sollen. Eine solche Infrastruktur stellt hohe Anforderungen an die IT-Sicherheit und den Datenschutz.

Der Gesetzentwurf wird diesen Anforderungen noch nicht gerecht und ist zumindest in folgenden Punkten zu korrigieren:

– Der Entwurf sieht vor, dass nur akkreditierte Anbieter Portale betreiben dürfen. Voraussetzung für die Akkreditierung darf nicht allein der Nachweis der technischen und administrativen Sicherheit, sondern muss auch die tatsächliche Einhaltung datenschutzrechtlicher Standards sein. Die dabei zu erfüllenden Mindestanforderungen müssen verbindlich im Gesetz vorgegeben werden. Portalbetreiber sollten zudem erst dann die Akkreditierung erhalten, wenn die Umsetzung dieser Anforderungen durch unabhängige Prüfstellen bescheinigt wurde.

– Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Diensteanbietern und durch die Sicherung des Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte gelesen oder verändert werden können. Deshalb muss die Kommunikation standardmäßig durch eine Ende-zu-Ende-Verschlüsselung zwischen Absendenden und Empfangenden nach dem Stand der Technik gesichert und nicht nur als Option angeboten werden.

– Das Bürgerportal soll gerade zwischen Bürgerinnen und Bürgern und Verwaltung eine rechtlich gesicherte Kommunikation ermöglichen. Insbesondere sind über das Bürgerportal förmliche Zustellungen mit den entsprechenden Rechtsfolgen beabsichtigt. Dies darf nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort wird abgelehnt.

– Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. Das ermöglicht Angriffe durch Schadsoftware auf dem Rechner der Nutzenden. So könnten Zugangsdaten beschafft und widerrechtlich dazu verwendet werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern oder unberechtigt auf Daten im De-Safe zuzugreifen. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen.

– Die Möglichkeit, eine pseudonyme Bürgerportaladresse zu nutzen, muss – entgegen der Stellungnahme des Bundesrates vom 3. April 2009 – erhalten bleiben. Denn die pseudonyme Nutzung ermöglicht gerade einen sinnvollen Kompromiss zwischen hinreichender Identifizierbarkeit im Rechtsverkehr und Datenschutz für die Nutzerinnen und Nutzer.

– Die Nutzerinnen und Nutzer müssen bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen – etwa zur verbindlichen Kommunikation mit staatlichen Stellen – hingewiesen werden. Die Aufklärungs- und Informationspflichten müssen im Gesetzestext klarer als bislang geschehen gefasst werden. Gleiches gilt für die Feststellung von Identitätsdaten und der Aufdeckung von Pseudonymen.

– Eine Benachteiligung von Bürgerinnen und Bürgern, die über kein Bürgerportalkonto verfügen, muss ausgeschlossen werden. Auch dürfen Bürgerportale nicht dazu führen, dass staatliche Stellen dazu übergehen, bei jeder Inan-

spruchnahme einer E-Government-Anwendung eine persönliche Identifizierung zu verlangen, selbst wenn dies für die konkrete Dienstleistung nicht erforderlich ist.

– Der Entwurf sieht vor, dass grundsätzliche Fragen der technischen Ausgestaltung der Bürgerportale und der darüber angebotenen Dienste in einer Rechtsverordnung geregelt werden sollen. Dies widerspricht der Rahmenkonzeption des Artikel 80 GG und dient auch sonst nicht der Normenklarheit des Gesetzes. Zumindest die grundsätzlichen technisch-organisatorischen Anforderungen an die Eröffnung des Kontos, den Postfach- und Versanddienst, den Speicherplatz, den Identitätsbescheinigungsdienst und das Akkreditierungsverfahren sollten in das Gesetz selbst aufgenommen werden.

– Der Entwurf des Bürgerportalgesetzes sieht jetzt auch vor, dass nicht nur die Datenerhebung, sondern auch die Verarbeitung und Nutzung der erhobenen Daten durch den akkreditierten Diensteanbieter an eine enge Zweckbestimmung gebunden ist. Allerdings ist der pauschale Verweis auf die Regelungen des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes in diesem Zusammenhang zu weitgehend, da so für die Diensteanbieter die Möglichkeit eröffnet wird, die personenbezogenen Daten für Werbung oder Marktforschungszwecke zu nutzen. Die Bürgerinnen und Bürger müssen jedoch sicher sein können, dass ihre Daten ausschließlich zur Teilnahme am Bürgerportal genutzt werden.

