Landtag von Baden-Württemberg **Drucksache 13 / 4910**

13. Wahlperiode **01. 12. 2005**

Mitteilung

des Landesbeauftragten für den Datenschutz

Sechsundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

Schreiben des Landesbeauftragten für den Datenschutz in Baden-Württemberg vom 1. Dezember 2005:

Anbei übersende ich Ihnen unseren 26. Tätigkeitsbericht, der nach § 31 Abs. 1 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 1. Dezember 2005 zu erstatten ist.

Zimmermann

Eingegangen: 01. 12. 2005 / Ausgegeben: 15. 12. 2005

Drucksachen und Plenarprotokolle sind im Internet abrufbar unter: www.landtag-bw.de/Dokumente

Sechsundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

INHALTSVERZEICHNIS

Seite

1. Teil: Zur Situation 9

2. Teil: Öffentliche Sicherheit und Justiz 11

1. Abschnitt: Öffentliche Sicherheit 11
1. Die präventive Telekommunikationsüberwachung 11
2. Änderung des Landesverfassungsschutzgesetzes 13
3. Die Arbeitsdatei „Politisch motivierte Kriminalität“ 16
3.1 Keine Akten/Unterlagen vorhanden 16
3.2 Politische Motivation nicht belegt 17
3.3 Die sog. anderen Personen 18
3.4 Zu lange gespeichert 20
4. Einzelfälle 22
4.1 Btm-Hinweis gelöscht 22
4.2 Kein Sexualtäter 22
4.3 Eine Schreckschusspistole 23

2. Abschnitt: Justiz 24
1. Die Neuregelung der akustischen Wohnraumüberwachung 24
2. Die Neuregelung der forensischen DNA-Analyse 26
3. DNA-Analysen für Vaterschaftstests 28
4. Mangelnde Unterstützung des Landesbeauftragten für den Datenschutz ... 29
4.1 ... durch das Justizministerium 29
4.2 ... durch eine Staatsanwaltschaft 30
5. Angaben im Sichtfenster von Gerichtsschreiben 31

3. Teil: Gesundheit und Soziales 33

1. Abschnitt: Gesundheit 34
1. Die elektronische Gesundheitskarte 34
2. Das Landeskrebsregister 36
2.1 Wird es künftig zwei landesweite Krebsregister geben? 37
2.2 Erste Überlegungen des Sozialministeriums 37
2.3 Vereinbarung von Eckpunkten im März 2005 38
2.4 Erster Gesetzentwurf im November 2005 38
2.5 Gravierende Unzulänglichkeiten des ersten Gesetzentwurfs 38
3. Mammographie-Screening 41
4. Einzelfälle 42
4.1 Patientendaten in „Grüner Tonne“ 42
4.2 Patientengeheimnis zu wörtlich genommen 44
4.3 Gutachten in falschen Händen 45
4.4 Telefonieren und Fotografieren in einem Zentrum für Psychiatrie 46

Seite

4.5 Bestellung eines externen Datenschutzbeauftragten im Krankenhaus 47

5. Einschulungsuntersuchungen 49

2. Abschnitt: Die gesetzliche Krankenversicherung 51

1. Datenschutzverstoß führt zur Kündigung 51
2. Datenschutz für Versicherte endet nicht mit Büroschluss 52
3. Einschaltung externer Gutachter 53

3. Abschnitt: Soziales 53

1. Arbeitslosengeld II 53
   1.1 Antragsberatung im Einzelzimmer? Fehlanzeige! 55
   1.2 Verschwundene Antragsunterlagen 56
   1.3 Das Antragsformular zur Ortsabwesenheit 57
   1.4 Die Anfrage der Polizei 57
2. Sozialamt: Die Anfrage beim Finanzamt 58

4. Teil: Kommunales und anderes 59

1. Abschnitt: Kommunales 59

1. Kontrollbesuch beim Gutachterausschuss 59
2. Was hat der Fahrzeughalter mit der Kurtaxe zu tun? 61
3. Datenerhebung beim Schwimmbadbesuch 62

2. Abschnitt: Personalwesen 63

1. Streichkonzert mit ungefragter Stellensuche 63
2. Veröffentlichung von Personaldaten 64

3. Abschnitt: Schul- und Hochschulwesen 65

1. Evaluation an Schulen 65
2. PISA und IGLU 66
3. Zum weiteren rechtlichen Schicksal der Schülerindividualdatei 67
4. Veröffentlichung von Schülerfotos auf der Internet-Seite einer Schule 68
5. Einführung allgemeiner Studiengebühren 69
6. Nochmals: Zur Filterung von E-Mails 70

4. Abschnitt: Finanzen und Steuern 72

1. Kontendatenabrufe nach dem Gesetz zur Förderung der Steuerehrlichkeit 72
2. Warum müssen Finanzämter in Baden-Württemberg bundesweit auf sämtliche Lohnsteuerbescheinigungen zugreifen können? 73
   2.1 Das Verfahren ELSTER-Lohn 74
      2.1.1 Datenübertragung von Arbeitgebern an die Clearingstellen 74
      2.1.2 Verarbeitung innerhalb der Clearingstellen 74
      2.1.3 Landesspeicher (eSpeicher) 75

Seite

2.2 Die datenschutzrechtlichen Mängel 75

2.2.1 Unklarheit über datenschutzrechtliche Verantwortlichkeit für die Verarbeitung personenbezogener Daten in den Clearingstellen sowie den Landesspeichern 75

2.2.2 Fehlende Authentifizierung der Absender elektronischer Lohnsteuerbescheinigungen 76

2.2.3 Keine technische Beschränkung der Zugriffsmöglichkeiten 76

5. Abschnitt: Sonstiges 78

1. Die wissbegierige Fahrerlaubnisbehörde 78

2. Verarbeitung von Gewinnspieldaten ohne wirksame Einwilligung 78

3. Das Projekt MigVIS des Innenministeriums 79

4. Begehungsrecht und Geheimhaltungspflicht des Schornsteinfegers 81

5. Schornsteinfeger als Datenquelle? 82

5. Teil: Technik und Organisation 83

1. Entwicklungen in der IuK in den letzten Jahren 83

1.1 EDV-Einsatz in der Verwaltung 83

1.2 Neue Herausforderungen für den Datenschutz 83

2. RFID 85

2.1 Was leistet die RFID-Technik? 86

2.2 Die virtuelle Welt integriert vernetzte Gegenstände 86

2.3 Datenschutzrisiken der RFID-Technik 87

2.4 Datenschutzmaßnahmen bei RFID-Systemen, die unmittelbar zur Verarbeitung personenbezogener Daten dienen 88

2.5 Datenschutzmaßnahmen bei RFID-Systemen, die nicht unmittelbar zur Verarbeitung personenbezogener Daten dienen sollen 88

2.6 Generelle Datenschutzmaßnahmen bei RFID-Systemen 89

3. Dokumentenmanagementsysteme 89

4. eGovernment 90

4.1 Virtuelle Poststellen 90

4.2 Das Problem unklarer Zuständigkeiten 93

4.3 Überprüfung der Identität bei elektronischer Antragstellung 94

4.4 Portal „service-bw“ 95

5. Vorratsdatenspeicherung von Telekommunikations- und Internet-Verbindungsdaten 97

6. Datenschutz bei VoIP 99

7. Datenschutz bei mobilen Geräten 102

Seite

8. Personenbezogene Daten in Web-Angeboten und Internet-Suchmaschinen 105

8.1 Es gibt ein Entkommen vor den Suchmaschinen 105

8.2 Löschungen personenbezogener Daten in Suchmaschinen 106

Inhaltsverzeichnis des Anhangs 108

1. Teil: Zur Situation

Die Entwicklung des Datenschutzes im Land ist einerseits durchaus positiv zu bewerten. So ist die Bereitschaft der öffentlichen Stellen, sich in datenschutzrechtlichen und -technischen Fragestellungen den Rat meiner Dienststelle zu holen, weiter gewachsen. Verbesserungsmöglichkeiten bestehen aber durchaus noch. So wäre es erstrebenswert, wenn bei einem Beratungswunsch auch in Rechnung gestellt würde, dass eine solche Beratung auch für meine Mitarbeiterinnen und Mitarbeiter Zeit erfordert. Zu kurze Beteiligungsfristen gehen auf Kosten der Qualität und erschweren häufig Lösungen, die erst nach einem gründlichen Austauschen der Argumente gefunden werden können. Ein Beispiel hierfür sind die Arbeiten am neuen Landeskrebsregister. So uneingeschränkt die Bereitschaft des Sozialministeriums zu begrüßen ist, meine Dienststelle von Beginn der Projektüberlegungen an am Verfahren zu beteiligen, so fragwürdig ist der Endspurt, der jetzt in großer Hast hingelegt wird. Man kann dem Vorhaben nur wünschen, dass es trotz der nicht nachvollziehbaren Hektik zu einem guten Ende geführt wird (im Einzelnen s. 3. Teil, 1. Abschnitt, Nr. 2). Dass es trotz der insgesamt durchaus vorhandenen Sensibilität öffentlicher Stellen für den Datenschutz weiter zu Fehlern kommt, vermag den Praktiker kaum zu überraschen. Verwunderlich ist es allerdings schon, dass trotz wiederholter Berichte in den vergangenen Jahren weiterhin der Inhalt von Mülltonnen offenkundig jederzeit als beliebte Fundgrube für – negative – Erkenntnisse gut ist (s. unten 3. Teil, 1. Abschnitt, Nr. 4.1). Im Übrigen hielten sich die auszusprechenden förmlichen Beanstandungen in einem überschaubaren Rahmen.

Welchen Stellenwert das Recht auf informationelle Selbstbestimmung besitzt, spiegelt sich aber nicht nur in der Alltagsarbeit der Behörden wieder; für die Zukunft ist vielmehr entscheidend, welche Weichenstellungen Bundes- und Landesgesetzgeber heute vornehmen. Hier stimmt es nachdenklich, dass das Bundesverfassungsgericht erneut als Reparaturinstanz tätig werden musste, als es die Regelungen des Niedersächsischen Polizeigesetzes zur vorbeugenden Telefonüberwachung für nichtig erklärte (s. 2. Teil, 1. Abschnitt, Nr. 1). Dies ist kein Ruhmesblatt, wenn man berücksichtigt, dass das Bundesverfassungsgericht erst im vergangenen Jahr die gesetzlichen Regelungen des Bundes zur akustischen Wohnraumüberwachung korrigieren musste. Dieser Entscheidung wäre jedenfalls unschwer zu entnehmen gewesen, dass der Kernbereich der informationellen Selbstbestimmung auch in anderen Bereichen verfassungsrechtliches Gewicht hat.

Nunmehr hat sich der Bundesgesetzgeber erneut sehr weit vorgewagt, indem er die Möglichkeiten der forensischen DNA-Analyse deutlich erweitert hat. Damit aber offensichtlich nicht genug: Im Koalitionsvertrag vom 11. November 2005 haben sich CDU, CSU und SPD darauf verständigt, diese neue gesetzliche Regelung nach zwei Jahren zu evaluieren, und zwar um zu prüfen, „ob die DNA-Analyse aus kriminalpolitischen Gründen ausgeweitet werden muss“. Dass eine gesetzliche Regelung nach einer gewissen Zeit der praktischen Anwendung auf den Prüfstand gestellt wird, ist grundsätzlich eine gute Sache. Allerdings sollte die Überprüfung dann nicht mit einer einseitigen Zielrichtung erfolgen, sondern offen, d. h. es sollten Dinge, die sich in der Praxis nicht als notwendig erwiesen haben, auch wieder zurückgenommen oder korrigiert werden können. Zur forensischen DNA-Analyse wird sich jedenfalls auch die Frage stellen, ob man mit der neuen Regelung nicht schon über das verfassungsrechtlich zulässige Maß hinausgegangen ist (hierzu s. 2. Teil, 2. Abschnitt, Nr. 2); sich einseitig darauf festzulegen, nur erneute Erweiterungsmöglichkeiten zu prüfen, erscheint vor diesem Hintergrund unangemessen.

Der Koalitionsvertrag gibt auch in anderem Zusammenhang Hinweise darauf, in welcher Richtung sich das Datenschutzrecht in den nächsten Jahren bewegen soll. Wenn dort festgestellt wird, dass das Datenschutzrecht vor dem Hintergrund der technischen Entwicklungen „der Überprüfung und an verschiedenen Stellen der Überarbeitung und der Fortentwicklung“ bedürfe, so ist dies sicherlich zu begrüßen, wenn man sich die vielfach unübersichtlichen und komplizierten Datenschutzregelungen vor Augen hält. Wenn es dann aber weiter heißt, dass man auch prüfen werde, „ob im Hinblick auf den Abbau überflüssiger Bürokratie Änderungen vorgenommen werden können“, bleibt zu

hoffen, dass dies nicht einseitig so verstanden wird, dass man den Datenschutz dort, wo er hinderlich werden kann, generell zurückstutzen will. Da der Datenschutz Verfassungsrang besitzt, ist er nicht beliebig disponibel. Es wird deshalb nicht einfach damit getan sein, den Datenschutz so lange zurückzunehmen, bis er beim Verwaltungsvollzug nicht mehr zu Unbequemlichkeiten führt. Es liegt vielmehr in der Natur der Sache, dass der Datenschutz hier und da auch spürbaren Mehraufwand erfordert. Eine absolute Vorfahrt für andere Ziele – und seien sie aus wirtschafts- oder finanzpolitischer Sicht auch noch so wünschenswert – kann es nicht geben.

Nach einigen Ländern hat jetzt auch der Bund ein Informationsfreiheitsgesetz erlassen, das am 1. Januar 2006 in Kraft treten wird. Darin wird ein Anspruch auf Zugang zu amtlichen Informationen bei Behörden und anderen Stellen des Bundes geregelt, der manchmal in einem Spannungsverhältnis zum Recht auf informationelle Selbstbestimmung stehen kann. Auf Landesebene wurde die Überlegung zu einem Landes-Informationsfreiheitsgesetz mittlerweile von der Landtagsfraktion Bündnis 90/Die Grünen aufgegriffen. In dem von der Fraktion vorgelegten Gesetzentwurf ist u. a. vorgesehen, dass zur Durchsetzung des Informationsanspruchs der Landesbeauftragte für den Datenschutz angerufen werden kann. Inwieweit sich hieraus spürbare Mehrbelastungen für die Dienststelle ergeben würden, bliebe abzuwarten.

Neues gibt es auch in Sachen Organisation der Datenschutzaufsicht. Ein Bürger der Bundesrepublik Deutschland hat bei der EG-Kommission eine Beschwerde eingereicht und geltend gemacht, dass die in den Ländern bestehende Organisation der Kontrollstellen gegen die EG-Datenschutzrichtlinie verstoße, wonach die Kontrollstellen die ihnen zugewiesenen Aufgaben „in völliger Unabhängigkeit“ wahrzunehmen haben. Der Beschwerdeführer greift damit vor allem die Praxis in denjenigen Ländern an, die für die Datenschutzaufsicht im nicht-öffentlichen Bereich Behörden der allgemeinen Verwaltung, also – wie in Baden-Württemberg – die Innenministerien oder die Mittelbehörden, bestimmt haben. Die EG-Kommission hat daraufhin gegen die Bundesrepublik ein förmliches Vertragsverletzungsverfahren eingeleitet, weil auch nach ihrer Auffassung die derzeitige Organisationsform für die Überwachung der Datenverarbeitung im nicht-öffentlichen Bereich – u. a. auch in Baden-Württemberg – nicht mit der EG-Datenschutzrichtlinie vereinbar sei. Die Bundesregierung ist mittlerweile dieser Auffassung in Abstimmung mit den Innenministerien der Länder entgegengetreten, sodass nunmehr wieder die EG-Kommission am Zuge ist.

Meine Auffassung zur organisatorischen Ausgestaltung der Datenschutzaufsicht habe ich mehrfach geäußert; ich sehe unverändert in der Zusammenlegung der Aufsicht im öffentlichen und im nicht-öffentlichen Bereich große Vorteile, die zu einer effizienteren Aufgabenerledigung im Datenschutz beitragen und nebenbei auch dem von der EG-Kommission angestrengten Vertragsverletzungsverfahren den Wind aus den Segeln nehmen könnte. Die mit diesem Verfahren erfolgte Verlagerung der Diskussion auf die rechtliche, vielleicht sogar gerichtliche Ebene halte ich im Ergebnis aber für wenig fruchtbar. Es sollte ungeachtet der unterschiedlichen rechtlichen Auffassungen versucht werden, eine pragmatische und zukunftsfähige Lösung zu finden.

2. Teil: Öffentliche Sicherheit und Justiz

1. Abschnitt: Öffentliche Sicherheit

1. Die präventive Telekommunikationsüberwachung

Die Strafprozessordnung regelt seit langem, dass und zur Verfolgung welcher Straftaten die Polizei auf Anordnung durch den Richter (oder bei Gefahr in Verzug durch die Staatsanwaltschaft) die Telekommunikation überwachen, also insbesondere Telefone abhören und E-Mails mitlesen und aufzeichnen kann. Von dieser Befugnis macht die Polizei immer mehr Gebrauch. Allein im Zeitraum von 1994 bis 2001 ist die Gesamtzahl der Telekommunikationsüberwachungen bundesweit von 3 730 um mehr als das Fünffache auf 19 896 gestiegen; Tendenz weiter steigend. Die Zahl der Jahr für Jahr davon Betroffenen hat sich im selben Zeitraum mehr als verdoppelt. Dem steht nach einer Untersuchung, die das in Freiburg ansässige Max-Planck-Institut für ausländisches und internationales Strafrecht im Auftrag des Bundesministeriums der Justiz über die Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung durchgeführt hat, gegenüber, dass es nur in 17 % der Fälle, in denen Telekommunikationsüberwachungsmaßnahmen geschaltet waren, Ermittlungserfolge gegeben hat, die sich direkt auf den die Telekommunikationsmaßnahmen begründenden Tatverdacht bezogen haben. Trotz dieses Ergebnisses werden Sicherheitspolitiker seit Jahren nicht müde zu fordern, dass die Polizei nicht nur zur Verfolgung von Straftaten, sondern auch noch zu deren Vorbeugung, also bereits im Vorfeld des Anfangsverdachts einer Straftat, Telefone abhören und den E-Mail- und Telefaxverkehr überwachen und aufzeichnen darf.

Bei der Umsetzung dieser Forderungen hat Baden-Württemberg – in hier durchaus angemessener schwäbischer Bescheidenheit getreu dem Motto der Sieben Schwaben: „Geh du voran“ – anderen Bundesländern den Vortritt gelassen. Denn wie schnell man dabei Schiffbruch erleiden kann, wenn man Sicherheitsinteressen allzu sehr den Vorrang vor dem Fernmeldegeheimnis, das nach Artikel 10 Absatz 1 des Grundgesetzes unverletzlich ist, einräumt, hat das Land Niedersachsen erfahren müssen. Ein Bürger hatte sich mit einer Verfassungsbeschwerde gegen die Regelungen des Niedersächsischen Polizeigesetzes zur vorbeugenden Telekommunikationsüberwachung gewandt. Seine Verfassungsbeschwerde war erfolgreich. Mit Urteil vom 27. Juli 2005 (1 BvR 668/04) hat das Bundesverfassungsgericht festgestellt, dass die Regelungen des Niedersächsischen Polizeigesetzes, die die Polizei zur Telekommunikationsüberwachung zum Zwecke der Verhütung und der Vorsorge für die Verfolgung von Straftaten ermächtigen, wegen Verstoßes gegen das Fernmeldegeheimnis nichtig sind.

- Der niedersächsische Gesetzgeber hatte seine Gesetzgebungskompetenz durch die Regelungen über die Vorsorge für die Verfolgung von Straftaten überschritten. Eine solche Verfolgungsvorsorge unterfällt der konkurrierenden Gesetzgebung über das Strafverfahren, von der der Bundesgesetzgeber im Bereich der Telekommunikationsüberwachung mit den Regelungen der Strafprozessordnung abschließend Gebrauch gemacht hat. Darin hat der Bundesgesetzgeber insbesondere auch geregelt, dass und unter welchen Voraussetzungen eine Überwachung der Telekommunikation bereits im Vorbereitungsstadium einer Straftat in Betracht kommen kann. Diese gezielten Eingrenzungen würden hinfällig, wenn die Länder vergleichbare Maßnahmen zur Telekommunikationsüberwachung im Hinblick auf eine spätere Strafverfolgung unter anderen, geringeren Voraussetzungen normieren könnten.
- Will der Gesetzgeber Regelungen treffen, die das Fernmeldegeheimnis beschränken, müssen sie dem rechtsstaatlichen Gebot der Normenbestimmtheit und Normenklarheit genügen. Dieses Gebot soll sicherstellen, dass die betroffenen Bürger sich auf mögliche belastende Maßnahmen einstellen können, dass die gesetzesausführende Verwaltung für ihr Verhalten steuernde und begrenzende Handlungsmaßstäbe vorfindet und dass die Gerichte die Rechtskontrolle durchführen können. Der Anlass, der Zweck und die Grenzen des Eingriffs müssen in der Ermächtigung

präzise festgelegt sein. Diesen verfassungsrechtlich gebotenen Anforderungen genügten die angegriffenen Regelungen des Niedersächsischen Polizeigesetzes nicht. Sie enthielten keine einschränkenden Tatbestandsmerkmale, die die – so das Bundesverfassungsgericht – gerade im Bereich der Vorfeldermittlung schwierige Abgrenzung von einem harmlosen zu einem in eine Straftat mündenden Verhalten ermöglichen. Die Ausrichtung auf „Straftaten von erheblicher Bedeutung“ trägt dazu nicht bei, weil dieses Tatbestandsmerkmal keine Anhaltspunkte dafür bietet, wann ein Verhalten auf die künftige Begehung solcher Straftaten hindeutet.

– Die angegriffenen Normen genügten auch nicht dem Grundsatz der Verhältnismäßigkeit. Sie ermöglichten schwer wiegende Eingriffe in das Fernmeldegeheimnis. Solche Eingriffe können jedoch nur dann als angemessen bewertet werden, wenn der damit zu schützende Allgemeinwohlbelang überragend wichtig ist. An einer solchen Einengung fehlte es. Insbesondere trug das Tatbestandsmerkmal der „Straftaten von erheblicher Bedeutung“ dem Erfordernis des Schutzes besonders hochrangiger Rechtsgüter nicht Rechnung. Dieses Defizit wurde noch durch das Fehlen einer hinreichend bestimmten Umschreibung der Tatsachen, die auf eine künftige Begehung von Straftaten hindeuten, verschärft. Eine solche Umschreibung ist aber notwendig, weil die Situation der Vorfeldermittlungen dadurch geprägt ist, dass die Indizien oder einzelne beobachtete Tätigkeiten in harmlosen, strafrechtlich unerheblichen Zusammenhängen verbleiben können; sie können aber auch der Beginn eines Vorgangs sein, der zu einer Straftat führt. Deshalb muss der Gesetzgeber die Tatsachen, die auf die künftige Begehung hindeuten, so bestimmt umschreiben, dass das im Bereich der Vorfeldermittlung besonders hohe Risiko einer Fehlprognose so gering wie möglich gehalten wird.

– Nicht ausgeschlossen ist, dass etwa bei einer Telefonüberwachungsmaßnahme Gesprächsinhalte mitgehört und aufgezeichnet werden, die sich auf den Kernbereich höchstpersönlicher Lebensgestaltung beziehen. Gleichwohl enthielten die angegriffenen Vorschriften keine hinreichenden Vorkehrungen zur Vermeidung von Eingriffen in den absolut geschützten Kernbereich privater Lebensgestaltung. Es fehlte auch an Sicherungen dafür, dass Kommunikationsinhalte des höchstpersönlichen Bereichs nicht verwertet und unverzüglich gelöscht werden, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist.

Was ist die Konsequenz aus dem Urteil des Bundesverfassungsgerichts? Kann man es wirklich – wie das Innenministerium meint – mit dem Hinweis darauf, dass unser Polizeigesetz keine Regelung über die präventive Telekommunikationsüberwachung kennt, ad acta legen? Eine solche Verfahrensweise hieße, Bedeutung und Tragweite des Urteils zu verkennen. Aus ihm folgt nämlich insbesondere auch, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung nicht nur im Rahmen der präventiven Telekommunikationsüberwachung, sondern im Rahmen aller verdeckten Datenerhebungsmaßnahmen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Dies gilt etwa für den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern und erst recht für die akustische Wohnraumüberwachung, die unter dem Begriff „Großer Lauschangriff“ besser bekannt ist. Dazu reichen bloße Verwertungsverbote nicht aus. Vielmehr muss eine solche Maßnahme grundsätzlich unterbleiben, wenn im konkreten Fall Anhaltspunkte für die Annahme bestehen, dass dabei Inhalte erfasst werden, die zum unantastbaren Kernbereich privater Lebensgestaltung gehören. Ferner geben die Hinweise des Bundesverfassungsgerichts zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit Anlass, die Datenverarbeitungsbefugnisse im Bereich der Vorfeldermittlungen einer kritischen Prüfung zu unterziehen mit dem Ziel, die Voraussetzungen der Befugnisse so klar zu bestimmen, dass das hier besonders hohe Risiko einer Fehlprognose so weit wie möglich minimiert wird. Darauf und auf weitere Konsequenzen aus dem Urteil des Bundesverfassungsgerichts haben die Datenschutzbeauftragten des Bundes und der Länder mit ihrer Entschließung vom 27./28. Oktober 2005 hingewiesen (s. Anhang 8).

2. Änderung des Landesverfassungsschutzgesetzes

Mit dem In-Kraft-Treten des Terrorismusbekämpfungsgesetzes im Januar 2002 eröffnete der Bundesgesetzgeber den Ländern die Möglichkeit, ihren Verfassungsschutzbehörden per Gesetz weiter gehende Befugnisse einzuräumen. Gedacht war dabei an die Möglichkeit, in bestimmten Fällen bei Kreditinstituten, Finanzdienstleistungsunternehmen und Finanzunternehmen Auskünfte zu Konten und Konteninhabern sowie zu Geldbewegungen und Geldanlagen, bei Postunternehmen Auskünfte über den Postverkehr, bei Luftfahrtunternehmen Auskünfte über die Inanspruchnahme von Transportleistungen und sonstige Umstände des Luftverkehrs und bei Telekommunikations- und Teledienstunternehmen Auskünfte zu Telekommunikationsverbindungsdaten und Teledienstenutzungsdaten einholen zu können. Fast drei Jahre lang bestand in Baden-Württemberg offenbar keine Notwendigkeit, von dieser Möglichkeit Gebrauch zu machen; jedenfalls sind Klagen des Landesamts für Verfassungsschutz über mangelnde Befugnisse nicht bekannt geworden. Ende 2004 leitete das Innenministerium uns dann einen Gesetzentwurf zur Änderung des Landesverfassungsschutzgesetzes zur Stellungnahme zu. Obwohl es darin dem Landesamt für Verfassungsschutz attestierte, dass es bisher seine Aufgaben bei der Bekämpfung des internationalen Terrorismus effektiv erfüllt hat, sah der Gesetzentwurf vor, dem Landesamt für Verfassungsschutz die Befugnis zur Einholung von Auskünften bei Kreditinstituten, Post-, Luftfahrt-, Telekommunikations- und Teledienstunternehmen einzuräumen. Darüber hinaus sollten die bisherigen Möglichkeiten des Amtes, Daten über Bürger zu erheben und zu speichern, noch weiter ausgedehnt werden.

Das Vorhaben des Innenministeriums stellt das in unserer Verfassung verankerte Recht des Einzelnen zu wissen, wer was wann bei welcher Gelegenheit über ihn weiß, ganz erheblich in Frage. Will der Gesetzgeber Eingriffe in dieses Grundrecht durch den Verfassungsschutz zulassen, ist es besonders wichtig, dem Verfassungsschutz möglichst klare Vorgaben für seine Aufgaben zu machen und dessen Befugnisse, Informationen über Bürger zu sammeln und zu speichern, auf das unumgänglich Notwendige zu begrenzen. Diesen Anforderungen entsprach der Gesetzentwurf in mancherlei Hinsicht nicht in gebotenem Maße: Beispielsweise lässt sich kaum absehen, bei welchen Verhaltensweisen jemand damit rechnen muss, dass er gegen den Gedanken der Völkerverständigung verstößt und demzufolge vom Verfassungsschutz beobachtet wird. Der Einsatz des sog. IMSI-Catchers, mit dem ein gravierender Eingriff in das Telekommunikationsgeheimnis einhergeht, sollte dem Verfassungsschutz recht großzügig ermöglicht werden. Vom Minderjährigenschutz wäre nach dem Gesetzentwurf nicht mehr viel übrig geblieben. Behörden und andere öffentliche Stellen sollten den Verfassungsschutz von sich aus bereits dann informieren, wenn die Daten zur Aufgabenerfüllung des Verfassungsschutzes erforderlich sein können. Die Pflicht des Verfassungsschutzes, über die Einsichtnahme in Register anderer Behörden gesonderte Nachweise zu führen, wollte der Gesetzentwurf dem Verfassungsschutz ersparen. Selbst bei (einfachen) extremistischen Bestrebungen wollte das Innenministerium die Speicherfrist auf 15 Jahre erhöhen.

Auf unsere Einwände gegen diese und eine Reihe anderer Regelungsabsichten hat das Innenministerium seinen Gesetzentwurf überarbeitet. An seiner Absicht, dem Landesamt für Verfassungsschutz die Möglichkeit zur Einholung von Auskünften bei Kreditinstituten, Post-, Luftfahrt-, Telekommunikations- und Teledienstunternehmen an die Hand zu geben, hat es festgehalten. Viele unserer Hinweise hat es erfreulicherweise aufgegriffen und berücksichtigt. Dies hätten wir uns auch noch in folgenden Punkten gewünscht:

– Zu den Aufgaben des Verfassungsschutzes gehört es u. a., an der Sicherheitsüberprüfung von Mitarbeitern des öffentlichen Dienstes mitzuwirken. Im Rahmen einer solchen Überprüfung durchleuchtet der Verfassungsschutz deren Lebensverhältnisse und unter bestimmten Voraussetzungen auch die ihrer Ehegatten, Verlobten und Lebensgefährten. Wer sich einer solchen Sicherheitsüberprüfung unterzieht oder in eine solche einbezogen wird, macht seine Angaben in der Erwartung, sie würden nur

für die Sicherheitsüberprüfung verwendet. Von derselben Vorstellung gehen auch die Auskunftspersonen, die der Verfassungsschutz im Rahmen eines solchen Überprüfungsverfahrens befragt, und die Mitarbeiter von Flughäfen und Kernkraftwerken aus, an deren Zuverlässigkeitsüberprüfung der Verfassungsschutz mitwirkt. Gegenüber diesem Personenkreis wäre es ein Vertrauensbruch, dürfte der Verfassungsschutz ihre Angaben auch für seine anderen Aufgaben, beispielsweise für die Beobachtung von Bestrebungen gegen die freiheitlich demokratische Grundordnung verwenden. Genau dies aber will das Innenministerium. Die bisherige Regelung des Verfassungsschutzgesetzes, die dem Verfassungsschutz die Verwendung solcher Angaben nur dann erlaubt, wenn es um die Abwehr geheimdienstlicher Tätigkeiten für eine fremde Macht oder die Beobachtung von Bestrebungen geht, die sich durch Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die freiheitlich demokratische Grundordnung oder auswärtige Belange der Bundesrepublik Deutschland richten, ist ihm offenbar ein Dorn im Auge. Unseren Vorschlag, die Verwendung solcher Daten wenigstens auf die Beobachtung von Bestrebungen von erheblicher Bedeutung zu beschränken, hat es verworfen.

– Dass das Landesamt für Verfassungsschutz auch auf Informationen von anderen Behörden und von Gerichten angewiesen ist, wird niemand in Abrede stellen. Zu weit geht es aber, wenn das Innenministerium – was bisher der mit den Aufgaben des Verfassungsschutzes vertrauten Polizei und den Staatsanwaltschaften vorbehalten war – nunmehr auch Bürgermeisterämter, Landratsämter, Schulen, Hochschulen, kurzum alle Behörden und Gerichte ermächtigen will, dem Landesamt für Verfassungsschutz von sich aus, also unaufgefordert, Informationen zukommen zu lassen, wenn „tatsächliche Anhaltspunkte“ dafür bestehen, dass diese Informationen zur Wahrnehmung der Aufgaben des Verfassungsschutzes erforderlich sind. Wollen die Behörden und Gerichte von einer solchen Ermächtigung korrekt Gebrauch machen, müssen sie umfassend über die Aufgaben des Verfassungsschutzes Bescheid wissen und sich damit eine zutreffende Vorstellung davon machen können, wann beispielsweise Bestrebungen vorliegen, die gegen „die freiheitlich demokratische Grundordnung“ oder „die Sicherheit des Bundes oder eines Landes“ oder gegen „den Gedanken der Völkerverständigung“ gerichtet sind – eine realitätsfremde Vorstellung. Zu befürchten ist deshalb, dass eine solche Ermächtigung eher zu einer überbordenden Mitteilungspraxis führt als dass sie dem Verfassungsschutz zuverlässige und für seine Arbeit wichtige Informationen verschafft. Wir schlugen vor, die Befugnis der Behörden und Gerichte, den Verfassungsschutz von sich aus zu informieren, in Anlehnung an die im Zuge des Terrorismusbekämpfungsgesetzes geänderte Vorschrift des § 18 des Bundesverfassungsschutzgesetzes vom Vorliegen einer Bestrebung, die sich durch Anwendung von Gewalt oder darauf gerichteter Vorbereitungshandlungen gegen solche Schutzgüter richtet, abhängig zu machen. Dieser Vorschlag fand beim Innenministerium jedoch kein Gehör.

– Das Landesamt für Verfassungsschutz soll künftig berechtigt sein, „die Polizei in eilbedürftigen Fällen außerhalb der regulären Dienstzeiten des Kraftfahrt-Bundesamts um eine Abfrage aus dem Fahrzeugregister des Kraftfahrt-Bundesamts im automatisierten Verfahren zu ersuchen.“ Diese Regelung liefe in zweierlei Hinsicht auf eine Umgehung des § 36 des Straßenverkehrsgesetzes hinaus. Zum einen zählt nach dieser bundesrechtlichen Vorschrift der Verfassungsschutz gerade nicht zu den Behörden, die im automatisierten Verfahren Halter- und Fahrzeugdaten aus dem Fahrzeugregister des Kraftfahrt-Bundesamts abrufen dürfen. Über den Umweg über die Polizei würde ihm dies jedoch ermöglicht. Zum anderen darf die Polizei solche Online-Abrufe nur für Zwecke einer Verkehrskontrolle sowie für die Verfolgung von Straftaten und bestimmten Ordnungswidrigkeiten und für die Abwehr von Gefahren für die öffentliche Sicherheit tätigen, nicht jedoch für Zwecke des Verfassungsschutzes. Gerade dies soll die Polizei mit Hilfe der neuen landesrechtlichen Regelung aber tun dürfen. Diese unzulässige Nachbarschaftshilfe ist keine Petitesse. Wer Daten online abfragen kann, braucht weder je-

mand um Erlaubnis zu fragen noch sein Auskunftsersuchen mündlich oder gar schriftlich zu begründen. Er kann zudem beliebig oft und beliebig viel abfragen, ohne sich dafür rechtfertigen zu müssen. Wer online abfragen kann, kann es sich auch leisten, prinzipiell die Richtigkeit dessen zu bezweifeln, was ihm der Bürger sagt, und ihm erst zu glauben, wenn der Computer nichts anderes meldet. Darin liegen die speziellen Gefahren von Online-Abfragen für den Datenschutz. Sie haben den Bundesgesetzgeber veranlasst, den Verfassungsschutz – wie manch andere Behörde auch – auf konventionelle Anfragen zu verweisen, wenn er Halter- und/oder Fahrzeugdaten aus dem Fahrzeugregister wissen will. Dies kann der Landesgesetzgeber nicht in eigener Regie ändern.

– Das Innenministerium will dem Verfassungsschutz ein weit reichendes Recht einräumen, Register und sogar Akten anderer Behörden und öffentlicher Stellen einzusehen. Weil dem Verfassungsschutz dabei sehr viel mehr Informationen zur Kenntnis gelangen, als er zur Erfüllung seiner Aufgaben benötigt, sind solche Einsichtsrechte auf das unabweisbar notwendige Maß zu beschränken. Unser Vorschlag, sich in diesem Punkt an die sonst so gern betonte Vorbildfunktion des Bundes zu erinnern und das Bundesverfassungsschutzgesetz in diesem Punkt zum Vorbild zu nehmen, stieß beim Innenministerium auf keine Gegenliebe. Immerhin hat es sich dazu bewegen lassen, dass das Landesamt für Verfassungsschutz über die Einsichtnahme einen Nachweis führen muss, aus dem der Zweck und die Veranlassung, die ersuchte Behörde und die Aktenfundstelle hervorgehen. Diese Dokumentationspflicht wollte das Innenministerium ursprünglich einfach streichen.

– Mit seinem Urteil vom 3. März 2004 hat das Bundesverfassungsgericht die damaligen Regelungen über die akustische Wohnraumüberwachung zur Straftatenverfolgung weitgehend für verfassungswidrig erklärt (vgl. 25. Tätigkeitsbericht, LT-Drucksache 13/3800). Zwar ist das Innenministerium mit uns einer Meinung, dass die Kernaussagen dieses Urteils auf die akustische Wohnraumüberwachung durch den Verfassungsschutz zu übertragen sind. Auf ein verfassungsrechtlich unbedenkliches Niveau will es die einschlägige Vorschrift des Landesverfassungsschutzgesetzes gleichwohl nicht bringen. Es wolle sich am Bund orientieren, bekamen wir zu hören, wo doch sonst, wenn es um die Ausweitung der Befugnisse des Landesamts für Verfassungsschutz geht, die Leitbildfunktion des Bundes nicht immer die entscheidende Rolle spielt (siehe oben). Erst recht vermag der Hinweis des Innenministeriums, durch innerorganisatorische Regelungen des Landesamts für Verfassungsschutz sei die Einhaltung der Vorgaben des Bundesverfassungsgerichts gewährleistet, sein Zuwarten nicht zu rechtfertigen. Die Entscheidung über die Beschränkung der Grundrechte darf nicht in das Ermessen der Verwaltung gestellt sein. Dem Gesetz kommt im Hinblick auf den Handlungsspielraum der Exekutive eine begrenzende Funktion zu, die rechtmäßiges Handeln des Staates sichern und dadurch auch die Grundrechte der Bürger schützen soll. Deshalb müssen vom Landesgesetzgeber selbst Vorkehrungen getroffen werden, die sicherstellen, dass bei einer akustischen Wohnraumüberwachung durch den Verfassungsschutz Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung unterbleiben.

Der Landtag hat das Gesetz zur Änderung des Landesverfassungsschutzgesetzes mit großer Mehrheit so verabschiedet, wie es die Landesregierung auf der Grundlage des überarbeiteten Entwurfs des Innenministeriums eingebracht hat; inzwischen steht es im Gesetzblatt. Damit scheint die Sache für den Landtag offenbar auf Dauer erledigt. Demgegenüber wäre es zu begrüßen gewesen, eine Evaluierung der neuen Befugnisse des Landesamts gesetzlich zu verankern. Dies haben jedenfalls der Bundesgesetzgeber für die entsprechenden Befugnisse des Bundesamts und andere Landesgesetzgeber hinsichtlich der dortigen Landesämter für Verfassungsschutz beschlossen, soweit es um die Einholung von Auskünften bei Kreditinstituten, Finanzdienstleistungsinstituten, Finanzunternehmen, Postunternehmen, Luftfahrtunternehmen sowie Telekommunikations- und Teledienstunternehmen oder um Berichte über die Durchführung sowie Art, Umfang und Anordnungsgründe solcher Maßnahmen geht.

3. Die Arbeitsdatei „Politisch motivierte Kriminalität“

Ende Oktober 2004 hatte sich ein junger Mann an unser Amt gewandt. Sein Anliegen war Folgendes: Im Nachbarort waren mehrere jüngere Personen beobachtet worden, wie sie nachts in die Schaufenster und in die Tür eines Ladens, der Freizeit- und Militärbekleidung verkauft, Löcher bohrten und durch die Löcher eine übel riechende Flüssigkeit in den Laden spritzten. Auf die Zufahrt zu dem Laden sprühten sie mit Farbe „Nazi-Laden“. Die Täter entkamen unerkannt. Die mit den Ermittlungen befasste Polizeidirektion ging von einer politisch motivierten Sachbeschädigung aus und bat u. a. den jungen Mann auf freiwilliger Basis um die Abgabe von Fingerabdrücken und einer Speichelprobe für eine DNA-Analyse. Dieser Bitte kam der junge Mann nach. Weil er mit der Sachbeschädigung nichts zu tun hatte, wollte er von uns geprüft wissen, ob die Polizeidirektion ihre Zusage eingehalten und seine Fingerabdrücke und die Speichelprobe vernichtet hat. Dies hat die Polizeidirektion dann im Zuge unserer Nachforschungen getan. Zugleich ließ sie uns wissen, dass sie den jungen Mann gleichwohl als Tatverdächtigen in der Arbeitsdatei „Politisch motivierte Kriminalität“ (AD PMK) erfasst hat. Weil manches dafür sprach, dass es sich dabei sozusagen um die Spitze eines Eisbergs handelte und weil wir bis dahin mit dieser Datei noch nicht befasst waren, entschlossen wir uns, die Verarbeitung personenbezogener Daten durch die Polizei in dieser Datei einmal ganz generell unter die Lupe zu nehmen. Dass wir damit ein heißes Eisen anfassten, war uns rasch klar.

Die AD PMK ist vom Landeskriminalamt mit Zustimmung des Innenministeriums eingerichtet worden; sie ist Anfang 2003 in Betrieb gegangen. Sie dient der Bekämpfung der politisch motivierten Kriminalität. Nach den Festlegungen des Landeskriminalamts werden in dieser Datei im Wesentlichen Personen erfasst, die mutmaßlich oder tatsächlich politisch motivierte Straftaten begangen haben und bei denen die Annahme gerechtfertigt ist, dass sie künftig solche Straftaten begehen, sowie Personen, von denen eine Gefahr für die öffentliche Sicherheit ausgeht. An die AD PMK sind alle Dienststellen des polizeilichen Staatsschutzes online angeschlossen. Sie können über ihre Online-Anschlüsse Daten in der AD PMK speichern und die gespeicherten Daten abrufen, und zwar ganz gleich, ob die abrufende oder eine andere Staatsschutzdienststelle die Daten eingespeichert hat. In der AD PMK sind nach einer Auswertung, die das Landeskriminalamt im Mai 2005 auf Bitten unseres Amtes durchgeführt hat, über 40.000 Personen erfasst, also praktisch vom Kleinkind bis zum Greis fast jeder zweihundertfünfzigste Einwohner Baden-Württembergs.

Um uns ein Bild von der Speicherpraxis der Polizei machen zu können, führten wir bei vier Staatsschutzdienststellen Kontrollbesuche durch. Dabei nahmen wir eine nach dem Zufallsprinzip gezogene Stichprobe von über 550 AD PMK-Speicherungen näher unter die Lupe. Hätte es damit sein Bewenden gehabt, dass drei der vier Staatsschutzdienststellen in diversen Fällen bei den Kontrollbesuchen – wozu sie aber nach § 29 des Landesdatenschutzgesetzes (LDSG) verpflichtet gewesen wären – trotz unserer rechtzeitig zuvor geäußerten Bitte die den jeweiligen AD PMK-Speicherungen zugrunde liegenden Akten nicht vorgelegt haben, gäbe es hier kein Wort zu verlieren. Bei der AD PMK war und ist jedoch manches nicht in Ordnung. So sind z. B. Personen erfasst, ohne dass es für die AD PMK-Speicherung irgendeinen Beleg gibt. In einer Reihe von Fällen ist nicht dargetan und auch sonst nicht ersichtlich, dass die Betroffenen mit ihrem Verhalten, das zu ihrer Erfassung in der AD PMK geführt hat, politisch motivierte Ziele verfolgen. Eine Vielzahl von Personen ist in der AD PMK erfasst, obwohl von ihnen nach eigener Einschätzung der Polizei keine Gefahr für die öffentliche Sicherheit ausgeht. Oft führten Ungenauigkeiten bei der Erfassung von Altfällen dazu, dass Personen zu lange in der AD PMK gespeichert sind. Doch der Reihe nach:

3.1 Keine Akten/Unterlagen vorhanden

Speichert die Polizei in einem automatisiert betriebenen Informationssystem wie der AD PMK Daten über Personen, so muss sie anhand von Akten oder sonstigen Unterlagen belegen können, worauf die Daten-

speicherung beruht. Aus den AD PMK-Datensätzen muss dazu jeweils ersichtlich sein, bei welcher Polizeidienststelle diese Akten/Unterlagen geführt werden. Diese Dokumentationspflichten sind kein Selbstzweck. Hierzu muss man wissen, dass in einer Datei wie der AD PMK das tatsächliche Geschehen in der Regel nur stichwortartig gespeichert wird. Dadurch entstehen nicht nur Informationslücken, die dazu führen können, dass aus den gespeicherten Daten zum Nachteil des Betroffenen unzutreffende Schlüsse gezogen werden. Ohne Rückgriff auf die einschlägigen Akten/Unterlagen und die darin dokumentierten Umstände des Einzelfalls lässt sich auch die Frage nach der Rechtmäßigkeit der Datenspeicherung nicht beantworten. Gibt es also solche Akten/Unterlagen nicht (mehr), entbehren die Datenspeicherungen in der AD PMK-Speicherungen der notwendigen Grundlage, mit der Folge, dass sie zu löschen sind. Genau so lagen die Dinge in einer Reihe von Fällen der Stichprobe. Beispielsweise hatte eine Staatsschutzdienststelle einen Mann, der aus dem Westjordanland stammt, im März 2004 als Beschuldigten mit dem Hinweis „Verdacht des kriminellen Islamismus“ und eine andere Staatsschutzdienststelle einen Mann aus dem Irak für drei Jahre als „Tatverdächtigen“ in der AD PMK gespeichert, obwohl es zu diesen Datenspeicherungen keinerlei Unterlagen gab und gibt. Deshalb ließ sich nicht feststellen, worauf der gravierende Vorwurf beruht, der besagte Mann stehe im Verdacht des kriminellen Islamismus, und weshalb der andere Mann als Verdächtiger einer politisch motivierten Straftat in der AD PMK gespeichert ist.

Immerhin hat sich eine der Staatsschutzdienststellen nach der Ankündigung unseres Kontrollbesuchs an die alte Datenschutzregel erinnert, nach der Datenspeicherungen ohne Aktenrückhalt in polizeilichen Informationssystemen unzulässig sind, und in dem Fall des Mannes, den sie wegen des Verdachts des kriminellen Islamismus in der AD PMK erfasst hatte, auf einem AD PMK-Ausdruck vermerkt: „Erfassung nicht nachvollziehbar, kein Aktenrückhalt“ und die unzulässige AD PMK-Speicherung gelöscht. Besser wäre es freilich gewesen, wenn sie den Mann erst gar nicht in der AD PMK gespeichert hätte. Selbstverständlich müssen auch die anderen Staatsschutzdienststellen ihre AD PMK-Speicherungen löschen, für die es keinen Aktenrückhalt gibt.

3.2 Politische Motivation nicht belegt

Nach den §§ 37, 38 des Polizeigesetzes (PolG) dürfen die Staatsschutzdienststellen jemanden in der AD PMK nur speichern, wenn eine politisch motivierte Straftat vorliegt. Die Annahme einer solchen Motivation setzt über die begangene Straftat hinaus Anhaltspunkte dafür voraus, dass der Täter mit seiner Tat eigentlich den demokratischen Willensbildungsprozess beeinflussen, politische Ziele erreichen oder verhindern oder sich gegen die Realisierung politischer Entscheidungen oder gegen die freiheitlich demokratische Grundordnung wenden will. Als politisch motiviert gilt eine Tat auch, wenn die Umstände der Tat oder die Einstellung des Täters darauf schließen lassen, dass sie sich gegen eine Person aufgrund ihrer politischen Einstellung, ihrer Nationalität, Volkszugehörigkeit, Rasse, Hautfarbe, Religion, Weltanschauung, Herkunft, sexuellen Orientierung, Behinderung oder ihres äußeren Erscheinungsbildes richtet und die Tathandlung in Kausalzusammenhang mit der Andersartigkeit des Opfers steht. Weil eine AD PMK-Speicherung einen besonders gravierenden Eingriff in die Rechte des Betroffenen darstellt, verlangt schon der Grundsatz der Verhältnismäßigkeit, strenge Anforderungen an die Darlegung der Speicherungsvoraussetzungen zu stellen. Die Staatsschutzdienststellen müssen deshalb in jedem Einzelfall prüfen, ob hinreichende Anhaltspunkte dafür vorhanden sind, dass der Betroffene mit seiner Verhaltensweise eigentlich solche politischen Ziele verfolgen wollte. Daran ließen es die Staatsschutzdienststellen jedoch in einer ganzen Reihe von Fällen der Stichprobe fehlen. Wozu dies führte, sei an wenigen Beispielen verdeutlicht:

– Ein 49 Jahre alter Mann aus Marokko ist aufgrund eines Vorfalls in der AD PMK erfasst, den die Polizei in ihrem Ermittlungsbericht so zusammengefasst hat:

  „Nachdem der Geschädigte (der 10-jährige Sohn des Mannes) nach seinem Aufenthalt bei seinem Vater (der Mann aus Marokko) wieder zurück zu seiner Mutter gebracht wurde, teilte er ihr mit, dass er von seinem Vater geschlagen worden sei. Der Geschädigte ist nach der Scheidung seiner Eltern alle 14 Tage am Sonntag bei seinem Vater. Daraufhin kam die Mutter, Anzeigeerstatterin, zusammen mit ihrem Sohn auf die hiesige Dienststelle und erstattete Anzeige. Maßnahmen: Vernehmung der Anzeigeerstatterin. Hier stellte sich heraus, dass der Vater dem Sohn aufgrund eines Missverständnisses eine Ohrfeige gegeben hatte. Verletzungen entstanden hierdurch nicht."

– Ein türkischstämmiger Gastwirt und sein Stellvertreter sind in der AD PMK erfasst, weil der Stellvertreter nach einem Bericht der Polizei über eine Gaststättenkontrolle noch acht Gäste in der Gaststätte bewirtet hatte, obwohl die Sperrzeit bereits eingetreten war.

– Ein Asylbewerber aus Kamerun ist in der AD PMK erfasst, weil die Polizei bei einer Personenkontrolle festgestellt hatte, dass er den räumlichen Geltungsbereich seiner Aufenthaltsgestattung verlassen hatte.

– Ein Mann mit türkischer Staatsangehörigkeit ist in der AD PMK erfasst, weil er beim Gewerbeamt an seinem Wohnort ein Taxiunternehmen angemeldet hat.

Weil in diesen und weiteren Fällen der Stichprobe von den Staatsschutzdienststellen eine politische Motivation in dem oben beschriebenen Sinn nicht dargetan und für das Vorliegen einer solchen Motivation auch sonst nichts ersichtlich war, forderten wir die Staatsschutzdienststellen auf, diese AD PMK-Speicherungen zu löschen.

3.3 Die sog. anderen Personen

Speichert die Polizei in ihren Informationssystemen Daten über jemand, so muss sie in dem jeweiligen Datensatz einspeichern, welcher Personengruppe sie ihn zurechnet, ob sie ihn also beispielsweise als Beschuldigten, Verdächtigen oder Störer erfasst hat. In den allermeisten der 550 kontrollierten Fälle hatten die Staatsschutzdienststellen in das hierfür vorgesehene AD PMK-Datenfeld jeweils „andere Person" eingespeichert. Grundlage für die AD PMK-Speicherung als „andere Person" waren unterschiedliche Verhaltensweisen, sei es, dass jemand seinen Ausweis als verloren gemeldet hat oder verlängern ließ, einen Waffenschein beantragt oder erhalten hat, ein Gewerbe an- oder abgemeldet hat, die Genehmigung für das Aufstellen eines Informationsstands beantragt hat, Mitglied oder Vorstand in einem islamischen Verein oder einer islamischen Gemeinde ist oder an einer Veranstaltung eines solchen Vereins oder einer solchen Gemeinde teilgenommen hat oder dass jemand beim Besuch einer Moschee oder sonst von der Polizei kontrolliert worden ist. Dies sei an wenigen Beispielen exemplarisch erläutert:

– Ein 23-jähriger Mann türkischer Staatsangehörigkeit ist als „andere Person" in der AD PMK gespeichert, weil er beim Ausländeramt, worüber dieses die Polizei informiert hat, seinen Ausweis als verloren gemeldet hat.

– Ein 31-jähriger Mann türkischer Staatsangehörigkeit ist als „andere Person" in der AD PMK gespeichert, weil die Waffenbehörde ihm eine waffenrechtliche Erlaubnis erteilt und die Polizei darüber informiert hat.

– Ein 31-jähriger Mann, der aus Zaire stammt, ist als „andere Person" in der AD PMK gespeichert, weil er beim Gewerbeamt, das der Polizei davon Mitteilung gemacht hat, einen Im- und Export von Gebrauchtwagen angemeldet hat.

– Ein 45-jähriger Mann, der aus Kairo stammt und hier Arzt ist, und alle weiteren 187 Personen, die wie der Arzt an einem Freitagnachmittag zum traditionellen Freitagsgebet eine Moschee besucht haben, sind jeweils als „andere Person“ in der AD PMK gespeichert, weil die Polizei an jenem Tag die Moschee einer Razzia unterzogen und dabei alle Moscheebesucher einer Personenkontrolle unterzogen hat.

Mit der Speicherung dieser und weiterer Personen als „andere Personen“ in der AD PMK haben die Staatsschutzdienststellen das Maß des nach den §§ 37, 38 PolG Zulässigen bei weitem überschritten. Unter „anderen Personen“ werden in der Terminologie des Polizeirechts die sog. Nichtstörer verstanden, mithin Personen, von deren Verhalten oder Sachen gerade keine Gefahr für die öffentliche Sicherheit oder Ordnung ausgeht. Die Speicherung solcher Personen ist in der AD PMK schon deshalb nicht zulässig, weil sich solche Datenspeicherungen nicht einmal im Rahmen der Vorgaben halten, die das Landeskriminalamt in seinem Verfahrensverzeichnis für Datenspeicherungen in der AD PMK selbst festgelegt hat. Dazu muss man wissen, dass nach dem Landesdatenschutzgesetz jede öffentliche Stelle ein Verzeichnis über die automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, erstellen und führen muss. Im Verfahrensverzeichnis ist nach § 11 Abs. 2 LDSG u. a. der Kreis der Betroffenen, also der Personen festzulegen, über die in dem automatisierten Verfahren Daten verarbeitet werden. Über welche Personengruppen die Staatsschutzdienststellen in der AD PMK Daten speichern können, hat das Landeskriminalamt in seinem Verfahrensverzeichnis für diese Datei abschließend bestimmt. Dazu zählen neben Beschuldigten und Tatverdächtigen auch solche Personen, bei denen Anhaltspunkte dafür vorliegen, dass sie künftig Straftaten begehen, sowie Personen im räumlichen Umfeld einer in besonderem Maße als gefährdet erscheinenden Person. Ferner zählen dazu Zeugen, Hinweisgeber und sonstige Auskunftspersonen sowie Personen, von denen eine Gefahr für die öffentliche Sicherheit ausgeht. „Andere Personen“ hat das Landeskriminalamt in seinem Verfahrensverzeichnis beim Kreis der Betroffenen, die in der AD PMK gespeichert werden können, nicht erwähnt und damit zum Ausdruck gebracht, dass ihre Erfassung in dieser Datei aus polizeilicher Sicht nicht erforderlich ist. Weil sich die Staatsschutzdienststellen in einer Vielzahl von Fällen über die klare und für sie verbindliche Festlegung des Landeskriminalamts hinweggesetzt haben, ist eine Vielzahl von Personen als „andere Person“ in die AD PMK gespeichert, obwohl es dafür keine Rechtfertigung gibt. Deshalb haben wir die Staatsschutzdienststellen aufgefordert, die unzulässige Speicherung „anderer Personen“ in der AD PMK zu löschen.

