Landtag von Baden-Württemberg **Drucksache 13 / 3800**
13. Wahlperiode **01. 12. 2004**

Mitteilung

des Landesbeauftragten für den Datenschutz

Fünfundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

Schreiben des Landesbeauftragten für den Datenschutz in Baden-Württemberg vom 1. Dezember 2004:

Anbei übersende ich Ihnen unseren 25. Tätigkeitsbericht, der nach § 31 Abs. 1 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 1. Dezember 2004 zu erstatten ist.

Zimmermann

Eingegangen: 01. 12. 2004 / Ausgegeben: 17. 12. 2004

Fünfundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

INHALTSVERZEICHNIS

3. Teil: Gesundheit und Soziales

4. Teil: Kommunales und anderes

5. Teil: Technik und Organisation

1. Teil: Zur Situation

Der Bericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg erfährt in diesem Jahr seine 25. Auflage. Der Datenschutz ist damit fast halb so alt wie das Land. Ist das Silber-Jubiläum nun ein Grund zur Freude oder ein Anlass zur Nachdenklichkeit? Wie häufig, so dürfte auch hier die Wahrheit einigermaßen in der Mitte liegen. Will man nochmals die gedankliche Verbindung zum Land bemühen, könnte einem zwar in Anlehnung an den Landes-Werbeslogan das Fazit einfallen: „Wir können alles – außer Datenschutz“. Aber so düster muss das Bild des Datenschutzes im Lande nun auch wieder nicht gemalt werden – wie dies wohl auch für die Beherrschung des Hochdeutschen hierzulande gelten dürfte.

Die Beratungstätigkeit meiner Dienststelle hat jedenfalls ergeben, dass im Großen und Ganzen bei den öffentlichen Stellen im Lande die offene Bereitschaft besteht, Hinweise und Ratschläge zum Datenschutz auch anzunehmen. Ebenso muss man allerdings konstatieren, dass es auch im Berichtsjahr wieder zahlreiche Verstöße gegen das Datenschutzrecht gegeben hat. Die im diesjährigen Tätigkeitsbericht geschilderten Vorgänge sind ein erneuter Beleg hierfür.

Der Takt der Entwicklung des Datenschutzes im gesetzgeberischen Bereich wird derzeit eindeutig durch die Bundesebene vorgegeben. Und dies ist insgesamt aus Datenschutzsicht nicht als Kompliment in Richtung Bund zu bewerten, sondern eher kritisch zu sehen. Denn zahlreiche bundesgesetzliche Vorhaben sind dazu geeignet, das Grundrecht auf Datenschutz wenn nicht gerade in den Grundfesten zu erschüttern, aber doch nach und nach auszuhöhlen. Angefangen beim Gesetz über die Förderung der Steuerehrlichkeit, das den Finanzbehörden und vor allem auch einer unbestimmten Vielzahl weiterer Behörden einen Zugriff auf Kontenstammdaten und andere Bankdaten aller Bankkunden einräumt, über die neuen Regelungen im Telekommunikationsgesetz, in dem die Speicherung von Telekommunikationsdaten umfassender zugelassen und bei der Telefonauskunft die sog. Inverssuche ermöglicht wird, bis hin etwa zur gesetzlichen Ausformung von Hartz IV: Allen Regelungen ist der Trend gemein, das Recht auf informationelle Selbstbestimmung zurückzudrängen zugunsten eines Allgemeininteresses an einer effizienteren und geschmeidigeren Aufgabenerledigung.