Anhang 31

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 18. 02. 2009

Stärkung der IT-Sicherheit – aber nicht zu Lasten des Datenschutzes!

Das Bundeskabinett hat am 14. Januar 2009 den Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes beschlossen (BR-Drs. 62/09). Mit dem Gesetz sollen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) umfassende Befugnisse eingeräumt werden, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Weiter sollen aber zugleich auch das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG) geändert werden.

Angriffe auf die IT-Sicherheit können nicht nur die ordnungsgemäße Abwicklung von Verwaltungsaufgaben beeinträchtigen, sondern auch Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger mit sich bringen. Daher sind Konzepte zu entwickeln und umzusetzen, die sowohl die IT-Sicherheit stärken als auch den Schutz der Privatsphäre gewährleisten.

In weiten Bereichen wurden in der jüngsten Vergangenheit Maßnahmen zur Stärkung der IT-Sicherheit getroffen, die eine detaillierte Registrierung und Auswertung des Nutzerverhaltens und sogar der Inhalte der Kommunikation ermöglichen. Entsprechende Ansätze gibt es nun auch in der Bundesverwaltung. So sieht der Gesetzentwurf vor, dem BSI sehr weitgehende Befugnisse einzuräumen. Kritisch sind insbesondere

1. die Ermächtigung des BSI, die gesamte Sprach- und Datenkommunikation aller Unternehmen, Bürgerinnen und Bürger mit Bundesbehörden ohne Anonymisierung bzw. Pseudonymisierung zu überwachen und auszuwerten (§ 5),
2. die vorgesehene Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen werden (§ 5 Abs. 4) und
3. die fehlende Verpflichtung des BSI, Informationen über ihm bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Unternehmen, Bürgerinnen und Bürger vor (zu erwartenden) Angriffen (Spionage und Sabotage) zu warnen (§ 7).

Äußerst bedenklich ist darüber hinaus die Regelung, dass im Zweifelsfall allein das Bundesministerium des Innern entscheiden darf, ob Daten dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind und wie damit weiter zu verfahren ist (§ 5 Abs. 6). In solchen Zweifelsfällen sollten diese Daten gelöscht oder einem Richter zur Entscheidung vorgelegt werden.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen zwar grundsätzlich alle Aktivitäten, in den gewachsenen, vernetzten IT-Strukturen des Bundes das Niveau der IT-Sicherheit zu erhöhen. Sie fordern aber auch, dass die zur Risikobegrenzung eingeführten Maßnahmen nicht den Datenschutz der Nutzerinnen und Nutzer beeinträchtigen. Deshalb ist schon bei der Konzeption von IT-Sicherheitsmaßnahmen vorzusehen, dass das erforderliche Sicherheitsniveau nur mit datenschutzgerechten Lösungen gewährleistet wird. Die Datenschutzbeauftragten fordern strengere Sicherheitsstandards und soweit möglich die Protokoll- und Inhaltsdaten vor der Auswertung durch das BSI zu anonymisieren bzw. zu pseudonymisieren. Damit ließen sich eine unnötige Registrierung des Nutzerverhaltens und Überwachung von Kommunikationsinhalten vermeiden. Die Auswertung der Daten durch das BSI muss revisionssicher ausgestaltet werden. Der vorgelegte Gesetzentwurf enthält keine solchen Regelungen.

Die Gesetzesänderung des Telemediengesetzes böte öffentlichen und privaten Anbietern von Telemedien die Möglichkeit einer umfassenden Protokollierung des Surfverhaltens ihrer Nutzer im Internet, da sie entsprechend der Gesetzesbegründung weit auslegbar ist. Der Gesetzgeber muss unmissverständlich klarstel-

len, dass die Erhebung und Auswertung personenbezogener Daten ultima ratio ist.

Sowohl die Betreiber der „Netze des Bundes“ als auch die Verantwortlichen für die übergreifenden Netze der Verwaltung in Europa sind aufgefordert, bei allen Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und den Datenschutz der Nutzerinnen und Nutzer zu gewährleisten.