Das Landeskriminalamt haben wir vorsorglich darauf hingewiesen, dass sich die ausufernde Praxis der Staatsschutzdienststellen bei der Erfassung „anderer Personen“ in der AD PMK auch nicht dadurch heilen lasse, dass das Landeskriminalamt den Kreis der Betroffenen in seinem Verfahrensverzeichnis einfach entsprechend erweitert. Denn mit einer Erfassung in der AD PMK gehen gravierende Eingriffe in das Grundrecht auf informationelle Selbstbestimmung einher. Die AD PMK ist ein besonders eingriffsintensives Informationssystem. Den klassischen Staatsschutzdelikten, die zu einer Speicherung in der AD PMK führen können, wird ein schwerer Unrechtsgehalt beigemessen, wie der jeweilige Strafrahmen und die bisweilen sogar auf Vorbereitungshandlungen ausgedehnte Strafbarkeit zeigen. Bei anderen Straftaten müssen über die normalen Ermittlungsergebnisse hinaus Anhaltspunkte dafür vorliegen, dass der Betroffene mit seiner Tat eigentlich politisch motivierte Ziele verfolgt. Ist jemand in der AD PMK erfasst, können nicht nur die speichernde Staatsschutzdienststelle, sondern alle Staatsschutzdienststellen im Lande rund um die Uhr in Sekundenschnelle die gespeicherten Daten online abfragen. Geht deshalb schon mit der Erfassung als Beschuldigter oder Tatverdächtiger in der AD PMK ein gravierender Eingriff in das Recht auf informationelle Selbstbestimmung einher, ist dieser Eingriff bei einer Erfassung als „andere Person“ noch belastender, weil damit der Betroffene in einen Zusammenhang mit klassischen

Staatsschutzdelikten oder anderen politisch motivierten Straftaten gerückt wird, obwohl von ihm keine Gefahr für die öffentliche Sicherheit ausgeht. Deshalb sind der Speicherung „anderer Personen“ nach dem Grundsatz der Verhältnismäßigkeit enge Grenzen gezogen. Sie dürfen, wenn überhaupt, in der AD PMK nur ausnahmsweise erfasst werden, wenn die erforderlichen Informationen durch Maßnahmen gegen den Beschuldigten, Tatverdächtigen oder den Störer nicht oder nicht rechtzeitig erhoben werden können und zureichende tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Aufklärung oder vorbeugenden Bekämpfung schwer wiegender politisch motivierter Straftaten oder zur Abwehr einer im Einzelfall bestehenden erheblichen Gefahr erforderlich ist.

Anhaltspunkte, die eine solche Annahme rechtfertigen könnten, haben sich in den Beispielsfällen und den weiteren Fällen, die Gegenstand unserer Stichprobe gewesen sind, aus den Akten der Staatschutzdienststellen jedenfalls nicht ergeben. So ermöglicht allein der in den polizeilichen Akten festgehaltene Umstand, dass der 23-jährige Mann seinen Ausweis beim Ausländeramt verlustig gemeldet hat, nicht den Schluss, dass er politisch motivierte Straftaten im Schilde führt. Ebenso wenig vermag der Umstand, dass der 31-jährige Mann türkischer Staatsangehörigkeit von der Waffenbehörde eine waffenrechtliche Erlaubnis erhalten hat, eine solche Annahme zu rechtfertigen; im Gegenteil: die Waffenbehörde hat ihm ja gerade seine Integrität und Zuverlässigkeit bescheinigt, sonst hätte sie ihm nach dem Waffenrecht eine solche Erlaubnis nicht erteilen dürfen. Allein aus der Anmeldung eines Im- und Exports von Gebrauchtwagen, mit der der 31-jährige Mann aus Zaire seiner Anmeldepflicht nach der Gewerbeordnung nachgekommen ist, lässt sich nicht auf die Begehung schwer wiegender politisch motivierter Straftaten oder das Herbeiführen einer erheblichen Gefahr für die öffentliche Sicherheit schließen. Deshalb und weil sich auch aus den Akten der Staatsschutzdienstellen keine Anhaltspunkte für die Annahme ergeben, dass diese Personen im Zusammenhang mit schwer wiegenden politisch motivierten Straftaten oder erheblichen Gefahren für die öffentliche Sicherheit stehen, war die AD PMK-Erfassung in den geschilderten Fällen unzulässig. Entsprechendes gilt bei dem Arzt aus Kairo und den 187 Personen, die wie er zum Freitagsgebet eine Moschee aufgesucht haben. Dass es in der Moschee durch Dritte zu strafbaren Verhaltensweisen gekommen war, lässt dabei noch lange nicht den Schluss zu, dass alle Besucher der Moschee mit den begangenen Straftaten in Zusammenhang stehen oder sie gar befürworten oder unterstützen. Eine solche Zielrichtung kann bei dem Arzt und den übrigen 187 Moscheebesuchern, die zum traditionellen Freitagsgebet in die Moschee gegangen und dabei von der Polizei einer Personenkontrolle unterzogen worden waren, nicht einfach pauschal unterstellt werden. Bei Moscheebesuchern handelt es sich, wie jeder weiß, der die öffentlichen Diskussionen um islamische Moscheen und deren Besucher verfolgt hat, keineswegs um eine homogene Gruppe mit einheitlicher Motivation. Deshalb gilt nach wie vor: Das Vorliegen der Voraussetzungen für eine Speicherung in der AD PMK muss bei jeder einzelnen Person belegt sein; ein Pauschalverdacht reicht dafür nicht aus.

3.4 Zu lange gespeichert

Speichern die Staatsschutzdienststellen in der AD PMK personenbezogene Daten, müssen sie in regelmäßigen Abständen überprüfen, ob die Speicherung der Daten zur vorbeugenden Bekämpfung politisch motivierter Straftaten noch erforderlich ist. Das Polizeigesetz gibt dazu je nach Alter des Betroffenen und nach der Schwere des ihm zur Last gelegten Delikts abgestufte Fristen vor, die nicht überschritten werden dürfen. Diese gesetzlichen Vorgaben hat das Landeskriminalamt in seinem Leitfaden für die AD PMK präzisiert und für Beschuldigte/Tatverdächtige eine drei- und für „andere Personen“ eine zweijährige Überprüfungsfrist festgelegt. Maßgebend für den Beginn der Überprüfungsfrist ist dabei seit jeher nicht der Tag der Speicherung, sondern der Zeitpunkt, in dem sich das der AD PMK-Speicherung zugrunde liegen-

de Ereignis/Delikt zugetragen oder in dem die Polizei davon erfahren hat. Statt sich an diese Vorgaben zu halten, haben die Staatsschutzdienststellen für den Beginn des Laufs der AD PMK-Überprüfungsfrist in einer Vielzahl von Fällen auf den ein Jahr und oft noch später liegenden Zeitpunkt der AD PMK-Speicherung abgestellt. Dies führte dazu, dass „andere Personen“ – nicht genug damit, dass sie überhaupt gespeichert worden sind – und Beschuldigte/Tatverdächtige in der AD PMK noch gespeichert sind, obwohl die zwei- bzw. drei-jährige Überprüfungsfrist (längst) abgelaufen ist. Wozu dies führt, sei an folgenden Beispielen erläutert:

– Eine 40-jährige Frau, die am 20. März 2001 im Zuge einer Demonstration gegen einen Castor-Transport vom Bundesgrenzschutz einer Personenkontrolle unterzogen und vom Bahnsteig verwiesen worden war, ist mittlerweile mehr als vier Jahre als „andere Person“ in der AD PMK gespeichert, weil die Staatsschutzdienstelle für den Beginn der Überprüfungsfrist statt auf den Tag der Personenkontrolle (20. März 2001) oder wenigstens auf den Tag, an dem sie kurz darauf davon Kenntnis erhalten hatte, auf den viel später liegenden Tag der Speicherung in der AD PMK (30. April 2003) abgestellt hat.

– Ein Mann, der im Januar 1997 als Zeuge in einem Strafprozess wegen Schutzgelderpressung aus Angst um seine Familie zunächst in Abrede gestellt hatte, von den Angeklagten geschlagen und erpresst worden zu sein, ist als Beschuldigter mit dem Tatvorwurf einer politisch motivierten uneidlichen Falschaussage immer noch in der AD PMK gespeichert, weil die Staatsschutzdienststelle ihn am 24. April 2003 für drei Jahre in der AD PMK gespeichert und für den Beginn der Speicherfrist auf diesen Tag abgestellt hat. Völlig unverständlich ist, dass die Staatsschutzdienststelle den Mann im Jahr 2003 überhaupt in der AD PMK gespeichert hat, weil sie schon 1997 nach der Einstellung des Ermittlungsverfahrens durch die Staatsanwaltschaft zutreffend in ihre Akte geschrieben hat, dass der Mann sich in einer notstandsähnlichen Lage befunden und nicht aus politischen Motiven, sondern aus Angst um seine Familie so gehandelt hat. Damit gibt es für die (weitere) Speicherung seiner Daten keine Rechtsgrundlage.

Als Fazit ist klar: Sicherlich ist es nicht damit getan, dass die vier Staatsschutzdienststellen die exemplarisch aufgeführten und vergleichbare AD PMK-Speicherungen bereinigen. AD PMK-Speicherungen, ohne dass es dafür einen Aktenrückhalt gibt und ohne dass die politische Motivation für die Straftat belegt ist, sind offenbar ebenso wenig eine Spezialität der überprüften vier Staatsschutzdienststellen wie die geschilderte unzulässige Praxis bei der Speicherung „anderer Personen“ und bei der Festlegung des Beginns der Überprüfungsfrist. Weil es sich dabei offenbar vielmehr um eine auch bei anderen Staatsschutzdienststellen weit verbreitete Praxis handelt, ist eine Revision der AD PMK angesagt. Dabei muss das Landeskriminalamt auch noch sein Verfahrensverzeichnis, das bisher bei den technischen und organisatorischen Datenschutzmaßnahmen praktisch nur weiße Stellen aufweist, auf Vordermann bringen.

PS: Mancher wird sich noch gefragt haben, wie der eingangs erwähnte Fall des jungen Mannes ausgegangen ist. Die Polizeidirektion hat gegen ihn wegen der erwähnten Sachbeschädigung kein Ermittlungsverfahren eingeleitet, weil sie selbst davon ausgegangen ist, dass gegen ihn kein Tatverdacht besteht. Deshalb war seine Speicherung in der AD PMK von Anfang an rechtswidrig. Erst nach einem längeren Schriftwechsel hat die Polizeidirektion seine AD PMK-Speicherung und die Speicherungen weiterer Jugendlicher, die sie nach dem gleichen Strickmuster im Zusammenhang mit der besagten Sachbeschädigung unzulässigerweise in der AD PMK erfasst hatte, dann doch gelöscht.

4. Einzelfälle

4.1 Btm-Hinweis gelöscht

Immer wieder wenden sich Bürger mit Eingaben an unser Amt, in denen so oder so ähnlich zu lesen steht: Neulich hat die Polizei mich kontrolliert und dabei meine Personalien überprüft. Nachdem die Polizeibeamten den Polizeicomputer anhand meiner Personalien abgefragt hatten, konfrontierten sie mich mit der Frage, ob ich Drogen genommen hätte, was ich guten Gewissens verneinen konnte. Gleichwohl musste ich meine Hosentaschen ausleeren und mein Auto inspizieren lassen. Auf meine Frage nach dem Grund erklärten mir die Polizeibeamten, ich sei wegen eines Btm-Delikts im Polizeicomputer gespeichert.

So schrieb uns ein junger Mann, der von uns geprüft wissen wollte, ob die Btm-Speicherung über ihn rechtens ist. Bei unseren Nachforschungen stellte sich heraus, dass er vor vier Jahren mit Bekannten frühmorgens nach einem Diskothekenbesuch nach Hause fahren wollte. An der Ausfahrt des Parkplatzes hatte die Polizei das Auto gestoppt und das Auto und die Insassen einer Kontrolle unterzogen. Dabei entdeckten die Polizeibeamten unter der Rückbank eine halbe Tablette Ecstasy. Wem von seinen Mitfahrern sie gehörte, ließ sich ebenso wenig klären wie die Frage, wie sie unter den Rücksitz des Autos gekommen war. Die Staatsanwaltschaft stellte das Ermittlungsverfahren gegen den jungen Mann mangels hinreichenden Tatverdachts umgehend ein und teilte dies der Polizei mit. Als wir die Polizeidienststelle, die den jungen Mann wegen dieses Vorfalls mit dem Tatvorwurf eines Verstoßes gegen das Betäubungsmittelgesetz im POLAS – das ist das automatisiert betriebene Informationssystem der baden-württembergischen Polizei – erfasst hatte, damit konfrontierten, drückte sie sofort die Löschtaste. Dies hätte sie freilich schon viel früher, nämlich sofort nach der Einstellung des Ermittlungsverfahrens, tun müssen, weil es – was aber Voraussetzung für eine Weiterspeicherung des Btm-Vorwurfs gewesen wäre – keine Anhaltspunkte für eine sog. Wiederholungsgefahr gegeben hatte.

4.2 Kein Sexualtäter

Ein 18 Jahre alter Schüler, der mit drei seiner Mitschüler nachmittags in der Stadt unterwegs gewesen und von der Polizei kontrolliert worden war, staunte nicht schlecht, als ihm die Polizeibeamten nach einer Abfrage des Polizeicomputers vorhielten, dass er als Sexualtäter gespeichert ist. Dass er damit vor seinen Mitschülern reichlich in Misskredit gebracht worden ist, könne man sich, wie er uns schrieb, leicht vorstellen; zu ändern sei dies – dessen sei er sich bewusst – jetzt nicht mehr. Wichtig sei für ihn, dass er im Polizeicomputer endlich nicht mehr als Sexualtäter erfasst sei.

Als wir die Polizeidienststelle, die den Schüler im Januar 2001 wegen einer Straftat des sexuellen Missbrauchs Widerstandsunfähiger im INPOL, also dem automatisiert betriebenen Informationssystem der Polizeien des Bundes und der Länder, und im POLAS erfasst hatte, darauf ansprachen, löschte sie die Datenspeicherungen sofort. Dies war entschieden zu spät. Bereits im März 2001 hatte die Staatsanwaltschaft der Polizeidienststelle mitgeteilt, dass sie das Ermittlungsverfahren gegen den Schüler mangels hinreichenden Tatverdachts eingestellt hat. Statt – wie geboten – die POLAS- und INPOL-Speicherung wenigstens jetzt zu löschen, entschied sich die Polizeidienststelle fürs Weiterspeichern. In ihrer Akte vermerkte sie dazu lapidar: „Tatverdacht bleibt letztendlich bestehen, triebbedingtes Verhalten.“ Davon konnte nach der Einstellungsverfügung der Staatsanwaltschaft jedoch keine Rede sein. Danach hatten sich der Schüler und seine Clique im Dezember 2000 in der Stadt getroffen und waren später zum Weiterfeiern in die elterliche Wohnung eines der Cliquenmitglieder, dessen Eltern gerade nicht zu Hause waren, gegangen. Nach einer Weile war der Schüler mit einem Mädchen aus der Clique in ein anderes Zimmer gegangen, um von den anderen ungestört zu sein. Als das Mädchen am anderen Tag von seiner

Mutter zur Rede gestellt wurde, erstattete es – wohl eher auf Druck seiner Mutter – Anzeige gegen den Schüler. In seiner polizeilichen Vernehmung gab das Mädchen an, dass sie beide in dem nicht abgeschlossenen Zimmer mit seinem Einverständnis Zärtlichkeiten ausgetauscht hatten und dass es auch damit einverstanden war, dass der Schüler es dabei teilweise ausgezogen hatte. Der Schüler hat das gemeinsame Tête-à-tête dann von sich aus beendet, als er bemerkte, dass das Mädchen wohl mehr Alkohol getrunken hatte, als es vertragen hat. Deshalb hatte die Staatsanwaltschaft in ihrer Einstellungsverfügung festgestellt, dass das Verhalten des Schülers nicht im strafrechtlich relevanten Bereich anzusiedeln war. An diese Feststellungen der Staatsanwaltschaft hätte sich die Polizeidienststelle halten und die Speicherungen des Schülers als Sexualtäter löschen müssen, weil es damit an Tatsachen für die Annahme des Verdachts einer Straftat des sexuellen Missbrauchs Widerstandsunfähiger fehlte. Dass die Polizeidienststelle den Schüler gleichwohl über Jahre hinweg im POLAS und im INPOL als Sexualtäter beließ, haben wir nur deshalb nicht beanstandet, weil sie im Zuge unserer Nachforschungen die Datenspeicherungen von sich aus prompt gelöscht hat. Fazit: Um solche unzulässigen Datenspeicherungen zu vermeiden, ist es für Polizeidienststellen erste Handlungsmaxime, sich nicht einfach über die Begründung staatsanwaltschaftlicher Einstellungsverfügungen hinwegzusetzen.

4.3 Eine Schreckschusspistole

Ein junger Mann aus Stuttgart war im April 2003 auf der Heimfahrt vom Bodensee von Beamten des Zolls gestoppt und einer zollrechtlichen Überprüfung unterzogen worden. Die Frage der Beamten, ob er Waffen mitführe, bejahte er und händigte ihnen seine Schreckschusspistole samt Magazin und den drei darin befindlichen Patronen aus. Die Beamten beschlagnahmten die Schreckschusspistole, weil der junge Mann für sie – was aber nach der erst wenige Tage zuvor in Kraft getretenen Änderung des Waffengesetzes jetzt Vorschrift war – keinen sog. kleinen Waffenschein hatte. Sein Einwand, sein Antrag auf Ausstellung eines solchen Waffenscheines liege unbearbeitet bei seiner Waffenbehörde, weil diese der durch das neue Waffenrecht ausgelösten Antragsflut nicht Herr geworden sei, blieb ungehört. Zwei Wochen später hatte er den kleinen Waffenschein bekommen. Seine Schreckschusspistole hatte der Zoll inzwischen zusammen mit einem Bericht zuständigkeitshalber an den benachbarten Polizeiposten weitergeleitet. Der Polizeiposten fertigte eine Anzeige wegen eines Vergehens gegen das Waffengesetz und füllte einen sog. POLAS-Erfassungsbeleg aus. Darin vermerkte der Polizeiposten, dass eine POLAS-Erfassung des jungen Mannes wegen des angeblichen Verstoßes gegen das Waffengesetz nicht in Frage kommt, weil es an der dafür erforderlichen Wiederholungsgefahr fehlt. Zugleich kreuzte der Polizeiposten in dem Formular auch die Rubrik „Fall mit normaler Speicherfrist“ an. Das Formular leitete der Polizeiposten an seine vorgesetzte Polizeidirektion weiter; dort kam es zu der für die POLAS-Erfassung zuständigen Datenstation, die ihn mit dem Tatvorwurf eines Vergehens gegen das Waffengesetz für fünf Jahre im POLAS erfasste.

Dies hatte für den jungen Mann – wie er uns geschrieben hat – Konsequenzen: Bei diversen Polizeikontrollen sei er jeweils nach der Abfrage des Polizeicomputers von den kontrollierenden Polizeibeamten mit dem gespeicherten Vorwurf des unerlaubten Waffenbesitzes konfrontiert worden. Wenn es damit jeweils sein Bewenden gehabt hätte, hätte er die Sache auf sich beruhen lassen. Alle Erklärungen und selbst das Vorzeigen seines kleinen Waffenscheins hätten jedoch nichts geholfen. Er sei jedes Mal einer „Spezialkontrolle“ unterzogen worden, die sich zum Teil über eine halbe Stunde hingezogen habe. Um nicht länger solchen Unannehmlichkeiten ausgesetzt zu sein, bat er uns zu prüfen, ob die Datenspeicherung über ihn rechtens ist.

Davon konnte keine Rede sein. Die Polizeidirektion hätte den jungen Mann mit dem Tatvorwurf des unerlaubten Waffenbesitzes auf keinen Fall im POLAS erfassen dürfen. Voraussetzung dafür ist, dass der Be-

troffene verdächtig ist, eine Straftat begangen zu haben, und tatsächliche Anhaltspunkte dafür vorliegen, dass er künftig eine Straftat begehen wird. An beiden Voraussetzungen fehlte es im Fall des jungen Mannes aus Stuttgart: Ein Verstoß gegen das Waffengesetz lag offensichtlich nicht vor. Deshalb hat die Staatsanwaltschaft das Ermittlungsverfahren eingestellt und zur Rehabilitation des jungen Mannes in den Gründen ihrer Einstellungsverfügung klargestellt, dass eine strafbare Handlung nicht feststellbar ist. Damit fehlte es zugleich an jeglicher Grundlage für die Annahme, der junge Mann werde künftig Straftaten begehen. Deshalb hatte der Polizeiposten zu Recht auf seinem POLAS-Erfassungsformular das Vorliegen einer sog. Wiederholungsgefahr verneint. Dass der junge Mann gleichwohl mit dem Tatvorwurf eines Vergehens gegen das Waffengesetz im POLAS erfasst worden und gespeichert geblieben ist, ist auf drei Fehler zurückzuführen: Zum einen hätte der Polizeiposten auf dem POLAS-Erfassungsformular nicht – wie aber geschehen – die Rubrik „Fall mit normaler Speicherfrist“ ankreuzen dürfen, sondern eintragen müssen, dass es sich um einen Fall für die Statistik handelt. Zum anderen hätte der Prüfdienst bei der Datenstation besser aufpassen und die widersprüchlichen Angaben des Polizeipostens auf dem POLAS-Erfassungsformular bemerken müssen und den (angeblichen) Verstoß gegen das Waffengesetz nicht einfach als Fall mit normaler Speicherfrist erfassen dürfen. Schief gelaufen ist zu allem Unglück auch noch etwas bei der vorgeschriebenen Mitteilung der Staatsanwaltschaft über den Ausgang des Ermittlungsverfahrens. Anhand dieser Mitteilungen müssen die Polizeidienststellen prüfen, ob sich die jeweiligen POLAS-Speicherungen noch im Rahmen der dafür geltenden Vorschriften halten. Weil entweder die Staatsanwaltschaft der Polizeidirektion keine Mitteilung über die alsbald nach der zollrechtlichen Kontrolle verfügte Einstellung des Ermittlungsverfahrens zukommen ließ oder weil die Mitteilung zwar erfolgte, jedoch bei der Datenstation der Polizeidirektion nicht ankam, war die Chance, dass es wenigstens auf die Mitteilung über den Ausgang des Ermittlungsverfahrens zur Löschung der POLAS-Speicherung gekommen wäre, vertan. Auf unsere Nachforschungen löschte die Polizeidirektion die POLAS-Speicherung sofort und bedauerte die von Anfang an unzulässige Datenspeicherung.

2. Abschnitt: Justiz

1. Die Neuregelung der akustischen Wohnraumüberwachung

In unserem 25. Tätigkeitsbericht für das Jahr 2004 (LT-Drucksache 13/3800) hatten wir ausführlich über das Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung vom 3. März 2004 und über den am 22. September 2004 vom Bundeskabinett beschlossenen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung berichtet.

Mit der Entscheidung vom 3. März 2004 hatte das Bundesverfassungsgericht Artikel 13 Abs. 3 des Grundgesetzes, der es dem Gesetzgeber ermöglicht, Ermächtigungen zur Wohnraumüberwachung zwecks Strafverfolgung zu schaffen, als verfassungsgemäß bewertet. Zugleich hatte das Bundesverfassungsgericht entschieden, dass die bisher geltenden Regelungen der Strafprozessordnung zur akustischen Wohnraumüberwachung im Hinblick auf den Schutz der Menschenwürde, den vom Rechtsstaatsprinzip umfassten Grundsatz der Verhältnismäßigkeit, die Gewährung effektiven Rechtsschutzes und den Anspruch auf rechtliches Gehör nicht den verfassungsrechtlichen Anforderungen genügen. Aus diesem Grund hatte es diese Regelungen in weiten Teilen für verfassungswidrig erklärt und dem Gesetzgeber aufgegeben, bis 30. Juni 2005 einen verfassungsgemäßen Rechtszustand herzustellen. Diese Zeitvorgabe konnte mit den Schlussberatungen in Bundestag und Bundesrat am 16. bzw. 17. Juni 2005 gerade noch eingehalten werden, sodass das Änderungsgesetz am 1. Juli 2005 in Kraft treten konnte. Im Vordergrund des Gesetzes stehen folgende Regelungen:

Die zentrale Eingriffsnorm des Gesetzes (§ 100 c der Strafprozessordnung [StPO]) regelt, dass das Abhören und Aufzeichnen des in einer Wohnung

nicht öffentlich gesprochenen Wortes voraussetzt, dass der Verdacht einer besonders schweren Straftat besteht. Eine solche liegt nach den Vorgaben des Bundesverfassungsgerichts nur vor, wenn die Straftat mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bedroht ist. Um diesem Erfordernis zu genügen, wurde der bisherige Anlasstatenkatalog unter dem Gesichtspunkt der Erheblichkeit überarbeitet. Der neue Straftatenkatalog, der die für eine akustische Wohnraumüberwachung in Betracht kommenden Delikte in § 100 c StPO abschließend aufzählt, enthält mehr als 60 Delikte unterschiedlichster Art. Sie entstammen dem Strafgesetzbuch, dem Ausländerrecht, dem Betäubungsmittelrecht, dem Kriegswaffenkontrollgesetz, dem Völkerstrafgesetzbuch und dem Waffengesetz. Im Hinblick auf den Umfang dieses Straftatenkatalogs ist auf eine Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht zur „Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung“ hinzuweisen. Diese stützt sich in erster Linie auf die Analyse der Verfahren, in denen Maßnahmen der akustischen Wohnraumüberwachung durchgeführt worden sind, über die der Bundestag – entsprechend der jährlichen Berichtspflicht – in den Jahren 1998 bis 2001 unterrichtet wurde. Die Studie kommt zu dem Ergebnis, dass ein erheblicher Teil der gesetzlich genannten Straftatbestände in keinem einzigen Fall im Untersuchungszeitraum zur Grundlage einer Abhörmaßnahme gemacht worden ist. Angesichts dessen sollte der Straftatenkatalog auch unter dem Aspekt der Erforderlichkeit einer kritischen Prüfung unterzogen werden.

Um auch das Organisationsdelikt „Bildung einer kriminellen Vereinigung“ in den Straftatenkatalog aufnehmen zu können, wurde der Strafrahmen des § 129 Abs. 4 des Strafgesetzbuchs für die Fälle, in denen der Zweck oder die Tätigkeit der „kriminellen Vereinigung“ auf bestimmte, als besonders schwer eingestufte Delikte gerichtet ist, „verdoppelt“, sodass die Höchststrafe von bisher fünf nun zehn Jahre beträgt. Diese Vorgehensweise ist nicht im Sinne des Bundesverfassungsgerichts. Denn die im Urteil des Bundesverfassungsgerichts vom 3. März 2004 bewusst vorgenommene Einschränkung auf besonders schwere Straftaten verliert ihre verfassungsrechtliche Bedeutung, wenn der Gesetzgeber diese Einschränkung dadurch umgeht, dass er den Strafrahmen in der erkennbaren Absicht erhöht, auf diesem Wege diese Deliktsform doch der akustischen Wohnraumüberwachung zugänglich zu machen.

Entsprechend den Vorgaben des Bundesverfassungsgerichts regelt das Gesetz, dass vertrauliche Gespräche zwischen sich nahe stehenden Personen, die keinen Bezug zu Straftaten aufweisen, nicht abgehört werden dürfen (absolut geschützter Kernbereich privater Lebensgestaltung). Die akustische Wohnraumüberwachung darf deshalb nur noch angeordnet werden, wenn aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass keine Äußerungen aus diesem absolut geschützten Bereich erfasst werden. Ergeben sich während der Überwachung Anhaltspunkte dafür, dass in den Kernbereich privater Lebensgestaltung eingegriffen wird, muss das Abhören und Aufzeichnen unterbrochen werden. Aufzeichnungen über solche Äußerungen sind zu löschen, die erlangten Informationen dürfen nicht verwertet werden. Die im Bundesrat diskutierte Vorgehensweise, die technische Aufzeichnung auch bei erkannten Eingriffen in den absolut geschützten Kernbereich fortzusetzen, was den Vorgaben des Bundesverfassungsgerichts eindeutig widersprochen hätte, wurde nicht in das Gesetz übernommen.

Die akustische Wohnraumüberwachung wird nun von eigens dafür eingerichteten Kammern der Landgerichte angeordnet, die mit dem späteren Strafverfahren nichts zu tun haben. Die anordnende Kammer ist über den Verlauf und die Ergebnisse der Maßnahme zu unterrichten. Sie entscheidet auch über den Abbruch der Maßnahme, deren Verlängerung und darüber, ob für erlangte Erkenntnisse ein Verwertungsverbot besteht.

Nach Abschluss der Überwachung sind die betroffenen Personen (Beschuldigte, gegen die sich die Maßnahme richtet, sonstige überwachte Personen, Inhaber und Bewohner der überwachten Wohnung) über die durchgeführten Maßnahmen zu unterrichten. Sie erhalten so die Möglichkeit, die Rechtsmäßigkeit der Anordnung und Durchführung der Maßnahme überprüfen zu lassen. In Ausnahmefällen kann die Benachrichtigung jedoch zurückgestellt werden.

Die Landesjustizverwaltungen müssen über die Bundesregierung dem Deutschen Bundestag jährlich über die Maßnahmen der akustischen Wohnraumüberwachung berichten. Um die parlamentarische Kontrolle der akustischen Wohnraumüberwachung zu stärken, wurde der Umfang der Berichtspflicht erweitert.

Ein Mangel des Gesetzes ist, dass wesentliche Begriffsbestimmungen wie der „unantastbare Kernbereich der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens“ offen geblieben sind. Diese werden wohl erst durch die Gerichtspraxis feste Konturen erlangen.

Auch wenn aus datenschutzrechtlicher Sicht noch Grund zur Kritik besteht, kann zusammenfassend festgestellt werden, dass die Neuregelung der akustischen Wohnraumüberwachung im Großen und Ganzen von dem Bemühen geprägt ist, das Urteil des Bundesverfassungsgerichts vom 3. März 2004 möglichst genau umzusetzen, was angesichts der umfangreichen und detaillierten Vorgaben des Gerichts sicher keine leichte Aufgabe war.

2. Die Neuregelung der forensischen DNA-Analyse

Am 1. November 2005 ist das Gesetz zur Novellierung der forensischen DNA-Analyse vom 12. August 2005 (BGBl. I S. 2360) in Kraft getreten. Vorausgegangen waren kontroverse Diskussionen über das Ausmaß der Erweiterung des Anwendungsbereichs der DNA-Analyse im Strafverfahren.

So brachten mehrere Bundesländer im Februar 2005 einen Gesetzentwurf im Bundesrat ein, mit dem sie die DNA-Analyse dem herkömmlichen Fingerabdruck gleichsetzen wollten. Der Entwurf sah vor, bei der DNA-Analyse zur Identitätsfeststellung in künftigen Strafverfahren den Richtervorbehalt und die materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten zu streichen. Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse führe zu keinem schwerwiegenderen Eingriff als herkömmliche erkennungsdienstliche Maßnahmen, trifft jedoch nicht zu: Bereits nach dem derzeitigen Stand der Technik lassen sich aus den sog. nicht codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus gewisse Zusatzinformationen entnehmen (z. B. Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, möglicherweise Hinweise auf bestimmte Krankheiten). Welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden, ist nicht absehbar. Darüber hinaus hat das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse für Zwecke künftiger Strafverfahren nur im Hinblick auf die damaligen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung vom 17. Februar 2005 (s. Anhang 1) daher dafür ausgesprochen, dass eine Prognose schwerer Straftaten und eine richterliche Anordnung im Hinblick auf diese Rechtsprechung Voraussetzung einer derartigen Maßnahme bleiben müssen und die besondere Qualität dieses Grundrechtseingriffs bei allen Überlegungen, die zu einer Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden muss. Da der genannte Gesetzentwurf im Bundesrat keine Mehrheit fand, kam es letztlich nicht zu einer Gleichsetzung der DNA-Analyse mit dem herkömmlichen Fingerabdruck.

Dafür ist der Anwendungsbereich der DNA-Analyse durch das eingangs genannte Gesetz vom 12. August 2005 erheblich erweitert worden: Der Richtervorbehalt für anonyme Tatortspuren entfällt. Gleiches gilt – und zwar sowohl für DNA-Analysen im laufenden Ermittlungsverfahren als auch bei solchen, die zur Identitätsfeststellung in Fällen künftiger Strafverfolgung eingesetzt werden –, wenn der Betroffene einwilligt. Bei DNA-Analysen für Zwecke künftiger Strafverfahren führt das Gesetz außerdem zu einer Absenkung der an die Anlasstat und die Negativprognose zu stellenden Anforderungen. So war die Durchführung von DNA-Analysen für Zwecke künftiger Strafverfahren nach § 81 g der Strafprozessordnung (StPO) bislang nur zulässig, wenn eine Straftat von erheblicher Bedeutung oder eine

Sexualstraftat begangen worden war (Anlasstat) und wenn zu erwarten war, dass gegen den Betroffenen künftig Strafverfahren wegen Straftaten von erheblicher Bedeutung zu führen sein werden (qualifizierte Negativprognose). Nun regelt § 81 g Abs. 1 Satz 2 StPO, dass die wiederholte Begehung sonstiger Straftaten im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen kann. Ferner wurden die in § 81 g StPO bisher enthaltenen Regelbeispiele für eine Straftat von erheblicher Bedeutung gestrichen. Außerdem wurde die DNA-Reihenuntersuchung im laufenden Ermittlungsverfahren erstmals gesetzlich geregelt. Wesentliche Voraussetzungen für einen Reihengentest sind, dass Verbrechen gegen Leben, Leib, Freiheit oder sexuelle Selbstbestimmung vorliegen, ein Richter den Reihengentest anordnet und der betroffene Personenkreis anhand von Prüfungsmerkmalen umschrieben ist. Außerdem ist klargestellt, dass die betroffenen Personen nicht zur Mitwirkung verpflichtet sind, dass sie über die Freiwilligkeit ihrer Mitwirkung zu belehren sind und die erhobenen Daten nicht in der DNA-Analysedatei gespeichert werden.

Obwohl es nicht zu einer Gleichstellung der DNA-Analyse mit dem herkömmlichen Fingerabdruck gekommen ist, sind auch die neuen gesetzlichen Regelungen aus datenschutzrechtlicher Sicht äußerst problematisch:

Feststellung, Speicherung und (künftige) Verwendung des DNA-Identifizierungsmusters greifen in das durch das Grundgesetz verbürgte Recht auf informationelle Selbstbestimmung ein. Einschränkungen seines Rechts auf informationelle Selbstbestimmung muss der Einzelne nur im überwiegenden Allgemeininteresse hinnehmen. Zwar hat das Bundesverfassungsgericht immer wieder die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung hervorgehoben, das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren betont und die wirksame Aufklärung von Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet. Es hat jedoch auch betont, dass dieses legitime Interesse Eingriffe in das Grundrecht des Betroffenen auf informationelle Selbstbestimmung nur insoweit zu rechtfertigen vermag, als dabei nicht gegen das Übermaßverbot verstoßen wird. So hat das Bundesverfassungsgericht in den bereits erwähnten Entscheidungen aus den Jahren 2000 und 2001 den Grundsatz der Verhältnismäßigkeit im Hinblick auf die damaligen Regelungen für die Durchführung einer DNA-Analyse für Zwecke künftiger Strafverfahren als gewahrt angesehen, weil Voraussetzung für die Durchführung einer solchen DNA-Analyse das Vorliegen einer Straftat von erheblicher Bedeutung und die auf bestimmte Tatsachen beruhende Prognose gewesen ist, dass gegen den Betroffenen künftig Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sein werden. Im Gegensatz zur früheren Rechtslage lässt der seit 1. November 2005 geltende § 81 g Abs. 1 StPO als Anlasstaten, aber auch im Rahmen der Negativprognose die wiederholte Begehung bzw. die zu erwartende wiederholte Begehung auch leichtester Straftaten genügen, sofern diese in ihrem Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen. Das Erfordernis einer einzelnen Straftat von erheblicher Bedeutung wird damit sowohl bei der Anlasstat als auch bei der Negativprognose aufgegeben. Die verfassungsrechtlich gebotene Anforderung einer Straftat von erheblicher Bedeutung wird damit in verfassungsrechtlich bedenklicher Weise relativiert. Unter welchen Voraussetzungen eine Gleichsetzung der wiederholten Begehung sonstiger Straftaten mit einer Straftat von erheblicher Bedeutung möglich und zulässig sein soll bzw. welche Kriterien für den Vergleich heranzuziehen sind, ist dem Gesetz nicht zu entnehmen. Aufgrund dieser Auslegungs- und Anwendungsprobleme ist zu befürchten, dass sich die Praxis in schematische Betrachtungen flüchten wird, die mit dem Erfordernis, in jedem Einzelfall eine am Verhältnismäßigkeitsgrundsatz orientierte Entscheidung zu treffen, unvereinbar sind und letztlich eine erhebliche Ausweitung des Anwendungsbereichs der DNA-Analyse für Zwecke künftiger Strafverfahren erwarten lassen. Dabei muss man sich stets vor Augen halten – was in der stark emotionalisierten öffentlichen Diskussion häufig übersehen wird –, dass es in diesem Zusammenhang nicht um den Einsatz der DNA-Analyse zur Aufklärung bereits geschehener Straftaten geht, sondern darum, in welchem Ausmaß Daten aus DNA-Analysen für die Aufklärung künftiger Straftaten erfasst und gespeichert werden dürfen. Da von einer

derartigen Vorratsdatenspeicherung zwangsläufig in einer Vielzahl auch solche Personen betroffen sind, die später überhaupt nicht mehr straffällig werden, kommt der Beachtung des Verhältnismäßigkeitsgrundsatzes besonderes Gewicht zu.

Die in § 81 g Abs. 1 StPO bislang genannten Regelbeispiele für eine Straftat von erheblicher Bedeutung (z. B. Verbrechen, gefährliche Körperverletzung oder Diebstahl in einem besonders schweren Fall) stellten eine geeignete Orientierungshilfe dar, die eine einheitliche Anwendung des Begriffs sicherstellte und dem Verhältnismäßigkeitsgrundsatz Rechnung trug. Aufgrund der Streichung der Regelbeispiele ist eine Absenkung der Anforderungen zu befürchten, die das Verfassungsrecht stark strapaziert.

Wäre eine maßvolle Senkung der rechtlichen Anforderungen an die Anlasstat noch zu akzeptieren gewesen, so dürfte die gleichzeitige starke Relativierung der Negativprognose praktisch zu einer Beseitigung dieser Rechtshürde führen. Denn wer würde in Frage stellen, dass sich – ist einmal die Voraussetzung einer Anlasstat in Form des Verdachts der mehrfachen Begehung von einfachen Straftaten gegeben – nicht jederzeit Gründe dafür finden lassen anzunehmen, dass eine in diesem Umfang auffällig gewordene Person künftig erneut weiterer nur einfacher Straftaten verdächtig werden kann? Auch das immer wieder gehörte Argument, mit einer Erweiterung des Einsatzes der DNA-Analyse wolle man frühzeitig Straftäterkarrieren auf die Schliche kommen, hätte eine derart starke Relativierung der Negativprognose nicht erfordert. Denn mit der neuen gesetzlichen Regelung wird gerade nicht nur die mögliche Entwicklung eines Straftäters von der einfachen zur mittleren und möglicherweise zur schweren Kriminalitätsebene erfasst, sondern es geraten auch Personen in die DNA-Datei, die ausschließlich dem Kleinkriminellenmilieu zuzuordnen sind, wenn man für die Prognose den künftigen Verdacht weiterer einfacher Straftaten genügen lassen will. Ob die grundsätzliche Beibehaltung des Richtervorbehalts hier ein ausreichendes Regulativ für einen allzu extensiven Einsatz der DNA-Analyse sein kann, wird abzuwarten sein.

Auch gegen die Entnahme und molekulargenetische Untersuchung von Körperzellen aufgrund einer schriftlichen Einwilligung des Beschuldigten zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren bestehen erhebliche Bedenken (§ 81 g Abs. 3 StPO). Denn zum einen kann die Einwilligung des Beschuldigten nicht das Vorliegen der materiell-rechtlichen Voraussetzungen einer solchen DNA-Analyse ersetzen. Zum anderen wird der Beschuldigte zu einer Beurteilung der Frage, ob diese Voraussetzungen vorliegen, in der Regel nicht in der Lage sein. Ihm ist auch nicht zuzumuten, dass er sich sozusagen selbst eine Negativprognose stellt. Der Verzicht auf die richterliche Anordnung lässt deshalb befürchten, dass die besonderen Voraussetzungen für eine DNA-Analyse zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren in der Praxis über das Instrument der Einwilligung zunehmend ausgehöhlt werden.

Die Regelungen zum DNA-Reihengentest sind zwar deshalb grundsätzlich zu begrüßen, weil damit für einen Bereich, der in der Praxis sehr unterschiedlich gehandhabt wurde, ein einheitlicher Rechtsrahmen gesetzt wird, der mehr Rechtsklarheit verspricht. Allerdings sind die Regelungen aus datenschutzrechtlicher Sicht ergänzungsbedürftig, und dies aus folgenden Gründen: Von einem DNA-Reihengentest werden regelmäßig ganz überwiegend unverdächtige Bürger betroffen. Sie werden dabei in eine persönliche Nähe zur aufzuklärenden Straftat gerückt. Dabei besteht die Gefahr, dass die klassische Unschuldsvermutung auf den Kopf gestellt wird. Praktisch kann jeder zumindest so lange verdächtig sein, bis er seine Unschuld durch eine DNA-Analyse nachgewiesen hat. Ein solcher DNA-Reihengentest kann daher nur ultima ratio sein. Im neuen § 81 h StPO sollte daher ausdrücklich geregelt werden, dass ein DNA-Reihengentest gegenüber anderen gesetzlich vorgesehenen Ermittlungsmaßnahmen subsidiär sein muss.

3. DNA-Analysen für Vaterschaftstests

Im Frühjahr 2005 hat das Land Baden-Württemberg im Bundesrat den Entwurf eines Gesetzes zum Schutz der Persönlichkeitsrechte bei Abstammungsuntersuchungen eingebracht (BR-Drucksache 280/05). Dieser Ent-

wurf sieht vor, den nach § 1600 Abs. 1 des Bürgerlichen Gesetzbuchs anfechtungsberechtigten Personen heimliche Vaterschaftstests zu erlauben. Zulässig wären heimliche Vaterschaftstests somit für den Scheinvater, den leiblichen Vater, die Mutter und das Kind. Da der Gesetzentwurf erhebliche rechtliche und praktische Fragen aufwirft, hat der Rechtsausschuss des Bundesrats im Mai 2005 beschlossen, die Beratung der Vorlage bis zum Wiederaufruf durch das Antrag stellende Land zu vertagen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich bereits in der Vergangenheit gegen heimliche Vaterschaftstests ausgesprochen. Im Jahr 2005 ist die Problematik vor allem im Zusammenhang mit zwei Entscheidungen des Bundesgerichtshofs vom 12. Januar 2005 (Az. XII ZR 60/03 und XII ZR 227/03) in das Blickfeld der Öffentlichkeit geraten. Nach diesen Entscheidungen sind heimliche Vaterschaftstests nach geltender Rechtslage rechtswidrig und im Vaterschaftsanfechtungsverfahren nicht verwertbar, weil die Verwertung einen erneuten Verstoß gegen das Persönlichkeitsrecht und das Grundrecht auf informationelle Selbstbestimmung des Kindes bedeuten würde.

Durch eine Legalisierung heimlicher Vaterschaftstests würde den Interessen der Väter, ihre Vaterschaft feststellen zu lassen, der Vorrang vor den Persönlichkeits- und Datenschutzrechten der Kinder eingeräumt werden. Im Gesetzentwurf von Baden-Württemberg wird dies damit begründet, dass die familiären Beziehungen durch heimliche Vaterschaftstests geschont würden bzw. die Verwendung des Genmaterials einem legitimen Ziel diene, weshalb die heimliche Verwendung von Genmaterial angesichts der verschiedensten grundrechtlich geschützten Positionen der Betroffenen zugelassen werden könne.

Bei allem Verständnis für die Interessen der Väter ist fraglich, ob diese Argumentation dem Grundrecht auf informationelle Selbstbestimmung der Kinder die gebührende Bedeutung beimisst und ob die genannten Gesichtspunkte heimliche Vaterschaftstests zu rechtfertigen vermögen. Denn mit heimlichen Vaterschaftstests gehen gravierende Eingriffe in das informationelle Selbstbestimmungsrecht derjenigen einher, deren DNA-Proben ohne Einwilligung untersucht werden, zumal diese Tests zugleich immer die Familie betreffen, der das Grundgesetz den besonderen Schutz des Staates zusichert.

Soweit die derzeitige Rechtslage unbefriedigend sein sollte, erscheint es zwar vertretbar, die Feststellung der Abstammung unter leichteren Voraussetzungen als bisher zuzulassen. Dabei darf jedoch nicht außer Betracht bleiben, dass der Bundesgerichtshof in seinen Entscheidungen vom 12. Januar 2005 betont hat, dass heimlich veranlasste DNA-Vaterschaftstests einen Verstoß gegen das Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung der betroffenen Kinder darstellen. Diesem Grundrecht des Kindes steht zwar ein ebenfalls aus dem allgemeinen Persönlichkeitsrecht abzuleitendes Recht des Vaters oder Scheinvaters auf Kenntnis seiner Vaterschaft gegenüber. Dieses ist jedoch – so der Bundesgerichtshof – auch dann nicht als höherrangig anzusehen, wenn es der Abwehr zivilrechtlicher Ansprüche, denen ein gesetzlicher Vater ausgesetzt ist, dienen soll. Um den Interessen aller Betroffenen gerecht zu werden, sollten DNA-Vaterschaftstests daher nur durchgeführt werden dürfen, wenn alle Betroffenen wirksam einwilligen oder wenn eine fehlende Einwilligung im Rahmen eines gerichtlichen Verfahrens ersetzt wird.

4. Mangelnde Unterstützung des Landesbeauftragten für den Datenschutz ...

Leider kommt es immer wieder vor, dass öffentliche Stellen nur sehr zögerlich der gesetzlich verankerten Pflicht nachkommen, den Landesbeauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm im Rahmen seiner Kontrollbefugnis Auskunft zu den abzuklärenden Datenschutzfragen zu geben. Auch im Justizbereich gibt es derartige Fälle:

4.1 ... durch das Justizministerium

Wie bereits im 25. Tätigkeitsbericht für das Jahr 2004 nachzulesen ist (LT-Drucksache 13/3800, S. 95), führten wir im Juni 2004 bei einer

Justizvollzugsanstalt eine Kontrolle durch, deren Schwerpunkt im Bereich der elektronischen Datenverarbeitung lag. Die anlässlich des Kontrollbesuchs festgestellten schwerwiegenden Mängel, die in unserem letztjährigen Tätigkeitsbericht beschrieben sind, hat das Justizministerium zwar unverzüglich behoben und unsere Dienststelle auch umgehend über seine Maßnahmen informiert. Die von uns mit Kontrollbericht vom August 2004 angeforderte umfassende Stellungnahme hat das Justizministerium jedoch trotz mehrerer telefonischer und schriftlicher Mahnungen erst im August 2005 vorgelegt.

Dass das Justizministerium der im Landesdatenschutzgesetz geregelten Unterstützungspflicht trotz wiederholter Bitten meiner Dienststelle nicht in angemessener Zeit, sondern erst nach Ablauf eines Jahres nachgekommen ist, musste ich schließlich förmlich beanstanden.

4.2 ... durch eine Staatsanwaltschaft

Bei der Bearbeitung von Bürgereingaben ist die verzögerte Abgabe von Stellungnahmen durch öffentliche Stellen oder die nur teilweise Beantwortung unserer Fragen besonders ärgerlich. Denn bevor die von uns bei Behörden angeforderten Stellungnahmen eingehen bzw. solange die von uns gestellten Fragen nicht vollständig beantwortet sind, ist die abschließende Bearbeitung einer Eingabe nicht möglich. Die zögerliche Beantwortung unserer Anfragen führt somit letztlich dazu, dass wir Eingaben von Bürgern nicht in angemessener Zeit bescheiden können. So geschehen im folgenden Fall, den uns der Beschwerdeführer bereits im Frühjahr 2004 vorgelegt hatte und den wir – mangels ausreichender Angaben der von uns angeschriebenen Behörde – erst im Frühjahr 2005 abschließen konnten:

Gegen den Beschwerdeführer, der sich an uns wandte, war ein Ermittlungsverfahren wegen des Verdachts des Verstoßes gegen das Urheberrechtsgesetz geführt worden, das letztendlich eingestellt wurde. Dem Beschwerdeführer war vorgeworfen worden, illegal vervielfältigte Computersoftware bezogen und auf seinem Computer installiert zu haben. Im Rahmen der Ermittlungen hatte sich die Staatsanwaltschaft mit Schreiben vom 2. September 2003 an ein Software-Unternehmen gewandt, das Rechteinhaber von zwei der betroffenen Programme war, und nach Auflistung der vom Beschwerdeführer vorgelegten und von ihm eingetragenen Product Keys (hierbei handelt es sich um Zeichenfolgen, die vor erstmaliger Benutzung der Software eingegeben werden müssen) folgende Fragen gestellt:

1. Lässt sich an diesen Product Keys feststellen, wann oder ab wann die betreffenden Programme im Handel erhältlich waren?
2. Kann anhand der Versionsnummern festgestellt werden, ab wann diese Programme im Handel erhältlich waren?
3. Kann festgestellt werden, ob diese Product Keys tatsächlich vergeben oder nur errechnet wurden?

Außerdem war in dem Schreiben der Name des Beschwerdeführers angegeben. Mit gleichem Schreiben wandte sich die Staatsanwaltschaft auch an eine Organisation, in der sich Soft- und Hardware-Unternehmen zusammengeschlossen haben und die sich als führend im Bereich der Förderung einer sicheren und gesetzesmäßigen Online-Welt bezeichnet.

Da sich die gestellten Fragen ausschließlich auf die Programme und nicht auf die Person des Beschwerdeführers bezogen, war nicht ersichtlich, weshalb in den Schreiben der Name des Beschwerdeführers angegeben worden war. Im Mai 2004 baten wir deshalb die Staatsanwaltschaft, uns den Grund hierfür mitzuteilen. Nachdem die erste Stellungnahme der Staatsanwaltschaft für eine datenschutzrechtliche Beurteilung des Vorgangs nicht ausreichte, erläuterte die Staatsanwaltschaft in einer zweiten von uns angeforderten Stellungnahme, dass mit den an die beiden Stellen gerichteten Schreiben insbesondere geklärt werden sollte, ob die vom Beschwerdeführer vorgelegten Product Keys, die

nicht mit denen auf den sichergestellten Rechnern des Beschwerdeführers übereinstimmten, an diesen vergeben worden waren, wofür die Nennung des Namens des Beschwerdeführers nötig gewesen wäre.

In unserem nächsten Schreiben vom August 2004 wiesen wir die Staatsanwaltschaft darauf hin, dass der von ihr angeschriebenen Software-Firma keine Informationen darüber vorliegen, welcher Kunde Software mit einem bestimmten Product Key im Fachhandel erworben hat, weshalb die Erforderlichkeit der Übermittlung personenbezogener Daten nach wie vor nicht nachvollziehbar sei. Ebenfalls nicht klar war, inwiefern sich die Staatsanwaltschaft von dem ebenfalls angeschriebenen Zusammenschluss von Soft- und Hardware-Unternehmen relevante Informationen für das Ermittlungsverfahren erhoffen konnte. Wir baten daher um nochmalige Äußerung und Zusendung des mit den beiden Stellen geführten Schriftverkehrs.

Auf diese mussten wir – trotz zweimaliger Erinnerungen – fünf Monate warten. Erst nach Ankündigung einer Beanstandung erhielten wir im Januar 2005 ein Antwortschreiben der Staatsanwaltschaft. Dieses enthielt jedoch keine neuen Argumente und auch der angeforderte Schriftverkehr war nicht beigefügt. Die Staatsanwaltschaft führte hierzu aus, dass durch die Vorlage einzelner Schriftstücke aus den Ermittlungsakten ein verzerrtes Bild entstehen könnte. Sie stellte daher ein Ersuchen um vollständige Akteneinsicht anheim. Erst auf unser weiteres Schreiben vom Februar 2005, in dem wir u. a. zur Vorlage der vollständigen Akten aufforderten, gab die Staatsanwaltschaft im März 2005 eine ausführliche Stellungnahme ab. Die vollständigen Akten übersandte die Staatsanwaltschaft jedoch nicht. Stattdessen legte sie lediglich nun doch die von uns bereits im August 2004 angeforderten Aktenstücke vor. Damit wurde uns erst durch das Schreiben der Staatsanwaltschaft vom März 2005 und die diesem Schreiben beigefügten Schriftstücke – also erst nach einem knappen Jahr seit Eingang der Beschwerde – die abschließende Bearbeitung des Falles möglich.

Dass die Behandlung unserer Anfrage durch die Staatsanwaltschaft nicht mit der in § 29 LDSG geregelten Unterstützungspflicht in Einklang zu bringen ist, bedarf keiner weiteren Erläuterung.

Zur Abrundung dieses Beitrags ist noch darauf hinzuweisen, dass die Einholung der rein produktbezogenen Fragen in dem an das Software-Unternehmen gerichteten Schreiben der Staatsanwaltschaft aus einer ex-ante-Sicht für die Führung des Ermittlungsverfahrens durchaus als erforderlich anzusehen ist. Die Übermittlung personenbezogener Daten des Beschwerdeführers war für die Beantwortung der in diesem Schreiben gestellten Fragen dagegen weder geeignet noch erforderlich und somit unzulässig. Die zweite Anfrage der Staatsanwaltschaft ging aber vollkommen ins Leere. Die Staatsanwaltschaft hatte wohl angenommen, dass es sich bei der angeschriebenen Organisation, in der sich Soft- und Hardware-Unternehmen zusammengeschlossen haben, um sich durch politische und informationelle Initiativen für die Förderung einer sicheren und gesetzesmäßigen Online-Welt einzusetzen, um ein Software-Unternehmen handelt, das Rechteinhaber eines auf den Rechnern des Beschwerdeführers installierten Programms ist. Da dies nicht der Fall ist, war diese Organisation bereits für die produktbezogenen Fragen die falsche Ansprechpartnerin, weshalb die Übermittlung personenbezogener Daten erst recht unzulässig war.

5. Angaben im Sichtfenster von Gerichtsschreiben

Im 25. Tätigkeitsbericht für das Jahr 2004 hatten wir von einem Fall berichtet, in dem ein Amtsgericht im Sichtfenster eines dem Kläger eines Zivilrechtsstreits formlos zugestellten Schreibens das Aktenzeichen des Verfahrens angegeben hatte. Da man den Aktenzeichen der ordentlichen Gerichtsbarkeit, also der Zivil- und Strafgerichtsbarkeit, entnehmen kann, ob es sich um ein zivilrechtliches oder um ein strafrechtliches Verfahren handelt, stellt die Angabe eines solchen Aktenzeichens im Sichtfenster eines Briefes ein personenbezogenes Datum dar. Dem Aktenzeichen ist zwar lediglich zu entnehmen, dass der Betroffene in einer Zivil- oder Strafrechtsangelegen-

heit mit dem Gericht zu tun hat und nicht, in welcher Funktion er beteiligt ist. Dennoch handelt es sich bei der Aktenzeichenangabe um eine – wenn auch nicht sehr aussagekräftige – Information, die Dritte nichts angeht und die auch für die Postzustellung nicht benötigt wird.

Das Justizministerium, an das wir uns wegen des Falles gewandt hatten, teilte inzwischen mit, dass die Aktenzeichenangabe im Sichtfenster von formlos zugestellten Briefen aus dem Bereich der ordentlichen Gerichtsbarkeit auf dem Einsatz von Computerprogrammen beruhe, die entsprechende Formatgestaltungen für gerichtliche Schreiben enthalten. Das Justizministerium ist zwar der Ansicht, dass die derzeitige Vorgehensweise datenschutzrechtlich nicht relevant und außerdem zur Erfüllung der Aufgaben der Gerichte erforderlich und zulässig sei. Dennoch ist davon auszugehen, dass im Sichtfenster von formlos zugestellten Briefen der ordentlichen Gerichtsbarkeit in einigen Monaten keine Aktenzeichen mehr erscheinen werden. Denn die derzeit eingesetzten Computerprogramme werden in absehbarer Zeit durch ein anderes Programm ersetzt werden, das voraussichtlich im Laufe des Jahres 2006 zum Einsatz kommen wird. Wie das Justizministerium hierzu ausführte, seien die Textmasken dieses Programms so gestaltet, dass das Verfahrensaktenzeichen nicht mehr im Sichtfenster der Briefe erscheint.

3. Teil: Gesundheit und Soziales

Dass das Problembewusstsein bei einer zunehmenden Zahl von Personen hinsichtlich des Schutzes ihrer personenbezogenen Daten im Bereich des Gesundheits- und Sozialwesens in den vergangenen Jahren zugenommen hat, ist eine Tatsache, die meine Dienststelle im Berichtszeitraum durch eine erneut gestiegene Anzahl von Bürgereingaben zu spüren bekam. Aber auch die Bitten von Behördenseite um Beratung nahm zu.

Auch wir spüren damit, dass das Gesundheits- und Sozialwesen angesichts der bekannten Rahmenbedingungen (Sparzwänge, Überlegungen zur Reform der Sozialversicherungssysteme u. a.) zu einem der zentralen Handlungsfelder der Politik geworden und dadurch auch in den Focus der Medienöffentlichkeit gerückt ist. Datenschutzverletzungen in diesem sensiblen Bereich können die soziale Stellung sowie die physische oder psychische Unversehrtheit der betroffenen Menschen unmittelbar bedrohen. Gerade deshalb ist die gewissenhafte Beachtung von Datenschutz und Datensicherheit in unserer Informationsgesellschaft eine ganz wichtige Voraussetzung zur Schaffung des notwendigen Vertrauens zwischen den jeweils Betroffenen und den sonstigen Akteuren im Gesundheits- und Sozialbereich.

Jede Person hat Anspruch darauf, dass ihre Sozial- bzw. Patientendaten nicht unbefugt erhoben, verarbeitet oder genutzt werden. Damit ergibt sich für den Gesetzgeber zum einen die Verpflichtung, dies durch die gebotene Zurückhaltung im Rahmen seiner gesetzgeberischen Aktivitäten zu berücksichtigen. Er sollte gerade in diesem sensiblen Datenschutzbereich entsprechenden Begehrlichkeiten und Wünschen nach zusätzlichen Informationen zunächst skeptisch begegnen, indem er bei der Frage der „Erforderlichkeit“ bzw. „Geeignetheit“ einen strengen Prüfungsmaßstab anlegt. Das Bundesverfassungsgericht hat in seinem als Volkszählungsurteil bekannt gewordenen Urteil vom 15. Dezember 1983 bekanntlich die Messlatte sehr hoch gelegt und dem informationellen Selbstbestimmungsrecht der Betroffenen Grundrechtscharakter verliehen, weil „Selbstbestimmung eine elementare Funktionsbedingung eines (...) freiheitlich-demokratischen Gemeinwesens ist“.

Zum anderen ergibt sich in diesem Bereich für die Daten verarbeitenden Stellen und die handelnden Personen die Verpflichtung, durch aktives Handeln das Patienten- und Sozialgeheimnis zu schützen und darüber hinaus ein unbefugtes Erheben, Verarbeiten und Nutzen von Daten Betroffener zu unterlassen. Diese Forderung hat gerade für Baden-Württemberg besonderes Gewicht, denn dem erst jüngst vom Statistischen Landesamt veröffentlichten Branchenspiegel ist zu entnehmen, dass die meisten Beschäftigten im Südwesten Deutschlands im Bereich des Gesundheits- und Sozialwesens arbeiten und nicht, wie mancher vielleicht zunächst vermutet hätte, im Maschinenbau, in der Kfz-Produktion oder im Einzelhandel.

Dass unser Rat bei gesetzgeberischen Aktivitäten des Landes in diesem Bereich von den Ministerien oft schon in einem frühen Stadium des Gesetzgebungsverfahrens gesucht wurde, sei positiv erwähnt. Andererseits erfordert eine seriöse Befassung meiner Dienststelle mit dieser schwierigen Materie auch einen zeitlichen Vorlauf, der mehr Zeit in Anspruch nimmt als es die bedauerlicherweise oft viel zu kurz gewählten Äußerungsfristen zulassen (zum Teil nicht einmal eine Kalenderwoche). Eine fundierte Beratung lässt sich für den Datenschutz bei einem so knapp bemessenen Zeitfenster nur sehr eingeschränkt gewährleisten. Hier ist in Zukunft dringend eine zeitlich großzügigere Beteiligung durch die Ministerien anzumahnen; schließlich wird meine Dienststelle auch sehr stark von anderen öffentlichen Stellen um Rat gefragt, was ich im Übrigen als Vertrauensbeleg für mein Amt und als Ausdruck für ein gestiegenes Datenschutzbewusstsein bewerte.

Gleichwohl verwundert es nicht, dass es in der täglichen Praxis immer wieder zu Datenschutzverletzungen gekommen ist, mit denen wir uns im Berichtszeitraum zu befassen hatten. Gibt es doch gerade im Bereich des Gesundheits- und Sozialwesens viele Institutionen, handelnde Personen und Betroffene sowie ein komplexes und zum Teil unübersichtliches Regelungsgeflecht mit schwierigen Abgrenzungs- und Auslegungsfragen. Der Tätigkeitsbericht und die nachfolgenden Ausführungen vermögen daher auch nur einen kleinen Teilaus-

schnitt dessen wiederzugeben, womit wir uns in diesem sensitiven Bereich des Datenschutzes im Jahre 2005 zu befassen hatten.

1. Abschnitt: Gesundheit

1. Die elektronische Gesundheitskarte

Die „elektronische Gesundheitskarte (eGK)“ als Träger nicht nur von Verwaltungsdaten, sondern auch als Medium zur Übermittlung von Rezepten und in weiteren Ausbaustufen als Träger von medizinischen Informationen bzw. als Zugangsmittel zur Speicherung von solchen Informationen stellt ein höchst komplexes Projekt dar. Sie hat mit dem am 1. Januar 2004 in Kraft getretenen Gesundheitsmodernisierungsgesetz ins Sozialgesetzbuch Eingang gefunden (vgl. § 291 a des Fünften Buchs des Sozialgesetzbuchs [SGB V]) und soll zum 1. Januar 2006 eingeführt werden.

Bei dem Projekt handelt sich um eines der weltweit größten IT-Vorhaben, durch das rd. 80 Mio. Versicherte mit intelligenten Chipkarten ausgestattet und etwa 185 000 Ärzte, 22 000 Apotheken, 2 200 Krankenhäuser und ca. 260 Krankenkassen miteinander vernetzt werden sollen. Da Datenzugriffe der Leistungserbringer auf besonders sensible Patientendaten nach § 291 a Abs. 5 SGB V nur mit Hilfe eines elektronischen Heilberufsausweises statthaft sein werden, sind ergänzende landesgesetzgeberische Aktivitäten zur Änderung des Heilberufekammergesetzes erforderlich. Die flächendeckende Ausstattung der Leistungserbringer (Ärzte, Apotheker etc.) mit neuen elektronischen Heilberufsausweisen durch die Standesorganisationen stellt darüber hinaus eine erhebliche logistische Herausforderung dar. Gleiches gilt für die Krankenkassen, die ihre Versicherten komplett mit neuen Gesundheitskarten ausstatten müssen, wozu neben Lichtbildern (von allen) auch immerhin für rd. 40 Mio. Versicherte neue Krankenversichertennummern gehören.

Als Ende 2003 die Einführung der eGK vom Bundesgesetzgeber beschlossen wurde, ging man noch optimistisch davon aus, dass diese Karte, die auf ihrer Rückseite auch die europäischen Vorgaben zur Inanspruchnahme von Leistungen in den Mitgliedstaaten der EU enthalten soll (entspricht dem früheren Auslandskrankenschein), Anfang des Jahres 2006 bundesweit eingeführt werden kann. Inzwischen zeigt sich jedoch, dass dieser Zeitplan stark von Wunschdenken geprägt und viel zu knapp kalkuliert war. Die über Jahrzehnte gewachsenen und eingespielten Kommunikationsabläufe zwischen Patienten und Leistungserbringern in einer schwierigen und komplexen IT-Architektur abzubilden, stellt nicht nur für den Technologie-Standort Deutschland eine gewaltige Herausforderung dar. Werden doch jährlich allein rd. 750 Mio. Rezepte herkömmlicher Art ausgestellt, die jeweils bis zu fünfmal von der Arztpraxis bis zur Apotheke durch verschiedene Hände wandern müssen. Die Verbindung von Rezept und eGK soll hier nach dem Willen des Gesetzgebers erhebliche Einsparungen bringen und darüber hinaus unerwünschte Arzneimittelnebenwirkungen schneller erkennen lassen, was durchaus im Interesse der Betroffenen und auch im Allgemeininteresse liegt.

Viele Bürgerinnen und Bürger verbinden mit der elektronischen Gesundheitskarte allerdings eher die Sorge, nunmehr „gläserner Patient“ zu werden. Unsere Dienststelle wurde daher vor allem im 1. Halbjahr 2005 wiederholt gefragt, was es mit der eGK denn nun auf sich habe. Wir möchten an dieser Stelle zunächst einige allgemeine Informationen zur eGK geben:

– Die eGK wurde vom Bundesgesetzgeber als Erweiterung der bisherigen Krankenversichertenkarte allgemein verbindlich eingeführt (vgl. § 291 a Abs. 1 SGB V). Mit ihr soll – so der Wille des Gesetzgebers – die Wirtschaftlichkeit, Qualität und Transparenz in der Krankenbehandlung in den in § 291 Abs. 2 und 3 SGB V genannten Fällen verbessert werden; Absatz 2 nennt dabei die Pflichtanwendungen, während Absatz 3 die zusätzlichen freiwilligen Anwendungen aufzählt. Der Gesetzgeber sieht dabei eine schrittweise Verwirklichung vor.

– Der Pflichtteil der eGK wird die administrativen Daten der bisherigen Krankenversichertenkarte (Name, Anschrift, Geburtsdatum, Kranken-

kasse, Versichertenstatus, Versicherungsnummer und – neu – Lichtbild) enthalten sowie die Möglichkeit zur papierlosen Übertragung von Rezepten vorsehen. In einem freiwilligen medizinischen Teil der Karte können Notfalldaten, wie z. B. Blutgruppe, chronische Erkrankungen oder Allergien gespeichert werden, darüber hinaus Befunde, Diagnosen, Therapieempfehlungen und Maßnahmen, Behandlungsberichte, Impfungen sowie Röntgenuntersuchungen. Ebenso können damit von Versicherten selbst zur Verfügung gestellte Daten gespeichert werden wie z. B. Hinweise auf Patientenverfügungen sowie Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten.

Entscheidend wird es aus Sicht des Datenschutzes darauf ankommen, die Vorgaben des Gesetzgebers, die vom Ansatz her durchaus datenschutzfreundlich gestaltet sind, auch in die Praxis umzusetzen. Zu nennen sind hier insbesondere folgende Gesichtspunkte, die die Datenhoheit der Versicherten gewährleisten sollen und in einer Entschließung der 69. Datenschutzkonferenz zur Einführung der eGK mündeten (s. Anhang 3). In dieser Entschließung wurden folgende Aspekte zum Schutz der Patientenrechte als essenziell angesehen:

– Die über die Karte erfolgende Datenverarbeitung muss nach den gesetzlichen Vorgaben weitgehend aufgrund der Einwilligung der Versicherten erfolgen.

– Um die hierfür nötige Akzeptanz bei den Versicherten zu erhalten, sind neben den rechtlichen auch die tatsächlichen – technischen wie organisatorischen – Voraussetzungen dafür zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind.

– Die Versicherten müssen auch darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben.

– Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt.

– Die Verfügungsbefugnis der Versicherten über ihre Daten muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen zu gewährleisten.

– Vor der obligatorischen flächendeckenden Einführung der eGK sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen.

– Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben. Vorgesehene Einführungstermine dürfen, so die Datenschutzkonferenz weiter, kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

Zum Stand der Einführung der eGK in Baden-Württemberg ist Folgendes zu vermelden:

Damit die eGK am Ende für die Patienten, die Leistungserbringer und die Leistungsträger im Echtbetrieb auch funktioniert, bedarf es eines Testlaufs. Die Funktionen der eGK müssen deshalb in einigen Testregionen ernsthaft erprobt werden. Diese Testphase sollte in Regionen stattfinden, die aufgrund der Infrastruktur, der demographischen Prägung und nicht zuletzt wegen des dort vorhandenen Know-hows hierfür besonders geeignet sind.

Nach Einschätzung der „Arbeitsgemeinschaft zur Einführung der eGK in Baden-Württemberg – eGK BW“, in der sich sämtliche Heilberufekammern, der Landesapothekerverband, die Kassenärztliche und die Kassen-

zahnärztliche Vereinigung, die Baden-Württembergische Krankenhausgesellschaft sowie mehrere Verbände sonstiger Leistungserbringer zusammengeschlossen haben, werden die Testvoraussetzungen in Baden-Württemberg derzeit am besten in der Region Heilbronn erfüllt. Leider haben die eingangs geschilderten Verzögerungen dazu geführt, dass zum Zeitpunkt der Drucklegung dieses Berichts noch nicht einmal die erforderlichen Kriterien zur Auswahl der Testregionen festgelegt waren. Sobald die baden-württembergische Testregion verbindlich feststeht, wird unsere Dienststelle das Pilotvorhaben im Rahmen ihrer personellen Möglichkeiten beratend begleiten.

Mit gewisser Sorge sehen wir allerdings derzeit laufende Bestrebungen des Bundes, den bereits eingetretenen Zeitverzug bei der Einführung der eGK dadurch kompensieren zu wollen, dass die Testverfahren insoweit „abgespeckt“ werden, als bestimmte essenzielle Funktionen der eGK nicht mehr zwingend Gegenstand des Testbetriebs sein müssen. Es geht hier insbesondere um die in § 291 a Abs. 3 Satz 3 ff. SGB V vorgesehene Versicherteneinwilligung, ihre Dokumentation auf der Karte, ihre Widerruflichkeit, ihre Beschränkung auf einzelne Anwendungen sowie um die in § 291 a Abs. 5 SGB V geforderten technischen Vorkehrungen zur Zugriffsautorisierung durch die Versicherten selbst. Im Übrigen sei darauf hingewiesen, dass bislang immer gefordert wurde, die Testphase dazu zu nutzen, verschiedene technische Realisierungsmöglichkeiten der eGK im Probebetrieb ergebnisoffen zu testen; von dieser Strategie ist zumindest im Augenblick nicht mehr viel erkennbar.

Bei der Einführung der eGK als einer der größten „elektronischen Baustellen“ der Welt ist präzise Arbeit gefordert; Sorgfalt muss daher vor Schnelligkeit gehen. Diese Forderung sollte im Interesse der Versicherten selbstverständlich sein und dient nicht etwa dazu, die üblichen Einwände von „berufsmäßigen Bedenkenträgern“, wie dies in einer Presseveröffentlichung zu lesen war, zu befriedigen. Nur wenn von Anfang an das Vertrauen der Betroffenen in die Sinnhaftigkeit und die Seriosität des Projekts erreicht wird, kann es auch gelingen, das Werk erfolgreich zu Ende zu bauen.

2. Das Landeskrebsregister

Geleitet von dem Wunsch, durch zentrale Sammlung und Auswertung von Daten über Krebspatienten Informationen über die Ursachen dieser Erkrankungen sowie deren typischen Verlauf zu gewinnen, richtete das Land bereits im Jahr 1994 ein sog. epidemiologisches Krebsregister ein. Dem ging eine mehr als 10-jährige Planungsphase voraus, in der deutlich wurde, dass es alles andere als einfach ist, die unterschiedlichen Anforderungen und Wünsche, die an ein solches Vorhaben gerichtet werden, miteinander in Einklang zu bringen. Auch wenn sich die an der Planung beteiligten Ärzte, Kliniken und Wissenschaftler in dem eingangs erwähnten Ziel einig waren, bestanden und bestehen auch heute noch sehr unterschiedliche Vorstellungen darüber, wie dieses Ziel am besten erreicht werden kann und welches die entscheidenden Erfolgsfaktoren eines Krebsregisters sind.

Aus Sicht des Sozialministeriums hat das Krebsregister in seiner bisherigen Form seine Ziele nicht erreicht, insbesondere habe es zu wenige Meldungen der Ärzte zu diesem Register gegeben. Im vergangenen Jahr zog die Landesregierung auf Vorschlag des Sozialministeriums daher die Reißleine für dieses Projekt und stellte die bisherige Krebsregistrierung ersatzlos ein. Parallel dazu begann es mit Planungen für eine andere Form der Krebsregistrierung, die eine höhere Meldequote als das bisherige Krebsregister erzielen soll.

Um dieses Ziel zu erreichen, setzt das Sozialministerium – wie wir bereits im letzten Jahr berichteten (25. Tätigkeitsbericht, LT-Drucksache. 13/3800) – auf Zuckerbrot und Peitsche: Zum einen will es die Ärzte zu möglichst vollständigen Meldungen motivieren, indem es ihnen als Anreiz Rückmeldungen aus dem Krebsregister über die Qualität ihrer Behandlungen in Aussicht stellt. Zum anderen will es die auch dann noch nicht zur Mitwirkung bereiten Ärzte durch eine mit einem Bußgeld belegte Meldepflicht dazu bringen.

2.1 Wird es künftig zwei landesweite Krebsregister geben?

Während sich die Meldepflicht ohne weiteres auch mit dem 1994 eingerichteten Krebsregister hätte verbinden lassen, sieht das Sozialministerium zur Umsetzung der Rückmeldungen an die Ärzte beträchtliche Änderungen an dem gesamten Modell der Krebsregistrierung vor. Danach soll künftig nicht nur ein landesweites epidemiologisches Krebsregister betrieben, sondern parallel dazu auch ein neuartiges, landesweites klinisches Krebsregister eingerichtet werden. Bedenkt man, dass es bislang schon regionale klinische Krebsregister gibt und diese auch künftig weiter bestehen bleiben sollen, so wird deutlich, dass jeder Krebspatient in Zukunft – wenn die Vorstellungen des Sozialministeriums Wirklichkeit werden – nicht nur in einem, sondern in zwei oder sogar drei unterschiedlichen Krebsregistern erfasst sein wird.

2.2 Erste Überlegungen des Sozialministeriums

Als uns das Sozialministerium seine ersten Überlegungen zur Neukonzeption der Krebsregistrierung in Baden-Württemberg mitteilte, wurde deutlich, dass es noch eine Reihe weiterer datenschutzrelevanter Änderungen plant:

– Widerspruch oder Einwilligung

Während eine personenbezogene Meldung zum bisherigen Krebsregister die vorherige Einwilligung der Betroffenen erforderte, plante das Sozialministerium, künftige Meldungen ohne Einwilligung der Betroffenen zu ermöglichen. Stattdessen sollte den Krebskranken allerdings die Möglichkeit eines (nachträglichen) Widerspruchs zur Meldung eröffnet werden. Das Sozialministerium begründete dies damit, dass sich die Patienten in der Phase, in der ihnen die Krebsdiagnose eröffnet wird, nicht auch noch mit der Frage nach der Einwilligung zur Datenverarbeitung im Krebsregister befassen sollen.

– Wunsch nach mehr Daten

Die im Krebsregister verarbeiteten Daten sollen u. a. Antwort auf die Frage geben, wie lange Krebspatienten mit ihrer Erkrankung leben. Für diesen Zweck sah bereits das frühere Krebsregistergesetz des Landes vor, dass Daten aus Todesbescheinigungen an das Krebsregister weitergeleitet werden durften und dieses daraus entnehmen konnte, welche Patienten mittlerweile verstorben sind. Die Tumorzentren und Onkologischen Schwerpunkte hielten diese Angaben allerdings nicht für ausreichend, weil die Todesbescheinigungen keine Rückmeldungen für Patienten ermöglichen, die außerhalb Baden-Württembergs versterben. Um auch in diesen Fällen noch vom Tod eines Patienten zu erfahren, möchte es das Sozialministerium gestatten, dass dafür regelmäßig die Daten aller in Baden-Württemberg an Krebs erkrankten Personen mit denen der Einwohnermelderegister sämtlicher Städte und Gemeinden des Landes darauf abgeglichen werden, welche Patienten darin mittlerweile als verstorben gemeldet sind.

– Zusammenführung verschiedener Meldungen

Da im Krebsregister nicht nur eine Meldung pro Patient verarbeitet wird, sondern insbesondere für das neu einzurichtende landesweite klinische Krebsregister unter Umständen zahlreiche Nachmeldungen mit Informationen über den weiteren Verlauf der Erkrankung und deren Behandlung erfolgen sollen, soll sichergestellt werden, dass diese zu den zum betreffenden Patienten bereits vorhandenen Daten jeweils korrekt hinzugefügt werden können. Da das Sozialministerium davon ausgeht, dass die im bisherigen Krebsregister praktizierte Meldung unter Verwendung eines Patientenpseudonyms an Stelle der Identitätsdaten eine solche Zusammenführung erschwert, sollen künftig alle Meldungen unter Angabe der Identitätsdaten der Patienten erfolgen.

2.3 Vereinbarung von Eckpunkten im März 2005

Bis Ende März 2005 konnte zwischen dem Sozialministerium, dem für den Datenschutz im privaten Bereich (z. B. bei niedergelassenen Ärzten und Pathologen) zuständigen Innenministerium sowie unserer Dienststelle eine grundsätzliche Verständigung über Eckpunkte der Neukonzeption erreicht werden. Dazu gehören:

– Ein Verzicht auf die aus datenschutzrechtlicher Sicht vorzuziehende Einwilligungslösung kann nur dann in Betracht kommen, wenn in den zum Krebsregister gehörenden Organisationseinheiten nicht dauerhaft die Möglichkeit besteht, auf personenbezogene Daten sämtlicher im Rahmen der Krebsregistrierung erfassten Patientinnen und Patienten zuzugreifen und diese im Klartext zur Kenntnis zu nehmen. Die Aufdeckung der Patientenidentität kann danach nur in gesetzlich näher zu regelnden Ausnahmefällen – nicht aber als Regelfall – in Betracht kommen.

– Außerdem sind im Hinblick auf die mit einem solchen Register verbundenen Risiken besonders hohe Anforderungen an technische und organisatorische Schutzmaßnahmen zu stellen.

2.4 Erster Gesetzentwurf im November 2005

Das Sozialministerium, das sich zu diesem Zeitpunkt schon mehr als ein Jahr lang mit der Frage der Neukonzeption der Krebsregistrierung befasst hatte, legte Anfang November 2005 einen ersten ausformulierten und mit Begründung versehenen Gesetzentwurf für die Neuorganisation der Krebsregistrierung in Baden-Württemberg vor. Dann allerdings sollte es auf einmal ganz schnell gehen: Nicht einmal zwei Arbeitstage verblieben uns bis zum Termin einer Besprechung, bei der das Sozialministerium den Gesetzentwurf mit den in der Arbeitsgruppe zur Neuordnung der Krebsregistrierung mitwirkenden Einrichtungen erörtern wollte. War dies angesichts der Komplexität der Materie schon ungewöhnlich genug, so teilte das Sozialministerium in der Einladung zu dieser Besprechung auch noch mit, dass der Gesetzentwurf sowie die dazu erstellte Konzeption des Sozialministeriums innerhalb dieser Arbeitsgruppensitzung abschließend beraten werden solle. Zudem ließ es bereits im Vorfeld dieser Sitzung wissen, dass „aufgrund des äußerst engen Zeitplans“ nur solche Änderungswünsche berücksichtigt werden könnten, „die zeitnah umsetzbar sind“. Auf diese Weise, so meine ich, sollte man nicht mit einer so anspruchsvollen Materie umgehen.

2.5 Gravierende Unzulänglichkeiten des ersten Gesetzentwurfs

Auch sachlich zeigte sich, dass ein unangemessener Zeitdruck dem Projekt nicht gut tut. Bereits die erste Durchsicht der vom Sozialministerium übersandten Unterlagen – und mehr ließ das Sozialministerium durch seinen viel zu knapp bemessenen Zeitplan gar nicht zu – offenbarte gravierende konzeptionelle Schwachpunkte, angesichts derer sich der vorgelegte Gesetzentwurf aus Sicht des Datenschutzes als noch nicht entscheidungsreif erwies. Zur Verdeutlichung seien hier nur einige dieser Schwachpunkte beispielhaft angesprochen:

– Trägerschaft und Rechtsform der maßgeblichen Einrichtungen bleiben ungeregelt

  Im Gesetzentwurf werden als wesentliche, an der Krebsregistrierung mitwirkende Stellen genannt: eine Vertrauensstelle, eine klinische Registerstelle, die das landesweite klinische Krebsregister führen soll, sowie das epidemiologische Krebsregister. Für keine dieser Stellen gibt das Gesetz aber an, welche Einrichtungen künftig Träger dieser Stellen sein sollen. Dies ist nicht bloße Formalie, sondern hat z. B. ganz konkreten Einfluss darauf, welches Datenschutzrecht für die einzelnen Stellen gilt. Ferner kann – je nach Wahl der Trägerschaft – die Stelle auch weiteren Gesetzen unterliegen, wie z. B. dem Landeskrankenhausgesetz. Erst wenn zu erkennen ist, welches (Datenschutz-)Recht für die Stellen gilt, lässt sich beurteilen, ob im

Krebsregistergesetz etwa noch Abweichungen von diesen gesetzlichen Regelungen aufgenommen werden müssen. Ebenso ist nicht ersichtlich, ob die in diesen Stellen verarbeiteten Daten vor einem Zugriff durch Strafverfolgungsbehörden geschützt sind.

– „Potemkinscher Gesetzentwurf“ hinsichtlich des neuen landesweiten klinischen Krebsregisters?

  Wie eingangs erwähnt, stellt gerade die geplante landesweite klinische Registerstelle im bundesweiten Ländervergleich eine Besonderheit dar. Da darin deutlich mehr Daten über die einzelnen Krebspatienten erfasst werden sollen als dies in einem epidemiologischen Krebsregister jemals der Fall sein kann, setzt eine datenschutzrechtliche Beurteilung voraus, dass man überhaupt weiß, welche Daten dabei für welche Zwecke verarbeitet und an welche Stellen weitergeleitet werden sollen. Leider ermöglichten uns weder der Gesetzentwurf noch dessen Begründung, dies zu beurteilen. Nicht nur dass darin ungeregelt bleibt, welche Einrichtung die „klinische Registerstelle“ betreiben soll, sondern er lässt auch offen, welche Datenarten darin erfasst und verarbeitet werden sollen. Zudem sieht der Gesetzentwurf vor, dass die Registerstelle regelmäßig Daten zum Zweck der Qualitätssicherung an sog. „Regionale Qualitätskonferenzen“ übermitteln soll. Der Haken daran ist allerdings, dass es diese Regionalen Qualitätskonferenzen noch gar nicht gibt. Der Gesetzentwurf enthält nicht einmal eine klare Verpflichtung, solche einzurichten. Er spricht lediglich davon, dass diese einzurichten sind und dass diese sich eine Geschäftsordnung geben müssen. Es lässt aber offen, wer dies zu tun hat und welche Stellen darin zusammengeschlossen werden sollen.

– Ungeklärtes Verhältnis zwischen landesweitem und regionalen klinischen Krebsregistern

  Zu dem Wenigen, was der Gesetzentwurf über die klinische Registerstelle zu erkennen gibt, gehört, dass mit ihrer Hilfe Daten zum Zweck der Qualitätssicherung der darin dokumentierten Krebsbehandlungen verarbeitet werden sollen. Damit deckt sich dessen Zweck mit den Zwecken der bereits bestehenden regionalen klinischen Krebsregister. Da Letztere nach den Vorstellungen des Sozialministeriums auch nach Einrichtung der landesweiten Registerstelle weiterbetrieben werden können, ist nicht auszuschließen, dass durch die Umsetzung der gegenwärtigen Pläne Parallelstrukturen aufgebaut werden, die datenschutzrechtlich den Nachteil haben, dass zukünftig mehr Stellen und Personen von besonders schutzbedürftigen medizinischen Daten Kenntnis erhalten können, als dies zur Erfüllung der sich überschneidenden Aufgaben dieser Stellen erforderlich ist. In gleichem Maß erhöhen sich dabei die Risiken für einen missbräuchlichen Zugriff auf die gespeicherten Daten. Sofern nicht ergänzend zum vorgelegten Gesetzentwurf deutlich gemacht wird, inwieweit die regionalen klinischen Krebsregister erkennbar anderen Zwecken dienen als das landesweite klinische Krebsregister, ist aus Sicht des Datenschutzes zu fragen, ob angesichts der mit beiden Registern verbundenen Datenschutzrisiken tatsächlich auch beide Arten der klinischen Krebsregistrierung unverzichtbar sind.

– Übermittlung der Namen der Krebspatienten an alle Städte und Gemeinden

  Um noch lückenloser als bisher zu erfahren, ob die registrierten Krebspatienten noch leben oder bereits verstorben sind, will das Sozialministerium gestatten, dass einmal jährlich die Namen und Anschriften sämtlicher in den Registern erfasster Krebspatienten aus Baden-Württemberg an die Einwohnermeldeämter übermittelt werden. Diese sollen dann zu den genannten Personen mitteilen, ob sie noch unter der genannten Anschrift gemeldet, verzogen oder bereits verstorben sind. Die Umsetzung dieses Vorschlags würde dazu führen, dass die besonders schutzbedürftigen Informationen darüber,

wer in Baden-Württemberg an Krebs erkrankt ist, auch Stellen außerhalb des Krebsregisters bekannt würden.

– Modalitäten zum Umgang mit Widersprüchen ungeklärt

Die vom Sozialministerium favorisierte Widerspruchslösung stellt die Betreiber der Krebsregister vor folgendes Dilemma: Auf der einen Seite bringt ein Widersprecher zum Ausdruck, dass er seine personenbezogenen Daten nicht dauerhaft gespeichert haben möchte. Es wäre diesem Personenkreis daher kaum zu vermitteln, wenn im Krebsregister ausgerechnet über die Tatsache des Widerspruchs dauerhaft personenbezogene Daten gespeichert würden. Auf der anderen Seite kann es den Betroffenen kaum zugemutet werden, dass sie jedes Mal, wenn sie einen neuen Arzt oder eine neue Klinik aufsuchen, ihren Widerspruch neu erklären. Der Gesetzentwurf geht nicht darauf ein, wie man diesem Dilemma entgehen will.

– Sicherheitsrelevante Festlegungen zur Realisierung der elektronischen Datenübertragung unvollständig

Der Gesetzentwurf sieht vor, dass künftig alle Meldungen zu den Krebsregistern elektronisch erfolgen müssen. Hieran sollen sich nicht nur sämtliche Kliniken, sondern auch alle niedergelassenen Ärzte und Zahnärzte sowie die Pathologen beteiligen. Zwar wird zur Wahrung der Vertraulichkeit bei der Datenübertragung vorgeschrieben, dass die Daten verschlüsselt übertragen werden müssen. Weitere mit der elektronischen Übertragung verbundene sicherheitsrelevante Fragen bleiben allerdings ungeklärt: Konzept und Gesetzentwurf lassen nicht erkennen, ob die Meldungen über Internet oder einen anderen Übertragungsweg erfolgen sollen. Entsprechende Festlegungen müssen aber getroffen werden, um die mit dem jeweiligen Übertragungsweg verbundenen Sicherheitsrisiken abschätzen zu können. In jedem Fall, besonders jedoch, wenn das Internet zur Datenübermittlung gewählt werden sollte, können sich für die meldenden Einrichtungen erhebliche Sicherheitsrisiken ergeben, wenn das interne Netz einer Arztpraxis oder einer Klinik, das möglicherweise noch nicht mit dem zur Datenübertragung vorgesehenen Netz verknüpft ist, ohne entsprechende Schutzmaßnahmen mit diesem Netz verbunden wird. In dem Zusammenhang muss geklärt werden, wie sichergestellt wird, dass auch die zur Absicherung des Netzanschlusses von Klinik- oder Praxisnetzwerken erforderlichen Schutzmaßnahmen ergriffen werden können. Ebenso muss geklärt werden, wie beispielsweise sichergestellt werden soll, dass die zur Meldung verwendeten Computer mit Virenschutzprogrammen ausgestattet und diese regelmäßig auf aktuellem Stand gehalten werden sollen.

– Begründung der vorgeschlagenen Lösungsvariante unzulänglich

Die bisherigen Ausführungen belegen, dass es bei der Neukonzeption der Krebsregistrierung durchaus datenschutzrelevante Gestaltungsmöglichkeiten gibt. Die datenschutzrechtliche Beurteilung eines solchen Vorhabens erfordert daher eine ganzheitliche Betrachtung der Ziele sowie der zu deren Erreichung vorgesehenen Maßnahmen. Soweit dabei alternative Realisierungsmöglichkeiten bestehen, sind deren datenschutzrechtliche Auswirkungen zu prüfen und gegeneinander abzuwägen. Die letztlich empfohlene Lösungsvariante sollte erkennen lassen, dass die mit den geringsten Eingriffen in das Recht auf informationelle Selbstbestimmung verbundene Alternative gewählt wurde. Im Rahmen unserer Beratung des Sozialministeriums sowie der Arbeitsgruppe zur Neuordnung der Krebsregistrierung in Baden-Württemberg haben wir mehrfach auf die entscheidende Bedeutung einer entsprechenden Analyse hingewiesen. Anstatt jedoch auf die bestehenden und bereits in der Vielfalt der Krebsregistergesetze anderer Bundesländer zum Ausdruck kommenden Lösungsalternativen offen aufzugreifen und unter diesen gezielt nach einer datenschutzfreundlichen Gesamtkonzeption zu suchen, heißt es im Vorblatt zum Gesetzentwurf lakonisch: „Alternativen: keine“.

Das Sozialministerium, das wir in der erwähnten Besprechung im November auf diese sowie eine Reihe weiterer datenschutzrechtlicher Unzulänglichkeiten hingewiesen haben, hält gleichwohl an seinem ambitionierten Zeitplan fest, nach dem der Gesetzentwurf vom Kabinett bereits Ende November 2005 zur Anhörung freigegeben und noch in dieser Legislaturperiode verabschiedet werden soll. Es bleibt zu hoffen, dass das Sozialministerium seine Augen gleichwohl nicht vor den beschriebenen Problemen und Unzulänglichkeiten des Gesetzentwurfs verschließt und auch trotz des hausgemachten Zeitdrucks noch eine datenschutzgerechte Lösung im Interesse der Krebspatienten und der guten Sache auf den Weg bringt. Grundsätzlich positiv ist jedenfalls das Angebot des Sozialministeriums zu bewerten, während der Anhörungsphase nochmals über die datenschutzrechtlichen Fragestellungen sprechen zu wollen. Es sollte dann aber nicht nur beim Sprechen bleiben; vielmehr sollten als Ergebnis konkrete Verbesserungen am gegenwärtigen Gesetzentwurf herauskommen.

Ich bin im Übrigen der festen Überzeugung, dass nach den Fehlschlägen mit der bisherigen Krebsregistrierung im Land ein neues Konzept nur dann auf längere Sicht Erfolg haben wird, wenn dieses fachlich ausgereift ist und dadurch auch die Akzeptanz der Krebspatienten findet. Dies setzt vor allem voraus, dass die Daten über ihre Krebserkrankung bestmöglich geschützt werden. Gut Ding braucht – wie der Volksmund zu Recht feststellt – Weile. Dies gilt gerade in einem so komplexen und sensiblen Bereich wie der Errichtung einer landesweiten Krebsregistrierung, noch dazu, wenn damit, wie das Sozialministerium es vorhat, bundesweit Neuland betreten werden soll.

3. Mammographie-Screening

Ein wichtiges Ziel zur Verbesserung der Gesundheit in Deutschland ist die Förderung der Früherkennung von Brustkrebserkrankungen und damit einhergehend die Senkung der Brustkrebssterblichkeit bei Frauen. Grundlage waren dafür die vom Bundesausschuss für Ärzte und Krankenkassen beschlossenen Krebsfrüherkennungsrichtlinien vom 15. Dezember 2003. Diese sehen u. a. vor, dass die anspruchsberechtigten Frauen im Alter von 50 Jahren bis zum Ende des 70. Lebensjahrs von einer zentralen Stelle zum Mammographie-Screening (Englisch: Screen = Sieb) eingeladen werden.

In unserem letztjährigen 25. Tätigkeitsbericht (LT-Drucksache 13/3800) haben wir bereits ausführlich darüber berichtet, dass sich nach einer gemeinsamen Besprechung Ende Juli 2004 alle Beteiligten auf Landesebene einig waren, dass gegenüber dem Bund ein erneuter Vorstoß unternommen werden sollte, damit dieser nunmehr auch die erforderlichen Rechtsänderungen für eine Durchführung des Screening-Verfahrens vornimmt. Es bestand wie zum Teil auch in anderen Bundesländern Konsens, dass außer Melderechtsänderungen, die selbstverständlich Ländersache sind, eine spezielle Rechtsgrundlage für die Einrichtung der sog. zentralen Stelle für das Einladungswesen erforderlich ist, die u. a. die Anforderungen an eine öffentliche Stelle im Sinne von § 18 des Melderechtsrahmengesetzes erfüllt. Eine Notwendigkeit hierfür wurde deshalb gesehen, weil die zentrale Stelle nicht nur die Meldedaten der gesetzlich krankenversicherten Frauen, sondern auch die der Privatversicherten verarbeiten sollte und § 219 Abs. 2 SGB V nur für gesetzliche Krankenkassen gilt. Die Schaffung einer bundeseinheitlichen Regelung wäre im Übrigen schon deshalb zweckmäßig gewesen, weil dadurch auf zahlreiche Gesetzesänderungen in den einzelnen Bundesländern hätte verzichtet werden können. Leider hat der Bund diese Überlegung nicht aufgegriffen, was letztlich zu einer weiteren Verzögerung der Einführung des Mammographie-Screenings führte.

Nachdem inzwischen vom Landesgesetzgeber mit dem Gesetz über die zentrale Stelle zur Durchführung des Einladungswesens im Rahmen des Mammographie-Screenings vom 28. Juli 2005 (GBl. S. 584) eine wesentliche Voraussetzung für die Einführung der Brustkrebsvorsorge in Baden-Württemberg geschaffen wurde, eine Rechtsverordnung des Sozialministeriums zur Bestimmung der Altersgruppe der einzuladenden Frauen noch in diesem Jahr in Kraft treten soll und auch das Innenministerium dabei ist, die erforderlichen flankierenden Melderechtsänderungen vorzubereiten, dürften die wesentlichen rechtlichen Hürden inzwischen überwunden sein, die bis dato

die Einführung eines flächendeckenden Mammographie-Screenings in Baden-Württemberg verhindert haben. Unsere Dienststelle war und ist bei den genannten Rechtsänderungen in beratender Funktion einbezogen. Wir werden das Projekt auch weiterhin konstruktiv beratend begleiten. Dies gilt auch für die von der Kassenärztlichen Vereinigung Baden-Württemberg (KV) – einer Körperschaft des öffentlichen Rechts – zu entwickelnde Konzeption für das Einladungswesen. Der KV wurde inzwischen die Funktion der o. g. „zentralen Stelle“ für das Einladungswesen in Baden-Württemberg übertragen. Aus Sicht des Datenschutzes sollte beim Einladungsverfahren im Interesse der betroffenen Frauen insbesondere darauf geachtet werden, dass eine möglichst weit gehende räumliche, organisatorische und personelle Trennung der zentralen Stelle von den anderen Aufgaben der KV stattfindet und der Aufbau eines „(Teil-)Melderegisters“ unterbleibt.

4. Einzelfälle

4.1 Patientendaten in „Grüner Tonne“

Bei Daten über ihre Gesundheit reagieren die betroffenen Personen meist sehr empfindlich. Und dies völlig zu Recht. Handelt es sich doch um sensitive Daten, die auch vom Landesdatenschutzgesetz besonders geschützt werden (§ 33 LDSG).

Wir staunten daher nicht schlecht, als Ende August 2005 eine aufmerksame Bürgerin unsere Dienststelle aufsuchte und ein Paket mit Patientendaten übergab. Der Fundort war eine sog. grüne Tonne, die für die Entsorgung von Papierabfällen vorgesehen ist. Wie eine Sichtung der Unterlagen durch uns ergab, handelte es sich insbesondere um

- ca. 50 handschriftlich ausgefüllte Unfallaufnahmebögen aus den Jahren 2002 bis 2005, die neben personenbezogenen Daten u. a. auch Röntgenaufnahmen, handschriftliche Notizen, Gutachten, Arztberichte sowie Messblätter für Wirbelsäule und Gliedmaßen enthielten;
- mehrere Gutachten mit personenbezogenem Inhalt, die in den Jahren 2003 bzw. 2004 für verschiedene Berufsgenossenschaften gefertigt wurden;
- mehrere Arztbriefe, die u. a. internen Klinikschriftverkehr zwischen der Radiologie und der Unfallchirurgie, Patientenstammdaten sowie Angaben über Untersuchungsbefunde und ärztliche Bewertungen enthielten;
- Schriftwechsel mit externen Krankenhäusern bzw. niedergelassenen Fachärzten;
- verschiedene Ausdrucke von Röntgenaufnahmen bzw. Ultraschalluntersuchungen, die namentlich gekennzeichnet waren.

Dass die papierenen Unterlagen in der „richtigen“ Abfalltonne steckten und nicht etwa in der braunen bzw. grauen Abfalltonne für Bioabfälle oder den Restmüll, mag zwar für ein ausgeprägtes Umweltbewusstsein des Entsorgers sprechen, nicht jedoch für ein normal entwickeltes Verantwortungsbewusstsein im Umgang mit Patientendaten.

Anlässlich eines Gesprächs mit den Verantwortlichen des Krankenhauses übergaben wir das Aktenbündel und baten den Krankenhausträger, den Sachverhalt unter Beteiligung des behördlichen Datenschutzbeauftragten zu klären und Stellung zu nehmen.

Inzwischen liegt uns der Untersuchungsbericht vor. Folgendes hatte sich zugetragen:

Ein bei einem Krankenhaus tätiger Arzt hatte dort gekündigt und anlässlich seines Wohnungswechsels die bei ihm zu Hause aufbewahrten Patientenunterlagen in der für diese Wohnanlage bestimmten Papiermülltonne entsorgt, wo sie von der eingangs genannten Bürgerin gefunden wurden. Wie sich bei den weiteren Überprüfungen ergab, betrafen die aufgefundenen Unterlagen den Nebentätigkeitsbereich des Arztes. Krankenhausärzte werden – was oft nicht bekannt ist – neben ihren an-

sonsten im Rahmen eines Beschäftigungsverhältnisses für den Arbeitgeber zu erbringenden Leistungen als Privatperson bei der Erstellung von fachärztlichen Gutachten tätig. Dafür werden sie dann auch vom Auftraggeber unmittelbar bezahlt. Für uns ist dies insoweit von Bedeutung, als der Landesbeauftragte für den Datenschutz aufgrund der bestehenden gesetzlichen Zuständigkeitsregelungen keinerlei Aufsichtsbefugnisse gegenüber Privatpersonen hat. Diese sind dem Innenministerium Baden-Württemberg übertragen. Darauf, dass es sich bei dieser Aufgabensplittung um einen von Anfang an bestehenden Webfehler des Gesetzes handelt, habe ich wiederholt hingewiesen. Allerdings können die im Gesetz klar bestimmten Zuständigkeiten nur dann beachtet werden, wenn im konkreten Fall deutlich wird, wer in welcher Eigenschaft handelt oder gehandelt hat. Weder die aufmerksame Bürgerin noch wir selbst konnten am Anfang eine eindeutige Zuständigkeitsabgrenzung vornehmen. So deutete die Verwendung des offiziellen Briefpapiers des Klinikums ursprünglich darauf hin, dass hier in unzulässiger Weise personenbezogene Daten durch eine öffentliche Stelle entsorgt worden sein könnten, für die unsere Dienststelle zuständig gewesen wäre. Die Verwendung des Klinikbriefpapiers und sonstiger Unterlagen des Krankenhauses erklärte der befragte Arzt später aber damit, dass er diese nur für seine handschriftlichen Konzeptunterlagen zur Erstellung der Gutachten benötigt und verwendet habe. Weil ihm diese Einlassung nicht zu widerlegen war, blieb uns an dieser Stelle nichts anderes übrig, als den Vorgang den dafür im Innenministerium zuständigen Kollegen mit der Bitte um weitere Veranlassung zu übergeben.

Hiervon unabhängig muss sich das Klinikum gleichwohl einiges ins Stammbuch schreiben lassen. Zwar gibt es dort auf den Stationen, Abteilungen und anderen Funktionseinheiten verschlossene Behältnisse, in denen der anfallende Datenmüll gesammelt und danach durch eine Fachfirma entsorgt wird. Diese erstellt über die fachgerechte Vernichtung der Krankenhausunterlagen auch ein entsprechendes Protokoll. Allerdings fehlen dazu verbindliche schriftliche Bestimmungen des Krankenhauses über eine datenschutzkonforme Vorgehensweise. Man sagte uns, diese würde – was selbstverständlich nicht ausreichend ist – durch mündliche Informationen des Betriebsdienstes an die Mitarbeiter weitergegeben. Man werde aber anlässlich der Zusammenführung der verschiedenen städtischen Krankenhäuser hierfür die noch fehlenden schriftlichen Ausarbeitungen vornehmen. Unsere Nachfrage, ob bisher schon einmal eine persönliche Kontrolle der Entsorgung von Krankenhausunterlagen durch den Datenschutzbeauftragten oder andere Mitarbeiter des Klinikums bei der Firma stattgefunden hätte, verlief – was uns nicht überraschte – ebenfalls negativ. Dass allein mit der schriftlichen Beauftragung einer Firma das Krankenhaus bereits aus dem Obligo wäre, ist eine Fehleinschätzung, die den zu ergreifenden organisatorischen und verfahrensrechtlichen Vorkehrungen zur Vermeidung von Verletzungen des informationellen Selbstbestimmungsrechts der Betroffenen nicht hinreichend Rechnung trägt. Darüber hinaus besteht dringender Regelungsbedarf für die Verwendung von offiziellen Kopfbögen des Klinikums; ebenso darüber, ob, wann und wie die Beschäftigten des Krankenhauses Patientenunterlagen mit nach Hause nehmen dürfen. Will ein Krankenhaus dies erlauben, muss es auf geeignete Weise regeln, wie sich ein datenschutzgerechter Umgang mit Daten auch außerhalb des Krankenhauses sicherstellen und kontrollieren lässt.

Dass man uns versprochen hat, die noch fehlenden schriftlichen Ausführungen im Zusammenhang mit der Zentralisierung der städtischen Krankenhäuser anzugehen, wird von uns begrüßt. Ärgerlich ist, dass es anscheinend noch immer nicht zum datenschutzrechtlichen Standard in allen Krankenhäusern gehört, die wichtigsten Grundsätze im Umgang mit Patientendaten in einem Datenschutzhandbuch festzuhalten. Dass ein Datenschutzbeauftragter eines Klinikums dieser Größe sich offensichtlich bis heute dieser Problematik noch nicht angenommen hatte, ist für uns nicht nachvollziehbar. Wir werden daher in absehbarer Zeit den Umsetzungsstand erneut abfragen.

4.2 Patientengeheimnis zu wörtlich genommen

Eine Bürgerin wandte sich Rat suchend an uns, nachdem ein Universitätsklinikum sich zunächst geweigert hatte, ihr Einsicht in die über sie angelegten Krankenunterlagen zu gewähren bzw. entsprechende Kopien gegen Kostenübernahme zu übermitteln.

Dieses Thema spielt in der Praxis unserer Dienststelle erstaunlicherweise noch immer eine Rolle, obwohl die datenschutzrechtliche Bewertung an und für sich nicht mehr zweifelhaft sein dürfte.

Ging man früher noch davon aus, dass die Aufzeichnungen eines Arztes diesem lediglich als eigene Gedächtnisstütze dienten und insofern für ein Einsichtnahmerecht des Patienten kein Grund bestehe, ist mittlerweile in der einschlägigen Literatur und Rechtsprechung unumstritten, dass die Dokumentation der Krankenbehandlung für den Arzt bzw. den Krankenhausträger eine echte Nebenpflicht aus dem Behandlungsvertrag darstellt (vgl. u. a. BGH, Urteil vom 23. November 1982 – VI ZR 222/79 in NJW 1983, S. 328 ff.). Aus dem der Behandlung zugrunde liegenden Vertragsverhältnis in Verbindung mit dem informationellen Selbstbestimmungsrecht des Patienten leitet sich auch dessen Anspruch auf Einsicht in die über seine Behandlung geführten Krankenunterlagen ab. Dem Patienten muss eine frei verantwortliche Entscheidung über die Möglichkeit, eine ärztliche Behandlung selbstständig und kritisch überprüfen zu können, eingeräumt werden. Dies erfordert die Kenntnis des Krankenbildes und des in den Akten dokumentierten Behandlungsablaufs. Als Ausfluss dieses Rechts auf informationelle Selbstbestimmung kann der Patient daher vom Arzt bzw. Krankenhausträger grundsätzlich auch außerhalb eines Rechtsstreits Einsicht in die ihn betreffenden Krankenunterlagen verlangen. Ein besonderes schutzwürdiges bzw. rechtliches Interesse an der Einsichtnahme wird hierfür nicht gefordert, da sich dieses bereits aus dem allgemeinen Persönlichkeitsrecht des Patienten ergibt.

Der Bundesgerichtshof hat in der genannten grundlegenden Entscheidung weiter ausgeführt, dass sich das Einsichtnahmerecht des Patienten nur auf naturwissenschaftlich objektivierbare Befunde und Behandlungsfakten beziehe. Aufzeichnungen des Arztes über persönliche Eindrücke, die oftmals zwangloser und deutlicher abgefasst würden, könnten hingegen dem Patienten (in dessen eigenem Interesse) vorenthalten werden. Diese Rechtsprechung wurde im Übrigen durch das Bundesverfassungsgericht bestätigt (Beschluss vom 16. September 1998 – 1 BvR 1130/98 in NJW 1999, S. 1777 ff.).

Eine Beschränkung des Einsichtnahmerechts des Patienten wegen entgegenstehender therapeutischer Gründe wird häufig als sog. therapeutisches Privileg bezeichnet. Dies bedeutet, dass der Arzt in Einzelfällen eine ungünstige Prognose oder eine schwerwiegende Erkrankung verschweigen oder verharmlosen darf, um die Heilungsaussichten nicht zu beeinträchtigen. Ein solches therapeutisches Privileg wird von der Rechtsprechung jedoch nur ganz ausnahmsweise anerkannt, da ansonsten die Gefahr besteht, dass das grundrechtlich garantierte Selbstbestimmungsrecht des Patienten ausgehöhlt würde.

Nachdem das Landeskrankenhausgesetz Baden-Württemberg (LKHG) – anders als zum Teil in anderen Bundesländern – keine datenschutzrechtlichen Sonderbestimmungen zu diesem Themenkomplex enthält, konnten wir der anfragenden Bürgerin noch mitteilen, dass über die Verweisung in § 43 Abs. 5 LKHG auf die allgemein geltenden Regelungen zum Schutz personenbezogener Daten § 21 LDSG entsprechend anwendbar ist; danach besteht ein grundsätzlicher Anspruch auf Auskunft/Akteneinsicht von Betroffenen über die zu ihrer Person gespeicherten (Patienten-)Daten.

Als sich die Bürgerin mit unserem schriftlichen Votum erneut an das Universitätsklinikum wandte, erhielt sie von dort die aus ihrer Sicht erfreuliche Mitteilung, dass sie selbstverständlich Anspruch auf die Übersendung von Kopien ihrer Behandlungsunterlagen habe. Die geschilderten Schwierigkeiten seien nicht generell beim Universitätsklinikum zu

suchen, sondern beruhten auf einem „individuellen Fehler“ eines Krankenhausarztes. Es bleibt die Frage, ob man von Seiten des Klinikums der Bürgerin auch ohne die Einschaltung unserer Dienststelle so rasch und bürgerfreundlich geholfen hätte. Zweifel scheinen aufgrund der Vorgeschichte jedenfalls erlaubt.

4.3 Gutachten in falschen Händen

Das Interesse jedes Einzelnen daran, persönliche Umstände nicht jedermann und insbesondere nicht seinem Arbeitgeber bekannt zu machen, ist – zu Recht – gerade bei medizinischen Daten besonders ausgeprägt. Der Gesetzgeber hat das unbefugte Offenbaren von Patientengeheimnissen durch den Arzt selbst und die für ihn berufsmäßig tätigen Gehilfen gemäß § 203 Abs. 1 und 3 Satz 2 des Strafgesetzbuchs (StGB) unter Strafe gestellt. Das Offenbaren von Patientengeheimnissen ist danach nur zulässig, wenn entweder eine Entbindung von der Schweigepflicht durch den Patienten vorliegt oder eine Rechtsvorschrift die Weitergabe (ausdrücklich) gestattet. Dass die Nichtbeachtung des Patientengeheimnisses nicht nur für Ärzte, sondern auch für Mitarbeiter (selbstverständlich neben dem Betroffenen) sehr unangenehme Folgen haben kann, bekam die Mitarbeiterin einer Universitätsklinik sehr deutlich zu spüren. Waren doch neben unserer Dienststelle noch mehrere Anwaltskanzleien und sogar die Staatsanwaltschaft mit ein und demselben Fall befasst.

Was war geschehen? Ein im öffentlichen Dienst Beschäftigter wandte sich, vertreten durch seine Rechtsanwälte, an unsere Dienststelle, weil er von seinem Arbeitgeber aufgefordert worden war, beim zuständigen Gesundheitsamt abklären zu lassen, ob er aufgrund einer bereits mehrere Jahre zurückliegenden Verletzung der rechten Hand noch in der Lage sei, einen Dienst-Pkw sicher zu steuern. Da das Gesundheitsamt diese Begutachtung nicht selbst vornehmen konnte, beauftragte es hiermit eine Orthopädische Universitätsklinik. Als die Ehefrau des Petenten kurze Zeit später bei der Geschäftsstelle der Behörde eine neue Arbeitsunfähigkeitsbescheinigung ihres Ehemannes abgeben wollte, wurde sie im Flur von einem leitenden Behördenmitarbeiter auf das Fachgutachten angesprochen, aus dem hervorgehe, dass ihr Gatte trotz der erlittenen Unfallverletzungen im Wesentlichen alle Schreibtischtätigkeiten ausführen könne und auch keine Bedenken bezüglich Fahrtüchtigkeit und Tätigkeiten im Außendienst bestünden.

Da weder dem Petenten noch seiner Ehefrau der Inhalt des Gutachtens bisher bekannt war, wandten sie sich an eine Verwaltungsangestellte der Orthopädischen Universitätsklinik mit der Bitte, ihnen ein Exemplar des Gutachtens zu überlassen, was ihnen jedoch zunächst verweigert wurde. Daraufhin schaltete der Betroffene unsere Dienststelle ein und erstattete Anzeige bei der Staatsanwaltschaft wegen Verletzung der ärztlichen Schweigepflicht. Unsere eigenen Überprüfungen sowie die der Staatsanwaltschaft förderten zu Tage, dass eine Mitarbeiterin der Universitätsklinik das über den Petenten erstellte fachmedizinische Gutachten, ohne dessen Einwilligung und ohne dass dies durch eine entsprechende (Datenübermittlungs-)Vorschrift gestattet gewesen wäre, unmittelbar an dessen Arbeitgeber übermittelt hatte. Die Angestellte war dabei der irrigen Meinung, dass die Übersendung des Gutachtens an den Kostenträger (Arbeitgeber des Petenten) erforderlich gewesen sei, um diesem eine Prüfung und Begleichung der Honorarrechnung zu ermöglichen.

Dass diese Argumentation weder unsere Dienststelle noch die Staatsanwaltschaft überzeugen konnte, bedarf keiner näheren Begründung. Fest steht, dass von der Verwaltungsangestellten der Universitätsklinik eine Datenschutzverletzung gemäß § 4 Abs. 1 LDSG begangen wurde, die auch ihrem Arbeitgeber als der datenschutzrechtlich dafür verantwortlichen Stelle nach § 3 Abs. 3 LDSG zugerechnet werden muss. Dass die Staatsanwaltschaft mit Zustimmung des Gerichts das Ermittlungsverfahren nach § 153 Abs. 1 der Strafprozessordnung (StPO) gleichwohl letztlich eingestellt hat, spielt für die datenschutzrechtliche Bewertung keine Rolle.

Für meine Dienststelle blieb somit nur noch die Frage zu prüfen, ob der festgestellte Datenschutzverstoß mit einer förmlichen Beanstandung geahndet werden muss oder ob unter Berücksichtigung der Gesamtumstände hiervon ausnahmsweise abgesehen werden kann. Zwar hat – wie oben dargestellt – die Mitarbeiterin des Klinikums unter objektiver Verletzung von § 203 StGB und unter Verstoß gegen die Bestimmung des § 4 Abs. 2 LDSG eine Kopie des orthopädischen Fachgutachtens zusammen mit der Arztabrechnung an den Arbeitgeber des Petenten übermittelt. Andererseits beruhte dieses Verhalten primär auf einer individuellen Fehlleistung einer Mitarbeiterin, die die Rechtslage irrtümlich falsch bewertet hatte. Auch war bei der Entscheidung zu berücksichtigen, dass im Rahmen unserer Kontrolltätigkeit bisher keine vergleichbaren datenschutzrechtlichen Verstöße durch die Orthopädische Universitätsklinik bekannt geworden sind.

Der dem Klinikum schließlich mitgeteilte Verzicht auf eine förmliche Beanstandung wurde mit der Erwartung verbunden, dass die Universitätsklinik als datenschutzrechtlich verantwortliche Stelle den vorliegenden Fall zum Anlass nimmt, ihre Mitarbeiter im Umgang mit Patientendaten (erneut) zu sensibilisieren. Im Übrigen haben wir dem Petenten – nachdem dies offensichtlich von seinen anwaltlichen Vertretern versäumt wurde – noch Folgendes mitgeteilt:

Nach § 24 Abs. 2 Satz 1 LDSG sind personenbezogene Daten in Akten zu sperren, wenn die speichernde Stelle im Einzelfall feststellt, dass die Daten unzulässig gespeichert sind. Unzulässig ist eine Speicherung, wenn sie nicht durch eine Rechtsvorschrift oder die Einwilligung des Betroffenen gedeckt ist. Die Unzulässigkeit der Datenerhebung bzw. Datenübermittlung an einen Empfänger setzt sich dabei in der dortigen Speicherung fort. Nachdem im vorliegenden Fall das fachmedizinische Gutachten nicht an den Arbeitgeber des Petenten hätte übersandt werden dürfen, hätte es von seinem Arbeitgeber zwingend gesperrt werden müssen. Aus Sicht des Datenschutzes gäbe es selbstverständlich auch keine Einwände, wenn die Behörde das Gutachten aus den Personalakten herausnimmt und an ihren Mitarbeiter übergibt.

4.4 Telefonieren und Fotografieren in einem Zentrum für Psychiatrie

Ein früherer Patient eines Zentrums für Psychiatrie informierte uns darüber, dass anlässlich von therapeutischen Aktivitäten in den forensischen Abteilungen der Klinik vom Personal ohne Einverständnis der betroffenen Patienten Fotos von diesen gemacht und danach sogar noch öffentlich aufgehängt würden. Wie uns weiter berichtet wurde, seien die für die Patienten bestimmten Wandtelefone genau gegenüber dem Personalbüro installiert und verfügten über keinerlei Mithörschutz, sodass Dritte den Inhalt der Telefongespräche zwangsläufig mitbekämen.

In der von uns daraufhin vom Zentrum für Psychiatrie erbetenen Stellungnahme wurden diese Angaben des Bürgers im Wesentlichen bestätigt.

Dass es bis dato versäumt wurde, jedwede technisch-organisatorische Maßnahme zur Verhinderung eines unbefugten Mithörens von Telefonaten in der Klinik zu realisieren, verletzt in nicht unerheblichem Umfang das Recht auf informationelle Selbstbestimmung der betroffenen Patienten. Von einer förmlichen Beanstandung dieser Datenschutzmängel konnte deshalb abgesehen werden, weil sich das Zentrum für Psychiatrie kooperativ und einsichtig zeigte und uns zusagte, auf den Stationen unverzüglich Telefonzellen durch eine Fachfirma installieren zu lassen; dadurch wird unter Berücksichtigung der örtlichen Gegebenheiten zukünftig ein Telefonieren ohne unbefugtes Mithören von Dritten möglich sein. Anhand der uns zur Verfügung gestellten Unterlagen konnten wir uns davon überzeugen, dass die Umbauten inzwischen tatsächlich abgeschlossen wurden.

Die Erklärungsversuche, weshalb von Mitarbeitern des Zentrums für Psychiatrie anlässlich von therapeutischen Aktivitäten, wie z. B. bei gemeinsamen Grillfesten und Putzaktionen, Patientenfotos gemacht wur-

den, klangen zumindest für Nicht-Mediziner reichlich konstruiert. Die Fotos seien – so wurde uns erklärt – jeweils aus therapeutischen Gründen zur Förderung einer Nachhaltigkeit dieser Gemeinschaftsaktionen gefertigt worden, wobei die einzelnen Patienten die Möglichkeit gehabt hätten, sich während dieser Ereignisse nicht fotografieren zu lassen. Man gab allerdings unumwunden zu, dass man es versäumt hatte, die Beteiligten vor dem Fotografieren ausdrücklich um Erlaubnis zu fragen, und sie auch nicht darüber informiert wurden, dass die Bilder danach noch auf den Patientenfluren der Stationen aufgehängt werden sollten. Wie uns das Zentrum für Psychiatrie in seiner Stellungnahme mitteilte, hat es die Eingabe und unsere Nachfrage zum Anlass genommen, dafür zu sorgen, dass vor der Anfertigung von Fotos zukünftig immer erst eine schriftliche Einwilligung bei den Betroffenen eingeholt wird. Diese sollen dabei sowohl über den Zweck des Fotografierens als auch über ihre Patientenrechte informiert werden.

Wir mussten dem Zentrum für Psychiatrie gleichwohl ins Stammbuch schreiben, dass solche Fotoaktionen ganz eindeutig gegen die Bestimmungen des Landesdatenschutzgesetzes verstoßen, zumal es sich dabei um sog. sensitive Patientendaten handelt (§ 33 LDSG). Es kann – trotz bei uns nach wie vor bestehender Zweifel – für die datenschutzrechtliche Bewertung letztlich dahingestellt bleiben, ob das Anfertigen von Fotos tatsächlich zur Erfüllung der Aufgaben des Zentrums für Psychiatrie erforderlich war. Dies ist primär eine medizinische Fachfrage. Nur wenn diese Frage positiv beantwortet werden könnte, wäre diese besondere Form der Datenerhebung nach § 13 Abs. 1 LDSG überhaupt gerechtfertigt. Unabhängig hiervon steht allerdings fest, dass man seinerzeit von Seiten der Klinik versäumt hatte, die betroffenen Patienten vor dem Anfertigen der Fotos ausdrücklich darauf hinzuweisen, dass diese nicht gegen ihren ausdrücklich erklärten Willen fotografiert werden dürfen (§ 14 Abs. 1 LDSG). Darüber hinaus hätte den Betroffenen nach der genannten Vorschrift zunächst erläutert werden müssen, zu welchen Zwecken die Aufnahmen gefertigt werden sollen. Dass die Fotos danach auch noch zusätzlich und ungefragt auf dem Patientenflur aufgehängt wurden – auch wenn es sich dabei „nur“ um eine kurzfristige Aktion gehandelt hat –, stellt einen weiteren Datenschutzverstoß dar.

Von einer förmlichen Beanstandung des Zentrums für Psychiatrie konnte auch insoweit abgesehen werden, weil man sich in der Sache einsichtig gezeigt und auch zugesagt hat, ab sofort keine Fotos mehr ohne schriftliche Einwilligung der Patienten zu fertigen und diese darüber hinaus vorher sowohl über die therapeutischen Zwecke der Aufnahmen als auch über die den Patienten zustehenden Rechte ausreichend zu informieren. Es bleibt allerdings die Frage, weshalb diese Mängel erst durch die Einschaltung des Landesdatenschutzbeauftragten abgestellt werden konnten und solche Verstöße nicht von vornherein durch den vom Zentrum für Psychiatrie bestellten Datenschutzbeauftragten vor Ort unterbunden worden waren. Bekanntlich hat jeder Krankenhausträger für das Krankenhaus einen Beauftragten für den Datenschutz nach § 51 Abs. 1 des Landeskrankenhausgesetzes zwingend zu bestellen.

4.5 Bestellung eines externen Datenschutzbeauftragten im Krankenhaus

Unsere Dienststelle musste sich bei diesem Thema als Streitschlichter betätigen, nachdem es in einem Klinikum im Osten Baden-Württembergs über diese Frage zu einem Zerwürfnis zwischen Personalrat und Krankenhausleitung gekommen war und die von der Leitung für diese Tätigkeit vorgesehene Person dadurch zwischen die „Kampflinien“ geraten war. Die nachfolgenden Ausführungen sind nicht nur für den inzwischen geklärten Einzelfall von Bedeutung, sondern können als allgemeine datenschutzrechtliche Orientierungshilfe dienen.

Die Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz in Krankenhäusern ergibt sich aus § 51 des Landeskrankenhausgesetzes. Danach hat jeder Krankenhausträger einen Beauftragten für den Datenschutz schriftlich zu bestellen, wobei für mehrere Krankenhäuser ein gemeinsamer Beauftragter bestellt werden kann. Eine aus-

drückliche Regelung, wonach die Bestellung eines externen Datenschutzbeauftragten ausgeschlossen wäre, ergibt sich hieraus und aus den hilfsweise anzuwendenden Vorschriften des Bundesdatenschutzgesetzes nicht. Es ist daher grundsätzlich zulässig, auch eine außenstehende Person mit der Aufgabe des Datenschutzbeauftragten in einem Krankenhaus zu betrauen. Dies sollte allerdings nur die „ultima ratio“ sein, denn gerade im datenschutzrechtlich sensiblen Krankenhausbereich, für den eine Pflicht zur Bestellung eines behördlichen Datenschutzbeauftragten besteht, empfehlen wir, zunächst zu prüfen, ob ein eigener geeigneter Mitarbeiter zur Verfügung steht und dieser auch willens ist – ggf. nach entsprechenden Fortbildungsmaßnahmen –, diese Funktion zu übernehmen. Erst wenn sich trotz entsprechender Bemühungen aus dem eigenen Klinikbereich niemand finden lässt, halten wir eine externe Lösung für vertretbar. Folgende Überlegungen sind dabei maßgeblich:

Das Herausverlagern von eigenen Aufgaben an externe Dienstleister (sog. Outsourcing) gilt inzwischen auch im Bereich der Medizin als modern und kostensenkend. Dass der Bereich des behördlichen Datenschutzes von solchen Überlegungen nicht ausgeklammert bleibt, war zu erwarten. Die Bundesärztekammer hat sich grundsätzlich dahin geäußert, dass ein Externer die Funktion eines behördlichen Datenschutzbeauftragten ausüben dürfe (§ 4 f Abs. 2 Satz 2 BDSG). Die Standesorganisation betont zu Recht ausdrücklich, dass die Regelungen zur Einhaltung der ärztlichen Schweigepflicht auch in diesem Fall zu beachten sind. Auf den Krankenhausbereich übertragen bedeutet dies, dass ein externer betrieblicher Datenschutzbeauftragter im klinischen Bereich ohne Einwilligung der Patienten keine Kenntnis von personenbezogenen Patientendaten erhalten darf, da andernfalls stets eine Verletzung des Arzt-Patienten-Geheimnisses vorliegen würde. Die Tätigkeit von externen Datenschutzbeauftragten kann sich daher grundsätzlich nur auf solche Bereiche erstrecken, in denen die Kenntnis von durch die ärztliche Schweigepflicht geschützten Daten nicht erforderlich ist. Damit würde sich jedoch bei der ausschließlichen Bestellung von externen Datenschutzbeauftragten in einem Krankenhaus eine wesentliche Kontroll- und hieraus resultierende Schutzlücke bei der Gewährleistung eines ausreichenden Datenschutzes auftun. Um dies im Interesse des Schutzes sensibler, dem Arzt-Patienten-Geheimnis unterliegender Daten zu vermeiden, ist es unseres Erachtens notwendig, zumindest ergänzend zu der Bestellung eines externen (privaten) Datenschutzbeauftragten zusätzlich einen Klinikmitarbeiter mit der Wahrnehmung von Aufgaben als behördlicher Datenschutzbeauftragter zu betrauen, der aufgrund seiner Stellung innerhalb des Krankenhauses als berufsmäßiger Gehilfe des Arztes im Sinne von § 203 Abs. 3 des Strafgesetzbuches angesehen werden kann.

Dieser „interne Datenschutzbeauftragte“ könnte auch ohne Einwilligung der Patienten zum Zwecke der Gewährleistung eines ausreichenden Datenschutzes innerhalb des Krankenhauses Einblick in die jeweiligen Patientendaten nehmen. Er wäre auch befugt, im Rahmen seiner Kontrollaufgaben die so erhaltenen Daten weiter zu verarbeiten. Der interne Datenschutzbeauftragte sollte dem externen Datenschutzbeauftragten für alle Bereiche, in denen die Kenntnis konkreter Patientendaten für die Aufgabenerfüllung des externen Datenschutzbeauftragten erforderlich sein könnte, z. B. im Wege der Durchführung von Stichproben, mit Echtdaten ergänzend und beratend zur Verfügung stehen. Er könnte die Daten, die dem Zugriff des externen Datenschutzbeauftragten nicht unterliegen, jeweils pseudonymisieren und anschließend dem externen Datenschutzbeauftragten zugänglich machen. Aufgrund von Hinweisen des externen Datenschutzbeauftragten könnte er bestimmte Kontrollen der personenbezogenen Patientendaten selbst durchführen, ohne dass dabei der externe Datenschutzbeauftragte Zugriff auf diese dem Arztgeheimnis unterliegenden Daten erhält.

Wir verkennen nicht, dass die aufgezeigte Lösung reichlich umständlich erscheint. Deshalb ist – wie eingangs ausgeführt – grundsätzlich die Lösung vorzuziehen, in einem Krankenhaus nur interne Datenschutzbeauftragte zu bestellen, die sich erforderlichenfalls durch externe Fach-

leute/Firmen bei ihren Kontrollaufgaben beraten und in sonstiger Weise unterstützen lassen. Dadurch würde eine eindeutige und einheitliche Zuordnung der Verantwortung für die Wahrnehmung der Aufgaben eines behördlichen Datenschutzbeauftragten im Krankenhaus gewährleistet und gleichzeitig eine ausreichende Datenschutz- und Datensicherheitsfachkunde vor Ort sichergestellt.

5. Einschulungsuntersuchungen

Für die Erkenntnis, dass die Einschulungsuntersuchung (ESU) in der herkömmlichen Form mittlerweile in die Jahre gekommen ist, bedurfte es wohl nicht zwingend eines Impulses von außen durch die Ergebnisse der PISA-Studie. Verschiedene bildungspolitische Neuerungen, die in Baden-Württemberg in den letzten Jahren eingeführt wurden, haben zunehmend komplexere Fragestellungen an die ESU herangetragen, die diese nicht mehr leisten konnte. Da ein Fünftel bis ein Viertel der Kindergartenkinder bereits vor der Einschulung gefördert werden müssen, damit sie den Anforderungen der Schule überhaupt gewachsen sind, wurden u. a. das Modellprojekt „Schulreifes Kind“ sowie die Aufstellung eines sog. Orientierungsplans in Angriff genommen; in diesem sollen die Bildungsziele für Kinder im Kindergarten vor allem hinsichtlich ihrer Sprachentwicklung und ihrer Schulfähigkeit festgelegt werden.

Für die Neukonzeption der ESU ergibt sich daraus die Notwendigkeit, mehr Zeit hierfür aufzuwenden, zeitlich schon viel früher anzusetzen und insbesondere auch die Beratung der Eltern unter Einbeziehung der Erzieherinnen zu intensivieren. Um sich etwaigen Risikogruppen gezielter zuwenden und Zeit für die Förderung dieser Kinder gewinnen zu können, wurden bereits in den letzten Jahren von der Sozial- und Kultusverwaltung verschiedene Untersuchungsmodelle entwickelt; dabei sollten auch nicht ärztlich durchgeführte Screening-Untersuchungen sinnvoll einbezogen werden (Englisch: Screen = Sieb).

Im Auftrag des Sozialministeriums wurde daher eine von einer Arbeitsgruppe erstellte Neukonzeption der ESU Anfang Oktober 2005 präsentiert, bei der uns erstmals Gelegenheit gegeben wurde, in einem sehr frühen Verfahrensstadium zu Fragen des Datenschutzes Stellung zu nehmen. Wir haben dies ausdrücklich begrüßt. Leider wurde bisher versäumt, die Kirchen zu beteiligen, obwohl sich rd. 60 % der rd. 6 000 Kindergärten in Baden-Württemberg in privater Hand befinden und auch meist von den Kirchen betrieben werden. Wir halten daher eine nachträgliche Beteiligung des kirchlichen Datenschutzes noch vor Beginn des neuen Untersuchungsverfahrens in ausgewählten Testregionen für zwingend geboten, damit auch dort die für ein solches Modellprojekt benötigte Akzeptanz erreicht werden kann.

Die ESU soll zukünftig in zwei aufeinander aufbauenden Schritten durchgeführt werden:

– Die erste Untersuchungsphase findet im vorletzten Kindergartenjahr statt (24 bis 16 Monate vor Einschulung), um Zeit für Maßnahmen der Prävention und der Gesundheitsförderung bei Risikokindern bzw. für Fördermaßnahmen zu gewinnen.

  Diese erste Screening-Untersuchung enthält folgende Elemente:

  • Dokumentation der Krankheitsfrüherkennungsuntersuchungen und des Impfstatus,

  • Erhebung ausgewählter Befunde durch sozialmedizinische Assistenten (Körpergröße und Körpergewicht, Sprachtest, Seh- und Hörtest),

  • standardisierte Befragung der Eltern mit Hilfe eines Elternfragebogens zum Entwicklungsverlauf sowie zu Krankheiten und sozialen Rahmenbedingungen des Kindes,

  • standardisierte Befragung der Erzieherinnen mit Hilfe eines Erzieherinnenfragebogens zum Entwicklungsstand des Kindes auf der Basis der im Rahmen des Orientierungsplans eingeführten obligatorischen Entwicklungsdokumentation.

Die ärztliche Untersuchung erfolgt nur noch bei denjenigen Kindern, bei denen in der Entwicklungsdokumentation der Kindertageseinrichtung, der U 8/U 9 oder in einem Elternfragebogen nach ärztlicher Bewertung Hinweise auf Entwicklungs- oder gesundheitliche Probleme enthalten sind. Nach Auffassung des federführenden Sozialministeriums erscheint dieses Verfahren vom Ansatz her zuverlässig, weil es die Beobachtungen zweier verschiedener Berufsgruppen und der Eltern einbezieht. Bei Kindern ohne Kindergartenbesuch wird der Entwicklungsstand durch den öffentlichen Gesundheitsdienst erhoben.

Ungefähr 15 Monate vor Einschulung soll im Rahmen eines runden Tisches „Schulreifes Kind“ (bestehend aus Vertretern von Schule, Kindergarten, Gesundheitsamt, Frühförderstelle, Eltern, Beratungslehrer) die Förderung der Risikokinder und förderbedürftiger Kinder besprochen und eine Empfehlung ausgesprochen werden. Dazu trägt das Gesundheitsamt die Ergebnisse aus der ersten Phase der ESU bei.

– Die zweite Phase der ESU folgt im letzten Kindergartenjahr (ca. drei Monate vor Einschulung) zur Frage der Schulfähigkeit und besteht aus folgenden Elementen:

  Bei denjenigen Kindern, die bei der Screening-Untersuchung in der ersten Phase (vorletztes Kindergartenjahr) ohne auffälligen Befund waren, wird anhand eines zweiten Erzieherinnenfragebogens drei Monate vor der geplanten Einschulung beurteilt, ob zwischenzeitlich Entwicklungsauffälligkeiten aufgetreten sind. Eine zweite Befragung der Eltern ist bei dieser Gruppe nicht vorgesehen.

  Bei Kindern, die einen auffälligen Befund hatten und in der Folge Fördermaßnahmen erhalten haben, wird eine Nachuntersuchung durch den öffentlichen Gesundheitsdienst zur Evaluation dieser Maßnahmen durchgeführt.

– Die Entscheidung zur Frage der Schulfähigkeit trifft letztlich die Schulbehörde bzw. Schule.

Wie uns vom Sozialministerium mitgeteilt wurde, soll die Umsetzung der Neukonzeption der ESU im Rahmen eines Modellprojekts in ausgewählten Kreisen im Laufe des Kindergartenjahrs 2005/2006 erprobt und danach ausgewertet und evaluiert werden. Aus Sicht des Datenschutzes ist dabei wichtig, dass – jedenfalls während der Pilotphase – alle Datenerhebungen mittels dafür vorgesehener Fragebögen (Eltern- bzw. Erzieherinnenfragebogen) nur dann stattfinden dürfen, wenn die Erziehungsberechtigten hierfür ihr ausdrückliches und schriftliches Einverständnis nach vorheriger Information erklärt haben. Darüber hinaus müssen die Eltern zuvor auch noch den Schularzt von ihrer Schweigepflicht entbinden. Nach Abschluss der Auswertung der Erfahrungen in den Modellregionen ist es danach Sache der zuständigen Ressorts (Sozialministerium zusammen mit Kultusministerium), darüber zu entscheiden, ob und in welcher Form eine neue ESU verbindlich eingeführt werden soll und demzufolge auch gesetzlich geregelt werden muss. Unsere Dienststelle ist dabei zu beteiligen.

So weit, so gut, könnte man meinen. Eine erste Durchsicht der Entwurfsfassung der von der Arbeitsgruppe für das Sozialministerium konzipierten Fragebögen ließ allerdings – ohne dies mangels entsprechender schriftlicher Begründung fachlich abschließend prüfen zu können – bei uns ernsthafte Zweifel darüber aufkommen, ob die vorgesehenen Angaben insgesamt für die vorgesehenen Zwecke geeignet und erforderlich sind.

Dies gilt insbesondere vor dem Hintergrund, dass diese Fragebögen für den Echtbetrieb projektiert wurden und nach dem erklärten Willen des Sozialministeriums diese später verbindlich zu beantworten sind. Das informationelle Selbstbestimmungsrecht der Betroffenen (Anmerkung: auch der Minderjährigen) kann aber nur im überwiegenden Allgemeininteresse eingeschränkt werden. Zudem ist auch bei Fragebogenaktionen der Grundsatz der Datensparsamkeit zu beachten; bei 31 Haupt- und zahlreichen weiteren Unterfragen (Elternfragebogen) sowie ca. 60 Einzelfragen an die Erzieherinnen ist dieser Grundsatz nicht mehr gewahrt. Unseres Erachtens greifen

auch einige Fragestellungen zu tief in den Kernbereich des Grundrechts auf Datenschutz ein. Ist es hiermit tatsächlich vereinbar, wenn z. B. die Eltern eines drei- bis vierjährigen Kindergartenkindes zukünftig gefragt werden sollen, ob es zurzeit gesundheitliche oder andere Probleme in der Familie gibt oder ob in Gegenwart ihres Kindes in der Wohnung geraucht wird? Soll man tatsächlich für eine zuverlässige Prognose über die Schulreife eines Kindes Erzieherinnen befragen dürfen, ob das ihnen anvertraute drei- bis vierjährige Kind lügt oder häufig mogelt bzw. zu Hause, im Kindergarten oder sonst wo stiehlt? Wir meinen, dass dies entschieden zu weit geht!

Nicht alles, was vielleicht aus anderen Gründen interessant und wünschenswert wäre zu erfahren, ist auch für den vorgesehenen Zweck zwingend erforderlich und geeignet. Sowohl das Sozialministerium als auch das Kultusministerium müssen daher selbstkritisch hinterfragen, ob die bisher vorgesehenen Fragestellungen nicht zu intim und zu umfänglich sind. Werden die Fragen in Inhalt und Umfang auf das gebotene Maß reduziert, bestehen im Übrigen von Seiten des Datenschutzes keine grundsätzlichen Bedenken, auf freiwilliger Basis in ausgewählten Testregionen mit dem Modellversuch „neue ESU“ zu starten.

2. Abschnitt: Die gesetzliche Krankenversicherung

1. Datenschutzverstoß führt zur Kündigung

Dass Datenschutzverstöße mitunter gravierende und nicht beabsichtigte Folgen haben können, musste eine Bürgerin leidvoll erfahren, die sich in ihrer Not an unsere Dienststelle wandte. Was war geschehen?

Die betroffene Bürgerin war bei einem kirchlichen Träger als Hauswirtschafterin in der Nachbarschaftspflege angestellt, obwohl sie von ihrer Ausbildung her die Qualifikation einer Haus- und Familienpflegerin – also eine höhere Qualifikation – besaß. Dennoch veranlasste sie ihr Arbeitgeber, die Abrechnungen mit dem Kennzeichen „P“ als Familienpflegerin/Pflegefachkraft zu versehen, damit er höhere Gebühren bei der Pflegeversicherung abrechnen konnte. Ihre Hinweise auf den Arbeitsvertrag, wonach sie nicht als Familienpflegerin eingestellt worden sei und damit diese Kennzeichnung möglicherweise abrechnungstechnisch nicht korrekt sein könnte, wurde von ihrem Arbeitgeber ignoriert.

Um sich selbst rechtlich abzusichern und nicht in den Verdacht einer Beihilfe zum Abrechnungsbetrug zu gelangen, wandte sich die Petentin an die Krankenkasse, bei der sie selbst versichert war. Sie nannte dabei ihren Namen; den ihres Arbeitgebers nannte sie hingegen nicht. Ohne Auftrag, Wissen und Genehmigung der um Rat suchenden Frau ermittelte der Sachbearbeiter der Krankenkasse im Anschluss an das Telefonat den Namen des Arbeitgebers und rief dort an, um sich nach den Abrechnungsmodalitäten in solchen Fällen zu erkundigen. Dabei bezog er sich ganz konkret auf die Anruferin.

Beim Arbeitgeber der Petentin entstand dadurch der Eindruck, dass diese ihn bei der Krankenkasse anschwärzen und ihm einen Abrechnungsbetrug habe vorwerfen wollen. Trotz der gegenteiligen Beteuerungen der Petentin zeigte sich ihr Arbeitgeber wenig christlich und schickte ihr eine außerordentliche Kündigung ins Haus. Im Verlauf des sich anschließenden Arbeitsgerichtsverfahrens wurde das Arbeitsverhältnis schließlich wegen Zerrüttung aufgelöst.

So weit, so schlecht. Die Bundesanstalt für Arbeit wurde danach ebenfalls gegenüber der inzwischen arbeitslosen Frau aktiv und verhängte eine sog. Sperrzeit, in der ihr kein Anspruch auf Arbeitslosengeld zugebilligt wird. Die Arbeitsverwaltung begründete ihre Entscheidung damit, dass sie eigenmächtig hinter dem Rücken ihres Arbeitgebers mit einer Krankenkasse Kontakt aufgenommen und dadurch selbst einen „unüberwindlichen Vertrauensbruch“ herbeigeführt habe.

Datenschutzrechtlich betrachtet handelt es sich bei der geschilderten Vorgehensweise des Krankenkassenmitarbeiters um eine unzulässige Daten-

übermittlung an den Arbeitgeber der Petentin, weil es dafür keine Rechtsgrundlage gibt und auch keine wirksame Einwilligungserklärung von der Betroffenen vorgelegen hatte (vgl. § 4 LDSG). Die Petentin wurde dadurch in ihrem Grundrecht auf informationelle Selbstbestimmung so nachhaltig verletzt, dass sie im Ergebnis sogar ihren Arbeitsplatz verlor. Positiv – wenn dieses Wort hier überhaupt passt – war für unsere Dienststelle zu vermelden, dass die Krankenkasse wenigstens zügig und vorbehaltlos bei der Aufklärung des Sachverhalts mithalf, das Fehlverhalten ihres Mitarbeiters glaubhaft bedauerte und darüber hinaus gegen diesen auch Personalmaßnahmen in die Wege leitete.

Gleichwohl sah ich mich veranlasst, wegen der Schwere der Datenschutzverletzung und deren Folgen für die Betroffene gegenüber der Krankenkasse eine förmliche Beanstandung auszusprechen. Im Übrigen habe ich die Krankenkasse gebeten, diesen Fall zum Anlass zu nehmen, ihre Beschäftigten erneut auf den sorgfältigen Umgang mit Versichertendaten hinzuweisen und auch exemplarisch darzustellen, welche gravierenden Auswirkungen ein nicht datenschutzkonformes Umgehen mit sensiblen Daten für die Betroffenen haben kann. Für die Frage, ob und inwieweit die Betroffene wegen der Folgewirkungen des Datenschutzverstoßes Schadensersatzansprüche gegen die Krankenkasse bzw. ihren Mitarbeiter durchsetzen kann, ist unsere Dienststelle nach dem Landesdatenschutzgesetz nicht zuständig. Dies ist Sache der Zivilgerichte.

2. Datenschutz für Versicherte endet nicht mit Büroschluss

Mit einem recht kuriosen Sachverhalt musste sich meine Dienststelle in einem anderen Fall befassen. Bestanden doch unter allen Hauptbeteiligten persönliche Verbindungen aus früherer Zeit, die zum Teil noch bis in die Gegenwart reichten. Die Handelnden: Eine Krankenkassenmitarbeiterin und ihr Lebensgefährte sowie unsere Petentin, die mit diesem zuvor eng befreundet war.

Um sich über aktuelle Veranstaltungsangebote einer unserer Aufsicht unterliegenden gesetzlichen Krankenkasse (GKV) zu informieren, hatte die Petentin eine eigens dafür eingerichtete Web-Seite der Krankenversicherung im Internet aufgerufen und danach eine entsprechende Anfrage per E-Mail an die zuständige Außenstelle der GKV gerichtet. Diese wurde daraufhin auch prompt durch die dort beschäftigte Marketing-Leiterin in elektronischer Form beantwortet. Was die Petentin allerdings nicht wusste, war, dass die Marketing-Leiterin inzwischen mit ihrem Ex-Freund eine Beziehung eingegangen war und – nur dies ist datenschutzrechtlich relevant – am Abend im privaten Kreis diesem brühwarm davon erzählte, wer sich heute mit welcher Frage an sie bzw. die Krankenkasse gewandt hatte. So weit, so schlecht. Auf wenig Gegenliebe stieß nämlich der nächste Schritt ihres früheren Partners. Dieser nahm die Information seiner aktuellen Freundin zum Anlass, um mit einer E-Mail wieder in Kontakt mit seiner Verflossenen zu treten. Danach waren wir als Streitschlichter gefragt.

Nach § 4 Abs. 1 LDSG ist die Verarbeitung personenbezogener Daten zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene darin eingewilligt hat. Nachdem dies hier ganz offensichtlich nicht der Fall war, stellt das Vergehen der Krankenkassenmitarbeiterin eine Datenschutzverletzung dar. Diese ist auch ihrem Arbeitgeber als der im Sinne des Datenschutzes dafür verantwortlichen Stelle gemäß § 3 Abs. 3 LDSG zuzurechnen. Daran ändert auch nichts, dass die Betroffene kein aktuelles Mitglied dieser Krankenkasse war, der Kernbereich der Aufgabenerfüllung dieser GKV nicht tangiert war und die Informationen auch nicht unmittelbar vom Arbeitsplatz aus weitergegeben wurden. Jeder, der sich an eine Krankenkasse wendet, vertraut nämlich darauf, dass die damit im Zusammenhang stehenden Informationen nicht unbefugt an Dritte weitergegeben werden.

So sah es auch die Krankenkasse von Anfang an und – inzwischen – auch die Mitarbeiterin, die von der Geschäftsleitung in einem persönlichen Gespräch ausdrücklich nochmals an die Einhaltung der datenschutzrechtlichen Anforderungen bei einer Tätigkeit in einer Krankenkasse hingewiesen wurde. Von einer förmlichen Beanstandung habe ich nicht zuletzt deshalb abgesehen, weil es sich um einen individuellen Fehler einer GKV-Ange-

stellten gehandelt hatte und dieser – ohne dass dies zu entschuldigen wäre – auch durch die besonderen persönlichen Verbindungen der Handelnden begünstigt worden war. Die Mitarbeiterin hat ihren Fehler bedauert; von der Krankenkasse wurden die erforderlichen Maßnahmen ergriffen, damit zukünftig solche Datenschutzverstöße möglichst nicht mehr vorkommen.

3. Einschaltung externer Gutachter

Es gibt Situationen, in denen es für die Krankenkasse geboten sein kann, einen externen Gutachter einzuschalten, um die Rechtmäßigkeit von Kostenvoranschlägen oder ärztlichen Verordnungen prüfen zu lassen. Sind doch die Kassen gehalten, mit den Beiträgen ihrer Versicherten wirtschaftlich umzugehen, was ja durchaus auch im Allgemeininteresse liegt. Allerdings sind bei der Übermittlung dieser sensiblen Versichertendaten bestimmte Spielregeln zu beachten. So enthält das von einer Krankenkasse für ihre Mitarbeiter erstellte Datenschutzhandbuch die Handlungsanweisung, dass ärztliche Verordnungen bzw. Kostenvoranschläge durch externe Gutachter nur dann begutachtet werden dürfen, wenn aus den Unterlagen kein Bezug zum betroffenen Versicherten sowie zum Leistungserbringer hergestellt werden kann. Bei Kopien, die der Gutachter erhält, sind die personenbezogenen Daten zu schwärzen. Als weitere Möglichkeit, einen externen Gutachter einzuschalten, ist der Weg über eine informierte Einwilligung des Versicherten beschrieben. Beide Vorgehensweisen sind datenschutzkonform.

Leider gibt es oftmals einen Unterschied zwischen Theorie und Praxis. Dies musste ein Bürger erfahren, der sich an unsere Dienststelle wandte, weil ein Krankenkassenmitarbeiter zunächst die von ihm beantragten orthopädischen Schuhe abgelehnt und, ohne sich an die o. g. Handlungsanweisung zu halten, die Unterlagen personenbezogen und ohne dessen Einverständnis an einen externen Gutachter weiterreichte.

Dem verärgerten Bürger konnten wir Folgendes mitteilen:

Mit der Einschaltung externer Gutachter durch eine Krankenkasse werden sensible Versichertendaten weitergegeben. Dies ist nur dann zulässig, wenn es hierfür gemäß § 67 d des Zehnten Buchs des Sozialgesetzbuchs (SGB X) eine Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder eine andere Rechtsgrundlage gibt bzw. der Betroffene in die Datenübermittlung wirksam eingewilligt hat. Ist doch gerade im Bereich des Sozialdatenschutzes besonders darauf zu achten, dass die Verarbeitung personenbezogener Daten so lange verboten ist, als sie nicht durch Gesetz ausdrücklich gestattet ist (sog. Verbot mit Erlaubnisvorbehalt). Die Grundsätze der Amtshilfe – dies wird gelegentlich verkannt – können eine Datenverarbeitung nicht rechtfertigen. Nachdem die vorgenannten Voraussetzungen für eine zulässige Datenübermittlung in dem von uns zu prüfenden Fall nicht vorlagen, lag in der beschriebenen Einschaltung des externen Gutachters ein Datenschutzverstoß nach § 4 Abs. 1 LDSG.

Die Krankenkasse selbst hat sich beim Betroffenen entschuldigt und uns mitgeteilt, dass die betroffene Bezirksdirektion aus Anlass dieses Falles explizit aufgefordert worden sei, zukünftige datenschutzrechtliche Anforderungen strikter zu beachten und einzuhalten. Des Weiteren werde der vorliegende Fall zum Anlass genommen, die fachlich zuständigen Krankenkassenmitarbeiter generell nochmals auf die datenschutzkonforme Umsetzung der internen Datenschutzanweisungen beim Einsatz externer Gutachter hinzuweisen. Letztlich wurde von einer förmlichen Beanstandung der Krankenkasse abgesehen.

3. Abschnitt: Soziales

1. Arbeitslosengeld II

In letzter Zeit vergeht kaum ein Tag, an dem Hartz IV nicht Thema in den Medien ist. Nach den Protesten zu Beginn der Reform sorgen derzeit vor allem die hohen Kosten für Schlagzeilen.

Aber der Reihe nach: Zu Beginn dieses Jahres trat das Zweite Buch des Sozialgesetzbuchs, die Grundsicherung für Arbeitssuchende, in einem wesentlichen Teil in Kraft. Viele Menschen erhalten seitdem das neue Arbeitslosengeld II an Stelle von Arbeitslosen- und Sozialhilfe.

Träger der Leistungen dieser Grundsicherung sind sowohl die Bundesagentur für Arbeit als auch kommunale Träger, d. h. Stadt- und Landkreise. Zur einheitlichen Wahrnehmung der Aufgaben sieht das Gesetz vor, dass die Leistungsträger Arbeitsgemeinschaften bilden. Seit Anfang des Jahres sind daher auch in Baden-Württemberg zahlreiche „ARGEn“ entstanden. Fünf Landkreise haben in Baden-Württemberg von der im Gesetz ebenfalls vorgesehenen Möglichkeit Gebrauch gemacht, die Aufgaben in alleiniger Verantwortung zu erfüllen. Diese – um es milde auszudrücken – unübersichtliche, da uneinheitliche Organisationsstruktur hat prompt zu einiger Verwirrung geführt, was die Zuständigkeiten in der Datenschutzaufsicht betrifft, und wohl nicht nur dort.

Klar ist, dass die sog. Optionskommunen als eindeutig der Landesebene zuzurechnende Verwaltungseinheiten der Aufsicht der Landesbeauftragten für den Datenschutz unterliegen. Die Landesbeauftragten sind darüber hinaus – übrigens in Übereinstimmung mit dem Bundesbeauftragten – der Auffassung, dass sie auch für die Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften bei den Arbeitsgemeinschaften zuständig sind. Genau dies akzeptiert die Bundesagentur für Arbeit aber derzeit nicht. Sie verschließt sich damit den Konsequenzen, die daraus zu ziehen sind, dass die Arbeitsgemeinschaften eigenverantwortlich handelnde Stellen sind, die nicht unmittelbar in die Organisation der Bundesagentur (die als solche der Aufsicht des Bundesbeauftragten für den Datenschutz unterliegt) eingebunden sind.

Oberflächlich betrachtet mag man zur Auffassung gelangen, dass diese Zuständigkeitsfrage keine Frage von Belang ist. Dies täuscht aber: Denn es führt gerade bei den Leistungsempfängern zu großer – weiterer – Frustration, wenn sie sich mit häufig recht heiklen Fragestellungen an meine Dienststelle wenden und dort erst mal erfahren müssen, dass man sich zunächst um die Klärung der Zuständigkeitsfrage bemühen müsse. Es ist deshalb zu hoffen, dass dieser Streitpunkt unter den Behörden bald zufrieden stellend ausgeräumt ist. Zumal noch weitere „Baustellen“ bei Hartz IV offen sind:

Schon in unserem Tätigkeitsbericht für 2004 hatten wir die umfangreichen Erhebungsvordrucke für das Arbeitslosengeld II thematisiert. Nicht alle Fragen in den Antragsvordrucken sind aus Sicht des Datenschutzes zulässig. Als Hilfestellung hatte die Bundesagentur daher auf Wunsch und mit Unterstützung der Datenschutzbeauftragten Ausfüllhinweise entwickelt und zugesagt, Änderungen am Vordruck bei dessen Neuauflage zu berücksichtigen.

Im Laufe dieses Jahres hat die Bundesagentur das Antragsformular und die Zusatzblätter nun überarbeitet. Hierbei waren auch die Datenschutzbeauftragten des Bundes und der Länder beteiligt. Um ein datenschutzgerechtes Ausfüllen der Unterlagen zu ermöglichen, sind aber weiterhin die Ausfüllhinweise zu überarbeiten. Jedenfalls sollten den Betroffenen nicht nur die neuen Antragsunterlagen, sondern auch die überarbeiteten Ausfüllhinweise so bald wie möglich zur Verfügung stehen.

Noch weniger erfreulich ist die Entwicklung bei einem anderen Projekt: Ebenfalls in unserem Tätigkeitsbericht für das Jahr 2004 berichteten wir von dem Datenbanksystem A2LL, das von den Arbeitsgemeinschaften zur Berechnung der auszuzahlenden Geldleistungen eingesetzt wird. Bereits früh war deutlich, dass dieses Verfahren schwer wiegende datenschutzrechtliche Mängel aufweist. Zum Beispiel lässt es einen uneingeschränkten bundesweiten Zugriff auf Daten der Hilfesuchenden zu. Jeder Mitarbeiter, der mit dem Datenbanksystem arbeitet, hat so die Möglichkeit, die Daten der Bezieher von Arbeitslosengeld II anderer Arbeitsgemeinschaften anzuschauen. Die Datenschutzbeauftragten des Bundes und der Länder forderten schon in einer Entschließung vom Oktober 2004 ein klar definiertes Zugriffsberechtigungskonzept. Der Bundesbeauftragte für den Datenschutz beanstandete Ende letzten Jahres förmlich die unveränderte Verwendung

der Software A2LL gegenüber der Bundesagentur für Arbeit. Entgegen den Zusagen des Bundesministeriums für Wirtschaft und Arbeit und der Bundesagentur für Arbeit gibt es bei dem elektronischen Verfahren auch fast ein Jahr danach immer noch keine erkennbaren Fortschritte. Weder ist ein klar definiertes Zugriffsberechtigungskonzept umgesetzt noch erfolgt eine Protokollierung der lesenden Zugriffe.

Inzwischen setzen die Arbeitsgemeinschaften zudem noch das elektronische Vermittlungsverfahren coArb ein. Jeder Mitarbeiter einer Arbeitsgemeinschaft kann aufgrund des bundesweiten lesenden Zugriffs hierüber Kenntnis äußerst sensibler Daten wie z. B. Vermerke über Schulden-, Ehe- oder Suchtprobleme der Bezieher des Arbeitslosengelds II erhalten.

Die Themen waren auch Gegenstand einer von den Datenschutzbeauftragten des Bundes und der Länder im Oktober 2005 gefassten Entschließung (s. Anhang 9). Darin werden die Bundesagentur für Arbeit und die sonstigen verantwortlichen Stellen aufgefordert, die gravierenden Datenschutzmängel beim Arbeitslosengeld II endlich zu beseitigen. Eine zweite Entschließung zu Hartz IV betrifft die von der Bundesagentur mit Hilfe privater Callcenter durchgeführten Telefonbefragungen von Leistungsbeziehern (s. Anhang 10).

Die ganze Brisanz des Themas spiegelt sich in zahlreichen Eingaben und Anfragen, die wir zum Arbeitslosengeld II erhalten, wieder.

1.1 Antragsberatung im Einzelzimmer? Fehlanzeige!

Aller Anfang ist schwer. Dass diese Binsenweisheit auch auf die Einführung des Arbeitslosengelds II zutraf, ist oben bereits angesprochen worden. Neben den dort geschilderten grundsätzlichen Problemen gab es auch erhebliche Schwierigkeiten im praktischen Behördenalltag. Diese hingen vor allem damit zusammen, dass der erfolgte organisatorische Zusammenschluss zu Arbeitsgemeinschaften auch räumliche Veränderungen und Umzüge mit sich brachte. Etwaige Anlaufschwierigkeiten sind da verständlich. Wie wenig sensibel sich allerdings eine Arbeitsgemeinschaft beim Thema Datenschutz zeigte, wunderte nicht nur die betroffenen Bürger:

So hatte ein Antragsteller bei der für ihn zuständigen Arbeitsgemeinschaft Ende April 2005 einen Termin zur Besprechung und Abgabe seines Antrags auf Arbeitslosengeld II. Zum vereinbarten Zeitpunkt fand er sich in dem ihm mitgeteilten Raum ein. Zu seinem Erstaunen befanden sich dort jedoch schon zwei weitere Antragsteller, mit denen er kurze Zeit später fast Schulter an Schulter seiner Sachbearbeiterin gegenüber saß. Der Bürger, der dies nicht einfach so hinnehmen wollte, wies darauf hin, dass er schon aus Gründen des Datenschutzes davon ausgegangen sei, in einem Einzelzimmer beraten zu werden. Die Sachbearbeiterin habe – so schilderte es uns der Bürger – diese Anmerkung mit einem wenig freundlichen „das sehen Sie doch“ quittiert. Der Bürger wandte sich daraufhin an uns. Im letzten Satz seines Eingabeschreibens merkte er an, dass beim Kauf einer Briefmarke bei der Post oder beim Kauf einer Fahrkarte bei der Bahn aufgrund der dort eingerichteten Diskretionszonen mehr Vertraulichkeit herrsche, als bei der Besprechung sehr persönlicher finanzieller Details bei der Abgabe seines Antrags auf Arbeitslosengeld II.

Die Arbeitsgemeinschaft erklärte auf unsere Anfrage, Anfang Januar dieses Jahres seien im Landkreis vier Standorte zur Wahrnehmung der Aufgaben nach dem Zweiten Buch des Sozialgesetzbuchs neu eingerichtet worden. Die Antragsabgabe habe von Januar bis Mitte Mai in zwei Räumen der Arbeitsgemeinschaft stattgefunden, die mit jeweils drei Arbeitsplätzen ausgestattet sind. Zum damaligen Zeitpunkt sei es aufgrund der Qualifikation der Mitarbeiter und der Räumlichkeiten nicht möglich gewesen, die Antragsannahme anders zu organisieren. Wäre der Wunsch eines Kunden, in einem Einzelzimmer beraten zu werden, an die Geschäftsleitung herangetragen worden, so hätte diese geraten, ein Büro aufzusuchen, das an diesem Tage aufgrund von Krankheit oder Außendienst eines Mitarbeiters nicht belegt sei.

Die Arbeitsgemeinschaft teilte weiter mit, dass sich seit Anfang Juni 2005 nun zwei Sachbearbeiter einen Raum teilen. Von der Geschäftsführung sei die Anweisung ergangen, die Terminierung so abzusprechen, dass jeweils nur ein Kunde im Zimmer beraten werde. Sollte der ausdrückliche Wunsch eines Kunden bestehen, dass der andere Sachbearbeiter bei dem Gespräch nicht anwesend sein solle, so werde dieser entweder den Raum verlassen oder der zuständige Sachbearbeiter sich nach einem anderen Beratungsplatz umsehen.

Durch diese organisatorischen Änderungen hat die Arbeitsgemeinschaft wesentliche Verbesserungen bei der Sicherstellung der Vertraulichkeit des gesprochenen Worts erreicht. Dies registrierte auch der betroffene Petent dankbar.

Zur Information der Kunden empfahlen wir, im Eingangsbereich einen Hinweis auf das Angebot der Arbeitsgemeinschaft, ein Beratungsgespräch auch in Abwesenheit des anderen Sachbearbeiters führen zu können, anzubringen. Außerdem sahen wir noch weiteren Verbesserungsbedarf: So, wie die Antragsberatung bei der Arbeitsgemeinschaft jetzt organisiert ist, besteht die Gefahr, dass ein Kunde Kenntnis von personenbezogenen Daten aus einem während der Beratung von dem anderen Sachbearbeiter geführten Telefonat erhält. Deshalb – so teilten wir der Arbeitsgemeinschaft mit – ist anzustreben, die Beratung auch ohne ausdrücklichen Wunsch des Kunden grundsätzlich außer Hörweite anderer Personen durchzuführen.

1.2 Verschwundene Antragsunterlagen

Wer Sozialleistungen beantragt, hat die Pflicht, alle Tatsachen anzugeben, die für die Leistung erheblich sind. Bürger, die das Arbeitslosengeld II beantragen, haben daher umfangreiche Formulare auszufüllen. Neben Name und Adresse haben die Antragsteller das Geburtsdatum, den Familienstand, eine etwaige bestehende Schwangerschaft, ihre Einkommens- und Vermögensverhältnisse, etwaige Krankheiten, bei deren Vorliegen zusätzliche Leistungen gewährt werden, und vieles mehr anzugeben. Daher ist es überaus verständlich, dass es einer Bürgerin unbehaglich zumute wurde, als ihr von der für sie zuständigen Arbeitsgemeinschaft mitgeteilt wurde, ihre Antragsunterlagen seien beim Umzug von Teilen des ehemaligen Sozialamts verloren gegangen. Die Bürgerin befürchtete, dass die Unterlagen noch in Umzugskisten liegen und irgendwann in „falsche Hände“ geraten könnten.

Auf unsere Nachfrage teilte die Arbeitsgemeinschaft mit, der Verlust der Unterlagen stehe nicht im Zusammenhang mit dem erfolgten Umzug, da er schon vorher bemerkt worden sei. Es werde vielmehr vermutet, dass die Unterlagen versehentlich in einer anderen Akte abgelegt worden seien. Die Befürchtung, die Unterlagen könnten in „falsche Hände“ geraten, werde für unbegründet gehalten.

Dem konnten wir, gerade aufgrund der Ausführungen der Arbeitsgemeinschaft, nicht zustimmen. Die Ablage der Unterlagen in einer anderen Akte birgt die Gefahr, dass die Sozialdaten der betroffenen Bürgerin im Rahmen einer Akteneinsicht tatsächlich in Hände Unbefugter geraten. Wir baten die Arbeitsgemeinschaft deshalb, nach dem Verbleib der Unterlagen in den Akten anderer Antragsteller zu schauen. Um die Suche sinnvoll einzugrenzen, könnten z. B. nur diejenigen Akten durchgeschaut werden, die von der zuständigen Sachbearbeiterin oder in dem Raum der zuständigen Sachbearbeiterin zu dem in Frage kommenden Zeitraum bearbeitet wurden.

Die Arbeitsgemeinschaft kam unserer Bitte nach und schaute die in Frage kommenden Akten durch. Damit hatte sie sich in angemessenem Maß um den Verbleib der Antragsunterlagen bemüht. Doch auch diese Recherche förderte die verschollenen Unterlagen nicht zutage. Wir haben die Arbeitsgemeinschaft daraufhin gebeten, eine Optimierung der internen Arbeitsabläufe zu prüfen, um den Verlust von Unterlagen wenigstens für die Zukunft nach Möglichkeit auszuschließen.

Das Unbehagen der betroffenen Bürgerin wird geblieben sein.

1.3 Das Antragsformular zur Ortsabwesenheit

Die Eingaben zum Arbeitslosengeld II betrafen nicht nur den organisatorischen Bereich. Auch zur Zulässigkeit der Datenerhebung erreichten uns Anfragen: Eine Bürgerin, die Arbeitslosengeld II bezieht, plante im August dieses Jahres, eine Woche in Urlaub zu fahren. An der Infotheke der für sie zuständigen Arbeitsgemeinschaft wurde ihr mitgeteilt, sie müsse zunächst ein Antragsformular zur Ortsabwesenheit ausfüllen.

Auf dem Antragsvordruck waren das Land und der Ort des Aufenthalts anzugeben. Außerdem sollte die Bürgerin mitteilen, wie die Reise finanziert wird. Weiter wurden Angaben zur Unterbringung vor Ort, zum Reiseverkehrsmittel und eine Begründung zur Notwendigkeit der Reise verlangt. Eine Sachbearbeiterin bewilligte den Urlaub schließlich. Die Bürgerin aber war erschrocken über den Wissensdurst der Arbeitsgemeinschaft.

Auf unsere Anfrage teilte die Arbeitsgemeinschaft mit, eine Ortsabwesenheit von bis zu drei Wochen im Kalenderjahr werde – in Anlehnung an Regelungen zum Arbeitslosengeld – grundsätzlich genehmigt. Über eine längere Abwesenheit entscheide der Vermittler im Einzelfall. Deshalb erfolgten auch die Nachfragen zur Notwendigkeit und Finanzierung der Reise.

Das Erheben von Sozialdaten ist aber nur zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach dem Sozialgesetzbuch erforderlich ist. Gründe, weswegen die Arbeitsgemeinschaft innerhalb der ersten drei Wochen Ortsabwesenheit pro Kalenderjahr Kenntnis von den oben genannten Sozialdaten benötigen könnte, hatte sie selbst nicht vorgetragen. Soweit die Ortsabwesenheit über drei Wochen pro Kalenderjahr hinausgeht, kann es durchaus zulässig sein, eine Begründung zur Notwendigkeit der Ortsabwesenheit zu verlangen. Die Erforderlichkeit einer generellen Erhebung der weiteren genannten Daten wie etwa über den Ort des Aufenthalts oder die Art der Unterbringung sehen wir jedoch nicht.

Die betroffene Arbeitsgemeinschaft hat ihre Antragsformulare zur Ortsabwesenheit inzwischen abgeändert.

1.4 Die Anfrage der Polizei

Schwierigkeiten kann nicht nur die Frage bereiten, welche Sozialdaten eine Behörde erheben, sondern auch, unter welchen Voraussetzungen sie diese weitergeben darf. Eine für das Arbeitslosengeld II zuständige Behörde war sich hier nicht sicher und wandte sich deswegen in folgender Sache an uns:

Ein Bezieher von Arbeitslosengeld II, nennen wir ihn X, gab in seinen Antragsunterlagen an, in Untermiete bei Y zu leben. Y selbst bezog kein Arbeitslosengeld II. Die Staatsanwaltschaft ermittelte gegen Y wegen des Verdachts des Vorenthaltens und Veruntreuens von Arbeitsentgelt. Im Verlauf dieser Ermittlungen bat die Polizei die für das Arbeitslosengeld II zuständige Behörde um die Unterlagen des X, die im Zusammenhang mit dessen Antrag auf Arbeitslosengeld II stehen, da diese für das Ermittlungsverfahren benötigt würden.

Klar ist zunächst, dass die für das Arbeitslosengeld II zuständige Behörde zur Wahrung des Sozialgeheimnisses verpflichtet ist. Dies gilt auch im Verhältnis zu den Strafverfolgungsbehörden und daher auch in staatsanwaltschaftlichen Ermittlungsverfahren. Eine Übermittlung von Sozialdaten ist – sofern der Betroffene nicht in diese eingewilligt hat – nur zulässig, soweit eine Vorschrift dies erlaubt. Eine solche Vorschrift ist § 68 des Zehnten Buchs des Sozialgesetzbuchs (SGB X). Danach ist es zulässig, den Polizeibehörden und der Staatsanwaltschaft im Einzelfall auf Ersuchen einen Standarddatensatz des Betroffenen zu übermitteln, soweit dies für die Erfüllung der Aufgaben der genannten Behörde erforderlich ist und kein Grund zur Annahme besteht, dass dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Dieser Standarddatensatz umfasst Name, Vorname, Geburtsdatum, Geburtsort,

derzeitige Anschrift des Betroffenen, seinen derzeitigen oder zukünftigen Aufenthalt sowie Namen und Anschriften seiner derzeitigen Arbeitgeber.

Dabei ist Betroffener keineswegs – wie die bei uns anfragende Behörde zunächst angenommen hatte – nur Y als Beschuldigter im Ermittlungsverfahren, sondern jede Person, zu der die Sozialbehörde im Hinblick auf ihre Aufgaben Sozialdaten erhebt, verarbeitet oder nutzt. Insoweit war auch eine Übermittlung von Sozialdaten des X, obwohl gegen diesen gar nicht ermittelt wurde, nicht von vornhinein ausgeschlossen.

Soweit die übrigen Voraussetzungen des § 68 SGB X tatsächlich vorlagen, durfte die für das Arbeitslosengeld II zuständige Behörde daher den Standarddatensatz des X an die Polizei übermitteln. Es ist also bei weitem nicht so, dass der Datenschutz als Argument dafür angeführt werden kann, dass er die Arbeit der Ermittlungsbehörden unangemessen behindere. Allerdings wäre eine Übermittlung von inhaltlich über den Standarddatensatz hinaus gehenden Daten nicht in Betracht gekommen, da es hierfür an einer entsprechenden Rechtsgrundlage gefehlt hätte.

2. Sozialamt: Die Anfrage beim Finanzamt

Ende letzten Jahres wandte sich ein älterer Herr an uns, dessen Sohn seinerzeit Sozialhilfe bezog: Der Sohn hatte beim Sozialamt angegeben, seine Wohnung von seinem Vater gemietet zu haben. Deshalb gewährte das Sozialamt im Rahmen der laufenden Hilfe zum Lebensunterhalt auch Leistungen zu den Unterkunftskosten. Das Sozialamt hatte dem Sohn nun mitgeteilt, bei einer Anfrage beim Finanzamt hätte es die Auskunft erhalten, dass der Vater seine Mieteinnahmen beim Finanzamt nicht angegeben bzw. versteuert habe. Deshalb bestehe der Verdacht, dass der Sohn an seinen Vater gar keine Miete zahle.

Auf unsere Anfrage teilte das Sozialamt mit, dass es die Auskunft bei der Finanzbehörde eingeholt habe, da auf den Kontoauszügen, die der Sohn bei der Beantragung der neuen Sozialleistung Arbeitslosengeld II vorgelegt hatte, Überweisungen von Miete oder größere Barabhebungen, die monatliche Mietzahlungen in dieser Höhe zuließen, nicht erkennbar gewesen seien. Da Vermieter des Leistungsempfängers dessen eigener Vater sei, wurde dieser vor der Anfrage beim Finanzamt nicht selbst um Auskunft gebeten. Durfte sich das Sozialamt in der Sache direkt an das Finanzamt wenden?

Grundsätzlich hat der Leistungsträger Daten beim Betroffenen oder mit dessen Mitwirkung zu erheben. Eine Datenerhebung bei anderen Stellen ist nur ausnahmsweise zulässig, beispielsweise dann, wenn eine spezielle Rechtsvorschrift dies gestattet. Das Zehnte Buch des Sozialgesetzbuchs enthält in der Tat eine Regelung, wonach die Finanzbehörden ermächtigt sind, Auskunft über ihnen bekannte Einkommens- und Vermögensverhältnisse bestimmter Personen zu geben. Voraussetzung hierfür aber ist, dass die Erhebung bei der Finanzbehörde tatsächlich überhaupt erforderlich ist. Dies war hier gerade nicht der Fall. Denn vorrangig hätte das Sozialamt an den Antragsteller herantreten können, dem es obliegt, alle Tatsachen anzugeben, die für die Leistung erheblich sind, auf Verlangen des Leistungsträgers Beweisurkunden vorzulegen und der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen.

So hätte das Sozialamt die Möglichkeit gehabt, vom Leistungsempfänger eine schriftliche Bestätigung des Vermieters über den Erhalt der Miete zu verlangen. Als Nachweis wäre unter Umständen sogar ein entsprechender Nachweis aus der Steuererklärung in Betracht gekommen. Weiter hatte das Sozialamt selbst bereits Quittungen oder ein Mietbuch als taugliche Beweisurkunden benannt. Wahlweise wäre auch die Zustimmung des Leistungsempfängers zur Kontaktaufnahme des Sozialamts direkt mit dem Vermieter in Betracht gekommen. Damit war es nicht zulässig, dass sich das Sozialamt ohne vorherige Kontaktaufnahme mit den Betroffenen an das Finanzamt gewandt hatte.

4. Teil: Kommunales und anderes

1. Abschnitt: Kommunales

1. Kontrollbesuch beim Gutachterausschuss

Bei Gütern des täglichen Lebens haben wir eine relativ genaue Vorstellung davon, welcher Preis für welches Produkt angemessen ist. Was aber ist ein Grundstück wert, was darf es kosten? Da der einzelne Bürger derartige Käufe nur selten in seinem Leben tätigt, die Preise oft schon innerhalb eines Gemeindegebiets stark differieren und sich unter Umständen auch schnell wieder ändern, fällt eine Einschätzung hier schwerer.

Eine wertvolle Hilfestellung bei der Bestimmung des Werts bieten die Gutachterausschüsse, die bei den Gemeinden eingerichtet sind. Zu deren Aufgaben gehört es, eine Kaufpreissammlung zu führen. Aus dieser geht hervor, welches Grundstück wann zu welchem Preis im Gemeindegebiet verkauft wurde. Aufgrund der Kaufpreissammlung ermittelt der Gutachterausschuss anschließend durchschnittliche Werte für die unterschiedlichen Lagen eines Gemeindegebiets, die sog. Bodenrichtwerte. Diese sollen, insbesondere auf dem privaten Sektor, für Transparenz auf dem Grundstücksmarkt sorgen. Deshalb kann auch jedermann von der Geschäftsstelle des Gutachterausschusses Auskunft über die Bodenrichtwerte verlangen. Auskünfte aus der Kaufpreissammlung erteilt der Gutachterausschuss bei Vorliegen bestimmter Voraussetzungen.

Um den Gutachterausschüssen das Führen der Kaufpreissammlung zu ermöglichen, sieht das Baugesetzbuch vor, dass jeder Vertrag über den Kauf eines Grundstücks von der beurkundenden Stelle in Abschrift an den Gutachterausschuss zu übersenden ist. Diese Verpflichtung verschafft einen ersten Eindruck davon, was ein Gutachterausschuss an personenbezogenen Daten verarbeitet. Eine weitere Aufgabe des Gutachterausschusses ist es – z. B. auf Antrag des Eigentümers –, Gutachten über den Verkehrswert eines Grundstücks zu erstellen.

Die Geschäftsstelle eines solchen Gutachterausschusses war dieses Jahr Ziel eines unserer Kontrollbesuche.

– Der Posteingang

  Vor Ort fiel uns zunächst auf, dass Kaufverträge den Eingangsstempel der zentralen Poststelle der Gemeinde trugen. Dies ist deswegen problematisch, weil der Gutachterausschuss eine unabhängige Institution ist, die außerhalb der Hierarchie der Gemeindeverwaltung steht. Hieraus folgt, dass erkennbar an den Gutachterausschuss gerichtete Schreiben von der zentralen Poststelle der Gemeindeverwaltung ungeöffnet der Geschäftstelle des Gutachterausschusses vorzulegen sind. Die Gemeinde will hierfür künftig Sorge tragen, indem sie die Mitarbeiter ihrer Poststelle entsprechend schriftlich anweist.

– Pflichten der Gutachter

  Der Vorsitzende des Gutachterausschusses und die weiteren ehrenamtlichen Gutachter werden von den Gemeinden auf vier Jahre bestellt. Personenbezogene Daten, von denen sie aufgrund ihrer Tätigkeit Kenntnis erlangen, haben sie auch nach Ende ihrer Tätigkeit geheim zu halten. Auf diese Geheimhaltungspflicht sind die Gutachter ausdrücklich hinzuweisen. Bei unserem Besuch stellte sich heraus, dass ein solcher Hinweis bisher noch nicht erfolgt war.

  Außerdem erfuhren wir, dass der Vorsitzende des Ausschusses seine Gutachten zu Hause fertigt. Hiergegen ist zunächst einmal nichts einzuwenden. Zu beachten ist aber, dass gerade im häuslichen Umfeld personenbezogene Angaben einer erhöhten Gefahr zufälliger Kenntnisnahme durch Familienmitglieder oder Besucher ausgesetzt sind. Das Recht eines Bürgers auf ordnungsgemäße Verarbeitung seiner personenbezogenen Daten muss aber auch gewährleistet sein, wenn die Datenverarbeitung in den eigenen vier Wänden des Gutachters stattfindet.

Aus diesem Grund baten wir, den Vorsitzenden darauf hinzuweisen, dass er geeignete Maßnahmen zu treffen habe, die eine Kenntnisnahme und Nutzung der Daten durch private Mitbewohner oder Besucher ausschließen. Beim Transport personenbezogener Unterlagen zwischen Behörde und häuslichem Arbeitsbereich sind verschlossene Behältnisse zur Aufbewahrung zu verwenden. Schlussendlich ist – soweit zu Hause mit dem PC gearbeitet wird – sicherzustellen, dass nur dem Gutachter ein Zugriff auf die gespeicherten Daten möglich ist.

– Aufbewahrung der Gutachten

Die Gutachten neueren Datums wurden in einem Schrank in den Räumen der Geschäftsstelle aufbewahrt. Ältere Gutachten hingegen gelangten nach den Ausführungen der Geschäftsstellenmitarbeiterin in die Registratur des Rathauses. Dort waren sie jedem Mitarbeiter der Stadtverwaltung zugänglich. Was aber aufgrund der Eigenständigkeit des Gutachterausschusses für den Posteingang gilt, hat selbstverständlich auch für die Aufbewahrung der Unterlagen Gültigkeit. Deshalb haben wir empfohlen, die in der Registratur eingestellten Wertgutachten keinesfalls so aufzubewahren, dass sie jedem Mitarbeiter der Stadtverwaltung zugänglich sind. Zudem ist auszuschließen, dass der für die Erstellung der Wertgutachten zuständige Gutachter zusätzlich eine Abschrift zu Hause aufbewahrt.

– Auskünfte aus der Kaufpreissammlung

Bei unserem Besuch bekamen wir mit, dass die Geschäftsstelle Auskünfte aus der Kaufpreissammlung auch telefonisch erteilt. Dies ist deswegen problematisch, weil die Geschäftsstelle vor Auskunftserteilung zu überprüfen hat, ob der Empfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft macht, überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen und eine sachgerechte Verwendung der Daten gewährleistet scheint. Insoweit sieht bereits die Gutachterausschussverordnung vor, dass Auskünfte nur auf schriftlichen Antrag zu erteilen sind. Die Geschäftsstelle will dies künftig beachten.

– Personenbezug in Statistiken

Die Stadt setzte seit wenigen Monaten ein Programm zur Verwaltung der Kaufpreissammlung ein. Dieses Programm wurde nach den Vorgaben des Geschäftsführers eines Gutachterausschusses von der Datenzentrale Baden-Württemberg programmiert. Obwohl vermutlich nicht dem Datenschutz das Hauptaugenmerk bei der Entwicklung gegolten hat, kann sich das Ergebnis insgesamt durchaus sehen lassen. Nur bei den statistischen Auswertungen ist den Entwicklern ein datenschutzrechtlicher Fehler unterlaufen:

Das Programm erlaubt zwei verschiedene statistische Auswertungsmöglichkeiten. Zum einen gibt es Statistiken für interne Zwecke. Zum anderen ist die Stadt, wie alle Kommunen, gehalten, dem Statistischen Landesamt eine Aufstellung der Übereignungen von Immobilien mitzuteilen. Wir konnten nur die Erzeugung und das Ergebnis einer internen Statistik prüfen, da das Programmmodul für die externe Statistik nicht installiert war. Die Entwickler und deren fachliche Berater machten bei der internen Statistik den Fehler, dass von dem Programm eine Auflistung der übereigneten Immobilien an Hand der Straße und Hausnummer generiert wurde. In eben dieser Statistik wurde auch der Kaufpreis genannt. Es wäre für einen Ortskundigen ein Leichtes gewesen, beispielsweise bei Einfamilienhäusern, deren Eigentümer zum überwiegenden Teil ihre Immobilie bewohnen, eine Zuordnung von der Straße und der Hausnummer auf den Namen der Bewohner herzustellen. Daraus hätte wiederum geschlossen werden können, wer welche Immobilie zu welchem Preis erworben hat.

Wenn man nun weiß, dass diese interne Statistik nicht nur den Mitarbeitern der Geschäftsstelle des Gutachterausschusses und dessen Mitgliedern, sondern auch Mitarbeitern der Gemeindeverwaltung und Ratsmitgliedern des Stadtrats zugänglich ist, erkennt man schnell, dass diese Gestaltung der auf einzelne Personen zurückführbaren Statistik zu weit geht.

Auf Anfrage wurde uns mitgeteilt, dass die Angabe der Hausnummer eigentlich nicht erforderlich ist. Daher haben wir angeregt, auf die Entwickler einzuwirken, sie mögen in einer nächsten Programmversion die Dinge so weit bereinigen, dass im Statistik-Programmteil steuerbar ist, ob die Hausnummer in Statistiken genannt wird oder nicht. Da an die externe Statistik noch höhere datenschutzrechtliche Anforderungen zu stellen sind, haben wir um Übermittlung einer derartigen Statistik gebeten, sobald das entsprechende Modul eingesetzt wird.

2. Was hat der Fahrzeughalter mit der Kurtaxe zu tun?

Ein Bürger eines anderen Bundeslandes wunderte sich, als er im Mai Post von einer kleinen Fremdenverkehrsgemeinde im Schwarzwald erhielt. Diese teilte ihm mit, er habe im Februar seinen Urlaub in der Gemeinde verbracht. Begründet wurde die schriftliche Kontaktaufnahme damit, ein bestimmter örtlicher Beherbergungsbetrieb habe bisher leider noch keine Angaben über die Aufenthaltsdauer des Adressaten sowie über dessen Mitreisende gemacht. Diese Angaben benötige die Gemeinde, um eine „ordnungsgemäße Anmeldung und Abrechnung“ durchführen zu können. Mit dieser verklausulierten Formulierung wollte der Bürgermeister zum Ausdruck bringen, dass der Zimmervermieter seine Meldepflicht nach der Kurtaxesatzung nicht erfüllt und diese Kommunalabgabe nicht an die Gemeinde abgeführt habe.

Der empörte Bürger wandte sich an uns, weil er sich durch die Gemeinde in seinem Persönlichkeitsrecht verletzt fühlte. Die zur Stellungnahme aufgeforderte Gemeinde begründete ihr Vorgehen wie folgt:

Nach den Schätzungen der Schwarzwald Tourismus GmbH würden 10 bis 20 % der kurtaxepflichtigen Übernachtungen von den Zimmervermietern den Gemeinden nicht gemeldet. Davon ausgehend entstehe der Gemeinde ein jährlicher Einnahmeausfall von 30.000 bis 60.000 Euro. Die Gemeinden seien gesetzlich verpflichtet, Abgaben nach Maßgabe der Gesetze gleichmäßig festzusetzen und zu erheben. Deshalb sei die Gemeinde hinsichtlich einiger Beherbergungsbetriebe folgendermaßen vorgegangen: Die Kennzeichen auswärtiger Fahrzeuge, die vor den Betrieben abgestellt waren, wurden notiert. Meldete der Zimmervermieter der Gemeinde keinen Gast aus dem Zuständigkeitsbereich der Zulassungsstelle, veranlasste die Gemeinde über den Polizeivollzugsdienst eine Halterabfrage. Die betroffenen Fahrzeughalter wurden von der Gemeinde – manchmal auch mehrmals – angeschrieben.

Wir haben die Vorgehensweise der Gemeinde datenschutzrechtlich so beurteilt:

Es trifft zwar zu, dass die Gemeinden Abgaben gleichmäßig festzusetzen und zu erheben haben. Richtig ist auch, dass die Beteiligten und andere Personen der Gemeinde ggf. die erforderlichen Auskünfte erteilen müssen. Das Auskunftsverlangen der Gemeinde muss aber nicht nur erforderlich, sondern auch verhältnismäßig, erfüllbar und zumutbar sein. Im vorliegenden Fall stand jedoch, ehe die Gemeinde an den Petenten schrieb, weder fest, dass der Petent Fahrer des von der Gemeinde notierten Fahrzeugs war und sich zum fraglichen Zeitpunkt dort aufgehalten hatte, noch dass er kurtaxepflichtig war, geschweige denn, dass er sich dieser Pflicht entziehen wollte. Es ist nämlich allgemein bekannt, dass Halter und Fahrer eines Kraftfahrzeugs – nicht nur bei Firmen- und Mietwagen – häufig nicht identisch sind. Im vorliegenden Fall kam hinzu, dass der Bürgermeister den Petenten noch Mitte Juni mit seinen Fragen drangsalierte, obwohl dem Zimmervermieter bereits Anfang März ein entsprechender Kurtaxebescheid der Gemeinde zugegangen war.

Wir haben deshalb gegenüber der Gemeinde erhebliche Zweifel daran geäußert, ob das von ihr praktizierte Verfahren verhältnismäßig, geeignet und damit rechtlich zulässig ist. Eine Halterabfrage kann unseres Erachtens in solchen Fällen allenfalls ausnahmsweise und nur dann in Betracht kommen, wenn Maßnahmen gegenüber dem Beherbergungsbetrieb, der der Gemeinde gegenüber meldepflichtig ist und für den Einzug der Kurtaxe haftet, nicht zum Erfolg führen und die Gemeinde, z. B. durch Hinweise von Drit-

ten, konkrete Anhaltspunkte dafür hat, dass ein Kurgast zugleich Halter und Fahrer des Fahrzeugs ist. Wir haben die Gemeinde gebeten, unsere Rechtsauffassung künftig zu beachten.

Die – oben verkürzt wiedergegebenen – Ausführungen der Gemeinde veranlassten uns ferner, diese auf Folgendes hinzuweisen:

Rechtlich ist zu unterscheiden zwischen dem besonderen Meldeschein für Beherbergungsstätten (Hotelmeldeschein) und dem Kurtaxemeldeschein. Der Hotelmeldeschein ist melderechtlich vorgeschrieben, von den beherbergten Personen am Tag der Ankunft handschriftlich auszufüllen und zu unterschreiben. Er verbleibt bei der Beherbergungsstätte und darf ausschließlich vom Polizeivollzugsdienst und von anderen Sicherheitsbehörden eingesehen werden. Eine Auswertung oder sonstige Nutzung durch die Meldebehörde bzw. durch die Gemeinde ist rechtlich unzulässig.

Dagegen findet sich die Rechtsgrundlage für die Kurtaxemeldepflicht in der auf dem Kommunalabgabengesetz beruhenden örtlichen Kurtaxesatzung. Demnach hat der Beherberger den Kurtaxemeldeschein innerhalb von 24 Stunden nach Ankunft bzw. Abreise der Gemeinde zuzuleiten; für die Meldungen sind die von der Gemeinde ausgegebenen Vordrucke zu verwenden.

Wird ein Durchschreibesatz verwendet, dürfen auf dem Hotelmeldeschein und auf dem Kurtaxemeldeschein nur diejenigen Daten erhoben werden, die zur jeweiligen Aufgabenerfüllung benötigt werden.

3. Datenerhebung beim Schwimmbadbesuch

Nicht nur in Reisepässen sollen biometrische Merkmale die Sicherheit erhöhen, sondern selbst Schwimmbadbesuche, von denen wir bisher annahmen, dass sie sicher genug sind, sollen auf diese Weise noch sicherer gemacht werden. So lässt das Einlasskontrollsystem eines kommunalen Schwimmbads Dauerkarteninhaber nur ein, wenn sie beim Erwerb einer Chipkarte einen Fingerabdruck hinterlassen, der dann auf einem zentralen Server gespeichert wird. Auf der Chipkarte ist eine Kennung gespeichert, unter der der jeweilige Fingerabdruck auf dem Server abgerufen werden kann. Bei jedem Eintritt muss ein Dauerkarteninhaber die Chipkarte in ein Lesegerät einstecken und einen Finger auf ein Abtastgerät legen, das erneut einen elektronischen Abdruck seines Fingers erzeugt. Dann wird vom Rechner geprüft, ob die beiden Abdrücke ähnlich sind. Bestätigt sich dies, darf der Badegast eintreten. Mit dieser Verfahrensweise soll die missbräuchliche Verwendung der nicht übertragbaren Jahreskarten verhindert werden. Auf diesen Sachverhalt wurden wir durch die Eingaben mehrerer Betroffener aufmerksam, die sich durch die Vorgehensweise einer Großen Kreisstadt in ihren Persönlichkeitsrechten verletzt fühlten.

Bei biometrischen Daten wie Fingerabdrücken handelt es sich um sensitive personenbezogene Daten. Es wird deshalb auch die Rechtsauffassung vertreten, die Verarbeitung solcher Daten bedürfe in jedem Fall einer speziellen Rechtsgrundlage (z. B. im Strafprozess-, Ausländer- oder Passrecht). Selbst wenn man nicht ganz so strenge Maßstäbe anlegt, muss man verlangen, dass ein Erlaubnistatbestand des allgemeinen Datenschutzrechts erfüllt ist. Jedenfalls halten wir die Verarbeitung von biometrischen Daten nur dann für zulässig, wenn diese zur Aufgabenerfüllung erforderlich ist. Das ist bei der von der Stadt praktizierten Vorgehensweise nicht der Fall.

Die Prüfung der Verhältnismäßigkeit kam den kommunalen Betreibern gar nicht in den Sinn. Diese Frage hätte spätestens bei der nach § 12 LDSG erforderlichen Vorabkontrolle, die bei Ausgabe eines Datenträgers wie einer Chipkarte durchgeführt werden muss, geprüft werden müssen. Die Vorabkontrolle hat der Betreiber aber unterlassen. In seiner Stellungnahme hat er versucht, dies damit zu entschuldigen, dass der Lieferant, der seinen Sitz in einem der Europäischen Union assoziierten Land hat, ihn nicht auf die Erforderlichkeit einer Vorabkontrolle hingewiesen habe.

Aufgrund der Sensitivität der verarbeiteten Daten ist der Verlust an Vertraulichkeit, d. h. die nicht auszuschließende Offenbarung gegenüber Unberechtigten, unter keinen Umständen hinnehmbar. Die technischen Systeme,

die bei der Anwendung eingesetzt werden, müssen daher hohen Anforderungen gerecht werden. Ebenso muss die Konfiguration des Systems professionell durchgeführt werden. Letztendlich geht es darum, den in § 9 LDSG formulierten Anforderungen an den technischen Datenschutz gerecht zu werden. Ob man sich im vorliegenden Fall über die Sicherheit des Systems überhaupt Gedanken gemacht hat, ist fraglich. Entsprechende Datenschutz- und Sicherheitskonzepte, die das Resultat derartiger Überlegungen gewesen wären, wurden uns jedenfalls nicht übermittelt.

In der Stellungnahme der Stadt wurde auch der Eindruck erweckt, dass die verformelte Darstellung von Einzelmerkmalen (sog. Minutien) eines Fingerabdrucks nicht personenbezogen sei. Im Wesentlichen würden nur zwei nicht auf eine Person rückführbare verformelte Abdrücke verglichen. Wie viele Einzelmerkmale bzw. was genau gespeichert wird, war der Stellungnahme nicht zu entnehmen. Hierzu ist zu sagen, dass dann unzweifelhaft von einem Personenbezug auszugehen ist, wenn acht Einzelmerkmale und das Grundmuster oder ersatzweise zwölf Einzelmerkmale ohne Grundmuster gespeichert werden.

Ebenso scheint man Implementierungsalternativen nicht verfolgt zu haben. Denn selbst wenn Daten in dem oben genannten Umfang im System zu speichern sind, hätte dies auch auf der Chipkarte selbst geschehen können und man hätte den gravierenden Nachteil der zentralen Speicherung auf einem Server umgangen. Außerdem wäre bei der dezentralen Speicherung der Benutzer immer Herr seiner Daten geblieben – ein Qualitätsmerkmal, das datenschutzrechtlich nicht hoch genug eingeschätzt werden kann. Kartensysteme mit entsprechender Speicherkapazität von ca. 1 000 Zeichen sollten für einen verformelten Fingerabdruck ausreichen. Sie sind vermutlich auch nicht wesentlich teurer als die gewählte Lösung.

Da damit zu rechnen ist, dass Systeme, zu deren Funktionieren die Speicherung biometrischer Merkmale erforderlich ist, zunehmend eingesetzt werden, weisen wir darauf hin, dass es insbesondere bei zentraler Speicherung von biometrischen Merkmalen erforderlich ist, die Verhältnismäßigkeit der Maßnahme sorgfältig zu prüfen. Denn fraglich ist, ob mit dem hierdurch erhofften Sicherheitsgewinn überhaupt derartig weitgehende Eingriffe in das Recht auf informationelle Selbstbestimmung zu rechtfertigen sind. Würden wir bei der Sicherung unserer Häuser und Wohnungen den gleichen Aufwand betreiben, müssten wir Türen und Fenster durch Stahlplatten und Panzerglas ersetzen.

2. Abschnitt: Personalwesen

1. Streichkonzert mit ungefragter Stellensuche

Bevor sie ihre Jugendmusikschule schloss, fragte eine Gemeinde alle anderen Gemeinden, öffentlichen Jugendmusikschulen, Landkreise und Ministerien in Baden-Württemberg, ob diese eine ihrer zu kündigenden Lehrkräfte beschäftigen könnten. Dazu übersandte die Gemeinde sämtlichen Adressaten u. a. eine Tabelle mit Angaben zu Lehrkräften und zum Leiter der Jugendmusikschule. Die Tabelle enthielt zwar nicht die Namen der 32 Beschäftigten, doch Angaben insbesondere zu Fächern, Geschlecht, Geburtsjahr, Kindern bzw. Ortszuschlag, Familienstand (verheiratet oder nicht verheiratet), Studienabschlüssen, Studienorten, Beschäftigungsumfang und Beginn der Beschäftigungszeit.

Diese Daten waren auch ohne Namen zumindest hinsichtlich derjenigen Beschäftigten personenbezogen, deren Fächer in der Tabelle lediglich einmal (jeweils bei einer Lehrerin oder bei einem Lehrer) genannt waren, etwa Kontrabass, Harfe, Musikgarten und Gesang. Entsprechendes gilt für nur einmal aufgeführte Fächerkombinationen. Personenbezogen waren auch die Angaben zum Leiter der Jugendmusikschule. Wenn jemand wusste oder herausfand, wer beispielsweise die Jugendmusikschule leitete oder wer dort Kontrabass unterrichtete, so konnte er in der Tabelle u. a. ohne weiteres nachlesen, ob diese Person verheiratet war und ob sie Kinder hatte.

Die Gemeinde durfte wegen dieses – von ihr bestrittenen – Personenbezugs die Daten ihrer Beschäftigten nur übermitteln, wenn eine Rechtsvorschrift dies erlaubte oder soweit die Beschäftigten eingewilligt hatten.

Etwa die Hälfte der Beschäftigten, deren Daten in der Tabelle aufgeführt waren, war nach dem Bundes-Angestelltentarifvertrag ordentlich unkündbar. Hinsichtlich dieser Beschäftigten musste die Gemeinde, worauf sie zu Recht hinwies, vor Ausspruch betriebsbedingter Kündigungen – vereinfacht gesagt – auch prüfen, ob eine Beschäftigung bei anderen Arbeitgebern möglich war. Soweit die Gemeinde personenbezogene Daten übermittelte, weil das aufgrund dieser arbeitsrechtlichen Vorgabe notwendig war, war das datenschutzrechtlich zulässig. Davon, dass die Gemeinde alle Angaben in der Tabelle (etwa die Angabe, ob eine Lehrkraft verheiratet ist) allen Adressaten mitteilen musste, um diese Vorgabe zu erfüllen, kann jedoch keine Rede sein. Hierbei begegnete nicht das Übermitteln personenbezogener Daten als solches datenschutzrechtlichen Bedenken, sondern der Umfang und der Adressatenkreis der übermittelten personenbezogenen Daten.

Bei den ordentlich kündbaren Beschäftigten galt diese arbeitsrechtliche Vorgabe nicht. Auch die Fürsorgepflicht der Gemeinde sowie das von ihr angenommene Interesse der Beschäftigten an der Stellensuche waren datenschutzrechtlich unerheblich: Es fehlte an einer Rechtsvorschrift, welche diese Stellensuche erlaubte. Deswegen hatten die ordentlich kündbaren Beschäftigten insoweit das Recht, selbst zu bestimmen, ob und ggf. welche Informationen über sie die Gemeinde weitergab – eben das Recht auf informationelle Selbstbestimmung. Da es eine Arbeitsplatzsuche um jeden Preis – so wichtig dies auch für die Allgemeinheit sein mag – ohne Zustimmung des Betroffenen nicht geben kann, war die ungefragte Fürsorge unzulässig.

Wir haben die Gemeinde gebeten, diese Rechtslage bei etwaigen künftigen vergleichbaren Fällen zu beachten.

2. Veröffentlichung von Personaldaten

Wegen aktueller Anfragen behandeln wir ergänzend zu den Ausführungen in unserem 23. Tätigkeitsbericht (LT-Drucksache 13/1500) hier insbesondere das Veröffentlichen personenbezogener Daten von Beschäftigten mit regelmäßigen Außenkontakten. Dies ist ohne Einwilligung nur zulässig, soweit es zur Abwicklung des Dienstbetriebs oder Geschäftsverkehrs erforderlich ist, wobei die Interessen des Dienstherrn oder Arbeitgebers mit denjenigen des Beschäftigten abzuwägen sind – wie stets vor dem Veröffentlichen von Personaldaten.

Zunächst stellt sich die Frage, welche Angaben in welcher Form überhaupt veröffentlicht werden müssen, damit Externe unmittelbar den Zuständigen erreichen können. Bei der zunehmend verbreiteten Veröffentlichung im Internet ist eben auch daran zu denken, dass die Daten weltweit abrufbar sowie vielfältig auswertbar und miteinander verknüpfbar sind. Deshalb sollte stets sorgfältig geprüft werden, ob nicht auf die Angabe des Namens des Beschäftigten verzichtet werden kann, weil die Angabe der dienstlichen Funktion und der dienstlichen Erreichbarkeit genügt. Eine funktionsbezogene E-Mail-Adresse kommt z. B. ohne den Namen des Beschäftigten aus.

Veröffentlicht eine Behörde lediglich funktionsbezogene Angaben, verringert sie damit zugleich die Gefahr, bei Abwesenheit eines Beschäftigten über das Ziel hinauszuschießen, etwa indem sie, wie in dem von uns beanstandeten Fall, auf ihrer Internet-Seite nicht nur die Funktion und den Namen eines Beschäftigten mitteilt, sondern – offenbar als besonderes Entgegenkommen gedacht – auch die Dauer und den Grund seiner Abwesenheit. Zudem führen persönliche E-Mail-Adressen häufig dazu, dass E-Mails im persönlichen elektronischen Postfach eines abwesenden Bearbeiters unbearbeitet bleiben (zum Umgang mit solchen E-Mails vgl. unseren 22. Tätigkeitsbericht, LT-Drucksache 13/520).

Bevor der Dienstherr oder Arbeitgeber Namen von Beschäftigten im Internet nennt, muss er zudem prüfen, ob dann Daten über den Beschäftigten dadurch aufzuspüren wären, dass dessen Name als Suchbegriff in eine Suchmaschine eingegeben wird (zu technischen Fragen dazu vgl. in diesem Tätigkeitsbericht 5. Teil, Nr. 8.1). Ein solcher Zugriff auf personenbezogene

Daten mag zwar für Dritte interessant sein, etwa um zu erfahren, wo der Nachbar arbeitet, ist jedoch nicht von dem Zweck gedeckt, Externen den unmittelbaren Kontakt mit dem für ihr Anliegen Zuständigen zu erleichtern. Daher darf in diesem Fall bei einer solchen Suchmöglichkeit der Name des Beschäftigten nur nach dessen wirksamer Einwilligung ins Internet.

3. Abschnitt: Schul- und Hochschulwesen

1. Evaluation an Schulen

Mit „§ 114 Evaluation“ überschrieben war der Entwurf eines neuen Paragrafen im Schulgesetz, den das Kultusministerium uns einschließlich Gesetzesbegründung mit der Bitte um Stellungnahme übersandt hatte. Da der Entwurf grundlegende Fragen zur Verarbeitung personenbezogener Daten offen ließ, konnten wir uns lediglich in allgemeiner Form damit befassen. Der Entwurf ließ beispielsweise nicht erkennen,

- welche Eingriffe in das Recht auf informationelle Selbstbestimmung etwa der Lehrer aufgrund der vorgesehenen Regelung im Einzelnen zulässig sein sollten, z. B.
  - ob die Aussage in der Begründung, die Schulen würden über die Methoden und die Untersuchungstiefe der Selbstevaluation entscheiden, so zu verstehen war, dass die Schulen durch solche Entscheidungen in das Recht auf informationelle Selbstbestimmung eingreifen können (z. B. indem die Schule bestimmt, welche Angaben zu Lehrern und deren Unterricht erfragt werden) und
  - ob das Landesinstitut für Schulentwicklung, das nach der Begründung bei der Fremdevaluation die Qualitätsdokumentation der Schule auswertet und zusätzlich weitere Erhebungen an der Schule durchführt, dabei jeweils personenbezogene Daten verarbeiten darf,
- was die im Entwurf verwandten Begriffe „Selbstevaluation“ und „Fremdevaluation“ bedeuten sollten und
- was unter „Zwecken der Schulverwaltung“ zu verstehen sein sollte; dies war deswegen bedeutsam, weil das Kultusministerium Schüler und Lehrer verpflichten können sollte, an Lernstandserhebungen von internationalen, nationalen oder landesweiten Vergleichsuntersuchungen teilzunehmen, die schulbezogene Tatbestände beinhalten und Zwecken der Schulverwaltung oder der Bildungsplanung dienen (zu Lernstandserhebungen vgl. auch den folgenden Beitrag im 4. Teil, 3. Abschnitt, Nr. 2).

Zwischenzeitlich hat das Kultusministerium einen in einigen Punkten geänderten Gesetzentwurf übersandt. Den Vorschlag zu einem abklärenden Gespräch haben wir aufgegriffen.

Aus aktuellem Anlass hatten wir das Kultusministerium auch darauf hingewiesen, dass es geboten sein kann, über den Erlass von Vorschriften hinaus Maßnahmen zu treffen, um rechtswidrige Eingriffe in das Recht auf informationelle Selbstbestimmung zu vermeiden. Hintergrund dafür war u. a. Folgendes: Ein nicht unbeachtlicher Teil der Meldungen über den Einsatz und die wesentliche Änderung automatisierter Verfahren, die Schulen uns zusandten, hatte weiterhin nicht den gesetzlich vorgeschriebenen Inhalt, obwohl die Anforderungen an solche Meldungen Gegenstand unseres vorangegangenen Tätigkeitsberichts gewesen waren (LT-Drucksache 13/3800). Das Kultusministerium hat hierauf reagiert und nicht nur die Schulen wiederholt schriftlich auf die Anforderungen hingewiesen, sondern dazu auch eine entsprechende neue Verwaltungsvorschrift erlassen. Das Kultusministerium ist dankenswerterweise auch darüber hinaus darum bemüht, den Schulen praktische Hilfestellung zu leisten, und bereitet gegenwärtig Musterhinweise für die Erarbeitung datenschutzrechtlicher Verfahrensverzeichnisse an Schulen vor.

2. PISA und IGLU

Mein Amt befasste sich in diesem Jahr zum wiederholten Mal mit datenschutzrechtlichen Aspekten der Befragungsreihe, die unter dem Kürzel PISA (Programme for International Student Assessment) Gegenstand breiter öffentlicher Erörterung war. Denn, so die Mitteilung des für die „Projektkoordination PISA 2006“ zuständigen Universitätsinstituts, im Mai 2006 steht die dritte Datenerhebung der geplanten PISA-Zyklen an. Zeitgleich soll mit IGLU (Internationale Grundschul-Lese-Untersuchung) auch eine weitere Untersuchung, welche die Bildungspolitik mit Informationen zur Qualität des Schulsystems versorgen soll, mit einem zweiten Zyklus fortgesetzt werden (vgl. die Beiträge im 20. Tätigkeitsbericht 1999, LT-Drucksache 12/4600 und im 21. Tätigkeitsbericht 2000, LT-Drucksache 12/5740). Diesmal ging es um Folgendes:

Das Kultusministerium teilte uns mit, dass im Zusammenhang mit der von der Kultusministerkonferenz beschlossenen „IGLU-Grundschuluntersuchung 2006“ Baden-Württemberg als eines der fünf Bundesländer ausgewählt worden sei, die am Feldtest zur Überprüfung der Untersuchungsinstrumente beteiligt seien. Hinsichtlich dieser sog. IGLU-Voruntersuchung übersandte uns das Kultusministerium verschiedene Unterlagen (u. a. eine sog. Prozedurenbeschreibung, den Entwurf eines Elternanschreibens sowie Entwürfe von Fragebögen für Schulleiterinnen und Schulleiter, Deutschlehrkräfte, Schülerinnen und Schüler sowie für deren Eltern) und bat uns um kurzfristige datenschutzrechtliche Prüfung unter Einbeziehung anderer Landesbeauftragter für den Datenschutz.

Leider gaben die vom Kultusministerium übersandten Unterlagen Anlass, auf verschiedene datenschutzrechtliche Unzulänglichkeiten und Unklarheiten hinzuweisen. So enthielt, um nur ein Beispiel zu nennen, der Entwurf eines Elternanschreibens die vieldeutigen Aussagen, dass sich Deutschland „auf Beschluss der Kultusminister der Länder dem IGLU-Projekt angeschlossen“ habe und in Deutschland „eine größere Anzahl von Wissenschaftlern aus verschiedenen Fachdisziplinen von mehreren Universitäten und Forschungseinrichtungen befasst“ sei, „die wissenschaftliche Koordination“ am Institut für International und Interkulturell Vergleichende Erziehungswissenschaft einer (namentlich genannten, nicht in Baden-Württemberg gelegenen) deutschen Universität stattfinde und „mit der praktischen Organisation der Untersuchung“ eine auf die technische Durchführung derartiger Studien spezialisierte Einrichtung in Hamburg (das IEA Data Processing Center, kurz DPC) beauftragt sei. Damit blieb unklar, welche Stelle oder welche Personen für die vorgesehene Verarbeitung personenbezogener Daten verantwortlich sein sollen. Die Klärung dieser Frage ist aber grundlegende Voraussetzung für eine sachgerechte datenschutzrechtliche Beurteilung. Denn solange keine Klarheit besteht, wer in welchem Bundesland als verantwortlich zu betrachten ist, bleibt zwangsläufig bereits die Frage offen, wer aus dem Kreis der Datenschutzbeauftragten des Bundes und der Länder für die datenschutzrechtliche Beurteilung überhaupt zuständig ist; aber auch für eine inhaltliche Bewertung des Projekts ist es wichtig zu wissen, bei wem die datenschutzrechtliche Verantwortung liegt.

Darüber hinaus ist es natürlich erforderlich, die Personen, deren personenbezogene Daten verarbeitet werden sollen, klar und unmissverständlich darüber zu informieren, wer für diese Datenverarbeitung verantwortlich ist. Erst durch eine solche Information werden die Betroffenen in Baden-Württemberg, deren Teilnahme an der IGLU-Voruntersuchung durchweg freiwillig war, beispielsweise in die Lage versetzt, darüber zu befinden, ob sie dem für die Datenverarbeitung Verantwortlichen vertrauen und deshalb an der Studie teilnehmen wollen. Daneben ist die Frage nach der datenschutzrechtlichen Verantwortung auch dafür entscheidend, mit wem sich die Betroffenen – eventuell auch rechtlich – auseinander zu setzen haben, wenn sich hinsichtlich der Verarbeitung personenbezogener Daten Unstimmigkeiten oder Probleme ergeben sollten. Ich habe das Kultusministerium u. a. auf das Erfordernis hingewiesen, die Personen, deren personenbezogene Daten verarbeitet werden sollen, hinsichtlich der Verantwortung für die Verarbeitung personenbezogener Daten deutlich zu informieren. Auf diesen Hinweis

gegenüber dem Kultusministerium leitete uns das IEA DPC einen überarbeiteten Entwurf eines Elternanschreibens zu, in welchem die Verantwortung für die Verarbeitung personenbezogener Daten mit hinlänglicher Deutlichkeit zum Ausdruck kam. In der Kürze der zur Verfügung stehenden Zeit war es uns allerdings nicht möglich, unsere datenschutzrechtliche Beurteilung mit anderen Landesbeauftragten für den Datenschutz abzustimmen. Wir haben daher dem Kultusministerium auch mitgeteilt, dass es zu begrüßen gewesen wäre, wenn wir früher die Gelegenheit erhalten hätten, die relevanten Unterlagen einzusehen und datenschutzrechtliche Fragen mit anderen Landesbeauftragten für den Datenschutz abzustimmen.

Dieser Gedanke wurde offenbar von dem für die Durchführung der IGLU-Studie zuständigen Institut der Universität Dortmund und dem für die PISA-Studie zuständigen Institut der Universität Kiel aufgegriffen. Auf Einladung dieser Institute wird nunmehr eine Informationsveranstaltung unter Beteiligung von Vertretern der Kultusverwaltungen und der Datenschutzbeauftragten der Länder stattfinden. Ich begrüße diesen Ansatz ausdrücklich. Diese Veranstaltung könnte, im angemessenen zeitlichen Vorfeld der im Mai 2006 vorgesehenen weiteren Zyklen von PISA und IGLU, dazu dienen, grundlegende datenschutzrechtliche Fragen dauerhaft zu klären und somit jeweils neue Diskussionen vor weiteren Studien oder Voruntersuchungen in der Zukunft zu vermeiden oder wenigstens abzukürzen.

3. Zum weiteren rechtlichen Schicksal der Schülerindividualdatei

Im Tätigkeitsbericht für das Jahr 2004 (LT-Drucksache 13/3800) wurden einige datenschutzrechtliche Aspekte des vom Kultusministerium entwickelten EDV-Verfahrens E-Stat und der damit vorgesehenen Einführung einer landesweiten Schülerindividualdatei angesprochen. Dabei war insbesondere problematisch, dass nach dem ursprünglichen Gesetzentwurf des Kultusministeriums eine weit über den bisherigen Umfang hinausgehende Vielzahl personenbezogener Daten aller Schülerinnen und Schüler von öffentlichen Schulen an das Kultusministerium übermittelt werden sollte. Es war aber nicht erkennbar, dass das Kultusministerium alle diese Daten zur Erfüllung eigener dienstlicher Aufgaben benötigt. Insofern begegnete das Projekt des Kultusministeriums zunächst gravierenden datenschutzrechtlichen Bedenken. Um diese auszuräumen, hatte ich im letzten Tätigkeitsbericht (und bereits zuvor in einem Schreiben an das Kultusministerium) einen aus datenschutzrechtlicher Sicht gangbaren Lösungsweg unter Nutzung des vom Landesdatenschutzgesetz vorgesehenen Instrumentariums der Datenverarbeitung im Auftrag aufgezeigt: Die jeweiligen öffentlichen Schulen beauftragen eine andere Stelle, beispielsweise das Kultusministerium, mit der zentralen Speicherung und sonstigen Verarbeitung personenbezogener Daten, bleiben damit aber die für die Datenverarbeitung jeweils verantwortlichen Stellen.

Überraschenderweise gestaltete sich die weitere Abstimmung mit dem Kultusministerium etwas langwierig. Der Stellungnahme der Landesregierung zum letzten Tätigkeitsbericht war u. a. noch zu entnehmen, dass meine Anregung, die zentrale Schülerindividualdatei rechtstechnisch als Datenverarbeitung im Auftrag der Schulen zu konstruieren, geprüft werde. Allerdings leitete mir das Kultusministerium dann einen im Wesentlichen unveränderten Gesetzentwurf zu, mit dem meine bis dahin geäußerten datenschutzrechtlichen Bedenken in keiner Weise aufgegriffen, geschweige denn ausgeräumt waren.

Erfreulicherweise gelang es letztlich doch noch, „den Knoten zu lösen“ und das Kultusministerium mit Unterstützung des Innenministeriums von der Notwendigkeit der datenschutzgerechten Überarbeitung des Gesetzentwurfs zu überzeugen. Der abgestimmte Gesetzestext sieht u. a. vor, dass

- die Schulen für die zentrale Speicherung und sonstige Verarbeitung personenbezogener Daten verantwortlich bleiben,
- die Schulen unter Nutzung des Instruments der Datenverarbeitung im Auftrag insofern jeweils als Auftraggeber der Datenverarbeitung fungieren,
- das Kultusministerium mit Wirkung für die Schulen eine oder mehrere Stellen entsprechend beauftragen kann und

– die Schulen verpflichtet sind, die Daten an die beauftragte Stelle weiterzugeben.

Diese Regelungen sind mit der Novellierung des Schulgesetzes am 22. Oktober 2005 in Kraft getreten.

4. Veröffentlichung von Schülerfotos auf der Internet-Seite einer Schule

Aufgrund einer Eingabe befasste sich mein Amt zum wiederholten Mal mit datenschutzrechtlichen Aspekten der Veröffentlichung von Schülerfotos auf der Internet-Seite von öffentlichen Schulen. Die Eltern eines minderjährigen Schülers teilten uns u. a. mit, dass ohne ihr Einverständnis auf der Internet-Seite einer Schule, die ihr Sohn besucht hatte, ein Klassenfoto veröffentlicht sei, auf welchem u. a. ihr Sohn erkennbar sei. Um den Dingen auf den Grund zu gehen, führten Mitarbeiter meiner Dienststelle einen Informations- und Kontrollbesuch bei der betroffenen Schule durch. Dabei teilte uns die Schule Folgendes mit:

Der Betroffene sei zu der Zeit, als das Klassenfoto gefertigt und von der Schule ins Internet gestellt wurde, 15 Jahre alt gewesen. Die Schule sei bislang so verfahren, dass sie sich wegen einer datenschutzrechtlichen Einwilligung bei minderjährigen Schülerinnen und Schüler immer an deren Erziehungsberechtigte gewandt habe. Eine schriftliche Einwilligung in die Veröffentlichung des angesprochenen Klassenfotos gebe es allerdings nicht.

Dies war so nicht in Ordnung. Öffentliche Schulen dürfen Fotos von (ehemaligen) Schülerinnen und Schülern nur dann im Internet veröffentlichen, wenn sie zuvor die grundsätzlich schriftliche Einwilligung der Betroffenen eingeholt haben. Die Schule hat das beanstandete Klassenfoto dann innerhalb weniger Tage nach diesem Kontrollbesuch aus ihrem Internet-Angebot gelöscht.

Die Beschwerde und unsere eigenen Recherchen im Internet-Angebot der Schule, das eine Vielzahl weiterer Klassenfotos und anderer Gruppen- und Portraitfotos enthielt (Letztere mit jeweils zugeordneten Vor- und Nachnamen der abgebildeten Personen), gaben Anlass, der Frage nachzugehen, ob bei den anderen auf den Fotos erkennbaren Personen die jeweils erforderlichen datenschutzrechtlichen Einwilligungen erteilt wurden. Die Schule musste einräumen, dass dies vielfach nicht der Fall war. Nach einem weiteren Besuch meiner Mitarbeiter bei der Schule erhielten wir von dort u. a. die Mitteilung, dass Personen-Fotos aus dem Internet-Angebot entfernt worden seien und seitens der Lehrerinnen und Lehrer sowie bestimmter weiterer Personen mittlerweile datenschutzrechtliche Einwilligungserklärungen vorliegen würden.

Ich habe die festgestellten datenschutzrechtlichen Verstöße gegenüber dem Kultusministerium als der zuständigen obersten Landesbehörde beanstandet und um Stellungnahme gebeten. Bislang gibt es hierzu keine Reaktion.

Angesichts der in diesem Fall und auch in anderem Zusammenhang deutlich gewordenen Unsicherheiten und Probleme hinsichtlich der Veröffentlichung von Klassenfotos und anderen personenbezogenen Daten durch öffentliche Schulen im Internet sollen die datenschutzrechtlichen Anforderungen im Folgenden nochmals in allgemeiner Form dargestellt werden:

Wenn öffentliche Schulen in Baden-Württemberg Namen von Personen oder Fotos von Schülerinnen und Schülern, deren Erziehungsberechtigten oder von Lehrerinnen und Lehrern im Internet veröffentlichen, verarbeiten sie damit personenbezogene Daten. Die Verarbeitung personenbezogener Daten durch öffentliche Stellen im Sinne des Landesdatenschutzgesetzes, zu denen öffentliche Schulen zählen, ist nach § 4 Abs. 1 LDSG nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Nachdem sich aus dem Landesdatenschutzgesetz oder einer anderen Rechtsvorschrift keine entsprechende Erlaubnis ergibt, kann sich die Zulässigkeit einer solchen Datenverarbeitung nur aus einer Einwilligung der Betroffenen ergeben. Zur Vermeidung von Wiederholungen verweise ich auf den Beitrag „Schulen im World Wide Web“ im 22. Tätigkeitsbericht für das Jahr 2001 (LT-Drucksache 13/520). Statt der darin enthaltenen Aussage, dass bei Schülern

unter 14 Jahren in jedem Fall die Eltern die Einwilligung erteilen müssen, gilt nun Folgendes: Mit Vollendung des 16. Lebensjahrs ist – im Sinne einer Regelannahme – grundsätzlich vom Vorliegen der Einsichtsfähigkeit auszugehen, die es den jeweiligen Schülerinnen und Schülern erlaubt, über die Frage einer datenschutzrechtlichen Einwilligung selbst zu entscheiden. Einzelheiten sind dem Beitrag „Handlungsfähigkeit minderjähriger Schülerinnen und Schüler“ in meinem 24. Tätigkeitsbericht für das Jahr 2003 (LT-Drucksache 13/2650) zu entnehmen. Zum Einstellen von Lehrerdaten ins Internet habe ich mich im 23. Tätigkeitsbericht für das Jahr 2002 (LT-Drucksache 13/1500) im Beitrag „Die Veröffentlichung von Personaldaten – im Internet und in anderer Form“ geäußert. Das Erfordernis, vor der Veröffentlichung personenbezogener Daten im Internet die datenschutzrechtliche Einwilligung der Betroffenen einzuholen, gilt grundsätzlich auch für andere Personen, beispielsweise Busfahrer oder Reiseführer, die auf Fotos von Studien- und Klassenfahrten zu erkennen sind.

Somit muss eine öffentliche Schule, wenn sie die Veröffentlichung von Klassenfotos oder anderen personenbezogenen Daten im Internet anstrebt, vor der Veröffentlichung alle Betroffenen über Inhalt und Zweck der Maßnahme aufklären und um eine datenschutzrechtliche Einwilligung bitten. Eine Verpflichtung zur Erklärung einer solchen Einwilligung besteht nicht. Die Betroffenen können vielmehr eine solche Einwilligung verweigern. Sie können auch eine erteilte Einwilligung widerrufen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Die Einwilligung kann auch elektronisch erklärt werden, wenn die empfangende Stelle sicherstellt, dass

1. die Einwilligung nur durch eine eindeutige und bewusste Handlung des Einwilligenden erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. ihr Urheber eindeutig erkannt werden kann und
4. die Einwilligung (Tag, Uhrzeit, Inhalt) protokolliert wird.

Nicht nur aufgrund der aufgeführten Beiträge meiner Dienststelle in früheren Tätigkeitsberichten, sondern insbesondere auch aufgrund der klaren und detaillierten Regelungen des Kultusministeriums müsste den öffentlichen Schulen in Baden-Württemberg und den dort für das jeweilige Internet-Angebot verantwortlichen Personen die Rechtslage eigentlich seit Jahren klar sein. Bereits die, inzwischen außer Kraft getretene, Verwaltungsvorschrift des Kultusministeriums zur Verarbeitung personenbezogener Daten von Schülerinnen und Schülern sowie von deren Erziehungsberechtigten durch öffentliche Schulen vom 18. September 2003 enthielt u. a. die folgende unmissverständliche Regelung: „Die Veröffentlichung von personenbezogenen Daten von Schülerinnen und Schülern sowie von deren Erziehungsberechtigten (z. B. Namen, Adressen oder Einzel- bzw. Gruppenfotografien von Schülerinnen und Schülern) in Medien wie z. B. Zeitungen oder Zeitschriften oder im Internet ist nur mit der schriftlichen oder elektronischen Einwilligung der jeweils betroffenen Person bzw. Personen zulässig.“ Das Kultusministerium hat die zitierte Regelung wortgleich in die mit Wirkung vom 1. September 2005 in Kraft getretene Verwaltungsvorschrift zur Verarbeitung personenbezogener Daten durch öffentliche Schulen und Einsichtnahme in schulische Prüfungsunterlagen übernommen. Bleibt nur zu hoffen, dass diese Anweisungen des Kultusministeriums künftig nun auch beachtet werden.

5. Einführung allgemeiner Studiengebühren

Die Erhebung von Studiengebühren ist bekanntlich ein besonders umstrittenes Thema auf der politischen Bühne. Es hat aber durchaus auch mit dem Datenschutz zu tun, wie bei der Lektüre des vom Wissenschaftsministerium übersandten Entwurfs eines Gesetzes zur Änderung des Landeshochschulgebührengesetzes und anderer Gesetze rasch deutlich wurde. Das Gesetz soll der Einführung allgemeiner Studiengebühren in Höhe von 500 Euro je Semester für das Studium an den Hochschulen und Berufsakademien des Landes, erstmals im Sommersemester 2007, dienen. Dabei waren für mein

Amt naturgemäß die Regelungen über die Verarbeitung personenbezogener Daten von besonderem Interesse.

Nach dem Entwurf dürfen Hochschulen und Berufsakademien von Studienbewerbern und Studierenden eine Erklärung über die von ihnen abgeleisteten Studienzeiten und die Vorlage geeigneter Unterlagen verlangen, wenn diese ein Darlehen der L-Bank (Landeskreditbank Baden-Württemberg – Förderbank) zur Finanzierung der Studiengebühren beantragen wollen. Die Hochschulen und Berufsakademien haben nämlich zu prüfen, ob der Darlehensanspruch zu Recht besteht. Außerdem kann von Studierenden im Einzelfall die Vorlage weiterer Unterlagen und nötigenfalls eine Versicherung an Eides statt verlangt werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Angaben der Studierenden über Studienzeiten unrichtig oder unvollständig sind. Bei näherer Betrachtung zeigten sich aber gewisse Ungereimtheiten: Während nach dem Wortlaut des Entwurfs die Hochschulen und Berufsakademien der L-Bank nur die zur Gewährung und Rückzahlung eines Darlehens „erhobenen“, erforderlichen Daten übermitteln dürfen, soll sich nach der Gesetzesbegründung die Datenübermittlung auch auf die „vorliegenden“ personenbezogenen Daten erstrecken (d. h. auch auf solche Daten, die von den Hochschulen und Berufsakademien selbst „erzeugt“ werden, beispielsweise wegen einer Exmatrikulation).

Insgesamt war von uns festzustellen, dass die vorgesehenen Regelungen zum Teil datenschutzrechtlich noch gar nicht abschließend bewertet werden konnten. Insbesondere war dem Gesetzentwurf nicht zu entnehmen, ob mit bestimmten Regelungen Eingriffe in das Recht auf informationelle Selbstbestimmung vorgesehen sind und aufgrund welcher Erwägungen und unter welchen Voraussetzungen diese ggf. zulässig sein sollen. Teilweise passten Gesetzestext und Begründung offenbar nicht zueinander, sodass für uns nicht ersichtlich war, welche der voneinander abweichenden Formulierungen nun maßgeblich sein soll. Wir haben das Wissenschaftsministerium daher auf eine Vielzahl noch klärungsbedürftiger Fragen hingewiesen und mitgeteilt, dass der Gesetzentwurf unter Berücksichtigung unserer Anmerkungen überarbeitet werden sollte.

6. Nochmals: Zur Filterung von E-Mails

Anlässlich einer Beschwerde über die Blockade bestimmter E-Mails durch eine Universität in Baden-Württemberg ist im 25. Tätigkeitsbericht für das Jahr 2004 (LT-Drucksache 13/3800) bereits in allgemeiner Form auf einige datenschutzrechtliche Aspekte der Filterung von E-Mails eingegangen worden. Die inzwischen abgeschlossene Prüfung zeigte, dass die Filterung von E-Mails nicht nur, wie bereits im letzten Tätigkeitsbericht erwähnt, datenschutzrechtliche Tücken hat, sondern auch strafrechtlich relevant sein kann.

Zunächst zu den datenschutzrechtlichen Aspekten. Aus der Stellungnahme der Universität ergab sich Folgendes:

Eine Fakultät der Universität schränkte die E-Mail-Kommunikation von Oktober 2003 bis November 2004 in drei unmittelbar aufeinander folgenden Phasen in jeweils unterschiedlicher Weise ein:

– In der ersten Phase erfolgte die Filterung von E-Mails dadurch, dass der IP-Adressbereich, zu dem auch der vom Beschwerdeführer zum Mail-Versand benutzte Computer gehörte, vom Mail-Austausch ausgeschlossen wurde. Damit war weder eine Mail-Kommunikation von noch zu den davon betroffenen Computern möglich. Neben dem Beschwerdeführer war von dieser Sperrung eine uns nicht bekannte Zahl weiterer E-Mail-Nutzer betroffen. Der Absender einer auf diese Weise blockierten Nachricht erhielt eine Fehlermeldung darüber, dass die Mail nicht zugestellt werden konnte. Der Empfänger erhielt über den Vorgang keine Nachricht.

– In der zweiten Phase wurden E-Mails, in deren Kopf – also z. B. unter „Absender“, „Empfänger“, „Cc“ und „Betreff“ – die Zeichenkette mit dem Namen des Beschwerdeführers vorkam, vom Mail-Server der Fakultät abgewiesen. Der Absender erhielt dann seine Nachricht mit einer (in der Stellungnahme der Universität nicht näher beschriebenen) Fehlermeldung zurück. Der Empfänger erhielt darüber keine Nachricht. Die Kommunikation von der Universität nach außen wurde nicht eingeschränkt.

– In der dritten Phase erfolgte die Filterung derart, dass E-Mails, in deren Kopf die Zeichenkette mit dem Namen des Beschwerdeführers vorkam, in einem besonderen elektronischen Postfach unter einer bestimmten Mail-Adresse abgelegt wurden, auf das nach Aussage der Universität nur der Administrator Zugriff hatte. Der Absender erhielt darüber keine Nachricht. Der Empfänger wurde unverzüglich nach dem Eingang der Mail benachrichtigt, dass für ihn eine Mail zur Abholung bereit liege. Unter Mitwirkung des Administrators konnten sich die Empfänger diese Mails beispielsweise auf Diskette aushändigen oder sich diese per E-Mail zuschicken lassen. Die Kommunikation per E-Mail von der Universität nach außen war davon nicht betroffen.

Die Universität erbrachte mit Hilfe der Systeme, auf denen die Filterung erfolgte, bis in den November 2004 auch Dienstleistungen für Dritte im Bereich der Telekommunikationsdienste. Im November 2004 wurde innerhalb der Universität mit sofortiger Wirkung angeordnet, dass durch die Fakultät keinerlei E-Mail-Filterung mehr erfolgt.

Nach Mitteilung der Universität war die Anordnung der E-Mail-Filterung zur Sicherung des ordnungsgemäßen Betriebs der Fakultät erforderlich. Zur Begründung führte die Universität im Wesentlichen aus, dass wegen eines „feindschaftlichen Tons“ (in Äußerungen des Beschwerdeführers) und seines unbestrittenen Wissens im Bereich der Sicherheit auch nicht ganz auszuschließen gewesen sei, dass der Beschwerdeführer versuchen würde, „an für einen Angriff nützliche Informationen zu kommen und den Kommunikationsweg per Mail dafür auszunutzen“.

Dazu ist aus datenschutzrechtlicher Sicht Folgendes zu sagen:

In den Phasen zwei und drei der Filterung verarbeitete die Universität die Zeichenfolge mit dem Namen des Beschwerdeführers elektronisch. Dabei wurden im Sinne der Begriffsbestimmungen des Landesdatenschutzgesetzes personenbezogene Daten des Beschwerdeführers sowie eventueller weiterer Personen, deren Daten ggf. im Kopf der gefilterten E-Mails (beispielsweise als Absender oder unter „Cc“ als weitere Empfänger zur Kenntnisnahme) enthalten waren, verarbeitet. Eine solche Verarbeitung personenbezogener Daten durch die Universität war nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubte oder soweit der Betroffene eingewilligt hat. Auf der Grundlage des für uns erkennbaren Sachverhalts ergab sich die Zulässigkeit dieser Verarbeitung personenbezogener Daten nicht. Weder hatten der Beschwerdeführer und andere betroffene Personen eingewilligt noch war das Vorgehen der Universität durch das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift gedeckt. Dabei gehen wir davon aus, dass die Universität selbstverständlich Maßnahmen zur Sicherung des ordnungsgemäßen Dienstbetriebs, beispielsweise der betroffenen Fakultät, ergreifen und eine dabei eventuell erforderliche Verarbeitung personenbezogener Daten vornehmen darf. Es war aber für uns nicht ersichtlich, aufgrund welcher Umstände für die Universität durch die vom Beschwerdeführer versandten E-Mails eine massive Störung der geordneten Abläufe, vergleichbar mit der Gefahr für die Infrastruktur durch Viren oder Schadprogramme, zu erwarten war.

In Phase drei der Filterung war zudem relevant, dass die Empfänger der vom Beschwerdeführer versandten Mails durch die gewählte „Quarantäne-Lösung“ erkennen konnten, dass diese Mails offensichtlich als potenzielle Störung für den Fakultätsbetrieb angesehen wurden, was für den Beschwerdeführer eine deutliche Stigmatisierungswirkung zur Folge hatte. Ferner brachte es die gewählte Lösung mit sich, dass – wenn ein Empfänger eine vom Beschwerdeführer versandte E-Mail in Empfang nehmen wollte – diese von einem Administrator aus einem speziellen E-Mail-Postfach entnommen und dem Empfänger zur Verfügung gestellt werden musste. Diese Vorgehensweise hatte zur Folge, dass neben Absender und Empfänger regelmäßig eine weitere Person Kenntnis davon erhielt, wer wann E-Mails vom Beschwerdeführer erhielt und in Empfang nahm. Zudem konnte der Administrator dabei möglicherweise auch den Betreff und ggf. den Inhalt der Nachrichten zur Kenntnis nehmen.

Soweit die Universität mit Hilfe der Systeme, auf denen die Filterung erfolgte, auch Dienstleistungen für Dritte erbrachte, nahm sie zudem die Rolle eines Telekommunikationsdiensteanbieters ein und musste die Datenschutzvorschriften des Telekommunikationsgesetzes einschließlich des Fernmeldegeheimnisses wahren. Dazu gehört, dass sie nicht ohne ausdrücklichen Wunsch der Kunden personenbezogene Verbindungs- oder Inhaltsdaten verarbeiten durfte, soweit dies nicht Gegenstand der zu erbringenden Dienstleistung war. Auf dieser Grundlage war es nicht zulässig, dass die Universität in dem Bereich, in dem sie als Telekommunikationsdienstanbieter nach dem Telekommunikationsgesetz tätig war, nach eigenem Ermessen ohne Rechtfertigungsgrund eingehende Nachrichten unterdrückte oder einer Quarantänebehandlung unterzog und dabei automatisiert personenbezogene Daten verarbeitete.

Im Ergebnis bedeutet dies, dass die im Rahmen der E-Mail-Filterung vorgenommene Verarbeitung personenbezogener Daten nicht erforderlich und damit datenschutzrechtlich nicht gerechtfertigt war. Da dieser Mangel von der Universität beseitigt wurde, habe ich von einer Beanstandung abgesehen.

Auch wenn sich meine Zuständigkeit nicht auf die strafrechtliche Seite der Angelegenheit erstreckt, verdient auch diese Erwähnung:

Der Beschwerdeführer hatte nämlich wegen der E-Mail-Filterung bei einer Staatsanwaltschaft Strafanzeige erstattet. Nachdem die Staatsanwaltschaft aus rechtlichen Gründen von der Einleitung eines Ermittlungsverfahrens abgesehen und die Generalstaatsanwaltschaft der dagegen eingelegten Beschwerde keine Folge gegeben hatte, ordnete ein Strafsenat eines Oberlandesgerichts auf Antrag des Beschwerdeführers in einem sog. Klageerzwingungsverfahren die Aufnahme von Ermittlungen wegen des Verdachts der Verletzung des Post- und Fernmeldegeheimnisses (§ 206 Abs. 2 Nr. 2 des Strafgesetzbuchs [StGB]) an. Gleichzeitig äußerte sich das Oberlandesgericht zu der bislang umstrittenen Frage, ob es sich bei einer Universität oder einer anderen öffentlichen Stelle um ein Unternehmen im Sinne des § 206 StGB handeln kann, das geschäftsmäßig Telekommunikationsdienste erbringt. Es kam zum Ergebnis, dass der Unternehmensbegriff weit auszulegen sei. Eine Universität sei dann als Unternehmen zu betrachten, wenn sie nicht ausschließlich hoheitlich tätig wird. Das sei der Fall, wenn die Universität ihre Telekommunikationsanlage ihren Mitarbeitern und anderen Nutzergruppen (beispielsweise Vereinen und außenstehenden Dritten) zum Austausch von E-Mails für private und wirtschaftliche Zwecke zur Verfügung stellt.

Diese Rechtsauffassung ist sinngemäß auf alle Behörden und sonstigen öffentlichen Stellen mit hoheitlichen Aufgaben übertragbar und gilt auch hinsichtlich anderer Telekommunikationsdienste, wie Telefon- oder Telefaxdienst. Kurz nachdem diese Gerichtsentscheidung ergangen war, habe ich u. a. sämtliche Ministerien des Landes sowie die kommunalen Landesverbände informiert. Die gerichtliche Klarstellung hat jedenfalls zur Folge, dass öffentliche Stellen beim Betrieb ihrer Telekommunikationsanlagen neben den Regeln des allgemeinen Datenschutzrechts stets auch das Fernmeldegeheimnis und die Datenschutzvorschriften des Telekommunikationsgesetzes im Blick zu behalten haben.

4. Abschnitt: Finanzen und Steuern

1. Kontendatenabrufe nach dem Gesetz zur Förderung der Steuerehrlichkeit

Im Tätigkeitsbericht für das Jahr 2004 (LT-Drucksache 13/3800) ist dargestellt, dass die Regelungen des Gesetzes zur Förderung der Steuerehrlichkeit über automatisierte Abrufe von Kontendaten mit Blick auf das verfassungsrechtliche Transparenzgebot und die Rechtsschutzgarantie des Artikels 19 Abs. 4 GG sowie auf das verfassungsrechtliche Gebot der Normenklarheit gravierenden datenschutzrechtlichen Bedenken begegnen. Wegen dieser Mängel hatten der Bundesbeauftragte für den Datenschutz und alle

Landesbeauftragten für den Datenschutz gefordert, diese Regelungen zu überarbeiten. Leider ist der Bundesgesetzgeber dieser Forderung bislang nicht nachgekommen. Soweit erkennbar, kann lediglich der vom Freistaat Bayern im April 2005 im Bundesrat eingebrachte Gesetzentwurf als ernsthafter Versuch gewertet werden, die datenschutzrechtlichen Bedenken auszuräumen. Leider blieb diese Gesetzesinitiative wegen der vorgezogenen Bundestagswahl ohne greifbares Ergebnis. Es bleibt zu hoffen, dass die Initiative des Freistaats Bayern so schnell wie möglich wieder aufgegriffen wird.

Einige Einzelpersonen und eine Bank haben Verfassungsbeschwerde beim Bundesverfassungsgericht erhoben und den Erlass einer einstweiligen Anordnung beantragt, um das In-Kraft-Treten der gesetzlichen Regelungen zum 1. April 2005 zu verhindern. Diese Anträge wurden vom Bundesverfassungsgericht mit Entscheidung vom 22. März 2005 abgelehnt. Was zunächst wie eine „Niederlage für den Datenschutz“ erscheint, ist nach einem Blick in die Entscheidungsgründe differenzierter zu betrachten:

Das Bundesverfassungsgericht bezeichnete den Ausgang der Verfassungsbeschwerdeverfahren ausdrücklich als offen und entschied über die Anträge auf Gewährung einstweiligen Rechtschutzes im Wege einer Folgenabwägung, die zu Lasten der Antragsteller ausging. Das Gericht gab zu erkennen, dass insbesondere durch einen Erlass des Bundesministeriums der Finanzen vom 10. März 2005 die möglichen Nachteile für die Betroffenen begrenzt wurden. Nach dem Erlass, der den datenschutzrechtlichen Bedenken in gewissem Umfang Rechnung trägt, sind Betroffene über einen automatisierten Abruf ihrer Daten in jedem Fall zu informieren. Zudem ist in diesem Erlass geregelt, dass automatisierte Abrufe auf Ersuchen von anderen Behörden als den Finanzbehörden nur zulässig sind, wenn es um die Gewährung von Sozialhilfe, Angelegenheiten der Sozialversicherung, sozialen Wohnraumförderung, Ausbildungsförderung, Aufstiegsförderung, der Gewährung von Wohngeld und Erziehungsgeld sowie um Leistungen zur Unterhaltssicherung geht.

Die mit diesem Erlass verhängte „behördliche Selbstbeschränkung“ ist zunächst zu begrüßen. Gleichwohl bleibt der Bundesgesetzgeber gefordert, die aus verfassungsrechtlicher und datenschutzrechtlicher Sicht gebotenen Regelungen klar und deutlich im Gesetz selbst zu verankern und die Reparatur bedenklicher gesetzlicher Vorschriften nicht der Verwaltung oder gar den Gerichten zu überlassen. Datenschutzrechtlichen Fragen zum Vollzug der Vorschriften durch die Finanzverwaltung in Baden-Württemberg gehe ich derzeit im Kontakt mit dem Finanzministerium nach.

2. Warum müssen Finanzämter in Baden-Württemberg bundesweit auf sämtliche Lohnsteuerbescheinigungen zugreifen können?

Jeder abhängig Beschäftigte kennt die Abläufe aus dem Effeff: Alljährlich ist gegenüber dem für den eigenen Wohnort zuständigen Finanzamt eine Lohn- oder Einkommensteuererklärung abzugeben. Anders als früher üblich erhalten die Beschäftigen solcher Arbeitgeber, die eine elektronische Lohnbuchhaltung führen, heutzutage nach Ablauf eines Kalenderjahres nicht mehr ihre Lohnsteuerkarte mit den vom Arbeitgeber hinzugefügten Einträgen über die Höhe des gezahlten Gehalts sowie der abgeführten Steuern und einiger anderer Angaben. Stattdessen bekommen sie eine zum Verbleib bei ihnen bestimmte Bescheinigung darüber, welche ehemals auf der Lohnsteuerkarte dokumentierten Angaben nun auf elektronischem Weg an die Steuerverwaltung weitergeleitet wurden. Diese für den einzelnen Steuerpflichtigen möglicherweise nur unbedeutend erscheinende Änderung ist allerdings Zeichen einer grundlegenden Veränderung der Arbeitsabläufe und der Datenflüsse im Steuerwesen, die das Ziel hat, auch die für die Besteuerung relevanten Vorgänge möglichst durchgängig elektronisch abwickeln zu können. Während den Beschäftigten in ihrer Rolle als Steuerpflichtigen bislang noch die Wahl bleibt, ob sie ihre Steuererklärung wie seit jeher in Papierform abgeben wollen oder ob sie von der Möglichkeit der elektronischen Übersendung der Steuererklärung Gebrauch machen wollen (wobei allerdings die Ankündigung der Steuerverwaltung, elektronisch eingereichte Erklärungen vorrangig bearbeiten zu wollen, rechtlich mehr als

fragwürdig ist), sind die Arbeitgeber, die eine elektronische Lohnbuchhaltung führen, inzwischen verpflichtet, die sog. Lohnsteuerbescheinigungen in elektronischer Form zu übersenden. Im Rahmen mehrerer bei der Oberfinanzdirektion Karlsruhe sowie einem Finanzamt durchgeführter Kontrollbesuche informierten wir uns auch darüber, wie die von den Arbeitgebern versandten elektronischen Lohnsteuerbescheinigungen den mit der Veranlagung der Lohn- und Einkommensteuer betrauten Finanzamtsbediensteten zugänglich werden.

Dabei traten gravierende Mängel bei der Nutzung des für die elektronische Entgegennahme und Weiterleitung verwendeten bundesweit eingesetzten EDV-Verfahrens ELSTER-Lohn zutage. Neben Unklarheiten über die datenschutzrechtliche Verantwortlichkeit beim Betrieb der dazu eingerichteten zentralen Komponenten (Clearingstellen, Landesspeicher) und einer fehlenden Authentifizierung der meldenden Arbeitgeber sind dabei insbesondere Mängel des Zugriffsschutzes zu erwähnen. Diese haben zur Folge, dass die mit der Veranlagung der Lohn- und Einkommensteuer betrauten Bediensteten der hiesigen Finanzämter bundesweit auf sämtliche elektronischen Lohnsteuerbescheinigungen zugreifen können.

2.1 Das Verfahren ELSTER-Lohn

Arbeitgeber, die eine maschinelle Lohnbuchhaltung führen, müssen der Steuerverwaltung für jeden ihrer Beschäftigten eine elektronische Lohnsteuerbescheinigung senden. Das EDV-Verfahren, mit dessen Hilfe die Steuerverwaltung diese Daten elektronisch entgegennimmt und den für die Besteuerung zuständigen Finanzämtern zur Verfügung stellt, wird als ELSTER-Lohn bezeichnet.

2.1.1 Datenübertragung von Arbeitgebern an die Clearingstellen

Die Datenübertragung von den Arbeitgebern an die Clearingstellen erfolgt über Internet. Dabei hat die Steuerverwaltung durch die Gestaltung der von ihr entwickelten Komponenten vorgegeben, dass die übertragenen Daten verschlüsselt sein müssen. Eine Authentifizierung der meldenden Arbeitgeber ist hingegen nicht vorgesehen. Die Systeme der Steuerverwaltung bieten bislang keine Funktionen, um eine solche Authentifizierung vornehmen zu können.

2.1.2 Verarbeitung innerhalb der Clearingstellen

Zur Entgegennahme dieser Meldungen gibt es bundesweit zwei Clearingstellen. Eine dieser Clearingstellen wird bei der bayerischen Finanzverwaltung in München betrieben, die andere bei der nordrhein-westfälischen Finanzverwaltung in Düsseldorf. Es gibt keine sachliche Aufgabenabgrenzung zwischen diesen beiden Clearingstellen. Vielmehr kann jeder Arbeitgeber nach Wahl an eine der beiden Clearingstellen melden.

Die Clearingstellen entschlüsseln die von den Arbeitgebern übersandten elektronischen Lohnsteuerbescheinigungen und prüfen, ob die darin angegebenen amtlichen Gemeindeschlüssel existieren. Ferner führen sie jeweils eine Plausibilisierung der aus dem Namen, dem Vornamen und den Geburtsdaten des Steuerpflichtigen gebildeten Identifikationsnummer (eTIN) durch. Nach erfolgreichem Abschluss dieser Plausibilitätstests leiten die Clearingstellen die elektronischen Lohnsteuerbescheinigungen, möglichst innerhalb von 24 Stunden nach ihrem Empfang, an einen der Landesspeicher weiter. An welchen Landesspeicher eine elektronische Lohnsteuerbescheinigung weitergeleitet werden soll, muss der Arbeitgeber in dem von ihm gemeldeten Datensatz festlegen. Maßgeblich dafür ist der zum Zeitpunkt der Meldung aktuelle Wohnsitz des Arbeitnehmers.

Vor der Weiterleitung einer elektronischen Lohnsteuerbescheinigung an einen Landesspeicher erfasst eine Clearingstelle den Namen und den Vornamen, das Geburtsdatum sowie die aus die-

sen Angaben abgeleitete eTIN des Steuerpflichtigen in ihrer Verweisdatenbank. Zudem hält sie darin fest, an welchen Landesspeicher sie die elektronische Lohnsteuerbescheinigung weiterleitet. Die beiden Clearingstellen tauschen die jeweils neu erfassten Verweisdaten regelmäßig untereinander aus. Anhand dieser Verweisdaten ist es möglich zu erkennen, in welchem Landesspeicher die zu einem Steuerpflichtigen übersandte Lohnsteuerbescheinigung auffindbar ist.

2.1.3 Landesspeicher (eSpeicher)

Für ELSTER-Lohn wurden in den einzelnen Bundesländern gleichartig aufgebaute Kommunikationsknoten und Landesspeicher installiert. In diesen werden die von den Clearingstellen weitergeleiteten Lohnsteuerbescheinigungen für zehn Jahre gespeichert und für einen Zugriff durch Bedienstete der Finanzämter bereitgehalten.

2.2 Die datenschutzrechtlichen Mängel

2.2.1 Unklarheit über datenschutzrechtliche Verantwortlichkeit für die Verarbeitung personenbezogener Daten in den Clearingstellen sowie den Landesspeichern

Im Rahmen des Verfahrens ELSTER-Lohn werden Angaben über die Höhe des jeweils erzielten Gehalts sowie weitere besonders schutzbedürftige personenbezogene Daten von mehreren Millionen Steuerpflichtigen allein aus Baden-Württemberg verarbeitet. Diese Verarbeitung findet zum Teil in den außerhalb Baden-Württembergs angesiedelten Clearingstellen und Landesspeichern statt. Datenschutzrechtlich ist dabei entscheidend, dass sich die Frage nach der datenschutzrechtlichen Verantwortlichkeit für die dort vorgenommene Verarbeitung personenbezogener Daten eindeutig beantworten lässt. Da jedoch die Informationen, die uns die Oberfinanzdirektion Karlsruhe dazu gab, keine Klarheit über den rechtlichen Status der Clearingstellen sowie der Landesspeicher schufen, bleibt unklar, welche Stellen für die in den Clearingstellen sowie die in den Landesspeichern durchgeführte Datenverarbeitung datenschutzrechtlich verantwortlich sind.

Dass bislang noch nicht durch entsprechende Rechtsvorschriften, Vereinbarungen oder Aufträge klargestellt wurde, wer als verantwortliche Stelle für welche Phasen der Datenverarbeitung sowie für welche in den Clearingstellen sowie den Landesspeichern verarbeiteten Datenbestände anzusehen ist, stellt einen datenschutzrechtlichen Mangel dar. Um diesen abzustellen, forderten wir das Finanzministerium auf, ggf. in Absprache mit dem Bundesfinanzministerium und den Finanzministerien der anderen Bundesländer, eine Klärung der Verantwortlichkeiten für die im Rahmen des Verfahrens ELSTER-Lohn vorgenommene Verarbeitung personenbezogener Daten herbeizuführen und die im Rahmen einer möglicherweise vorliegenden Auftragsdatenverarbeitung erforderlichen schriftlichen Aufträge alsbald abzuschließen.

Mittlerweile ist uns ein Entwurf für ein Abkommen zwischen den Finanzministerien des Bundes und der Länder über die Datenverarbeitung im Projekt ELSTER (zu dem neben ELSTER-Lohn noch mehrere weitere Module gehören) bekannt geworden. Allerdings wären auch dann, wenn dieses Abkommen in der uns vorliegenden Fassung geschlossen würde, noch nicht alle oben angesprochenen Fragen geklärt. Insbesondere müsste der Auftragsgegenstand im Hinblick auf die mit ELSTER-Lohn verbundenen Besonderheiten präziser formuliert werden. Dazu sind auch ELSTER-Lohn-spezifische Festlegungen über die Zahl und die Betreiber der Clearingstellen sowie der Länderspeicher zu treffen. Zudem sind schriftliche Vereinbarungen über die notwendigen technischen und organisatorischen Maßnahmen zu verein-

baren und es ist die Befugnis des Auftraggebers festzulegen, dass er hinsichtlich der Verarbeitung personenbezogener Daten dem Auftragnehmer Weisungen erteilen darf.

2.2.2 Fehlende Authentifizierung der Absender elektronischer Lohnsteuerbescheinigungen

Bei ELSTER-Lohn ist technisch nicht ausgeschlossen, dass der Steuerverwaltung auch Meldungen übermittelt werden, die zwar im Namen eines Arbeitgebers erfolgen, aber nicht von diesem, sondern einem Dritten abgesandt wurden. Eine gezielte Falschmeldung gegenüber der Steuerverwaltung kann mithin zu einer Speicherung und Verarbeitung unrichtiger Daten über Steuerpflichtige führen und sich für diese nachteilig auswirken. Es sollten daher Maßnahmen ergriffen werden, die, soweit möglich, derartige Fehlmeldungen verhindern oder die es zumindest ermöglichen, diese besser als bisher zu erkennen. Als Maßnahme kommt hierfür der Einsatz eines Authentifizierungsverfahrens in Betracht, mit dessen Hilfe sich die Steuerverwaltung von der Identität des Absenders der elektronischen Lohnsteuerbescheinigungen, hier also der jeweiligen Arbeitgeber, überzeugen kann. Ich halte es daher für erforderlich, Maßnahmen zu ergreifen, um künftig Falschmeldungen im Rahmen von ELSTER-Lohn zuverlässig erkennen und dementsprechend behandeln zu können. Das geschilderte Problem betrifft übrigens nicht nur das Verfahren ELSTER-Lohn, sondern auch andere Verfahren, mit denen die Unternehmen der Steuerverwaltung elektronisch Umsatzsteuervoranmeldungen sowie Lohnsteueranmeldungen zuleiten. Da zumindest für Letztere bereits die Einführung eines Authentifizierungsverfahrens in Aussicht gestellt wurde (vgl. 5. Teil, Nr. 4.3), habe ich gegenüber dem Finanzministerium meine Erwartung zum Ausdruck gebracht, dass ein solches Verfahren möglichst bald auch im Zusammenhang mit der Übermittlung der Lohnsteuerbescheinigungen eingeführt wird.

2.2.3 Keine technische Beschränkung der Zugriffsmöglichkeiten

Die gegenwärtige Lösung ermöglicht es den mit der Veranlagung der Lohn- und Einkommensteuer betrauten Bediensteten der baden-württembergischen Finanzämter, auf eine beliebige, in einem der Landesspeicher zum Abruf bereitgehaltene Lohnsteuerbescheinigung zuzugreifen. Die Suche kann dabei sowohl anhand der eTIN als auch anhand von Namen, Vornamen und Wohnort erfolgen. Zur Begründung der auf diese Weise eingeräumten bundesweiten Such- und Zugriffsmöglichkeiten auf beliebige Lohnsteuerbescheinigungen wurde ausgeführt, dass auch in folgenden Fällen ein Zugriff auf die für die Besteuerung benötigte elektronische Lohnsteuerbescheinigung möglich sein müsse:

- ein Steuerpflichtiger zieht, nachdem der Arbeitgeber die Lohnsteuerbescheinigung an die Steuerverwaltung übermittelt hat und bevor er seine Steuererklärung abgibt, von einem Bundesland in ein anderes,
- ein Steuerpflichtiger ändert, nachdem der Arbeitgeber die Lohnsteuerbescheinigung an die Steuerverwaltung übermittelt hat und bevor er seine Steuererklärung abgibt, seinen Nachnamen, etwa aufgrund Eheschließung,
- ein Steuerpflichtiger ändert, nachdem der Arbeitgeber die Lohnsteuerbescheinigung an die Steuerverwaltung übermittelt hat und bevor er seine Steuererklärung abgibt, Nachnamen und Wohnort,
- ein Steuerpflichtiger gibt seinen Vornamen in anderer Schreibweise an, als dies der Arbeitgeber bei der Erstellung der elektronischen Lohnsteuerbescheinigung tat.

Wenn man sich vergegenwärtigt, dass jeder dieser Bediensteten nur für die Durchführung des Besteuerungsverfahrens bei einem im Verhältnis zur Gesamtzahl der in ELSTER-Lohn erfassten Steuerpflichtigen kleinen Teil der Steuerpflichtigen zuständig ist, so bedeutet dies, dass ELSTER-Lohn jedem einzelnen Finanzamtsbediensteten, der überhaupt Zugriff auf diese Daten erhält, viel zu umfassende Zugriffsmöglichkeiten zur Verfügung stellt. Diese weit über das erforderliche Maß hinausgehenden Zugriffsberechtigungen stellen einen datenschutzrechtlichen Mangel dar. Dieser wird auch nicht dadurch behoben, dass zumindest ein Teil der Suchanfragen protokolliert wird. Denn diese Protokollierung kann – anders als die technische Beschränkung der Zugriffsmöglichkeiten – unberechtigte Zugriffe nicht von vornherein zuverlässig verhindern, sondern lediglich helfen, unberechtigte Zugriffe nachträglich nachweisen zu können. Die Protokollierung kann daher nicht als gleichwertiger Ersatz für fehlende technische Maßnahmen der Zugriffskontrolle dienen. Um diesen Mangel abzustellen, ist es daher nötig, die Zugriffsmöglichkeiten auf das dienstlich erforderliche Maß zu beschränken.

Dabei ist zu berücksichtigen, dass Fälle vorkommen können, in denen die für einen Steuerpflichtigen ausgestellte elektronische Lohnsteuerbescheinigung nicht in dem Landesspeicher des Bundeslandes abgelegt sind, in dem der Steuerpflichtige seine Steuererklärung abgibt. Aber weder diese noch andere von der Steuerverwaltung zur Begründung der umfassenden Zugriffsmöglichkeiten angeführten Fallkonstellationen vermögen die bundesweiten Such- und Zugriffsmöglichkeiten auf elektronische Lohnsteuerbescheinigungen in ihrer bestehenden Form zu rechtfertigen.

Zur Lösung dieser datenschutzrechtlichen Probleme könnte etwa beitragen, wenn die Lohnsteuerbescheinigungen zwar, ähnlich wie im bisherigen Modell, in zentralen Clearingstellen oder den mit diesen verbundenen Landesspeichern abgelegt werden, diese Ablage aber nicht im Klartext, sondern verschlüsselt erfolgt. Die Arbeitgeber könnten dazu die für einen Steuerpflichtigen zu meldenden Daten mit Hilfe eines von ihnen für diese Meldung gebildeten Schlüssels an die Steuerverwaltung melden. Ein Bediensteter eines Finanzamts könnte die elektronische Lohnsteuerbescheinigung in diesem Fall erst dann im Klartext lesen, wenn der Steuerpflichtige ihm den zum Zugriff erforderlichen Schlüssel in seiner Steuererklärung mitgeteilt hat. Der Arbeitgeber könnte den Steuerpflichtigen im Rahmen der Lohnsteuerbescheinigung, die er ihm ohnehin zusenden muss, auch über diesen Schlüssel informieren.

Abschließend sei angemerkt, dass eGovernment-Vorhaben aufgrund der Flexibilität der zu deren Gestaltung eingesetzten IuK-Technik aus meiner Sicht durchaus zu einer Verbesserung des Datenschutzes beitragen können. Leider kann ELSTER-Lohn aufgrund der dargestellten datenschutzrechtlichen Mängel nicht als Beispiel für eine datenschutzfreundliche Einführung eines eGovernment-Vorhabens dienen. Im Gegenteil: Durch ELSTER-Lohn wird ein bislang papiergebundener Datenfluss zwischen Arbeitgebern, Arbeitnehmern und den Finanzämtern durch ein elektronisches Verfahren abgelöst, bei dem anders als zuvor bundesweite Zugriffsmöglichkeiten auf Millionen individueller Lohnsteuerbescheinigungen neu geschaffen und die damit einhergehenden Risiken für die Vertraulichkeit der Steuerdaten immens ausgeweitet wurden.

5. Abschnitt: Sonstiges

1. Die wissbegierige Fahrerlaubnisbehörde

Im Verfahren zur Erteilung einer neuen Fahrerlaubnis verwendete die Fahrerlaubnisbehörde eines Landratsamts ein Formular mit folgendem Wortlaut:

> Erteilung einer neuen Fahrerlaubnis
> hier: Einverständniserklärung
>
> 1. Mit der Veranlassung von 4 polytoxikologischen Untersuchungen über einen Zeitraum von 12 Monaten beim Gesundheitsamt ... bin ich einverstanden. ...
> [Felder für Ort, Datum und Unterschrift]
>
> 2. Gleichzeitig befreie ich die Gutachter der Untersuchungsstelle von der Schweigepflicht und erkläre mich mit der Übersendung der Ergebnisse an das Landratsamt ... einverstanden.
> [Felder für Ort, Datum und Unterschrift]

Das war unzulässig: Hat eine Fahrerlaubnisbehörde aufgrund bekannt gewordener Tatsachen berechtigte Zweifel daran, dass jemand zum Führen von Kraftfahrzeugen geeignet ist, darf sie zwar anordnen, dass dieser ein ärztliches oder ein medizinisch-psychologisches Gutachten beibringt. Gleichwohl sieht keine Rechtsvorschrift vor, dass die untersuchende Stelle in jedem Fall der Fahrerlaubnisbehörde die Untersuchungsergebnisse mitteilt. Vielmehr ist das Gutachten nach einem Erlass des (damaligen) Verkehrsministeriums Baden-Württemberg aus dem Jahre 1992 ausschließlich dem Betroffenen zuzusenden, der dann selbst darüber zu entscheiden hat, ob er das Gutachten der Behörde vorlegt. Lässt der Betroffene sich nicht untersuchen oder legt er der Behörde kein Gutachten vor, ist die Behörde zwar berechtigt, auf seine Nichteignung zu schließen; sie kann ihn jedoch nicht unmittelbar dazu zwingen, ein Gutachten einzuholen oder ihr vorzulegen. Rechnet sich der Betroffene selbst keine Chancen aus, dass ihm die Behörde bei Vorlage des Gutachtens die Eignung zuerkennt und ihm die Fahrerlaubnis erteilt (etwa weil der Gutachter zum Ergebnis gekommen ist, dass der Betroffene voraussichtlich wieder ein Kraftfahrzeug unter Einfluss von Alkohol führen wird), kann er durch die Nichtweitergabe des Gutachtens wenigstens ausschließen, dass die Behörde die Feststellungen der untersuchenden Stelle erfährt, also etwa Informationen über die Vorgeschichte (etwa die Alkoholabhängigkeit des Betroffenen) und den gegenwärtigen Befund erhält.

Wenn das Landratsamt gleichwohl die unmittelbare Vorlage des Gutachtens forderte, hätte es den Betroffenen über den Wortlaut des genannten Formulars hinaus zumindest über die Freiwilligkeit sowie die möglichen Folgen einer solchen Einwilligung hinweisen müssen (vgl. § 4 Abs. 1 und 2 sowie § 14 Abs. 1 Satz 2 LDSG). Stattdessen war das Formular zumindest geeignet, dem Betroffenen einen unzutreffenden Eindruck über sein Recht auf informationelle Selbstbestimmung zu vermitteln: Es wurde nicht deutlich, dass der Betroffene sich zunächst die Untersuchungsergebnisse selbst anschauen darf, um dann zu entscheiden, ob er diese der Fahrerlaubnisbehörde vorlegt. Bei der gewählten Formulierung war es durchaus möglich, dass ein Betroffener unter dem Druck des Verfahrens fälschlicherweise annahm, zur Abgabe der Erklärung in jedem Fall verpflichtet zu sein.

2. Verarbeitung von Gewinnspieldaten ohne wirksame Einwilligung

Mit Befremden reagierte ein Petent, als er im Briefkasten ein Info-Schreiben einer Behörde fand, in dem die Rede von Altbau-Modernisierung war. Er konnte sich nicht erklären, woher die Behörde wusste, dass er Eigentümer eines älteren Hauses war.

Die Stellungnahme der Behörde brachte zu Tage, dass sie für ihre Schreiben Adressen von Teilnehmern an einem Gewinnspiel im Rahmen einer Informationskampagne des Landes zum Thema „Altbau“ verwandt hatte. Auf der Gewinnspielkarte befand sich kein Hinweis auf die Absicht, die erbetenen Angaben über das Gewinnspiel hinaus auch für andere Zwecke personenbezogen zu verarbeiten. Falls ein solcher Hinweis an die Betroffenen

erfolgt sei, sei dies mündlich geschehen, wenn z. B. ein Interessent vor Ort von sich aus wegen der Verarbeitung seiner Daten beim Personal des Info- und Gewinnspielstands nachgefragt habe, hieß es von Seiten der Behörde. Das genügte den datenschutzrechtlichen Anforderungen nicht: Die Betroffenen hätten auch ohne Nachfrage über die beabsichtigte (Weiter-)Verarbeitung ihrer Daten unterrichtet werden müssen. Weil dies nicht geschehen war, lagen keine wirksamen Einwilligungen hierzu vor (vgl. § 4 Abs. 2 LDSG). Das Verwenden der Daten über das Gewinnspiel hinaus auch für die spätere Information von Teilnehmern war deshalb unzulässig (vgl. § 4 Abs. 1 LDSG). Meine Dienststelle hat die Behörde gebeten, dies bei künftigen Vorhaben dieser Art zu beachten. Geschieht dies, ist auf jeden Fall der Datenschutz auf der Gewinnerseite.

3. Das Projekt MigVIS des Innenministeriums

Bislang werden im sog. Datenverarbeitungsverfahren-Asyl (DV-Asyl) die Daten von Flüchtlingen elektronisch verwaltet, die bei deren Unterbringung oder in ausländerrechtlichen bzw. asylverfahrensrechtlichen Verfahren anfallen. Bereits im Jahr 2003 hatte das Innenministerium angekündigt, dass es wegen der Schwachstellen dieses Verfahrens eine Neukonzeption betreibe. In diesem Jahr teilte das Innenministerium mit, dass der mittlerweile erreichte Projektstand des – nun als MigVIS (Migranten-Verwaltungs- und Informations-System) bezeichneten – Projekts eine Konkretisierung der datenschutzrechtlichen bzw. -technischen Vorgaben zulasse, übersandte mehrere datenschutzrechtlich relevante Projektdokumente (u. a. ein Datenschutz- und Sicherheitskonzept, einen Datenkatalog und ein Berechtigungskonzept) und gab erneut Gelegenheit zur Stellungnahme.

Den umfangreichen Projektdokumenten war die Beschreibung eines sehr komplexen EDV-Verfahrens mit einer Vielzahl personenbezogener Daten zu entnehmen: Als sog. Stammdaten waren neben dem Namen und Vornamen auch Geburtsdatum, Geburtsort, Familienstand, Religion, Staatsangehörigkeit, Volkszugehörigkeit und Muttersprache vorgesehen. Außerdem betrifft das Verfahren unterschiedliche Gruppen von Betroffenen (neben Asylbewerbern auch jüdische Emigranten und sonstige Flüchtlinge) und verschiedene Dienststellen (neben dem Innenministerium selbst das Regierungspräsidium Karlsruhe als Landesaufnahmestelle für Flüchtlinge und als Ausländerbehörde, die Regierungspräsidien Freiburg, Stuttgart und Tübingen als Ausländerbehörden und höhere Aufnahmebehörden sowie die Landratsämter und die Bürgermeisterämter der Stadtkreise in Baden-Württemberg als untere Aufnahmebehörden). Das Innenministerium räumte meinem Amt unter Hinweis auf bereits geschlossene vertragliche Vereinbarungen mit der Datenzentrale leider nur ein sehr knappes Zeitfenster für eine datenschutzrechtliche Beurteilung der Projektunterlagen ein. Folgende Punkte wurden von uns aufgegriffen:

– Zugriffsmöglichkeiten des Innenministeriums

  Wie bereits erwähnt, soll das geplante Verfahren auch die Verarbeitung personenbezogener Daten durch das Innenministerium selbst ermöglichen. Nach dem Datenschutz- und Sicherheitskonzept soll das Innenministerium im Rahmen eines automatisierten Abrufverfahrens lesenden Zugriff auf alle gespeicherten Daten haben. Zur Begründung führte das Innenministerium u. a. an, dass sich die Erforderlichkeit des Zugriffs auf alle Personengruppen in MigVIS bereits aus der vom Innenministerium wahrzunehmenden Fach- und Rechtsaufsicht ergebe. Diese Rechtsauffassung teile ich nicht. Wenn man diesen Gedanken verallgemeinert, würde dies bedeuten, dass alle Fach- und Rechtsaufsichtsbehörden in gleichem Maß Zugriff auf personenbezogene Daten haben dürfen wie die jeweils für die unmittelbare Sacherledigung zuständigen Stellen. Ein solches Ergebnis ist mit dem geltenden Datenschutzrecht schlechterdings unvereinbar. Unter bestimmten Voraussetzungen kann es selbstverständlich für das Innenministerium zur Erfüllung seiner eigenen Aufgaben erforderlich sein, auf bestimmte in MigVIS gespeicherte personenbezogene Daten zuzugreifen und diese zu verarbeiten. Diese Voraussetzungen sind beispielsweise gegeben, soweit das Innenministerium ihm nach den Regelungen des Aufenthaltsgesetzes zugewiesene eigene Aufgaben wahr-

nimmt oder Petitionen bearbeitet. Es ist ohne weiteres nachvollziehbar, dass das Innenministerium in Eilfällen – z. B. zur Bearbeitung von Petitionen, die sich gegen eine unmittelbar bevorstehende Abschiebung richten – durch einen lesenden Zugriff in die Lage versetzt werden soll, auf die erforderlichen Daten zeitnah und direkt zuzugreifen, ohne erst Berichte nachgeordneter Stellen einholen zu müssen. Dagegen war nicht nachvollziehbar, warum ein lesender Zugriff des Innenministeriums auch in anderen von dort genannten Fällen, beispielsweise „zur Überwachung der Kostenerstattung“ oder zur „Evaluierung der Neuregelung für die Aufnahme, Verteilung usw. der jüdischen Emigranten“ erforderlich sein soll. Ich habe das Innenministerium daher gebeten zu überprüfen, ob und in welchem Umfang Mitarbeitern des Innenministeriums Zugriffsmöglichkeiten auf die in MigVIS gespeicherten personenbezogenen Daten gewährt werden dürfen. Zudem bat ich, dafür Sorge zu tragen, dass die Mitarbeiter des Innenministeriums aufgrund entsprechend zu gestaltender Zugriffsberechtigungen nur auf diejenigen Daten zugreifen können, die sie zur Erfüllung ihrer dienstlichen Aufgaben benötigen. Es ist mir nicht bekannt, ob meine Hinweise vom Innenministerium bei der weiteren Arbeit an diesem Projekt berücksichtigt wurden. Da der lesende Zugriff des Innenministeriums im Rahmen eines automatisierten Abrufverfahrens erfolgen soll, ist vom Innenministerium nach den Vorschriften des Landesdatenschutzgesetzes jedenfalls eine Vorabkontrolle unter Beteiligung des behördlichen Datenschutzbeauftragten durchzuführen. Unter Umständen werden meine Bedenken im Rahmen einer solchen Vorabkontrolle noch ausgeräumt.

– Statistische Auswertungen

Das meinem Amt zugeleitete Datenschutz- und Sicherheitskonzept sieht vor, dass

- die in MigVIS gespeicherten Daten „in dienstlich erforderlichem Umfang“ auch für statistische Auswertungen genutzt werden und
- „über die Erstellung anonymisierter Statistiken hinaus gehende Auswertungen personenbezogenen Inhalts“ aktenkundig zu machen sind.

Wir wiesen darauf hin, dass die danach vorgesehenen statistischen Auswertungen einer datenschutzrechtlichen Rechtsgrundlage bedürfen, soweit im Rahmen dieser Auswertungen personenbezogene Daten verarbeitet werden. Dies gilt auch für den im Datenschutz- und Sicherheitskonzept enthaltenen Gliederungspunkt „Statistik bzw. statistische Auswertung“. Hierzu kommentierte das Innenministerium allerdings lapidar: „Auswertung in ‚anonymisierter Form‘, d. h. aus der Auswertung kann kein Rückschluss auf konkrete Personen gezogen werden (z. B. Anzahl der Asylbewerber einer bestimmten Nationalität)“. Diesen Ausführungen liegt unter Umständen das (Miss-)Verständnis zugrunde, dass es aufgrund der „anonymisierten Form“ der Auswertungen nicht erforderlich sei, eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten in Betracht zu ziehen und zu prüfen. Ich habe dem Innenministerium mitgeteilt, dass nach unserem Verständnis für solche Auswertungen personenbezogene Daten verarbeitet würden. Daran ändert auch der Umstand nichts, dass die aufgrund dieser Verarbeitung personenbezogener Daten gewonnenen Auswertungen für sich genommen eventuell „anonym“ und somit nicht personenbezogen wären.

– Ergänzung des Datenschutz- und Sicherheitskonzepts

Nach Mitteilung des Innenministeriums wurden bei der Ausarbeitung des Datenschutz- und Sicherheitskonzepts bislang vorrangig solche Aspekte aufgenommen, die in unmittelbarem Zusammenhang mit der von der Datenzentrale zu leistenden Programmentwicklung stehen. Ein Datenschutz- und Sicherheitskonzept für MigVIS muss allerdings wesentlich umfassender angelegt sein und sämtliche Datenschutz- und Sicherheitsaspekte abdecken, die sich im Zusammenhang mit dem Einsatz des Verfahrens MigVIS ergeben. Wir haben dem Innenministerium beispielhaft einige Punkte genannt, bei denen Ergänzungsbedarf besteht. Nach unseren Informationen ist der Start der Pilot-Phase Anfang 2006 vorge-

sehen. Sofern in dieser Pilot-Phase bereits eine Verarbeitung personenbezogener Daten stattfinden soll, müssen bis zum Beginn dieser Datenverarbeitung alle noch offenen datenschutzrechtlichen Fragen, einschließlich der Aspekte des technischen und organisatorischen Datenschutzes, so abgearbeitet sein, dass der Persönlichkeitsschutz der Betroffenen sichergestellt ist.

4. Begehungsrecht und Geheimhaltungspflicht des Schornsteinfegers

– Begehungsrecht des Schornsteinfegers

Immer wieder erkundigen sich Bürger bei unserer Dienststelle, ob das Begehungsrecht des Schornsteinfegers mit dem Datenschutz zu vereinbaren ist. Dazu ist zu sagen, dass der Bundesgesetzgeber das Begehungsrecht des Schornsteinfegers ausdrücklich gesetzlich geregelt hat, um eine lückenlose Verantwortung für die Feuersicherheit zu gewährleisten. Nach § 1 Abs. 3 des Schornsteinfegergesetzes (SchfG) sind die Eigentümer und Besitzer von Grundstücken und Räumen verpflichtet, dem Bezirksschornsteinfegermeister und den bei ihm beschäftigten Personen zum Zwecke des Kehrens und der Überprüfung der kehr- und überprüfungspflichtigen Anlagen Zutritt zu den Grundstücken und Räumen zu verschaffen. Die gleiche Pflicht besteht, wenn Beauftragte der zuständigen Verwaltungsbehörde die Tätigkeit des Bezirksschornsteinfegermeisters zu überprüfen oder eine verweigerte Kehrung oder Überprüfung aufgrund eines vollziehbaren Verwaltungsaktes zwangsweise durchzusetzen haben. Das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) wird insoweit eingeschränkt.

Nach dem Schornsteinfegergesetz hat der Bezirksschornsteinfegermeister die Aufgabe, die durch die Kehr- und Überprüfungsordnung vorgeschriebenen Arbeiten auszuführen. Verweigert der Hauseigentümer die vorgeschriebene fristgerechte Überprüfung und Reinigung der Heizungsanlage durch den Bezirksschornsteinfeger, so kann sich die zuständige Verwaltungsbehörde zur zwangsweisen Durchsetzung dieser Maßnahmen ggf. auch durch die (zuvor angedrohte) Anwendung unmittelbaren Zwangs Zutritt zu den betreffenden Räumen verschaffen. Einer vorherigen richterlichen Durchsuchungsanordnung bedarf es hierzu in der Regel nicht.

– Geheimhaltungspflicht des Schornsteinfegers

Das Schornsteinfegergesetz verpflichtet den Schornsteinfeger generell, seine Aufgaben ordnungsgemäß und gewissenhaft auszuführen. Diese sog. allgemeine Berufspflicht (vgl. § 12 Abs. 1 SchfG) umfasst auch eine besondere Sorgfalts- und Obhutspflicht, die insbesondere dann bedeutsam ist, wenn sich der Bezirksschornsteinfegermeister in die unmittelbare Intimsphäre des Bürgers begibt, wie z. B. bei Messungen an Gasfeuerstätten in Badezimmern. Es muss dann von ihm verlangt werden, dass er die aufgrund der besonderen Situation gebotene Rücksichtnahme walten lässt.

Vor einigen Jahren wurde unser Amt auf das Problem aufmerksam gemacht, dass die Eigentümer und Besitzer von Grundstücken und Räumen nicht die freie Wahl zwischen mehreren Bezirksschornsteinfegermeistern haben, sondern den für ihren Bezirk amtlich bestellten Bezirksschornsteinfegermeister akzeptieren müssen. Umso mehr sollten sie sich darauf verlassen können, dass dieser auch über alles, was ihm bei der Ausübung seiner Tätigkeit zur Kenntnis gelangt, Verschwiegenheit bewahrt und diese Erkenntnisse nicht anderweitig nutzt. Rechtlich ist dies aber nicht ausreichend sichergestellt. Das Schornsteinfegergesetz regelt zwar, wie der Schornsteinfeger mit den in Ausübung seiner Tätigkeit erhobenen und gespeicherten Daten umzugehen hat. Nicht ausdrücklich geregelt ist jedoch, wie er mit den Umständen umgehen muss, die er gelegentlich seiner Tätigkeit aus dem häuslichen und privaten Bereich „mitbekommen“ hat. Dieser Rechtszustand ist nach Auffassung unserer Dienststelle unbefriedigend. Wir haben uns deshalb schon vor einigen Jahren dafür eingesetzt, dass in das Schornsteinfegergesetz – gewissermaßen als Pendant zu den Duldungspflichten der Grundstückseigentümer und Nutzungsberech-

tigten – eine Verpflichtung des Bezirksschornsteinfegermeisters und seiner Mitarbeiter zur Verschwiegenheit auch über solche Umstände aufgenommen wird, die ihm gelegentlich seiner Tätigkeit zur Kenntnis gelangen. Als Vorbild einer solchen denkbaren Regelung hatten wir beispielhaft auf § 14 Abs. 2 des Bundesstatistikgesetzes hingewiesen. Das auf Landesebene für das Schornsteinfegerwesen zuständige Wirtschaftsministerium hat sich seinerzeit aufgeschlossen für unseren Vorschlag gezeigt und zugesagt, diesen an das Bundesministerium für Wirtschaft weiterzugeben. Zudem hat der Bundesbeauftragte für den Datenschutz das Bundesministerium für Wirtschaft und Technologie bereits vor Jahren gebeten, eine entsprechende Änderung des Schornsteinfegergesetzes zu prüfen. Leider wurde unser Vorschlag vom Bundesgesetzgeber bislang nicht aufgegriffen.

5. Schornsteinfeger als Datenquelle?

Das Wirtschaftsministerium Baden-Württemberg hatte unsere Dienststelle gebeten zu prüfen, ob der Bezirksschornsteinfegermeister in einem von ihm geschilderten Fall befugt bzw. verpflichtet ist, der unteren Wasserbehörde eines Landratsamts im Zusammenhang mit der Ausweisung eines neuen Wasserschutzgebiets personenbezogene Daten der Betreiber von Ölheizungen des gesamten Kehrbezirks zu übermitteln. Die Kernfrage war hier zunächst, ob die Datenübermittlung zur Bekämpfung der Gewässerverschmutzung und damit zur Aufgabenerledigung der unteren Wasserbehörde überhaupt erforderlich ist. Denn nach § 19 Abs. 3 des Schornsteinfegergesetzes darf der Bezirksschornsteinfegermeister personenbezogene Angaben aus seinen Aufzeichnungen an öffentliche Stellen nur dann übermitteln, wenn dies für die Erfüllung seiner Aufgaben, für die Bekämpfung der Luft-, Boden- und Gewässerverschmutzung, für die rationelle Energieverwendung, die Bauaufsicht oder für die Brandbekämpfung erforderlich ist. Diese Voraussetzungen lagen hier jedoch nicht vor. Denn wie sich letztendlich herausstellte, hatte das Landratsamt den Bezirksschornsteinfegermeister lediglich deshalb um die Übermittlung der Daten gebeten, um als Serviceleistung die Betreiber von Ölheizungen auf die mit der Ausweisung eines Wasserschutzgebiets verbundenen Rechtsänderungen hinweisen zu können.

Wie uns das Umweltministerium Baden-Württemberg auf Nachfrage mitteilte, könne bei der Ausweisung eines Wasserschutzgebiets vom Verordnungsgeber nicht verlangt werden, alle möglicherweise von der Schutzgebietsverordnung betroffenen Anlagen ausfindig zu machen und vor Ort zu prüfen. Vielmehr müssten nach Erlass der jeweiligen Schutzgebietsverordnung die Betreiber der Anlagen von sich aus aktiv werden. Die Anlagenverordnung wassergefährdender Stoffe gehe von der Betreiberverantwortung aus. Sie kenne keine Anzeigepflichten der Betreiber gegenüber der Behörde. Nur wenn besondere Umstände vorliegen, z. B. eine besondere Gefahrensituation oder Unfälle in der Vergangenheit, könne es zur Bekämpfung einer Gewässerverschmutzung erforderlich sein, die Betreiber von Tankanlagen über die rechtlichen Anforderungen einzeln zu unterrichten und deren Einhaltung zu überwachen (§ 82 des Wassergesetzes). Solche besonderen Umstände waren im vorliegenden Fall jedoch nicht gegeben. Nachdem die Datenerhebung des Landratsamts bei dem Bezirksschornsteinfegermeister zur Aufgabenerledigung der unteren Wasserbehörde nicht erforderlich war, war der Bezirksschornsteinfegermeister nicht befugt, personenbezogene Daten der Betreiber von Heizöllagertanks an das Landratsamt zu übermitteln. Das haben wir dem Wirtschaftsministerium, das zunächst eine andere Rechtsauffassung vertreten hatte, mitgeteilt.

5. Teil: Technik und Organisation

1. Entwicklungen in der IuK in den letzten Jahren

In diesem Jahr feierte unsere Dienststelle ihr 25-jähriges Bestehen. Im Vergleich mit anderen Rechtsgebieten ist der Datenschutz damit noch sehr jung. Gemessen an der Lebensdauer informationstechnischer Produkte und Trends stellen die 25 Jahre hingegen einen Zeitraum dar, innerhalb dessen sich viele grundlegende Veränderungen ergeben haben. Das 25-jährige Jubiläum soll daher Anlass sein, einige wichtige Änderungen aus dieser Zeit Revue passieren zu lassen:

1.1 EDV-Einsatz in der Verwaltung

Als die Dienststelle der Landesbeauftragten für den Datenschutz im Jahr 1980 ihre Arbeit aufnahm, fand die elektronische Verarbeitung personenbezogener Daten noch vorwiegend in Großrechnern statt, die in einigen wenigen staatlichen und kommunalen Rechenzentren betrieben wurden. Auf diese Weise nutzte beispielsweise die Polizei ihre Personenauskunftsdatei (PAD), die Finanzämter ließen Steuerbescheide maschinell ausfertigen und die Kommunen nutzten die Großrechnertechnik, um ihre Melderegister automatisiert zu führen. Viele Behörden verfügten noch nicht über eigene Computer und am typischen Büroarbeitsplatz befand sich weder ein zur Nutzung der Großrechner verwendbares Terminal noch gar ein PC. Wie eh und je spielte sich die Datenverarbeitung der Verwaltung noch vorwiegend in Akten und Karteien ab.

Mit dem im Jahr 1985 verabschiedeten Landessystemkonzept kamen ressortübergreifende EDV-Projekte in Gang. Damit fiel auch der Startschuss für den Aufbau des speziell für die Behördenkommunikation vorgesehenen Landesverwaltungsnetzes. Bis dahin hatten einzelne Ressorts unabhängig voneinander überregionale Datennetze aufgebaut. Der Polizei stand beispielsweise ein landesweites Netz zur Verfügung, an das weniger als 300 Terminals angeschlossen waren. Diese Netze wurden ab 1986 Schritt für Schritt im Landesverwaltungsnetz zusammengeführt. Als Datendrehscheibe diente eine Dreiecksverbindung (Backbone) zwischen Rechenzentren in Stuttgart, Karlsruhe und Freiburg. Noch bis 1991 wurden die Daten dabei mit einer aus heutiger Sicht bescheidenen Übertragungsrate von 19 200 Bit pro Sekunde übertragen. Heute steht jedem Internet-Nutzer, der die ISDN- oder DSL-Technik einsetzt, ein Vielfaches davon zur Verfügung.

Mit der weiteren Verbreitung der Arbeitsplatz-PCs, dem Ausbau der lokalen Netzwerke und deren Anschluss an das Landesverwaltungsnetz ging eine immer intensivere Nutzung der elektronischen Kommunikationsmöglichkeiten einher. Folgende Zahlen mögen dies verdeutlichen:

- Im September 1993 tauschten die Ministerien 5 000 E-Mails aus.
- Im April 1999 versandten und empfingen die an das LVN angeschlossenen Stellen bereits 370 000 Mails. Nach der Koppelung des LVN mit dem Internet hat sich die Anzahl weiter sprunghaft erhöht.
- Im Jahr 2004 wurden monatlich im Durchschnitt mehr als 5 Millionen E-Mails über das LVN ausgetauscht, viele davon waren an Empfänger im Internet gerichtet oder stammten aus dem Internet. Die damit verbundenen Sicherheitsprobleme lassen sich erahnen, wenn man bedenkt, dass mehr als ein Drittel aller aus dem Internet kommenden E-Mails virenverseucht war.

1.2 Neue Herausforderungen für den Datenschutz

Die neuen technischen Möglichkeiten brachten auch neue Herausforderungen für den Datenschutz mit sich:

- Zunehmende Nutzung der PCs

  Die Verbreitung der PCs führt dazu, dass die EDV auch physisch die Rechenzentren verließ und mittlerweile an fast jedem Büroarbeits-

platz Datenverarbeitungsmöglichkeiten bereitstellt. Maus und grafische Benutzeroberfläche machen den Einsatz vieler Computerprogramme inzwischen fast zum Kinderspiel. Der Nutzungskomfort ging zumindest zeitweise mit Einbußen in der Sicherheit einher, denn PC-Betriebssysteme boten lange Zeit keinen ausreichenden Schutz gegen unberechtigte Zugriffe. Aufgrund der starken Zunahme dezentraler Speicher- und Verarbeitungsmöglichkeiten können heutzutage Daten prinzipiell in zahllosen Computern gespeichert sein. Dies erschwert die Umsetzung der Datenschutzrechte der Betroffenen auf Auskunft, Berichtigung und Löschung.

– Verbreitung von Telefaxgeräten

  Insbesondere wenn Telefaxgeräte an Telefonnebenstellenanlagen betrieben werden, kann es leicht zu Irrläufern kommen. Anders als beim Telefon bemerkt der Absender eine Telefax-Fehlleitung oft erst, nachdem die Daten bereits übermittelt wurden. Ein weiteres Datenschutzproblem besteht darin, dass die empfangenen Nachrichten offen im Gerät des Empfängers liegen und dieses vielfach so aufgestellt ist, dass viele Personen diese Nachrichten lesen können.

– Immer mehr, immer komplexere Anwendungen

  Diese Entwicklung führt dazu, dass die Systeme immer schwerer zu durchschauen sind. Die Beteiligung mehrerer Stellen führt dazu, dass auch datenschutzrechtlich relevante Verantwortlichkeiten verschwimmen (vgl. Nr. 4.2 dieses Teils).

– Integrierte Verwaltungsnetze

  Der Aufbau landesweiter Kommunikationsnetze, die von allen staatlichen und zum Teil auch kommunalen Behörden genutzt werden können, macht eine Abschottung der verschiedenen Verwaltungszweigen angehörenden Nutzergruppen und der bereitgestellten Kommunikationsdienste erforderlich.

– Automatisierte Abrufverfahren

  Die Besonderheit bei automatisierten Abrufverfahren besteht darin, dass sich die abrufende Stelle im Datenpool einer anderen Stelle selbst bedienen kann. Dies eröffnet auch die Möglichkeit missbräuchlicher Nutzung. Die Kontrolle der Rechtmäßigkeit der einzelnen Abrufe ist in der Praxis jedoch meist nur stichprobenweise möglich.

– Koppelung der Verwaltungsnetze mit dem Internet und anderen öffentlichen Netzen

  Mit der Koppelung der Verwaltungsnetzwerke mit dem Internet oder anderen öffentlichen Kommunikationsnetzen erhöhen sich die für die Verwaltungscomputer und die darin verarbeiteten Daten bestehenden Sicherheitsrisiken erheblich. Man denke hier nur an die von Hackern und Viren ausgehenden Gefahren. Zudem wächst die Gefahr, dass Unberechtigte von übertragenen schutzbedürftigen Daten Kenntnis erhalten, diese speichern oder verändern.

– Chipkarten

  Die Ausgabe von Chipkarten an Bürgerinnen und Bürger führt dazu, dass ein Teil der von der ausgebenden Stelle betriebenen Hard- und Software nicht mehr im Besitz und unter ständiger Kontrolle der öffentlichen Stelle verbleibt. Dies führt zu besonderen datenschutzrechtlichen Anforderungen. Beispielsweise muss sichergestellt sein, dass nur berechtigte Stellen die auf einer Chipkarte gespeicherten personenbezogenen Daten lesen oder ändern können. Um dieser Besonderheit Rechnung zu tragen, wurden spezielle Vorschriften in die Datenschutzgesetze des Bundes und der Länder aufgenommen.

– Videoüberwachung

Bei den meisten EDV-Verfahren, mit denen personenbezogene Daten verarbeitet werden, besteht ein unmittelbarer Zusammenhang zwischen dem Zweck des Verfahrens und jeder einzelnen Person, deren Daten damit verarbeitet werden. Bei einer Videoüberwachung, die etwa der Verfolgung und der Verhinderung von Straftaten dienen soll, besteht ein solcher Zusammenhang für den weit überwiegenden Teil der von dieser Maßnahme betroffenen Personen gerade nicht.

– Outsourcing des EDV-Betriebs

Die in vielen Verwaltungsbereichen bestehende Möglichkeit, Datenverarbeitungsaufgaben von Dritten erledigen zu lassen, wirft spezifische Datenschutzprobleme auf. Beispielsweise besteht in einer solchen Konstellation die Gefahr des Mitlesens und Veränderns schutzbedürftiger Daten durch Mitarbeiter der mit der Durchführung der Datenverarbeitung beauftragten öffentlichen oder privaten Stelle. Weitere Fragen ergeben sich, wenn der Auftrag an einen Auftragnehmer mit Sitz außerhalb der EU erteilt werden soll.

– eGovernment; elektronische Bürgerdienste

Eine zuverlässige Identifizierung der Beteiligten, eine sichere und vertrauliche Kommunikation und ein angemessener Schutz personenbezogener Daten müssen gewährleistet sein. Mehr Datenspuren als unbedingt nötig dürfen nicht entstehen.

– Zunehmende Nutzung bundesweit ausgerichteter EDV-Verfahren

Mittlerweile machen immer mehr Computeranwendungen etwa im Gesundheitswesen (z. B. Anwendung der elektronischen Gesundheitskarte, Krebsregistrierung), der Sozialverwaltung (z. B. Job-Card-Verfahren), der Steuerverwaltung (z. B. Kontendatenabrufe, ELSTER-Lohn), der Justiz (z. B. elektronisches Grundbuch, zentrales Staatsanwaltschaftliches Verfahrensverzeichnis), im Bereich der zur Betreuung der Hilfeempfänger des Arbeitslosengeldes II eingerichteten Arbeitsgemeinschaften (z. B. Nutzung des Verfahrens A2LL) oder anderen Verwaltungszweigen von der bestehenden Vernetzung Gebrauch und ermöglichen nicht selten bundesweite Zugriffe auf personenbezogene Daten. Datenschutzrechtlich bedeutsam ist dabei, dass konzeptionelle oder technische Unzulänglichkeiten, etwa hinsichtlich der differenzierten Zugriffskonzepte, dabei weitaus schwerer wiegende Folgen haben als dies bei einem Einsatz in engerem Rahmen der Fall wäre.

– Allgegenwärtige Datenverarbeitung (Ubiquitous/pervasive computing)

Die intensive Nutzung mobiler Kommunikationstechniken sowie der unter Nr. 2 beschriebenen RFID-Technik ermöglicht die Durchdringung aller Lebensbereiche mit informationsverarbeitenden Systemen. Dies macht es möglich, vielfältige Aktivitäten des täglichen Lebens zu erfassen, zu speichern und zu verknüpfen. Durch Auswertung dieser Datenbestände lassen sich Bewegungs-, Konsum- und Nutzungsprofile erstellen. Ziel des Datenschutzes muss es sein, auf die Gestaltung der Verfahren dahingehend einzuwirken, dass die Anonymität bei Handlungen des Alltagslebens erhalten bleibt.

2. RFID

In „intelligenten Mülltonnen“ sind sie ebenso zu finden, wie in den seit November dieses Jahres ausgegebenen neuen Reisepässen. Die Stadtbücherei Stuttgart markiert damit ihre Medien und auch in den zur Fußball-WM ausgegebenen Eintrittskarten werden sie zu finden sein. Sie können in Ausweisen verwendet werden, die zur Zutrittskontrolle dienen und manch ein Auto lässt sich nur starten, wenn auch der Autoschlüssel mit dieser Technik ausgerüstet ist. Nicht zuletzt sollen sie die bislang schon auf vielen Produkten aufgedruckten Barcodes ablösen und daher in immer mehr Gegenstände

des täglichen Lebens integriert werden. Die Rede ist von RFID-Tags. RFID ist die Abkürzung von „Radio Frequency Identification“ und steht für eine Technik, bei der sich alles um winzig kleine und in der Massenproduktion nur wenige Cent teure Minicomputer, eben die RFID-Tags, dreht. Da diese ausschließlich drahtlos mit anderen Systemen Daten austauschen und zum Teil nicht einmal auf eine eigene Stromversorgung angewiesen sind, können RFID-Tags beispielsweise so in ein Plastikgehäuse eingebettet sein, dass sie auch bei genauem Hinschauen nicht zu erkennen sind.

2.1 Was leistet die RFID-Technik?

Auf den ersten Blick kann der Eindruck entstehen, hier handele es sich um eine Entwicklung wie viele andere, die mit Datenschutz allenfalls am Rande zu tun hat. Denn die Verkleinerung elektronischer Bauteile gehört für uns schon ebenso zu den Selbstverständlichkeiten wie die Reduzierung der Herstellungskosten. Und auch von der Möglichkeit der drahtlosen Kommunikation wird in der Computertechnik mittlerweile vielfach Gebrauch gemacht. Zudem können manche Anbieter derartiger Systeme auch darauf verweisen, dass in den von ihnen in Umlauf gebrachten RFID-Tags keine personenbezogenen Daten, sondern beispielsweise nur Bezeichnungen der jeweiligen Gegenstände gespeichert sind, in denen sie eingebaut sind.

Bei näherem Hinsehen wird jedoch rasch deutlich, dass die RFID-Technik schon bald unser künftiges Alltagsleben verändern und dabei auch vielfältige Auswirkungen auf den Datenschutz haben kann:

– Gegenstände werden „smart“

Die RFID-Technik macht es möglich, jeden Gegenstand mit der Fähigkeit zur Datenverarbeitung auszustatten. Er kann dann viel mehr, als nur auf Anforderung eine Produktnummer mitzuteilen. Vielmehr ist beispielsweise denkbar, dass die Produkte die Nutzer erkennen (etwa weil diese ebenfalls individuelle RFID-Tags mit sich führen) und dementsprechend nutzerspezifische Funktionen zur Verfügung stellen. Somit werden die Produkte in die Lage versetzt, interaktiv und situationsbezogen zu reagieren.

– Gegenstände werden vernetzt

Derart ertüchtigte Produkte können untereinander sowie mit herkömmlichen Computersystemen Daten austauschen. Der bereits zur Marktreife entwickelte „intelligente“ Kühlschrank erkennt, welche mit RFID-Tags versehene Produkte mit welchen Haltbarkeitsfristen noch vorrätig sind und welche wann ersetzt werden müssen. Er kann selbstständig Einkaufslisten zusammenstellen und diese dem Nutzer etwa per E-Mail oder SMS mitteilen.

2.2 Die virtuelle Welt integriert vernetzte Gegenstände

Bisher bildeten die vernetzten Computer eine virtuelle Welt, in der Gegenstände bildlich und in vielen anderen Eigenschaften immer überzeugender abgebildet und ihr Verhalten simuliert werden konnten. Gleichwohl stand ihr die reale Welt der Gegenstände weitgehend unvermittelt gegenüber. Mit der RFID-Technik ist die Entwicklung jedoch so weit, dass praktisch jeder Gegenstand mit einem speziell darauf zugeschnittenen RFID-Tag versehen und damit unmittelbar auch Teil der virtuellen Welt werden kann. Manche Anwendungen sehen darüber hinaus auch vor, Tiere oder sogar Menschen mit RFID-Tags zu versehen.

Grundlegende technische Entwicklungen wie diese werfen eine Vielzahl neuer Fragen auch für den Datenschutz auf. In der Vergangenheit führte die Realisierung solcher Entwicklungen, wie am Beispiel der Vernetzung stationärer Computer oder dem Aufkommen des Internets zu beobachten, dazu, dass bereits vorhandene Datenschutz- und Sicherheitsprobleme in dem neuen Zusammenhang wie in einem Brennglas gebündelt wurden und noch größere Schäden hervorrufen konnten. Es ist abzusehen, dass auch die RFID-Technik solche Folgen nach sich

ziehen kann: Man denke nur daran, was geschehen kann, wenn Computerviren, die bereits heute erhebliche wirtschaftliche Schäden verursachen, künftig auch vernetzte Gegenstände befallen und etwa massenhaft Gefriertruhen abtauen oder gar sicherheitsrelevante Fahrzeugelektronik beeinflussen.

2.3 Datenschutzrisiken der RFID-Technik

Bei der datenschutzrechtlichen Bewertung der RFID-Technik stellt sich zunächst die Frage, inwieweit durch diese Technik personenbezogene Daten berührt sind. Bei einigen Anwendungen wie etwa den biometrischen Reisepässen und Personalausweisen werden die RFID-Tags selbst personenbezogene Daten enthalten. Auch in Krankenhäusern wird RFID-Technik bereits zur Identifizierung der Patienten erprobt. In Patientenarmbänder integrierte RFID-Tags sollen es Ärzten und Pflegepersonal im Notfall ermöglichen, schnell auf die Krankengeschichte und Medikamentendosierung zugreifen zu können. Aber auch, wenn ein RFID-Tag selbst keine personenbezogenen Daten enthält, kann dessen Verwendung dazu beitragen, dass personenbezogene Daten über den Inhaber des mit dem RFID-Tag versehenen Gegenstands wesentlich leichter als bisher gesammelt und ausgewertet werden können. Folgende datenschutzrechtliche Risiken gehen mit der Nutzung der RFID-Technik einher:

– Bewegungsprofile

Insbesondere wenn Personen bestimmte mit RFID-Tag versehene Gegenstände häufig mit sich führen (z. B. bestimmte Kleidungsstücke, Schuhe, Taschen, Handys), kann jeder, der einmal die Zuordnung zwischen Person und der Produkt-ID vorgenommen hat, ein Bewegungsprofil der Person erstellen. Dies ist umso leichter möglich, je mehr Geräte zum Auslesen der Daten in Behörden, Unternehmen oder öffentlichen Bereichen betrieben werden und je intensiver deren Betreiber die erfassten Daten untereinander austauschen.

– Nutzungs- und Verhaltensprofile

Verknüpft man Daten über Personen mit den per RFID bei ihnen nachgewiesenen Waren, lässt dies Rückschlüsse auf Interessen, Vorlieben und andere Persönlichkeitsmerkmale zu. Da beim Einsatz der RFID-Technik zur Warenkennzeichnung vorgesehen ist, jedes einzelne Produkt mit einer individuellen Nummer zu versehen, wird sich unter Umständen für jeden Gegenstand, der künftig irgendwo angetroffen wird, nachvollziehen lassen, wer diesen Gegenstand wann wo gekauft hat. Solche Informationen, die in erster Linie den Verkäufern der Waren zur Verfügung stehen, können bei Vorliegen entsprechender Voraussetzungen aber auch von Strafverfolgungsbehörden oder anderen Sicherheitsbehörden für deren Zwecke genutzt werden.

– Fehlende Transparenz

RFID-Tags können versteckt an oder in Waren angebracht sein. Da der Inhaber eines mit RFID-Tag versehenen Gegenstands auch nicht ohne weiteres etwas davon bemerkt, wenn ein RFID-Tag mit einem externen System Daten austauscht, besteht beim Einsatz der RFID-Technik das Risiko, dass unbemerkt Daten über den Inhaber der Gegenstände erhoben werden.

– Große Datenmengen

Bei einer systematischen Ausstattung der Alltagsgegenstände mit RFID-Tags und einer systematischen Speicherung der mit Hilfe der RFID-Technik ausgetauschten Daten können riesige Datenbestände entstehen.

– Komplexe Auswertungen

Diese Datenmengen können auf vielfältige Weise automatisiert ausgewertet werden. Insbesondere können in diesen Datenbeständen Verfahren des sog. Data Mining zum Einsatz kommen, bei denen – zunächst noch ohne bestimmtes Ziel – diese auf formale Besonderheiten hin untersucht werden können.

– „Datenschatten“

Führt jemand mit RFID-Tags versehene Gegenstände in Taschen oder einem Rucksack mit sich, so können diese von einem Dritten, der über ein RFID-Lesegerät verfügt, identifiziert werden. Der Einblick in den Tascheninhalt wird damit auch gegen den Willen des Inhabers der Gegenstände möglich. Die dabei gewonnenen Erkenntnisse können zudem mit weiteren, zu der Person bekannten Informationen zusammengeführt werden. Auch wenn auf diese Weise der Name der Person noch nicht direkt ermittelt werden kann, wirft der Einzelne einen „Datenschatten“, der von Dritten wahrgenommen und für deren Zwecke ausgewertet werden kann.

– RFID-Funkverkehr abhörbar

Wenn keine weiteren Schutzmaßnahmen ergriffen werden, können die zwischen einem RFID-Tag und dessen Kommunikationspartnern ausgetauschten Daten von Dritten abgehört werden.

2.4 Datenschutzmaßnahmen bei RFID-Systemen, die unmittelbar zur Verarbeitung personenbezogener Daten dienen

Dass Systeme, bei denen personenbezogene Daten in den RFID-Tags gespeichert werden, datenschutzrechtlich sorgsam konzipiert werden müssen, entspricht den auch bislang schon geltenden Regeln des Datenschutzes. Derartige Systeme müssen insbesondere folgenden Anforderungen entsprechen:

– Es ist eine Vorabkontrolle durchzuführen. Dabei ist zu prüfen, welche Gefahren sich bei Realisierung des geplanten Projekts für die Persönlichkeitsrechte der Betroffenen ergeben, was zur Reduzierung dieser Gefahren getan werden soll sowie ob das danach verbleibende Restrisiko tragbar ist.

– Spätestens mit Beginn des Echtbetriebs müssen technisch-organisatorische Datenschutzmaßnahmen ergriffen werden und nachvollziehbar dokumentiert sein.

– Es muss sichergestellt sein, dass die Betroffenen die ihnen zustehenden Rechte ohne unvertretbaren Aufwand wahrnehmen und so etwa Auskunft über die zu ihrer Person gespeicherten Daten erhalten oder die Berichtigung unrichtiger Daten verlangen können.

2.5 Datenschutzmaßnahmen bei RFID-Systemen, die nicht unmittelbar zur Verarbeitung personenbezogener Daten dienen sollen

Eine Besonderheit der RFID-Technik liegt darin, dass auch Systeme, die nicht unmittelbar zur Verarbeitung personenbezogener Daten genutzt werden sollen, nachhaltig in die Persönlichkeitsrechte von Bürgerinnen und Bürgern eingreifen können. Denn ein Personenbezug lässt sich mitunter auch in diesen Fällen leicht herstellen, etwa wenn die Identität der Person, die RFID-markierte Waren bei sich trägt, durch Auslesen personenbezogener Daten etwa aus einer Kreditkarte bestimmt werden kann. Werden die aus RFID-Tags ausgelesenen Daten z. B. in zentralen Datenbanken gespeichert, so können Bewegungs-, Nutzungs- und letztlich auch Persönlichkeitsprofile erstellt werden, deren Zustandekommen für den Betroffenen vollkommen intransparent ist und auf deren Entstehen er keinen Einfluss hat. Das bedeutet, dass das Recht des Betroffenen auf informationelle Selbstbestimmung durch diese Technologie erheblich gefährdet ist. Geboten ist daher eine frühzeitige Berücksichtigung datenschutzrechtlicher Anforderungen auch

bei solchen RFID-Anwendungen, die unmittelbar nur auf die Verarbeitung nicht-personenbezogener Daten gerichtet sind.

2.6 Generelle Datenschutzmaßnahmen bei RFID-Systemen

Bei allen datenschutzrechtlich relevanten RFID-Anwendungen ist zu fordern, dass

- der Grundsatz der Erforderlichkeit der Datenverarbeitung beachtet wird,
- dem Grundsatz der Datensparsamkeit folgend die Systeme so gestaltet werden, dass so weit wie möglich auf die Verarbeitung personenbezogener Daten verzichtet wird,
- die Bürgerinnen und Bürger stets erkennen können, wenn eine Ware mit dieser Technik ausgestattet ist; ferner muss zu erkennen sein, welche Daten damit verarbeitet werden und welche Art der Datenverarbeitung damit ermöglicht wird,
- technische Maßnahmen gegen das unbefugte Auslesen von auf RFID-Tags gespeicherten Daten und das Abhören der drahtlos übertragenen Daten ergriffen werden,
- den Betroffenen die Möglichkeit geboten werden sollte, die Funktion der RFID-Tags zu deaktivieren, sofern diese ihre Aufgabe erfüllt haben.

Insbesondere hinsichtlich des Umgangs mit RFID-Tags, die nicht unmittelbar der Verarbeitung personenbezogener Daten dienen sollen, bleibt abzuwarten, ob deren Anbieter die hier dargestellten Maßnahmen ergreifen. Sofern dies nicht in ausreichendem Maße geschieht, ist eine entsprechende gesetzliche Verpflichtung zu erwägen.

3. Dokumentenmanagementsysteme

Die Einführung durchgängiger elektronischer Arbeitsabläufe rückt neben der Verbesserung der Kommunikationsinfrastruktur (z. B. durch virtuelle Poststellen) oder der Erreichbarkeit interaktiver Bürgerdienste (z. B. durch Einrichtung von Internet-Portalen) auch dienststelleninterne Veränderungen in den Blickpunkt. Dokumentenmanagementsysteme sollen die Sachbearbeitung zunehmend von der Notwendigkeit entlasten, sich zu einem Vorgang stets erst die Papierakten kommen zu lassen und sich ggf. erst noch mit anderen Kollegen abzustimmen, die diese Akten zur gleichen Zeit ebenfalls benötigen. Außerdem zielen die entsprechenden Vorhaben darauf ab, einen „elektronischen Aktenlauf“ einzurichten. Einige Bundesländer haben bereits Projekte auf den Weg gebracht, die dazu führen sollen, dass derartige Systeme in der gesamten Landesverwaltung eingeführt werden.

Auch in Baden-Württemberg befasst sich der vom Innenministerium geleitete und mit Fragen ressortübergreifender IuK-Projekte betraute Arbeitskreis Informationstechnik mit der Auswahl eines für die Zwecke der Landesverwaltung geeigneten Dokumentenmanagementsystems, das das bisherige, als technisch überholt geltende Verfahren ersetzen soll. Auch wenn dieser Auswahlprozess noch am Anfang steht, ist es wichtig, bereits jetzt zu berücksichtigen, dass ein solches Vorhaben stets auch die möglichen datenschutzrechtlichen Auswirkungen im Blick haben muss. Aus Sicht des Datenschutzes kommt dabei der Gewährleistung des Zugriffsschutzes zentrale Bedeutung zu. Ganz entscheidendes Merkmal eines jeden solchen Systems muss sein, dass sich darin genau festlegen lässt, welche Nutzer auf welche Dokumente zugreifen dürfen. Auch bei der Nutzung elektronischer Systeme dürfen jedem Bediensteten nur die Möglichkeiten zum Zugriff auf diejenigen Daten gewährt werden, die er zur Erfüllung seiner dienstlichen Aufgaben benötigt.

Bei einer im Arbeitskreis Informationstechnik geführten Diskussion zu diesem Thema zeigte sich freilich, dass aus dem Kreis der IuK-Verantwortlichen teilweise ganz andere Erwartungen mit einem elektronischen Dokumentenmanagementsystem verbunden werden. Es wurde deutlich, dass die bisherige Form des Umgangs mit Papierakten sowie mit elektronischen Do-

kumenten aus Sicht einiger IuK-Verantwortlicher zu viele Einschränkungen für einen Zugriff auf Unterlagen mit sich bringe und sie sich stattdessen eine einfache Such- und Zugriffsmöglichkeit innerhalb des gesamten Dokumentenbestands wünschen. Die Suche soll dabei – so die in einem Diskussionsbeitrag geäußerte Vorstellung – so einfach zu handhaben sein wie die mit Google oder mit einer vergleichbaren Suchmaschine im Internet durchgeführte Informationssuche. Dabei rückte neben den bislang schon auf zentralen Servern abgelegten elektronischen Dokumentenbeständen auch beispielsweise der Inhalt persönlicher E-Mail-Postfächer der Bediensteten ins Blickfeld.

Zwar ist es verständlich, dass die Verwaltung die Einführung eines geeigneten Dokumentenmanagementsystems anstrebt, um zu erreichen, dass sich vorhandene Dokumente leichter finden lassen. Dabei darf die Verwaltung aber nicht über das Ziel hinausschießen. Es muss sichergestellt sein, dass jeder Nutzer nur solche Suchergebnisse angezeigt erhält und nur auf solche personenbezogenen Informationen zugreifen kann, die er zur Erfüllung seiner dienstlichen Aufgaben benötigt. Zweifellos stellt dies eine anspruchsvolle Aufgabe dar: Denn durch die mit der Einführung eines neuen Systems verbundene Erwartung, viel mehr Datenbestände erfassen zu können, als dies bislang möglich war, wachsen auch die Anforderungen an die Festlegung und Fortschreibung sachgerechter Zugriffsberechtigungen für die in all diesen Datenbeständen enthaltenen Dokumente. Da bei der Auswahl eines solchen Dokumentenmanagementsystems der Aspekt der nutzerfreundlichen Handhabbarkeit eine entscheidende Rolle spielt, sollte zudem darauf geachtet werden, dass jedes in die engere Wahl gezogene System nicht nur überhaupt die Möglichkeit bietet, eine entsprechende Zugriffsberechtigungsverwaltung vorzunehmen, sondern dass auch diese Möglichkeiten komfortabel ausgestaltet sind.

4. eGovernment

Wer sich heutzutage mit dem EDV-Einsatz in der Verwaltung auseinander setzt, kommt um den Begriff eGovernment nicht herum. Nicht alle Beteiligten verstehen hierunter das Gleiche: Mitunter richtet sich der Blick vorwiegend auf elektronische Datenflüsse, die zwischen Verwaltung und Bürgern oder zwischen Verwaltung und Unternehmen stattfinden. Während mittlerweile vielen Beteiligten diese Sichtweise zu eng ist und der Blick daher vielfach auch auf verwaltungsinterne Datenflüsse gerichtet wird, wird möglicherweise nicht jeder bereit sein, eGovernment so umfassend zu sehen, wie es die Landesverwaltung im Rahmen ihrer eGovernment-Richtlinie tut: Dort wird jedes IuK-Vorhaben der Verwaltung zum eGovernment gezählt. Zur besseren Einordnung der folgenden Ausführungen sei darauf hingewiesen, dass wir unter eGovernment-Projekten solche verstehen, die darauf gerichtet sind, elektronische Wege zur Kommunikation zwischen Verwaltung und Bürgern einzurichten und auch verwaltungsintern elektronische Wege zur Bearbeitung einer bestimmten Art von Vorgängen einzurichten. Unter diesem Blickwinkel waren in den vergangenen Monaten für uns folgende Aspekte des eGovernment von besonderer Bedeutung:

4.1 Virtuelle Poststellen

Der Austausch von E-Mails ist mittlerweile zum festen Bestandteil heutiger Kommunikation zwischen Bürgern und Behörden sowie zwischen Behörden untereinander geworden. Ohne weitere Schutzmaßnahmen sind über Internet versandte E-Mails wegen der fehlenden Vertraulichkeit jedoch nicht zur Übertragung schutzbedürftiger Dokumente geeignet. Ebenso wenig sind diese geeignet, wenn Absender und Empfänger sicherstellen wollen, dass der Absender zuverlässig als solcher zu identifizieren ist. Um einen E-Mail-Austausch zu ermöglichen, der auch diesen Anforderungen gerecht wird, müssen sich die Dienststellen darauf vorbereiten, auch den Austausch verschlüsselter und digital signierter Dokumente zu ermöglichen. Da die Bearbeitung derartiger E-Mails zusätzliche Arbeitsschritte und entsprechendes Know-how erfordert, beabsichtigen manche Dienststellen, diese Funktionen dienststellenintern oder sogar dienststellenübergreifend in einer sog. virtuellen Poststelle zu bündeln.

Zwar stellen Behörden im Einzelnen oft unterschiedliche Anforderungen an eine solche virtuelle Poststelle. In der Regel soll sie aber zumindest folgende Grundfunktionen erfüllen:

– Entschlüsselung eingehender E-Mails,

– Verschlüsselung ausgehender E-Mails,

– Überprüfung der Signaturen eingehender E-Mails sowie das

– Signieren ausgehender E-Mails.

Darüber hinaus sollen virtuelle Poststellen mitunter auch

– eingehende Nachrichten auf Computerviren oder andere schädliche Inhalte überprüfen,

– behördeninterne E-Mail-Adressbücher und Schlüsselverzeichnisse pflegen,

– elektronische Laufzettel für die empfangenen elektronischen Dokumente erzeugen und diese gemeinsam mit den Dokumenten an die zuständigen Bearbeiter weiterleiten,

– ein- oder ausgehende Nachrichten mit einem Zeitstempel versehen.

Eine virtuelle Poststelle erfüllt somit im Einzelfall ganz unterschiedliche, meist jedoch komplexe Funktionen in vernetzten IuK-Umgebungen. Ein solches Projekt wirft daher zahlreiche datenschutzrechtliche Fragen auf. Gerade wegen der vielfältigen möglichen Erscheinungsformen virtueller Poststellen gibt es dafür auch von Seiten des Datenschutzes keine Patentlösung. Vielmehr ist jede ins Auge gefasste Lösung auf die damit einhergehenden datenschutzrechtlichen Auswirkungen zu überprüfen. Gleichwohl lassen sich einige allgemeine Hinweise geben, welche Datenschutzprobleme sich bei der Realisierung einer virtuellen Poststelle ergeben können und wie damit umgegangen werden kann:

– Vertraulichkeit empfangener Nachrichten

  Wenn die virtuelle Poststelle verschlüsselte Nachrichten entschlüsselt, so haben die dort beschäftigten Bediensteten im Rahmen der für sie gewährten Zugriffsberechtigungen die Möglichkeit, die Nachrichten im Klartext zu lesen. Dies kann insbesondere dann ein Problem darstellen, wenn es sich bei den übertragenen Inhalten um besonders schutzbedürftige Daten handelt, die vor ihrer Zustellung an den Empfänger (z. B. einen Sozialarbeiter oder einen Amtsarzt) nicht von anderen Bediensteten zur Kenntnis genommen werden dürfen. Dieses Problem ergibt sich in verstärktem Maße bei dienststellenübergreifenden virtuellen Poststellen.

  Ein datenschutzgerechter Umgang mit dieser Problematik kann so aussehen, dass die virtuelle Poststelle nur solche verschlüsselten Nachrichten entschlüsselt, die explizit an eine der virtuellen Poststelle zugeordnete E-Mail-Adresse (z. B. poststelle@behörde.de) gesandt wurden. Hingegen sollte – auch wenn dies technisch ermöglicht werden könnte – nicht zugelassen werden, dass Bedienstete der virtuellen Poststelle auch solche Nachrichten entschlüsseln, die an die persönlichen E-Mail-Adressen einzelner Bediensteter gerichtet wurden und die unter Umständen sogar mit einem für diese Bediensteten individuell ausgestellten Schlüssel verschlüsselt wurden.

  Eingehende Nachrichten, die an Organisationseinheiten gerichtet sind, in denen besonders sensible Daten verarbeitet werden (innerhalb eines Landratsamts etwa an das Sozial- oder Jugendamt, die (Schul-)Psychologische Beratungsstelle oder das Gesundheitsamt) sollten nicht in der virtuellen Poststelle entschlüsselt werden können. Stattdessen sollten dafür amtsbezogene Postfächer eingerichtet werden, auf die nur eine amtsinterne Poststelle Zugriff hat. Soweit die Daten der ärztlichen Schweigepflicht oder einem anderen besonderen Berufsgeheimnis unterliegen, sollte eine verschlüsselte Kommunikation nur mit dem jeweiligen Bediensteten ermöglicht werden.

– Signatur ausgehender Dokumente

Sofern die virtuelle Poststelle ausgehende Dokumente mit qualifizierten elektronischen Signaturen versehen soll, ist zu berücksichtigen, dass derartige Signaturen nicht im Namen einer Behörde, sondern stets nur im Namen einer natürlichen Person, hier also eines Bediensteten der virtuellen Poststelle erfolgen können. Da die qualifizierten Signaturen rechtlich vielfach auf eine Stufe mit eigenhändigen Unterschriften gestellt werden, sollte Folgendes beachtet werden:

- Es sollte nicht zugelassen werden, dass jemand mit fremdem Namen signiert (etwa weil ihm der zur Signatur Berechtigte seine Signaturkarte sowie die zur Nutzung erforderliche PIN zur Verfügung stellt).
- Es sollte ferner nicht zugelassen werden, dass eine Vielzahl von Dokumenten von einem Programm und ohne individuelle Mitwirkung des Signaturinhabers signiert werden.
- Außerdem sollte bei jedem Signaturvorgang sichergestellt werden, dass der zur Signatur Berechtigte den Signaturvorgang veranlasst. Das bedeutet, dass es bei eingesteckter Signaturkarte nicht genügt, nur einmal am Tag, etwa nach dem Einschalten des PCs, die zur Nutzung des Signaturschlüssels erforderliche PIN einzugeben. Denn ansonsten könnten auch Dritte, die zufällig in die Nähe des PCs kommen, per Mausklick Signaturen unter fremdem Namen vornehmen. Um dies zu verhindern, sollte bei jedem Signaturvorgang die PIN eingegeben werden (keine Signatur auf Mausklick).

– Outsourcing der virtuellen Poststelle

Übernimmt die Dienststelle die Funktion der virtuellen Poststelle nicht selbst, sondern will sie damit einen öffentlichen oder privaten Auftragnehmer betrauen, so sind dabei die Anforderungen an eine derartige Datenverarbeitung im Auftrag einzuhalten. Der Auftrag ist beispielsweise schriftlich zu erteilen und es sind darin u. a. die vom Auftragnehmer zu ergreifenden technischen und organisatorischen Sicherheitsmaßnahmen zu dokumentieren. Gleichwohl bleibt der Auftraggeber für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich.

Beim Outsourcing der virtuellen Poststelle verschärfen sich die mit der Signatur ausgehender Nachrichten verbundenen Probleme hinsichtlich der Zeichnungsbefugnisse: Bedienstete eines Unternehmens, die möglicherweise auch ausgehende Nachrichten signieren sollen, dürfen dies jedoch nicht mit Signaturen tun, die den Eindruck erwecken, die Bediensteten gehörten der Auftrag gebenden Behörde an.

– Berücksichtigung des Telekommunikations- und Teledienstерechts

Bei den über eine virtuelle Poststelle erbrachten Dienstleistungen kann es sich auch um Telekommunikationsdienste (z. B. im Fall der E-Mail-Weiterleitung) oder um Teledienste (z. B. im Fall einer interaktiv nutzbaren Web-Mail-Oberfläche) handeln. In diesen Fällen sind die Datenschutzvorschriften des Telekommunikationsgesetzes (z. B. Wahrung des Fernmeldegeheimnisses bei den erbrachten Telekommunikationsdienstleistungen) oder des Teledienstegesetzes sowie des Teledienstedatenschutzgesetzes zu beachten.

– Weitere Informationen zum Datenschutz bei virtuellen Poststellen

Unter Leitung des Landesbeauftragten für den Datenschutz Niedersachsen wurde die Handreichung „Die virtuelle Poststelle im datenschutzgerechten Einsatz“ erarbeitet. Dieses auch über das Internet-Angebot unserer Dienststelle *(www.baden-wuerttemberg.datenschutz.de)* abrufbare Dokument behandelt datenschutzrechtliche Fragestellungen, die sich insbesondere auf solche Lösungen beziehen, die unter Verwendung des ursprünglich für Bundesbehörden entwickelten Produkts

„VPS des Bundes“ (Vers. 2.0) sowie der Basiskomponente „Datensicherheit“ des Vorhabens BundOnline 2005 realisiert werden.

Ferner behandelt auch das Bundesamt für Sicherheit in der Informationstechnik in seinem „E-Government-Handbuch“ *(www.bsi.bund.de/fachthem/egov/vps.htm)* datenschutzrechtliche Fragen hinsichtlich der Realisierung einer virtuellen Poststelle.

4.2 Das Problem unklarer Zuständigkeiten

Die Vernetzung behördlicher EDV-Systeme ermöglicht mittlerweile die dienststellenübergreifende, elektronische Verarbeitung personenbezogener Daten, etwa im Rahmen elektronischer Bürgerdienste. Zudem ermöglicht die Vernetzung, dass EDV-technische Unterstützungsleistungen räumlich weit entfernt von den rechtlich verantwortlichen Dienststellen durchgeführt werden können. Ein Beispiel stellt das Verfahren ELSTER-Lohn dar (s. 4. Teil, 4. Abschnitt, Nr. 2): Dabei nutzen alle Länder eine bundesweit einheitliche, aber nur von zwei Länderfinanzverwaltungen betriebene EDV-Infrastruktur. ELSTER-Lohn ist dabei beileibe nicht das einzige Beispiel für diese Entwicklung: Bei dem Verfahren E-Stat (s. 4. Teil, 3. Abschnitt, Nr. 3) kooperieren Schulen, die Regierungspräsidien, das Statistische Landesamt sowie das Kultusministerium bei der Verarbeitung personenbezogener Daten insbesondere von Schülern, Erziehungsberechtigten und Lehrern. Im Rahmen der Verwaltungsreform in Baden-Württemberg wurde ferner ausdrücklich die Möglichkeit sog. „gemeinsamer Dienststellen“ geschaffen, bei denen Mitarbeiter unterschiedlicher Stellen unter einem Dach zusammenarbeiten. Schließlich nutzen auch die zur Betreuung der Hilfeempfänger des Arbeitslosengeldes II eingerichteten Arbeitsgemeinschaften zwischen der Bundesagentur für Arbeit und den Stadt- und Landkreisen von der Bundesagentur entwickelte und betriebene Datenverarbeitungsverfahren. Im Rahmen der Realisierung von eGovernment-Anwendungen nehmen aber nicht nur solche Kooperationen mehrerer öffentlicher Stellen zu, sondern es werden vermehrt auch Möglichkeiten zur Zusammenarbeit zwischen öffentlichen und privaten Stellen gesucht. Als Beispiel hierfür können medizinische Forschungsprojekte dienen, bei denen vielfach zahlreiche öffentliche und private Stellen intensiv zusammenarbeiten.

Mit diesen Entwicklungen befasst sich auch ein Positionspapier des „Strategiezirkels eGovernment“ der Kommunalen Gemeinschaftsstelle für Verwaltungsvereinfachung (KGSt). Danach könne sich die Verwaltung künftig darauf beschränken, gegenüber den Bürgern ein „Front-Office“ einzurichten, an das sich die Bürger mit ihren Anliegen wenden können. Die in dem Positionspapier als „Produktion“ bezeichnete Bearbeitung dieser Anliegen könne anschließend unabhängig davon in einem sog. BackOffice erfolgen, das weder räumlich noch organisatorisch mit der örtlichen Verwaltung verbunden sein muss. Folgende Zitate mögen verdeutlichen, mit welchen Veränderungen die KGSt in diesem Zusammenhang rechnet:

„ ... Die Produktion der Leistungen im BackOffice erfolgt seltener als heute in der Verwaltung selbst. Vielmehr bewegt sich die Verwaltung in einem vielfältigen Geflecht von arbeitsteiligen Leistungsprozessen, von öffentlichen und privaten Akteuren. ...

Die Verwaltung versteht sich weniger als Produzent, sondern mehr als Garant, Initiator, Partner in Netzwerken und Steuerer ...

Die Produktion erfolgt ... vermehrt auch außerhalb der Verwaltung oder in Mischformen in einem Produktionsnetzwerk mit öffentlichen und privaten Partnern. Dabei gewinnen externe Leistungserstellung und Mischformen erheblich an Bedeutung. ...“

Datenschutzrechtlich sind solche Formen der Kooperation keineswegs unzulässig. Schon seit jeher kennt das Datenschutzrecht die sog. Datenverarbeitung im Auftrag, bei der eine Stelle eine andere Stelle damit beauftragen kann, bestimmte Datenverarbeitungsaufgaben für sie durch-

zuführen. Datenschutzrechtlich bleibt der Auftraggeber dabei für die Einhaltung der Datenschutzvorschriften auch in den Phasen der Datenverarbeitung verantwortlich, in denen diese vom Auftragnehmer durchgeführt wird. Mitunter soll bei einer Kooperation verschiedener Stellen der Auftragnehmer aber nicht nur eine Bearbeitung nach den Weisungen des Auftraggebers vornehmen, sondern es soll ihm beispielsweise auch zugestanden werden, Ermessensentscheidungen eigenständig zu treffen. In einem solchen Fall spricht man von einer Funktionsübertragung. Die mit der heutigen, vernetzten EDV-Infrastruktur möglich gewordenen Kooperationsformen können in vielfältiger Weise von diesen Möglichkeiten Gebrauch machen. Datenschutzrechtlich ist dabei entscheidend, dass neben den Rollen, die die einzelnen Beteiligten dabei einnehmen, auch geklärt wird, in welchem Ausmaß jeder einzelne Beteiligte für die im gemeinsamen Projekt durchgeführte Verarbeitung personenbezogener Daten verantwortlich ist. Fehlt es daran, wirft dies nicht selten erhebliche datenschutzrechtliche Probleme auf. Bereits die Beantwortung der Frage, welches Datenschutzrecht für welche Teile der gemeinschaftlich durchgeführten Datenverarbeitungsvorgänge anzuwenden ist, setzt eine klare Zuständigkeitsabgrenzung voraus. Als Folge davon ist bei einem solchen Projekt mitunter auch nicht mehr auf Anhieb zu erkennen, welche Datenschutz-Aufsichtsbehörde für die Kontrolle des Datenschutzes in diesem Projekt zuständig ist. Leider stellen wir in unserer Beratungs- und Kontrolltätigkeit immer wieder Unzulänglichkeiten hinsichtlich der nötigen Abgrenzung der Rollen, Aufgaben und Verantwortlichkeiten der an einem Projekt Beteiligten fest. Hier seien nur drei Beispiele dafür genannt:

– Für das gemeinsam von den Länderfinanzministerien und dem Bundesministerium der Finanzen genutzte Verfahren ELSTER-Lohn fehlen ausreichend klare Vereinbarungen der kooperierenden Finanzverwaltungen, aus denen sich ergibt, wer dabei datenschutzrechtlich für die Verarbeitung personenbezogener Daten verantwortlich ist (s. auch 4. Teil, 4. Abschnitt, Nr. 2).

– Im Rahmen unserer Beratung des Kultusministeriums hinsichtlich der datenschutzrechtlichen Grundlagen für das Projekt E-Stat lag ein inhaltlicher Schwerpunkt auf der Erörterung der Frage, inwieweit zum einen das Kultusministerium und zum anderen die Schulen für die in E-Stat vorgesehene Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich sein können.

– Hinsichtlich der für die Bearbeitung der Anträge auf Arbeitslosengeld II zuständigen Arbeitsgemeinschaften zwischen der Bundesagentur für Arbeit und den Stadt- und Landkreisen ist leider festzustellen, dass die beteiligten Akteure völlig unterschiedliche Auffassungen über den rechtlichen Status der Arbeitsgemeinschaften haben. Dies zieht auch Probleme bei der datenschutzrechtlichen Beurteilung der von den Arbeitsgemeinschaften sowie der Bundesagentur gemeinsam genutzten EDV-Verfahren nach sich (s. Anhang 9).

Um diesen Schwierigkeiten aus dem Weg zu gehen, ist bei solchen Projekten von Anfang an für die notwendige datenschutzrechtliche Klarheit zu sorgen. Insbesondere sollte dieses Anliegen bei der Abfassung schriftlicher Vereinbarungen über die gemeinsame Durchführung des Vorhabens sowie bei der Formulierung mitunter notwendiger Rechtsvorschriften berücksichtigt werden.

4.3 Überprüfung der Identität bei elektronischer Antragstellung

Sieht eine öffentliche Stelle eine elektronische Antragstellung vor, muss sie damit rechnen, dass ihr gelegentlich auch manipulierte Anträge, z. B. Anträge unter falschem Namen, zugehen. Sie muss daher auch dafür sorgen, dass sie zuverlässig erkennen kann, ob die als Antragsteller bezeichnete Person den entsprechenden Antrag tatsächlich hat stellen wollen. Die sorgfältige Beachtung dieses Aspekts ist auch von entscheidender datenschutzrechtlicher Relevanz: Wenn es nämlich möglich wäre, im Rahmen eines solchen elektronischen Bürgerdienstes Anträge oder Erklärungen im Namen Dritter abzugeben, die davon gar

nichts wissen, so könnte dies dazu führen, dass die Behörde falsche personenbezogene Daten über diesen Dritten speichert, verarbeitet oder an andere Stellen übermittelt.

Dass diese Frage auch in der Praxis von Bedeutung ist, zeigte sich in diesem Jahr im Zusammenhang mit dem von der Steuerverwaltung vorgesehenen Verfahren zur elektronischen Datenübermittlung für die Lohnsteuer-Anmeldung sowie die Umsatzsteuer-Voranmeldung:

– Das Antragsverfahren

  Unternehmen, die der Steuerverwaltung regelmäßig Angaben im Rahmen der Lohnsteuer-Anmeldung sowie der Umsatzsteuer-Voranmeldung machen müssen, sind seit Anfang 2005 verpflichtet, diese Angaben grundsätzlich in elektronischer Form zu übermitteln. Das Bundesfinanzministerium und die Finanzministerien der Länder stellen den Unternehmen dazu spezielle Computerprogramme zur Verfügung.

– Datenschutzrechtliche Risiken

  Zur Identifizierung des Steuerpflichtigen muss dabei neben dessen Namen auch dessen Steuernummer angegeben werden. Da die meldepflichtigen Unternehmen diese Steuernummer auch auf ihren Rechnungen angeben müssen, erscheint es nicht ausgeschlossen, dass jemand, dem diese Informationen über einen Dritten bekannt sind, eine solche elektronische Datenübermittlung an die Steuerverwaltung unter dessen Namen vornimmt. Sofern die Steuerverwaltung eine derart manipulierte Mitteilung als authentisch ansieht, können diese Angaben zur Steuerveranlagung herangezogen werden und auf diese Weise unter Umständen auch eine Zahlungsforderung der Steuerverwaltung gegenüber dem Unternehmer begründen.

– Reaktion der Finanzministerien

  Das hiesige Finanzministerium hat die Manipulationsanfälligkeit des Steueranmeldungsverfahrens bestätigt und den Verzicht auf eine elektronische Unterschrift u. a. mit dem Ziel der Verfahrensvereinfachung in diesem weitgehend automatisierten und bearbeiterlosen Massenverfahren begründet. Zudem hat es auf eine geringe Zahl aufgetretener Manipulationsversuche sowie auf das aus seiner Sicht „überschaubare Risikopotential“ verwiesen und sieht daher keinen „akuten Handlungsbedarf“. Gleichwohl – und das ist aus meiner Sicht die entscheidende Mitteilung – stellt es Abhilfe in Aussicht. Im kommenden Jahr sollen die Manipulationsmöglichkeiten durch ein in das elektronische Mitteilungssystem integriertes Authentifizierungsverfahren beseitigt werden, das zur Überprüfung der Identität der Antragsteller dienen soll.

  Auch wenn es bislang nicht zu einer größeren Zahl von Missbrauchsfällen gekommen ist, bleibt festzustellen, dass die Steuerverwaltung mit der Entscheidung, die elektronische Meldung zum einen verbindlich vorzuschreiben, es zum anderen aber an den zur Prüfung der Authentizität erforderlichen Maßnahmen fehlen zu lassen, wohl kaum dazu beitragen konnte, die Akzeptanz elektronischer Bürgerdienste zu fördern. Es bleibt zu hoffen, dass mit dem in Aussicht gestellten geänderten Verfahren die bestehenden Mängel künftig ausgeräumt werden können. Anbieter vergleichbarer elektronischer Dienstleistungen sollten daraus die Lehre ziehen und jeweils von vornherein Maßnahmen einplanen, anhand derer sich die Identität der Antragsteller zuverlässig überprüfen lässt.

4.4 Portal „service-bw“

Um den Bürgern des Landes im Internet eine zentrale Anlaufstelle für elektronische Bürgerdienste anzubieten, richtete das Innenministerium das Internetportal www.service-bw.de ein. In früheren Jahren haben wir bereits mehrfach zu den mit diesem Portal verbundenen Datenschutz-

fragen Stellung genommen (vgl. 24. Tätigkeitsbericht, LT-Drucksache 13/2650, 23. Tätigkeitsbericht, LT-Drucksache 13/1500, 22. Tätigkeitsbericht, LT-Drucksache 13/520). In diesem Jahr wurden zusätzliche Portalfunktionen freigeschaltet, die erneut datenschutzrechtliche Fragen aufwarfen. Dabei ging es insbesondere um Funktionen, mit denen Nutzer eine Regionalisierung und eine Kategorisierung des Angebots durchführen können sowie um die Funktion des sog. One-Stop-Government:

Regionalisierung und Kategorisierung:

- Im Fall der Regionalisierung können die Nutzer einen Ort auswählen, der bei der weiteren Nutzung der Portalfunktionen als örtliche Voreinstellung verwendet wird. Die Nutzung im Portal könnte dann beispielsweise wie folgt aussehen: Sucht eine Bürgerin oder ein Bürger die Anschrift der Kfz-Zulassungsstelle, so präsentiert das Portal die Anschrift der für den voreingestellten Ort zuständigen Kfz-Zulassungsstelle.
- Im Fall der Kategorisierung können sich die Nutzenden einer oder zwei Personengruppen zuordnen (z. B. Zuordnung zur Gruppe „Studierende“). Bei der weiteren Nutzung präsentiert das Portal an den Stellen, an denen es unterschiedliche Informationen für unterschiedliche Personengruppen enthält, den Nutzern diejenigen Informationen, die sich speziell auf die von ihnen ausgewählten Personengruppen beziehen.

Die im Wege der Regionalisierung und der Kategorisierung voreingestellten Werte werden auf jeder Portalseite angezeigt und können jederzeit geändert werden.

Diese Funktionen können ohne vorherige Registrierung genutzt werden. In diesem Fall stehen die voreingestellten Werte nur für die Dauer der Session zur Verfügung. Nutzer, die diese voreingestellten Werte auch bei kommenden Nutzungen verwenden und nicht jedes Mal erneut eingeben wollen, können die im Rahmen der Regionalisierung und Kategorisierung ausgewählten Werte im Portal hinterlegen. Die Nutzenden müssen dazu eine von ihnen frei wählbare Benutzerkennung eingeben. Es entspricht den Anforderungen an eine datenschutzfreundliche Systemgestaltung, dass sie dabei nicht ihren Namen eingeben müssen, sondern auch eine frei gewählte Bezeichnung verwenden können. Datenschutzfreundlich ist daran auch, dass die Nutzenden jederzeit die Löschung der Benutzerkennung sowie der dazu hinterlegten Daten veranlassen können.

One-Stop-Government (OSG):

Den Nutzern des One-Stop-Government stehen zum einen die Funktionen der Regionalisierung und Kategorisierung zur Verfügung. Zum anderen können sie personenbezogene Daten im Portal hinterlegen. Spezielle eBürgerdienste, die auf diese Funktion hin abgestimmt sein müssen, bieten den Nutzenden die Möglichkeit, die hinterlegten Daten per Mausklick in elektronische Antragsformulare zu übernehmen. Es handelt sich hierbei um ein Angebot, das den Nutzenden die wiederholte Eingabe dieser personenbezogenen Daten ersparen soll. Die OSG-Funktion ist wie folgt realisiert:

- Die Funktion OSG wird nur für Nutzer angeboten, die sich mit Hilfe einer Chipkarte identifizieren.
- Im Portal können gegenwärtig folgende Angaben hinterlegt werden: Titel, Nachname, Namensbestandteil, Vorname, Rufname, Geburtstag, Hausnummer, Postleitzahl, Straße, Wohnort. Dabei steht es den Nutzenden frei, ob sie alle, einige oder keines der Felder ausfüllen.
- Die Nutzer sehen in allen Fällen, welche personenbezogenen Daten in ein Formular übernommen werden, und können diese vor Absenden des Formulars ändern.

– Die im Portal hinterlegten personenbezogenen Daten werden verschlüsselt gespeichert. Meldet sich ein Bürger mit seiner Chipkarte am Portal an, so werden die hinterlegten Daten mit Hilfe eines auf der Chipkarte gespeicherten Schlüssels entschlüsselt und stehen dann bis zum Ende der Session unverschlüsselt zur Nutzung zur Verfügung.

– Melden sich Nutzer 24 Monate lang nicht mit ihrer Chipkarte am Portal an, so werden deren Benutzerkennungen sowie die von ihnen im Portal hinterlegten Daten automatisch gelöscht.

Da die für diese Funktionen erstellten Sicherheitskonzeptionen aus Sicht des Datenschutzes noch verbesserungsbedürftig waren, forderten wir das Innenministerium zu entsprechenden Änderungen auf. Neben der Präzisierung der Rechtsgrundlagen für die mit der OSG-Funktion verbundene Verarbeitung personenbezogener Daten kam es uns dabei vor allem darauf an, dass die in den Erläuterungen zum OSG gegebenen Zusicherungen hinsichtlich des Zugriffsschutzes tatsächlich zuverlässig umgesetzt werden. Dies war bislang nicht ausreichend der Fall. Das Innenministerium hat inzwischen mitgeteilt, dass es unsere Hinweise beachten wird.

5. Vorratsdatenspeicherung von Telekommunikations- und Internet-Verbindungsdaten

Wenn heute jemand ein Telefonat führt, eine SMS sendet, ein Fax verschickt oder sich ins Internet einwählt, werden darüber bei den Telekommunikationsunternehmen sog. Verbindungsdaten gespeichert. In diesen, vorrangig der Abrechnung dienenden Datensätzen erfassen die Telekommunikationsunternehmen, von welchem Anschluss aus wann mit welchen anderen Anschlüssen Telefonate oder andere Kommunikationsverbindungen zustande kamen. Selbst wenn sich diesen Angaben nicht entnehmen lässt, um welche Inhalte es bei den Telefonaten, den SMS, den Telefax-Sendungen und den Internet-Verbindungen ging, stellen diese Verbindungsdaten sensible Daten dar. Denn sie gewähren bereits detaillierte Einblicke in die Lebens- und Verhaltensweisen der Kommunikationsteilnehmer. Aufgrund dessen unterliegen die Verbindungsdaten auch dem durch Artikel 10 des Grundgesetzes garantierten Fernmeldegeheimnis.

In der Vergangenheit wurde immer wieder erörtert, in welchen Fällen Telekommunikationsunternehmen solche Verbindungsdaten an Strafverfolgungsbehörden herauszugeben haben. Bislang können diese oder andere Sicherheitsbehörden von Telekommunikationsunternehmen in bestimmten, gesetzlich festgelegten Fällen Auskunft über diejenigen Verbindungsdaten verlangen, die die Telekommunikationsunternehmen zur Erstellung ihrer Rechnungen oder für andere gesetzlich zugelassene Zwecke speichern. Strafverfolgungs- und andere Sicherheitsbehörden beklagen dabei mitunter, dass ihre Auskunftsersuchen unbeantwortet bleiben, da das Telekommunikationsunternehmen die gewünschten Verbindungsdaten bereits gelöscht hat. Sie fordern deshalb bereits seit längerem, die Telekommunikations- sowie die Internet-Diensteanbieter zu verpflichten, Verbindungsdaten, die Auskunft über die Nutzung der Dienstleistungen geben, selbst dann für eine bestimmte Mindestdauer zu speichern, wenn das Unternehmen diese Daten zur Abrechnung oder anderen gesetzlich zugelassenen Zwecken gar nicht oder nicht mehr benötigt.

– Mit mehreren Initiativen versuchte der Bundesrat in der Vergangenheit, eine Vorratsspeicherung für Telekommunikationsverbindungsdaten einzuführen. Diese scheiterten jedoch an der ablehnenden Haltung der Bundesregierung.

– Im vergangenen Jahr beantragten Frankreich, Irland, Schweden und Großbritannien, durch einen Ministerratsbeschluss der EU eine Vorratsspeicherung von Verbindungsdaten auf europäischer Ebene einzuführen. Datenschutzrechtlich höchst bedenklich war daran nicht nur, dass eine Speicherdauer von bis zu 36 Monaten ins Auge gefasst wurde, sondern auch, dass neben den Telekommunikationsdiensten wie Telefon, E-Mail und SMS auch die Nutzung sämtlicher Internet-Dienste erfasst werden

sollte. Aus Sicht des Datenschutzes war es daher sehr zu begrüßen, dass der Bundestag die Bundesregierung am 17. Februar 2005 aufgefordert hat, diese Pläne abzulehnen.

– Mittlerweile hat auch die EU-Kommission das Thema Vorratsdatenspeicherung aufgegriffen und einen Entwurf für eine entsprechende EU-Richtlinie vorgelegt. Darin ist vorgesehen, Telekommunikationsverbindungsdaten zwölf Monate lang und Internet-bezogene Verbindungsdaten sechs Monate lang aufzubewahren. Die Umsetzung dieses Vorschlags hätte zur Folge, dass nicht nur Daten über die an sämtlichen Telefongesprächen, SMS und Telefax-Sendungen beteiligten Kommunikationspartner erfasst werden, sondern etwa auch Zeitpunkt und Dauer der Einwahl ins Internet, die dabei zugeteilte IP-Adresse, Daten über den Versand jeder einzelnen E-Mail sowie stets auch die Standorte bei der Mobilkommunikation. Allein die auf diese Weise erfassten Standortdaten würden es mit sich bringen, dass für einen großen Teil der Bevölkerung europaweite Bewegungsprofile erstellt und für jeweils ein Jahr auf Vorrat gespeichert werden.

In den letzten Wochen haben auch das hiesige Innen- und das Justizministerium zu dem Thema Position bezogen:

– Das Innenministerium hält eine Vorratsdatenspeicherung wie im Entwurf der EU-Richtlinie vorgeschlagen, für unzureichend. Insbesondere sieht das Innenministerium die von der EU-Kommission geplante Sechsmonatsfrist für die Speicherung der Internet-Verbindungsdaten als zu kurz an und verlangt auch für diese eine mindestens zwölfmonatige Speicherdauer.

– Demgegenüber gehen dem Justizminister die Vorschläge der EU-Kommission deutlich zu weit. Ihn erinnerten diese, so erklärte er in einer Pressemitteilung, an ein „emsiges Eichhörnchen, das für den Winter Vorräte in einem Umfang sammle, der in keinem Verhältnis zum tatsächlichen Nutzen stehe“. Ferner bestehe „die Gefahr, dass eine sinnvolle Verwendung der Datenflut gar nicht mehr möglich ist und wir uns in einem gigantischen Datenberg verlieren“. Und da sei für ihn die Grenze der Verhältnismäßigkeit überschritten. Trotz dieser deutlichen Worte lehnt der Justizminister die Pläne zur Vorratsdatenspeicherung allerdings nicht per se ab, sondern plädiert für eine Vorratsdatenspeicherung von maximal drei Monaten.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich zuletzt im Rahmen ihrer Herbstkonferenz am 27. und 28. Oktober 2005 mit der Vorratsdatenspeicherung befasst und in einer Entschließung (s. Anhang 6) hierzu deutlich gemacht, dass sie ein solches Vorhaben unabhängig von der dafür vorgesehenen Speicherdauer ablehnen. Dabei stehen für sie folgende Aspekte im Mittelpunkt:

– Der Kommissionsvorschlag und erst recht der Ministerratsvorschlag würden zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung führen.

– Jede Person, die in Zukunft solche Netze nutzt, würde unter Generalverdacht gestellt.

– Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, wäre zum Scheitern verurteilt. Derartige Datenbestände würden Begehrlichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnten. Auch aus diesem Grund müsse bereits den ersten Versuchen, eine solche Vorratsdatenspeicherung einzuführen, entschieden entgegengetreten werden.

– Zudem sei eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten zu befürchten. Schon jetzt sei die Trennlinie zwischen Verbindungs- und Inhaltsdaten gerade bei der Internet-Nutzung nicht mehr zuverlässig zu ziehen. Dieselben unzutreffenden Argumente, die jetzt für eine flächendeckende Speicherung von Verkehrsdaten angeführt werden, würden nach deren Einführung alsbald auch für die anlassfreie Vorratsspeicherung von Kommunikationsinhalten ins Feld geführt werden.

Im Übrigen kann es auch bei der Diskussion derartiger Vorschläge hilfreich sein, einmal 25 Jahre in der Technikgeschichte zurückzublicken. Seinerzeit wurden Kommunikationsverbindungen noch mit elektro-mechanischen Anlagen vermittelt, die lediglich die Anzahl der in Anspruch genommenen Gebühreneinheiten, aber keine Angaben über die jeweiligen Kommunikationspartner, die Uhrzeit oder die Dauer der Verbindungen registrierten. In den heutigen digitalen Vermittlungsstellen der Telekommunikationsunternehmen werden dagegen für Abrechnungszwecke wesentlich detailliertere Verbindungsdaten gespeichert. Diese stehen den Sicherheitsbehörden schon heute bei Vorliegen der dafür relevanten gesetzlichen Voraussetzungen zur Verfügung. Die Ablösung der elektro-mechanischen durch digitale Vermittlungsstellen führte somit stillschweigend dazu, dass den Sicherheitsbehörden heutzutage weitaus umfassendere und detailliertere Informationen über das Kommunikationsverhalten der Bürger zur Verfügung stehen, als das noch vor Jahren der Fall war. Die Nutzung immer mehr elektronischer Kommunikationsdienste führt ebenso stillschweigend dazu, dass den Sicherheitsbehörden Informationen aus immer mehr Lebensbereichen zugänglich sind. Auch unter Berücksichtigung dieser Entwicklungen ist eine Ausweitung der Speicherung und Verarbeitung von Telekommunikations- und Internet-Verbindungsdaten als, wie sie mit der Vorratsdatenspeicherung einherginge, unverhältnismäßig anzusehen.

6. Datenschutz bei VoIP

Der Ausbau des Internets ist mittlerweile so weit fortgeschritten, dass an jedem Anschluss so viel Bandbreite zu konkurrenzfähigen Preisen zur Verfügung gestellt werden kann, dass Benutzer über das Internet auch miteinander telefonieren können. Hierfür wurde der Begriff VoIP (Voice over IP) geprägt. Die entsprechenden Protokolle wurden im Jahr 2002 definiert und stehen jetzt in Form von Anwendungen zur Verfügung. Findige Provider bieten ihren Kunden neben der reinen Internet-Telefonie auch an, Kommunikationspartner in herkömmlichen Telefonnetzen anzurufen bzw. von ihnen angerufen zu werden.

Technisch deckt VoIP ein breites Spektrum ab. Angefangen bei Telefonanlagen von Unternehmen, die von den Benutzern unbemerkt Gespräche in oder über das Internet vermitteln, bis zu Lösungen, bei denen mit Kopfhörer und Mikrofon ausgerüstete PCs und bestimmte darauf ablaufende Programme, sog. Softphones, herkömmliche Telefone überflüssig machen. Andere Lösungen sehen spezielle Telefone vor, die über einen LAN-Anschluss verfügen und mit Hilfe weiterer Server Verbindungen in das Internet aufbauen können.

Die Betreiber und Anbieter von herkömmlichen Telefondiensten unterliegen den gesetzlichen Regelungen des Telekommunikationsgesetzes. Insbesondere müssen sie in einem Sicherheitskonzept darlegen, dass sie Maßnahmen zur Gewährleistung des Fernmeldegeheimnisses ergriffen haben. Entsprechende gesetzliche Regelungen gibt es für VoIP noch nicht. Die Einbindung derjenigen Anbieter, die ihren Sitz in einem außereuropäischen Land haben, dürfte dabei noch besondere Probleme bereiten. Wie beim herkömmlichen Telefonsystem ist aber auch beim Telefonieren mit der VoIP-Technik zu verlangen, dass das Fernmeldegeheimnis gewahrt wird. Bei den technischen Maßnahmen, die ein Anbieter zum Schutz von personenbezogenen Daten ergreift, sind zwei Aspekte besonders zu beachten: Wie bei herkömmlichen Telefonsystemen muss die Vertraulichkeit der Mediendaten, d. h. der Daten der Sprach- und ggf. Bildkommunikation gewährleistet werden. Zum anderen können auch die Signaldaten, die zum Aufbau einer Verbindung ausgetauscht werden, personenbezogene Daten enthalten. Auch deren Vertraulichkeit muss gewahrt bleiben.

Während der Berichtsperiode wurden wir von Kommunen hinsichtlich der datenschutzrechtlichen Anforderungen an VoIP um Rat gebeten. Wir haben ihnen sinngemäß Folgendes geantwortet:

VoIP-Lösungen übertragen Daten, die auch personenbezogen sein können, über das öffentliche Internet. Damit ist die Kommunikation den gleichen Gefahren ausgesetzt, wie wir sie vom Surfen im WWW oder von der E-Mail her kennen. Zu nennen sind hier Programme, die es Unbefugten er-

lauben, einen PC fernzusteuern (Trojaner), Viren sowie Programme, mit denen Teilnehmer im Internet getäuscht werden können, indem man ihnen gefälschte Daten schickt. Auch besteht die Gefahr, dass durch bewusst herbeigeführte Störungen ein Internet-Telefonanschluss nicht genutzt werden kann (denial-of-service). Jeder einzelne Teilnehmer setzt sich bei der Nutzung von VoIP daher einem erheblichen zusätzlichen Risiko aus. Dass beispielsweise sog. Trojaner vor dem Fernmeldegeheimnis Halt machen und Telefonate über das Internet nicht ausspionieren, ist nicht zu erwarten.

Daneben gibt es weitere Gefahren, die mit der eingesetzten Technik zusammenhängen:

– Vertraulichkeit

  Die Vertraulichkeit von personenbezogenen Daten bei der Internet-Telefonie ist in verschiedener Hinsicht bedroht:

  • Verbindungsaufbau

    Der Aufbau einer Verbindung zwischen zwei Kommunikationspartnern wird bei VoIP wie beim herkömmlichen Telefonsystem durch Vermittlungsinstanzen hergestellt. Dabei wird häufig das Protokoll SIP (session initiation protocol) verwendet. Das Protokoll selbst bietet die Möglichkeit der Verschlüsselung bestimmter Teile der Kommunikation. Allerdings werden andere Teile im Klartext übertragen. Dieser Klartext könnte, wie bei E-Mail, an mehreren Stellen im Internet von Personen eingesehen werden. Im Gegensatz zum herkömmlichen Telefonsystem sind diese jedoch nicht auf das Fernmeldegeheimnis verpflichtet. Besonders problematisch ist die Übermittlung des Anrufers und des Angerufenen im Klartext dann, wenn einer der Kommunikationsteilnehmer zu einer Berufsgruppe gehört, die einem besonderen Berufsgeheimnis, wie beispielsweise Ärzte, unterliegt. Hier muss nicht nur der Inhalt des Gesprächs geschützt sein, sondern es dürfen auch die Kommunikationspartner nicht offenbart werden. Diese Gruppe von Bediensteten sollte, solange keine gesetzlichen Regelungen getroffen werden, von der Nutzung von VoIP für dienstliche Zwecke absehen, wenn die Kommunikation zwischen Teilnehmer und Vermittlungsinstanz oder zwischen zwei Vermittlungsinstanzen unverschlüsselt durchgeführt wird.

  • Mediendaten

    Nachdem die Verbindung zwischen zwei Kommunikationspartnern hergestellt wurde, weiß die Software der verwendeten Rechner, wo sich der jeweils andere Kommunikationspartner befindet. Jetzt können die Teilnehmer mit dem Telefongespräch beginnen. Die digitalisierten Sprachdaten werden dabei mit einem speziellen Protokoll in Echtzeit (real time protocol/RTP) direkt zwischen den Teilnehmern übertragen. Aber was heißt im Internet schon direkt? Dass keine exklusiv für das Gespräch geschaltete Leitung zwischen den teilnehmenden Stellen existiert, dürfte heutzutage allgemeiner Erkenntnisstand sein. Deshalb muss darauf geachtet werden, dass die Mediendaten verschlüsselt übertragen werden. Ansonsten könnten sie von Dritten abgehört werden. Entsprechende Programme, mit denen man in einem sog. LAN die unverschlüsselte Kommunikation mit RTP mithören kann, sind im Internet frei erhältlich. Die Entwickler des Protokolls haben diese Möglichkeit bedacht und festgelegt, dass der Standard VoIP mehrere Verschlüsselungsmechanismen, die bei der Übertragung der Mediendaten verwendet werden können, unterstützt. So kann beispielsweise das von https-Verbindungen im WWW her bekannte Verschlüsselungsverfahren SSL/TLS, die verschlüsselte Variante des RTP-Protokolls SRTP (secure RTP) oder die Standardverschlüsselung von TCP/IP namens IPSec verwendet werden. Da die Unterstützung von SSL/TLS durch Firewalls im Allgemeinen gegeben ist, spricht nichts dagegen, dass die Mediendaten von Telefongesprächen über das Internet verschlüsselt übertragen werden.

- Anrufumleitung

  Eine weitere Bedrohung besteht darin, dass Dritte, die sich netztechnisch zwischen Vermittlungsserver und Kommunikationspartner befinden, den Verbindungsaufbau umleiten könnten. Die dabei verwendete Technik – sog. spoofing – ist schon im Zusammenhang mit anderen Internet-Diensten bekannt.

– Authentifizierung

  Um dem VoIP-System mitzuteilen, dass ein Empfänger für Verbindungen bereit ist, meldet sich dieser bei der Vermittlungsstelle mit dem Protokoll SIP an. Das ist bei Telefonen, die jederzeit einen Anruf entgegennehmen können, kein Problem. Anders ist es bei sog. Softphones, d. h. einer Software, die wie beispielsweise ein E-Mail-Programm auf einem Rechner aufgerufen werden muss. Gelingt es beispielsweise jemandem in einem Rechnernetz, die Identität eines anderen anzunehmen, dann könnte er auch Anrufe in dessen Namen tätigen bzw. entgegennehmen. Und dies selbst dann, wenn der Betreffende an seinem Rechner sitzt. Denn genau wie bei vielen anderen Internet-Diensten können PCs von der Nutzung eines Dienstes ausgeschlossen werden, indem man den PC durch einen sog. Denial-of-service-Angriff blockiert.

  Berichtet wird außerdem von der Möglichkeit, dass Dritte während des Signalisierungsablaufs gezielt Veränderungen der Signalisierungsdaten vornehmen könnten, um sich als gewünschter Kommunikationspartner auszugeben. Es ist dann auch nur eine Frage der Zeit, bis Anrufe eingehen, in denen sich ein angeblicher Mitarbeiter der Bank, bei der der Angerufene ein Konto unterhält, darum bittet, man möge doch das persönliche Passwort für das Online-Banking mitteilen, da es zur Wartung des Kontos benötigt werde. Tatsächlich dürfte es sich aber mit an Sicherheit grenzender Wahrscheinlichkeit um sog. Telefon-Phishing handeln, d. h. dem Anrufer ist es gelungen, einen falschen Anschluss vorzuspiegeln.

  Ein weiteres Problem wird vermutlich darin bestehen, dass für Dritte nachvollziehbar wird, wer wann und wo Telefonanrufe über das Internet entgegennehmen kann, ohne direkt anzurufen. Wir gehen nicht so weit zu sagen, dass mit diesen Daten aussagefähige Bewegungsprofile erstellt werden könnten, aber personenbezogen sind sie allemal. Denn wer will schon, dass Dritte wissen, wann er morgens an seinen Arbeitsplatz kommt und wann er ihn abends wieder verlässt.

– Firewall-Systeme

  Damit es mit der Internet-Telefonie richtig klappt, will man natürlich nicht nur anrufen, sondern auch angerufen werden. Und da man im Allgemeinen nicht weiß, wer anrufen will, muss das Ganze so konfiguriert sein, dass auch jedermann anrufen kann. Technisch bedeutet das, dass man seinen PC für Anrufe von jedem beliebigen Rechner im Internet öffnen muss. Das allein ist schon ein Problem, weil ein Angreifer diesen Umstand dazu ausnützen könnte, durch irreguläre Datenpakete das Betriebssystem durcheinander zu bringen. Auf diese Weise könnte er eventuell vorhandene Lücken, deren es in der Vergangenheit leider viele gab, nutzen, um die Sicherheit der Rechner auf vielfältige Weise zu untergraben. Vor solchen Angriffen sollen eigentlich sog. Firewall-Systeme schützen. Um aber ein eingehendes Telefonat passieren zu lassen, müssen Firewall-Systeme so konfiguriert werden, dass sie auch irregulär aufgebaute Datenpakete passieren lassen. Ein Angriffsszenario könnte darin bestehen, einem Softphone laufend ein Klingel-Signal zu schicken und es so lahm zu legen. Wenn es dem Angreifer jetzt noch gelingt, Gegenstellen zu täuschen, könnte er Telefonate anstatt des Angegriffenen entgegennehmen oder mit dessen Kennung und auf dessen Rechnung vornehmen. Die eigentliche Aufgabe von Firewall-Systemen, die unsicheren Rechner eines Intranets vor Angriffen aus dem Internet zu schützen, wird dann, wenn VoIP unterstützt wird, konterkariert. Und ob sog. Intrusion Detection Systeme (IDS), die den Netzverkehr eines Intranets auf Angriffe überwachen, diese Bedrohung abwehren können, muss sich zeigen.

– Verfügbarkeit

  Weiterhin ist zu bedenken, dass bei VoIP-Lösungen die Ausfallsicherheit wesentlich geringer ist als bei herkömmlichen Telefonsystemen. Dies liegt zum einen daran, dass bei VoIP mehr Komponenten im Spiel sind, die die Funktionalität des Ganzen mittragen müssen. Die Wahrscheinlichkeit des Ausfalls erhöht sich grundsätzlich mit jeder zusätzlichen Komponente. Ist das Telefonsystem auf VoIP umgestellt, dann werden die Benutzer den IT-Administratoren nicht mehr telefonisch mitteilen können, dass der Server abgestürzt ist, denn mit dem Ausfall ist vermutlich auch die Funktion des Telefonierens gestört. Auch nicht unterschätzt werden sollte, dass das herkömmliche Telefonsystem selbst bei Stromausfall noch funktioniert, ein im Notfall nicht zu unterschätzender Vorteil. Wenn man mit VoIP die gleiche Verfügbarkeit erreichen will, muss die Dimensionierung der Notstromversorgung des gesamten Systems (Server, PCs, Netzkomponenten) entsprechend erweitert werden.

– Separation der Netze

  Mit einer Trennung von IP-Sprach- und IP-Datennetz könnte an sich ein sicherer Betrieb mit relativ hoher Verfügbarkeit erreicht werden. Diese Möglichkeit, die gelegentlich als Kernstück einer Sicherheitsstrategie empfohlen wird, verlangt allerdings in den meisten Fällen, dass entweder sog. virtuelle lokale Netze (VLANs) aufgebaut werden oder eine zusätzliche Verkabelung erfolgt, ganz zu schweigen von den erhöhten Kosten für zusätzliche Serverfunktionalität und den zweiten Internet-Anschluss. Ob die Internet-Telefonie dann auch noch die wirtschaftlich günstigere Variante ist, muss wohl mit spitzem Stift nachgerechnet werden.

Lediglich eine Frage der Zeit dürfte es auch sein, bis bei der Internet-Telefonie die von E-Mail und Instant-Messaging bekannten Missbrauchsformen wie z. B. unaufgeforderte Werbeanrufe um sich greifen. Einen Namen dafür gibt es auch schon: SPIT (Spam über Internet-Telefonie). Neue Deliktsformen wie Anrufe auf Kosten anderer und Entgelt-Betrug zeichnen sich ebenfalls ab.

Die in diesem Rahmen nur ansatzweise erläuterten datenschutzrechtlichen Probleme bei VoIP mündeten in eine Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, in der die Hersteller, Anbieter und Anwender der VoIP-Technik aufgefordert werden, die zum Schutz von personenbezogenen Daten erforderlichen Maßnahmen zu ergreifen und den Schutz des Fernmeldegeheimnisses bei VoIP ebenso zu wahren wie bei der herkömmlichen Telefonie (s. Anhang 7).

7. Datenschutz bei mobilen Geräten

Vorbei sind die Zeiten, als die Damen und Herren des gemeindlichen Vollzugsdienstes einer badischen Kommune mit Kugelschreiber und Notizblock bewaffnet dem Geschäft der Parkraumüberwachung nachgingen. Bietet die Computerindustrie doch kleine handliche Geräte an, mit denen die Datenerfassung genauso gut durchgeführt werden kann und bei denen die Weiterverarbeitung der personenbezogenen Daten von Parksündern auf zentralen Systemen nur eines Mausklicks bedarf. Aber auch die Fahrkartenkontrolleure einer württembergischen Stadt nutzen für die Erfassung von Bürgern, die ohne gültigen Fahrausweis in öffentlichen Verkehrsmitteln angetroffen werden, die handlichen Geräte. Und wie es sich für eine fortschrittliche Verwaltung gehört, können Bedienstete der Landesverwaltung, die zu jeder Tages- und Nachtzeit an jedem Ort auf ihr dienstliches E-Mail-Postfach zugreifen müssen, beim Provider des Landesverwaltungsnetzes (LVN) handflächengroße Computer, sog. MDAs (mobile digital assistants) erhalten, mit denen sie über ein GSM-Netz ihre E-Mails abrufen können.

Technisch gesehen handelt es sich bei diesen Geräten um Computer, die über einen nicht-flüchtigen Speicher verfügen. Der Datenaustausch zwischen den Geräten und der EDV der jeweiligen Dienststelle wird dadurch bewerkstelligt, dass man die Rechner an einen mit einem speziellen Anschluss ausgerüsteten PC, der sich in der Dienststelle befindet, anschließt und mit spezieller Software den Datentransport durchführt. Aber auch die

Variante, dass nur die Speicherkarte entnommen und in den Kartenleser eines PCs gesteckt wird und dann die gespeicherten Daten auf den Rechner der Dienststelle übertragen werden, haben wir angetroffen. MDAs dagegen brauchen gar keine feste Verbindung zu anderen Rechnern, da sie mit Schnittstellen ausgerüstet sind, über die sie sich an einem Funknetz anmelden und Daten versenden und empfangen können. Und weil es sich anbietet, haben die meisten Geräte dieser Klasse auch eine Schnittstelle, um in ein sog. WLAN eingebunden zu werden oder um mit anderen Geräten eine Bluetooth-Verbindung aufzubauen. Auf den Geräten wird mindestens eine Anwendung zur Erfassung von Daten oder zur Anzeige von E-Mails ausgeführt. Fortschrittlichere Modelle werden mit einem Betriebssystem betrieben, das mehrere Anwendungen ausführen kann und Verbindungen zu den oben genannten Netzen unterstützt.

Durch Eingaben und Anfragen wurden wir in der Berichtsperiode erstmals auf Fragen zum technischen Datenschutz bei mobilen Geräten gelenkt. Dazu haben wir Folgendes gesagt:

– Zugriffsschutz

  Bei keinem technischen Gerät ist das Problem des Zugriffsschutzes von so zweischneidiger Natur wie bei mobilen Geräten. Das kommt daher, dass der Sachbearbeiter im Regelfall das Gerät mit sich trägt und es praktisch immer beaufsichtigt. Daher kann jedem Unbefugten effektiv der Zugriff verwehrt werden. Aber bedingt durch die Größe kann es sein, dass das Gerät liegen gelassen wird oder abhanden kommt. Wenn dann keine Maßnahmen zum Schutz der mit den Geräten gespeicherten Daten getroffen wurden, werden möglicherweise personenbezogene Daten gegenüber Dritten offenbart. Wenn der Bedienstete das Gerät über Nacht in seine Privatwohnung mitnehmen kann, sollten von ihm Vorkehrungen zur Sicherung gegen unerlaubten Zugriff getroffen werden, indem das Gerät beispielsweise unter Verschluss aufbewahrt wird.

– Datenträgerkontrolle

  Weil die Geräte so klein sind, müssen die darin enthaltenen Datenträger nicht erst umständlich ausgebaut werden, um in ihren Besitz zu gelangen; dies erschwert die Datenträgerkontrolle erheblich. Häufig sind auch Geräte anzutreffen, deren Speicher durch zusätzliche Speicherkarten, die die Größe einer Briefmarke haben, aufgerüstet werden können. Und diese Aufrüstung – es soll ja schnell gehen – geschieht einfach dadurch, dass man die Karten an von außen zugänglichen und ungesicherten Kartenschächten einstecken bzw. auch entnehmen kann. Da eine effektive Datenträgerkontrolle sehr schwierig ist, sollten unbedingt Maßnahmen der Verschlüsselung ergriffen werden, damit personenbezogene Daten nicht offenbart werden. Bei MDAs wird vom Provider des LVN sogar die Funktionalität angeboten, dass nur durch ihn autorisierte Speicherkarten in den Geräten verwendet werden können. Von dieser Möglichkeit sollte immer dann, wenn personenbezogene Daten mit im Spiel sind, Gebrauch gemacht werden.

– Speicherkontrolle

  Bei einfacheren Geräten ist der Speicher gegenüber dem Benutzer transparent. Die Einsicht in die gespeicherten Daten erfolgt über das zur Erfassung eingesetzte Programm. Geräte mit Betriebssystem verfügen über ein Dateisystem, auf das zugegriffen werden kann. Bei diesen Geräten und bei Geräten, deren Speicher mit Zusatzkarten erweitert werden können, sollten Maßnahmen zur Speicherkontrolle ergriffen werden. Sofern das System Zugriffsrechte auf der Dateisystemebene unterstützt, sollten diese entsprechend konfiguriert werden. Ansonsten sollte die Anwendung, mit der personenbezogene Daten verarbeitet werden, die Daten nur in verschlüsselter Form in den Speicher schreiben, wenn ein alternativer Zugriff möglich ist.

– Benutzerkontrolle

Um mit dem mobilen Gerät arbeiten zu können, musste bei den von uns in Augenschein genommenen Geräten zur Aktivierung ein mehrstelliger Zahlencode, der von Benutzer zu Benutzer unterschiedlich war, eingegeben werden. Im Unterschied dazu sind Geräte, die keine Benutzeranmeldung erfordern, das heißt, die wie Taschenrechner nach dem Einschalten von jedermann benutzt werden können, datenschutzrechtlich äußerst problematisch.

– Zugriffskontrolle

Maßnahmen der Zugriffskontrolle müssen bei einfachen Geräten, auf denen nur eine Anwendung abläuft, durch die Anwendung realisiert werden. Bei einem von uns untersuchten Gerät mussten sich die Benutzer, nachdem sie das Gerät mit einer mehrstelligen Zahlenkombination aktiviert hatten, nochmals mit einer mehrstelligen Zahlenkombination an der Anwendung anmelden. Maßnahmen der Zugriffskontrolle bei Geräten, die mit einem Betriebssystem arbeiten, das mehrere Anwendungen unterstützt, müssen ebenfalls von den Anwendungen selbst getroffen werden.

– Eingabekontrolle

Vorbildlich war die Eingabekontrolle in einem Fall gelöst: Die Anwendung zeichnete die Benutzerkennung bei jedem neu eingegebenen Fall auf, sodass später am Auswertungs-PC nachvollziehbar war, wer wann mit dem Gerät welche personenbezogenen Daten erfasst hat.

Die Löschung der Daten erfolgt bei einfachen Geräten, indem die personenbezogenen Daten im Speicher der Geräte gelöscht werden, wenn die Geräte an eine Feststation angeschlossen und die Daten in einen zentralen Datenbestand überführt worden sind. Bei MDAs hingegen muss die Löschung von personenbezogenen Daten durch den Benutzer erfolgen. Eine automatische Löschung ist im Allgemeinen nicht vorgesehen.

– Auftragskontrolle

Wird, wie bei den MDAs, das Gerät von einem Provider in vorkonfigurierter Form zur Verfügung gestellt und haben die IT-Administratoren der betreffenden Dienststelle keine Möglichkeit, das Gerät zu administrieren, dann wäre zu prüfen, ob es sich dabei um eine Datenverarbeitung im Auftrag handelt, wenn personenbezogene Daten mit dem Gerät gespeichert werden. Auf unsere Anfrage, ob die Geräte laufend administriert werden oder ob nur einmalig bei der Ausgabe eine Vorkonfiguration erfolgt, haben wir bisher noch keine Antwort erhalten. Wenn sich herausstellen sollte, dass die Administratoren des Providers regelmäßig auf die Rechner zugreifen, dann handelt es sich unserer Meinung nach wie bei der Fernwartung von stationären Systemen um eine Datenverarbeitung im Auftrag. Hierzu wäre ein entsprechender datenschutzrechtlicher Vertrag abzuschließen.

– Transportkontrolle

Maßnahmen zur Transportkontrolle müssen bei den Geräten ergriffen werden, die über eine Netzwerkschnittstelle verfügen. Über diese Schnittstelle können sie in ein Funknetz wie ein GSM-Netz, ein WLAN oder ein Bluetooth-Netz eingebunden werden. Die Maßnahmen können beispielsweise darin bestehen, dass über das GSM-Netz eine Segmentierung erfolgt, die die Einteilung in einzelne Benutzergruppen erlaubt. Dann können MDAs nur mit Teilnehmern dieses Segments in Verbindung treten, von denen ein Teilnehmer ein sog. Einwahlpunkt ist, über den in einem Festnetz die Verbindung zu Servern der Verwaltung aufgebaut wird. Bei WLAN-Netzen sollte bei der Übertragung über öffentliche TCP/IP-Netze ein sog. virtuelles privates Netz (VPN) gebildet werden. Außerdem muss darauf geachtet werden, dass die Rechner in diesen Netzen nicht angreifbar sind. Ob auf den Rechnern die entsprechenden Vorkehrungen wie beispielsweise ein Firewall-System getroffen werden kön-

nen, ist uns nicht bekannt, aber die im 24. Tätigkeitsbericht (LT-Drucksache 13/3800) im fünften Abschnitt unter der Nummer 5.1 und 5.2 formulierten Anforderungen gelten sinngemäß.

Der Erfolg der mobilen Kleinrechner beruht auf der Möglichkeit, überall auf seine Daten zugreifen zu können. Dies lässt auch die Hersteller von Speichersticks, daumengroßen Halbleiterspeichern, die an jeden gängigen PC angeschlossen werden können, nicht ruhen. Sie haben eine Technik ersonnen und standardisiert, mit der man seine Arbeitsumgebung auf einem USB-Speicherstick speichern und an jeden PC, der natürlich mit dem gleichen Betriebssystem arbeiten muss, übertragen kann, indem man den Speicher einsteckt und durch ein Passwort den Zugriff darauf legitimiert. Dadurch sollen die Benutzer auf jedem Wirts-PC, z. B. im Internet-Cafe, bei Bekannten oder zu Hause mit ihrer vom Büro her gewohnten Umgebung arbeiten können. Hinsichtlich des technischen Datenschutzes ist dabei wichtig, dass auf dem Wirts-PC keine Rückstände und insbesondere keine personenbezogenen Daten nach der Benutzung zurückbleiben. Das versprechen die Anbieter dieser U3 genannten Technik. Die Zukunft wird zeigen, ob dieser Anspruch auch immer sicher, d. h. frei von Viren und sog. Trojanern, erfüllt werden kann. Unsere bisherige Erfahrung ist die, dass nach Benutzung eines PCs eigentlich immer Spuren zurückbleiben. Aber immerhin: Die Daten auf dem Speicherstick sind durch ein Passwort vor unbefugtem Zugriff geschützt.

8. Personenbezogene Daten in Web-Angeboten und Internet-Suchmaschinen

Wenn eine öffentliche Stelle in ihrem Internet-Angebot personenbezogene Daten von Beschäftigten und Bürgern veröffentlicht, dann sollte sie dabei so vorgehen, dass die personenbezogenen Daten nicht bei den automatischen Suchanfragen einer Suchmaschine sichtbar werden. In der Berichtsperiode hatten wir die Eingaben mehrerer Petenten, von denen personenbezogene Daten auf behördlichen Web-Sites veröffentlicht wurden, zu bearbeiten. Wir haben ihnen Folgendes mitgeteilt.

8.1 Es gibt ein Entkommen vor den Suchmaschinen

Wenn es zulässig ist, Beschäftigte mit ihrer Funktion im Internet namentlich zu veröffentlichen, wie wir oben dargestellt haben (4. Teil, 2. Abschnitt, Nr. 2), dann sollte dabei so vorgegangen werden, dass die personenbezogenen Daten lokal auf den Aufgabenbereich der betreffenden Stelle beschränkt werden. Dies setzt aber voraus, dass die Daten nicht gegenüber Suchmaschinen offenbart werden und von Dritten durch Suchanfragen weltweit abgerufen werden können. Die Vorgehensweise von Suchmaschinen besteht darin, dass sie die Inhalte von Web-Sites katalogisieren, indem sie die in einer WWW-Seite gespeicherten Verweise auf weitere Seiten analysieren, diesen Verweisen folgen und die Seiten abrufen. Diese so gewonnenen neuen Seiten werden dann mit dem gleichen Mechanismus wieder auf Verweise durchsucht. Dieses Spiel wiederholt sich so lange, bis die Suchmaschine auf einer Seite angelangt ist, die keine Verweise enthält.

Will man nicht die Aufmerksamkeit von Suchmaschinen auf Seiten lenken, die personenbezogene Daten enthalten, bieten sich zwei Möglichkeiten an, die Suche in einem WWW-Angebot auf bestimmte Seiten zu beschränken:

– Eine Möglichkeit besteht darin, die Seiten, deren Indexierung durch Suchmaschinen nicht gewünscht wird, zu kennzeichnen. Die Kennzeichnung besteht aus einer Datei mit Namen „robots.txt“, in der ein bestimmter Text gespeichert sein muss. Im Allgemeinen muss die Datei in Verzeichnissen stehen, in denen nur der Systemverwalter der Web-Site Dateien speichern kann.

  In einer abgewandelten Form dieser Methode wird im Kopftext aller Seiten, die nicht indexiert werden sollen, ein entsprechender Vermerk in Form eines sog. „META“-Elements eingefügt.

– Eine weitere Möglichkeit besteht darin, dafür zu sorgen, dass die Verweise auf Seiten, in denen personenbezogene Daten von Mitarbeitern veröffentlicht werden, nicht im Klartext auftreten, sondern dass entweder die Verweise oder die Seiten dynamisch erzeugt werden. Das bedeutet, dass die Verweise nicht im Klartext erscheinen und sie dadurch vor den Analysemechanismen der Suchmaschinen geschützt sind. Konkret könnten in einem Auswahlmenü die zu veröffentlichenden Sachbereiche wie Personal, Haushalt etc. aufgeführt werden. Nur bei expliziter Selektion durch einen Benutzer würden die dahinter stehenden Inhalte, die dann personenbezogene Daten enthalten können, abgerufen bzw. dargestellt. Hierbei könnte entweder eine direkte Abbildung von Menübegriffen auf statischen Seiten erfolgen oder die Seiten selbst könnten mit Rückgriff auf eine Datenbank dynamisch generiert werden. Da Suchmaschinen Dialoge nicht abarbeiten können, bleiben ihnen die dahinter stehenden Seiten verborgen.

  Außerdem muss noch darauf geachtet werden, dass auf den so erzeugten Seiten keine Verweise auf andere Seiten enthalten sind. Dies deshalb, weil sonst die Adresse einer geheim zu haltenden Seite in einer Hinweisdatei des Servers gespeichert wird, wenn aus ihr heraus einem Verweis gefolgt wird. Nicht selten können diese Hinweisdateien abgerufen werden. Auf diese Weise könnte die Adresse dann einer Suchmaschine bekannt werden.

Insgesamt ist die zweite Methode aufwändiger zu realisieren als die erste Alternative. Sie hat aber den Vorteil, dass sie auch dann funktioniert, wenn sich die Suchmaschinen nicht an die Konvention halten und Seiten, die mit dem „robots.txt“-Mechanismus verborgen werden sollten, indexieren.

8.2 Löschungen personenbezogener Daten in Suchmaschinen

Aber was ist zu tun, wenn das Kind schon in den Brunnen gefallen ist, d. h. wenn das Internet-Angebot der Stelle, die unzulässigerweise personenbezogene Daten veröffentlicht hat, von einer Suchmaschine erfasst und die Inhalte indexiert worden sind? Das führt häufig nicht nur dazu, dass die personenbezogenen Daten mit einfachen Anfragen in Erfahrung gebracht, sondern mit weiteren in Suchmaschinen gespeicherten personenbezogenen Daten (Veröffentlichung in der Vereinsrangliste des Tennis-Clubs, Aktivitäten im Schulförderverein, Anbieter bei Online-Versteigerungen, etc.) verknüpft werden können. Selbst wenn die Stelle einsichtig ist und die personenbezogenen Daten aus ihrem Angebot entfernt, wird möglicherweise von Suchmaschinen die Originalseite in einem sog. Cache zwischengespeichert und kann von jedermann abgerufen werden.

Zunächst muss gesagt werden, dass im Allgemeinen die Betreiber von Suchmaschinen Unternehmen des privaten Bereichs sind und daher nicht der Kontrolle des Landesbeauftragten für den Datenschutz unterliegen. Es bestehen daher keine direkten Einwirkungsmöglichkeiten von Seiten des Landesbeauftragten für den Datenschutz auf die Unternehmen, die darüber hinaus meist ihren Firmensitz im Ausland haben.

Die Betroffenen selbst können sich zwar mit den Betreibern der Suchmaschinen in Verbindung setzten, erhalten aber für gewöhnlich als Antwort den Hinweis, dass die Daten von einer öffentlichen Web-Site erhoben wurden. Und genau diese Verarbeitung, d. h. die Speicherung und den Abruf von personenbezogenen Daten aus öffentlich zugänglichen Quellen, erlauben sowohl das Bundesdatenschutzgesetz wie auch das Landesdatenschutzgesetz, das bei öffentlichen Stellen des Landes anzuwenden ist. Die Betreiber von Suchmaschinen sind also in rechtlicher Hinsicht auf der sicheren Seite.

Es sind die Betreiber der Web-Site, die Anstrengungen unternehmen müssen, um den Missstand zu beseitigen. Sie können gegenüber den Suchmaschinenbetreibern die zeitnahe Löschung von personenbezogenen Daten, die sie in ihrem Angebot veröffentlicht haben, beantragen.

Ist der Betreiber einer Web-Site eine öffentliche Stelle und unterliegt damit dem Landesdatenschutzgesetz, besteht insofern eine Einwirkungsmöglichkeit des Landesbeauftragten gegenüber der öffentlichen Stelle. Wenn nämlich die datenschutzrechtliche Prüfung ergeben hat, dass personenbezogene Daten unzulässigerweise auf dem WWW-Server der Stelle veröffentlicht wurden, dann wird die Stelle regelmäßig aufgefordert, die Daten aus ihrem Angebot zu löschen. Ist das Angebot der Stelle zum Zeitpunkt, in dem die personenbezogenen Daten veröffentlicht wurden, von einer Suchmaschine indexiert worden, ist es sachgerecht, dass der Betreiber der Web-Site die Löschung der zu Unrecht veröffentlichten personenbezogenen Daten aus dem Suchindex beim Suchmaschinenbetreiber beantragt. Ebenso sollte er darauf hinwirken, dass die Daten in Zwischenspeichern des Suchmaschinenbetreibers gelöscht werden.

Um ganz sicher zu gehen, dass die Betroffenen die sie betreffenden Seiten nicht mehr sehen, müssen sie diese dann nur noch aus dem lokalen Zwischenspeicher auf ihrem PC, in dem der Browser Kopien der abgerufenen Seiten speichert, löschen.

Inhaltsverzeichnis des Anhangs

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Anhang 1: Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck

Anhang 2: Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006

Anhang 3: Einführung der elektronischen Gesundheitskarte

Anhang 4: Einführung biometrischer Ausweisdokumente

Anhang 5: Appell der Datenschutzbeauftragten des Bundes und der Länder: Eine moderne Informationsgesellschaft braucht mehr Datenschutz

Anhang 6: Keine Vorratsdatenspeicherung in der Telekommunikation

Anhang 7: Telefonieren mit Internet-Technologie (Voice over IP – VoIP)

Anhang 8: Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

Anhang 9: Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen

Anlage 10: Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten

Anlage 11: Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

Anhang 1

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder zur Bundesratsinitiative mehrerer Länder zur Ausweitung der DNA-Analyse vom 17. Februar 2005

Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck

Die strafprozessuale DNA-Analyse ist – insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten – ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial z. B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments „DNA-Analyse“, weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es birgt aber – auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung – in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den sog. nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich, welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im Übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

Anhang 2

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 10./11. März 2005

Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006

Die Datenschutzbeauftragten des Bundes und der Länder betrachten das Vergabeverfahren für die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 mit großer Sorge. Bei der Bestellung von Tickets müssen die Karteninteressentinnen und interessenten ihre persönlichen Daten wie Name, Geburtsdatum, Adresse, Nationalität sowie ihre Ausweisdaten angeben, um bei der Ticketvergabe berücksichtigt zu werden. Die Datenschutzbeauftragten befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und –interessenten. Der Gesetzgeber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. des inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticket-Vergabe sollte daher überarbeitet werden. Eine solche Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

Anhang 3

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 10./11. März 2005

Einführung der elektronischen Gesundheitskarte

Die Datenschutzbeauftragten des Bundes und der Länder begleiten aufmerksam die Einführung der elektronischen Gesundheitskarte. Sie weisen darauf hin, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend aufgrund der Einwilligung der Versicherten erfolgen muss. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind neben den rechtlichen auch die tatsächlichen – technischen wie organisatorischen – Voraussetzungen zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind.

Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschließungen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.

Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen. Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben.

Für die Bewertung der Gesundheitskarte und der neuen Telematikinfrastruktur können unabhängige Gutachten und Zertifizierungen förderlich sein, wie sie ein Datenschutz-Gütesiegel und ein Datenschutz-Audit vorsehen. Vorgesehene Einführungstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

Anhang 4

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 1. Juni 2005

Einführung biometrischer Ausweisdokumente

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützter Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen, sollen in Deutschland noch im laufenden Jahr die ersten Pässe ausgegeben werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, dass mit der Ausgabe von elektronisch lesbaren biometrischen Ausweisdokumenten erst begonnen werden kann, wenn die technische Reife, der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Diese Voraussetzungen sind bisher jedoch noch nicht in ausreichendem Maße gegeben.

Daher sind in einem umfassenden Datenschutz- und IT-Sicherheitskonzept zunächst technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen. Darüber hinaus sind im Passgesetz Regelungen zur strikten Zweckbindung der Daten erforderlich. Die Konferenz begrüßt das Eintreten des Europäischen Parlaments für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten. Die Konferenz bedauert es jedoch, dass die Einführung dieser Pässe beschlossen wurde, ohne dass die Chancen und Risiken der Technik ausreichend diskutiert wurden. Besonders problematisch ist es, dass die Entscheidung durch den Europäischen Rat der Regierungsvertreter entgegen der entsprechenden Stellungnahme des Europäischen Parlaments und der nationalen Gesetzgeber der EU-Mitgliedstaaten getroffen wurde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Einführung biometrischer Merkmale nicht automatisch zur Verbesserung der Sicherheit führt. Noch immer weisen manche biometrische Identifikationsverfahren hohe Falscherkennungsraten auf und sind oft mit einfachsten Mitteln zu überwinden. Scheinbar besonders sichere Ausweisdokumente werden durch den Einsatz unsicherer biometrischer Verfahren somit plötzlich zu einem Risikofaktor. Fehler bei der Erkennung von Personen haben zudem erhebliche Konsequenzen für die Betroffenen, weil sie einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine objektive Bewertung von biometrischen Verfahren und tritt dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. Mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten darf erst begonnen werden, wenn durch rechtliche, organisatorische und technische Maßnahmen gewährleistet wird,

- dass die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden,
- dass die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,
- dass die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden,
- dass die verwendeten Lesegeräte in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,
- dass eine verbindliche Festlegung der zur Ausgabe oder Verifikation von Dokumenten zugriffsberechtigten Stellen erfolgt,

– dass vor der Einführung biometrischer Ausweise Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten (sicheres Enrollment), beim weiteren Verfahren und bei der Kartennutzung verhindern,

– dass diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden.

Darüber hinaus muss sichergestellt sein, dass keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden. Die biometrischen Identifizierungsdaten dürfen ausschließlich auf dem jeweiligen Ausweisdokument gespeichert werden. Durch international festzulegende Standards sowie Vorschriften und Vereinbarungen ist anzustreben, dass die bei Grenzkontrollen erhobenen Ausweisdaten weltweit nur gemäß eines noch festzulegenden einheitlichen hohen Datenschutz- und IT-Sicherheitsstandards verarbeitet werden.

Anhang 5

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 2005

Appell der Datenschutzbeauftragten des Bundes und der Länder:
Eine moderne Informationsgesellschaft braucht mehr Datenschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die 16. Legislaturperiode des Deutschen Bundestags großen Handlungsbedarf im Bereich des Datenschutzes. Der Weg in eine freiheitliche und demokratische *Informationsgesellschaft* unter Einsatz modernster Technologie zwingt alle Beteiligten, ein verstärktes Augenmerk auf den Schutz des Rechts auf informationelle Selbstbestimmung zu legen. Ohne wirksameren Datenschutz werden die Fortschritte vor allem in der Informations- und der Biotechnik nicht die für Wirtschaft und Verwaltung notwendige gesellschaftliche Akzeptanz finden.

Es bedarf einer grundlegenden *Modernisierung des Datenschutzrechtes*. Hierzu gehört eine Ergänzung des bisher auf Kontrolle und Beratung basierenden Datenschutzrechtes um Instrumente des wirtschaftlichen Anreizes, des Selbstdatenschutzes und der technischen Prävention. Es ist daher höchste Zeit, dass in dieser Legislaturperiode vom Deutschen Bundestag ein Datenschutz-Auditgesetz erarbeitet wird. Datenschutzkonforme Technikgestaltung als Wettbewerbsanreiz liegt im Interesse von Wirtschaft, Verwaltung und Bevölkerung. Zugleich ist die ins Stocken geratene umfassende Novellierung des Bundesdatenschutzgesetzes mit Nachdruck voranzutreiben. Eine Vereinfachung und Konzentration der rechtlichen Regelungen kann Bürokratie abbauen und zugleich den Grundrechtsschutz stärken.

Die Bürgerinnen und Bürger müssen auch in Zukunft frei von Überwachung sich informieren und miteinander kommunizieren können. Nur so können sie in der Informationsgesellschaft ihre Grundrechte selbstbestimmt in Anspruch nehmen. Dem laufen Bestrebungen zuwider, mit dem Argument einer vermeintlich höheren Sicherheit immer mehr alltägliche Aktivitäten der Menschen elektronisch zu registrieren und für Sicherheitszwecke auszuwerten. Die längerfristige Speicherung auf Vorrat von Verkehrsdaten bei der Telekommunikation, die zunehmende Videoüberwachung im öffentlichen Raum, die anlasslose elektronische Erfassung des Straßenverkehrs durch Kfz-Kennzeichenabgleich, die Erfassung biometrischer Merkmale der Bevölkerung oder Bestrebungen zur Ausdehnung der Rasterfahndung betreffen ganz überwiegend völlig unverdächtige Bürgerinnen und Bürger und setzen diese der Gefahr der *Ausforschung ihrer Lebensgewohnheiten* und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem immer ein adäquater Sicherheitsgewinn gegenübersteht. Freiheit und Sicherheit bedingen sich wechselseitig. Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.

Den Sicherheitsbehörden steht bereits ein breites Arsenal an gesetzlichen Eingriffsbefugnissen zur Verfügung, das teilweise überstürzt nach spektakulären Verbrechen geschaffen worden ist. Diese Eingriffsbefugnisse der Sicherheitsbehörden müssen einer umfassenden systematischen *Evaluierung durch unabhängige Stellen* unterworfen und öffentlich zur Diskussion gestellt werden. Unangemessene Eingriffsbefugnisse, also solche, die mehr schaden als nützen, sind wieder zurückzunehmen.

Die Kontrolle der Bürgerinnen und Bürger wird auch mit den Argumenten der Verhinderung des Missbrauchs staatlicher Leistungen und der Erhöhung der Steuerehrlichkeit vorangetrieben. So richtig es ist, in jedem Einzelfall die Voraussetzungen für staatliche Hilfen zu prüfen und bei hinreichenden Anhaltspunkten Steuerhinterziehungen nachzugehen, so überflüssig und rechtsstaatlich problematisch ist es, alle Menschen mit einem Pauschalverdacht zu überziehen und Sozial- und Steuerverwaltung mit dem Recht auszustatten, verdachtsunabhängig Datenabgleiche mit privaten und öffentlichen Datenbeständen vorzunehmen. Es muss verhindert werden, dass mit dem Argument der *Leistungs- und Finanzkontrolle*

die Datenschutzgrundsätze der Zweckbindung und der informationellen Gewaltenteilung auf der Strecke bleiben.

Die Entwicklung in Medizin und Biotechnik macht eine Verbesserung des Schutzes des Patientengeheimnisses notwendig. Telemedizin, der Einsatz von High-Tech im *Gesundheitswesen*, gentechnische Verfahren und eine intensivierte Vernetzung der im Gesundheitsbereich Tätigen kann zu einer Verbesserung der Qualität der Gesundheitsversorgung und zugleich zur Kosteneinsparung beitragen. Zugleich drohen die Vertraulichkeit der Gesundheitsdaten und die Wahlfreiheit der Patientinnen und Patienten verloren zu gehen. Diese bedürfen dringend des gesetzlichen Schutzes, u. a. durch ein modernes Gendiagnostikgesetz und durch datenschutz- und patientenfreundliche Regulierung der Computermedizin.

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, insbesondere durch neue Möglichkeiten der Kontrolle bei der Nutzung elektronischer Kommunikationsdienste, Videotechnik, Funksysteme und neue biotechnische Verfahren. Schranken werden bisher nur im Einzelfall durch Arbeitsgerichte gesetzt. Das seit vielen Jahren vom Deutschen Bundestag geforderte *Arbeitnehmerdatenschutzgesetz* muss endlich für beide Seiten im Arbeitsleben Rechtsklarheit und Sicherheit schaffen.

Die *Datenschutzkontrolle* hat mit der sich fast explosionsartig entwickelnden Informationstechnik nicht Schritt gehalten. Immer noch findet die Datenschutzkontrolle in manchen Ländern durch nachgeordnete Stellen statt. Generell sind Personalkapazität und technische Ausstattung unzureichend. Dem steht die europarechtliche Anforderung entgegen, die Datenschutzaufsicht in völliger Unabhängigkeit auszuüben und diese adäquat personell und technisch auszustatten.

Die Europäische Union soll ein „Raum der Freiheit, der Sicherheit und des Rechts“ werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen wird.

Die grenzüberschreitende Zusammenarbeit von Polizei- und Justizbehörden darf jedoch nicht zur Schwächung von Grundrechtspositionen der Betroffenen führen. Der vermehrte Austausch personenbezogener Daten setzt deshalb ein hohes und gleichwertiges Datenschutzniveau in allen EU-Mitgliedstaaten voraus. Dabei ist von besonderer Bedeutung, dass die Regelungen in enger Anlehnung an die Datenschutzrichtlinie 95/46/EG erfolgen, damit ein möglichst einheitlicher *Datenschutz in der Europäischen Union* gilt, der nicht zuletzt dem Ausgleich zwischen Freiheitsrechten und Sicherheitsbelangen dienen soll.

Die Datenschutzbeauftragten des Bundes und der genannten Länder appellieren an die Fraktionen im Bundestag und an die künftige Bundesregierung, sich verstärkt für den Grundrechtsschutz in der Informationsgesellschaft einzusetzen.

Anhang 6

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 2005

Keine Vorratsdatenspeicherung in der Telekommunikation

Die Europäische Kommission hat den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten über die elektronische Kommunikation vorgelegt. Danach sollen alle Telekommunikationsanbieter und Internet-Provider verpflichtet werden, systematisch eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum (ein Jahr bei Telefonaten, sechs Monate bei Internet-Nutzung) für mögliche Abrufe von Sicherheitsbehörden selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke (z. B. zur Abrechnung) gar nicht benötigen. Die Annahme dieses Vorschlags oder des gleichzeitig im Ministerrat beratenen, weiter gehenden Entwurfs eines Rahmenbeschlusses und ihre Umsetzung in nationales Recht würde einen Dammbruch zulasten des Datenschutzes unverdächtiger Bürgerinnen und Bürger bedeuten. Sowohl das grundgesetzlich geschützte Fernmeldegeheimnis als auch der durch die Europäische Menschenrechtskonvention garantierte Schutz der Privatsphäre drohen unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre bereits seit 2002 geäußerte grundsätzliche Kritik an jeder Pflicht zur anlassunabhängigen Vorratsdatenspeicherung. Die damit verbundenen Eingriffe in das Fernmeldegeheimnis und das informationelle Selbstbestimmungsrecht lassen sich auch nicht durch die Bekämpfung des Terrorismus rechtfertigen, weil sie unverhältnismäßig sind. Insbesondere gibt es keine überzeugende Begründung dafür, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig wäre.

Die anlassunabhängige Vorratsdatenspeicherung aller Telefon- und Internetdaten ist von großer praktischer Tragweite und widerspricht den Grundregeln unserer demokratischen Gesellschaft. Erfasst würden nicht nur die Daten über die an sämtlichen Telefongesprächen und Telefax-Sendungen beteiligten Kommunikationspartner und partnerinnen, sondern auch der jeweilige Zeitpunkt und die Dauer der Einwahl ins Internet, die dabei zugeteilte IP-Adresse, ferner die Verbindungsdaten jeder einzelnen E-Mail und jeder einzelnen SMS sowie die Standorte jeder Mobilkommunikation. Damit ließen sich europaweite Bewegungsprofile für einen Großteil der Bevölkerung für einen längeren Zeitraum erstellen.

Die von einigen Regierungen (z. B. der britischen Regierung nach den Terroranschlägen in London) gemachten Rechtfertigungsversuche lassen keinen eindeutigen Zweck einer solchen Maßnahme erkennen, sondern reichen von den Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Straftatenverfolgung. Alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) sind bisher nicht ernsthaft erwogen worden.

Mit einem Quick-freeze-Verfahren könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen.

Der Kommissionsvorschlag würde zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung führen. Eine freie und unbefangene Telekommunikation wäre nicht mehr möglich. Jede Person, die in Zukunft solche Netze nutzt, würde unter Generalverdacht gestellt. Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, wäre zum Scheitern verurteilt. Derartige Datenbestände würden Begehrlichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnten. Auch aus diesem Grund muss bereits den ersten Versuchen, eine solche Vorratsdatenspeicherung einzuführen, entschieden entgegengetreten werden. Zudem ist eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten zu befürchten. Schon jetzt ist die Trennlinie zwischen Verkehrs- und Inhaltsdaten gerade bei der Internetnutzung

nicht mehr zuverlässig zu ziehen. Dieselben – unzutreffenden – Argumente, die jetzt für eine flächendeckende Speicherung von Verkehrsdaten angeführt werden, würden bei einer Annahme des Kommissionsvorschlags alsbald auch für die anlassfreie Speicherung von Kommunikationsinhalten auf Vorrat ins Feld geführt werden.

Die Konferenz appelliert an die Bundesregierung, den Bundestag und das Europäische Parlament, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen. Auf der Grundlage des Grundgesetzes wäre eine anlasslose Vorratsdatenspeicherung verfassungswidrig.

Anhang 7

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 2005

Telefonieren mit Internet-Technologie (Voice over IP – VoIP)

Die Internet-Telefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kunden und Kundinnen oft nicht bekannt, dass diese Verbindungen in den meisten Fällen noch wesentlich unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz.

Bei Telefongesprächen über das Internet kommt die Internet-Technologie Voice over IP (VoIP) zum Einsatz. In zunehmendem Maße wird angeboten, Telefongespräche mit Hilfe der Internet-Technologie VoIP zu führen. Das Fernmeldegeheimnis ist auch für die Internet-Telefonie zu gewährleisten. Während jedoch bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis. Vielmehr werden diese Daten mit Hilfe des aus der Internet-Kommunikation bekannten Internet-Protokolls (IP) in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internet-Nutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden. Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden. Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb Hersteller und Herstellerinnen, Anbieter und Anbieterinnen sowie Anwender und Anwenderinnen von VoIP-Lösungen auf, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren und hierfür

- angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen,
- Verschlüsselungsverfahren für VoIP anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen,
- Sicherheits- und Datenschutzmängel, die die verwendeten Protokolle oder die genutzte Software bisher mit sich bringen, durch Mitarbeit an der Entwicklung möglichst schnell zu beseitigen,
- auf die Verwendung von offenen, standardisierten Lösungen zu achten beziehungsweise die verwendeten Protokolle und Algorithmen offen zu legen,
- VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und
- bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen angemessene Sicherheitsmaßnahmen umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.

Anhang 8

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 2005

Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.

Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.

Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber aufgrund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.

Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes – insbesondere die Angemessenheit der Datenerhebung – und eine strikte Zweckbindung umzusetzen.

In der Entscheidung vom 27. Juli 2005 hat das Gericht erneut die Bedeutung der – zuletzt auch in seinen Entscheidungen zum Großen Lauschangriff und zum Außenwirtschaftsgesetz vom 3. März 2004 dargelegten – Verfahrenssicherungen zur Gewährleistung der Rechte der Betroffenen hervorgehoben. So verpflichtet beispielsweise das Gebot der effektiven Rechtsschutzgewährung die Sicherheitsbehörden, Betroffene über die verdeckte Datenerhebung zu informieren.

Diese Grundsätze sind sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, u. a. bei der Novellierung der §§ 100 a und 100 b StPO, zu beachten.

Die Konferenz der DSB erwartet, dass nunmehr zügig die erforderlichen Gesetzgebungsarbeiten in Bund und Ländern zum Schutz des Kernbereichs privater Lebensgestaltung bei allen verdeckten Ermittlungsmaßnahmen aufgenommen und die Vorgaben des Bundesverfassungsgerichts ohne Abstriche umgesetzt werden.

Anhang 9

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 2005

Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass bei der Umsetzung der Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe weiterhin erhebliche datenschutzrechtliche Mängel bestehen. Die Rechte der Betroffenen werden dadurch stark beeinträchtigt. Zwar ist das Verfahren der Datenerhebung durch die unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder überarbeiteten Antragsvordrucke auf dem Weg, datenschutzkonform ausgestaltet zu werden. Bei der Leistungs- und Berechnungssoftware A2LL gibt es jedoch entgegen den Zusagen des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und der Bundesagentur für Arbeit (BA) immer noch keine erkennbaren Fortschritte.

Weder ist ein klar definiertes Zugriffsberechtigungskonzept umgesetzt, noch erfolgt eine Protokollierung der lesenden Zugriffe. Damit ist es über 40.000 Mitarbeiterinnen und Mitarbeitern in der BA und den Arbeitsgemeinschaften nach SGB II (ARGEn) nach wie vor möglich, voraussetzungslos auf die Daten aller Leistungsempfänger und empfängerinnen zuzugreifen, ohne dass eine Kontrolle möglich wäre.

Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensible Daten, wie z. B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne ARGEn reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem VerBIS, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Löschungskonzept beinhaltet. Der Datenschutz muss auch bei der Migration der Daten aus coArb in VerBIS beachtet werden.

Mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder hat die BA den Antragsvordruck und die Zusatzblätter überarbeitet. Soweit die Betroffenen auch die ergänzenden neuen Ausfüllhinweise erhalten, wird ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit eine Erhebung von nicht erforderlichen Daten vermieden. Doch ist immer noch festzustellen, dass die bisherigen Ausfüllhinweise nicht überall verfügbar sind. Es ist daher zu gewährleisten, dass allen Betroffenen nicht nur baldmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den Ausfüllhinweisen ausgehändigt werden („Paketlösung“).

Es handelt sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der Landesbeauftragten für Datenschutz unterliegen. Dies haben die Bundesanstalt und die ARGEn zu akzeptieren. Es ist nicht hinnehmbar, dass über die Verweigerung einer Datenschutzkontrolle rechtsfreie Räume entstehen und damit in unzumutbarer Weise in die Rechte der Betroffenen eingegriffen wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene auf, selbst und im Rahmen ihrer Rechtsaufsicht die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Für den Fall einer völligen Neugestaltung des Systems A2LL wegen der offenbar nicht zu beseitigenden Defizite erwarten die Datenschutzbeauftragten ihre zeitnahe Beteiligung. Es ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben, wie die Protokollierung der lesenden Zugriffe und ein klar definiertes Zugriffsberechtigungs- und Löschungskonzept, ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

Anhang 10

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 2005

Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist anlässlich von durch die Bundesanstalt mit Hilfe privaten Callcentern durchgeführten Telefonbefragungen bei Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II darauf hin, dass es den Betroffenen unbenommen ist, sich auf ihr Grundrecht auf informationelle Selbstbestimmung zu berufen. Da die Befragung freiwillig war, hatten sie das Recht, die Beantwortung von Fragen am Telefon zu verweigern.

Die Ablehnung der Teilnahme an einer solchen Befragung rechtfertigt nicht den Verdacht auf Leistungsmissbrauch. Wer seine Datenschutzrechte in Anspruch nimmt, darf nicht deshalb des Leistungsmissbrauchs bezichtigt werden.

Die Konferenz fordert daher das Bundesministerium für Wirtschaft und Arbeit und die Bundesanstalt für Arbeit dazu auf, die Sach- und Rechtslage klarzustellen und bei der bereits angekündigten neuen Telefonaktion eine rechtzeitige Beteiligung der Datenschutzbeauftragten sicherzustellen.

Anhang 11

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26./27. Oktober 2005

Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

Anlässlich eines von der Europäischen Kommission am 5. Juli 2005 eingeleiteten Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland zur Unabhängigkeit der Datenschutzkontrolle fordert die Konferenz erneut eine völlig unabhängige Datenschutzkontrolle.

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedstaaten von Stellen überwacht wird, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. In Deutschland ist indessen die Datenschutzkontrolle der Privatwirtschaft überwiegend in den Weisungsstrang der jeweiligen Innenverwaltung eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle der Privatwirtschaft verstößt nach Ansicht der Europäischen Kommission gegen Europarecht.

Die Datenschutzbeauftragten des Bundes und der Länder können eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Sie sollten dazu in allen Ländern und im Bund als eigenständige Oberste Behörden eingerichtet werden, die keinen Weisungen anderer administrativer Organe unterliegen.

Demgegenüber ist die in Niedersachsen beabsichtigte Rückübertragung der Datenschutzkontrolle des privatwirtschaftlichen Bereichs vom Landesdatenschutzbeauftragten auf das Innenministerium ein Schritt in die falsche Richtung. Die Konferenz wendet sich entschieden gegen diese Planung und fordert den Bund sowie alle Länder auf, zügig europarechtskonforme Aufsichtsstrukturen im deutschen Datenschutz zu schaffen.