Deshalb ist es von besonderem Gewicht, dass dieser Trend in einem wichtigen Bereich brüsk gestoppt wurde. Allerdings nicht durch den Gesetzgeber selbst, sondern durch das Bundesverfassungsgericht, das seinem Attribut, Hüter unserer Verfassung zu sein, wieder einmal gerecht wurde. In seiner wegweisenden Entscheidung zum sog. Großen Lauschangriff hat das Bundesverfassungsgericht die Maßstäbe wieder zurechtgerückt, die zu gelten haben, wenn der Staat in Kernbereiche der privaten Lebensgestaltung überwachend einzugreifen beabsichtigt (Einzelheiten hierzu im 2. Teil, 2. Abschnitt). Wenn in der Diskussion dieses Urteils seitens der sog. „Praktiker“ spontan kritisiert wurde, dass die Vorgaben des Bundesverfassungsgerichts kaum umzusetzen seien, weil die praktische Arbeit dadurch über Gebühr erschwert werden würde, kann man nur antworten: Genau diese Erschwerung der Eingriffe in das Recht auf informationelle Selbstbestimmung ist verfassungsrechtlich letztlich gewollt. Oder anders ausgedrückt: Staatliche Eingriffe in das Grundrecht auf Datenschutz sind nicht schon immer dann gerechtfertigt, wenn die jeweilige Aufgabenerledigung ohne diese Eingriffe aufwendiger oder komplizierter wäre. Dabei ist sicherlich einzuräumen, dass es bei der akustischen Wohnraumüberwachung nicht einfach sein wird, etwa die Forderung des Bundesverfassungsgerichts umzusetzen, ein Abhören von Gesprächen unter Ehegatten in deren Wohnung äußerstenfalls dann zuzulassen, wenn es Anhaltspunkte für eine Beteiligung eines Gesprächspartners an bestimmten schweren Straftaten gibt, das Abhören aber sofort abzubrechen, wenn die Unterhaltung in eine strafrechtlich unverfängliche Thematik wechselt. Der Gesetzgeber wäre hier gut beraten, die vom Bundesverfassungsgericht vorgegebene Linie eindeutig einzuhalten und nicht etwa zu erwägen, „aus praktischen Gründen“ das Abhören solcher Vorgänge großzügiger zuzulassen und etwa erst im Nachhinein die verantwortlichen Stellen prüfen zu lassen, ob die einmal erfassten Daten überhaupt hätten erfasst werden dürfen. Diese Vorgehensweise, nämlich die Voraussetzungen für das Erheben von Daten herunterzuschrauben – etwa nach dem Motto: „Wir erhe-

ben die Daten zunächst einmal und sehen danach, ob es sich dabei um Daten handelt, die überhaupt relevant sind“ – ist ein Weg, der dem Stellenwert des Rechts auf informationelle Selbstbestimmung in keiner Weise gerecht wird. Auch die Erhebung von Daten ist bereits ein Eingriff in dieses Recht, der nicht voraussetzungslos geschehen darf. Um zurückzukommen auf den Großen Lauschangriff: Anstatt auch die letzte Möglichkeit des Abhörens etwa von Gesprächen unter Ehegatten auszuschöpfen, wäre durchaus auch daran zu denken, dass der Gesetzgeber – gerade um den aufgezeigten praktischen Problemen auszuweichen – auf eine Überwachung von Ehegattengesprächen völlig verzichtet. Die eben angesprochene Rechtsschwelle für die Erhebung von personenbezogenen Daten wird im Übrigen auch in anderen Bereichen zunehmend relativiert. So ist etwa auf die Überlegungen zu verweisen, Kraftfahrzeugkennzeichen aus dem fließenden Verkehr allgemein durch die Polizei zu erfassen und dann erst im Nachhinein durch Abgleichung mit anderen Dateien festzustellen, inwieweit man die erfassten Daten überhaupt benötigt. Diese Relativierung der rechtlichen Schwelle für die Datenerhebung ist eine insgesamt bedenkliche Entwicklung.

Im Gegensatz zur Entwicklung auf Bundesebene hat sich der Landesgesetzgeber im Berichtsjahr mit datenschutzrelevanten Gesetzgebungsvorhaben zurückgehalten. Es wäre zu begrüßen, wenn dies so bliebe. Insbesondere im Sicherheitsbereich kann es nicht so falsch sein, auch weiterhin Zurückhaltung zu üben, was die Erweiterung von Eingriffsmöglichkeiten in das informationelle Selbstbestimmungsrecht des einzelnen Bürgers angeht. Diese Zurückhaltung rechtfertigt sich auch daraus, dass Baden-Württemberg – obwohl es manche Gesetzgebungsschritte anderer Länder nicht nachvollzogen hat – dank der qualifizierten Arbeit der Sicherheitsbehörden im Ländervergleich unverändert den Spitzenplatz einnimmt.

Für die nahe Zukunft zeichnen sich im Land allerdings schon heute einige Gesetzgebungsprojekte ab, die u. a. auch einer gründlichen datenschutzrechtlichen Prüfung zu unterwerfen sind. So ist beispielsweise an die Umstrukturierung des Landeskrebsregisters (s. 3. Teil, 1. Abschnitt) oder an die neuen Statistiküberlegungen im Schulbereich (s. 4. Teil, 3. Abschnitt) zu denken. Hierzu kann der folgende Bericht noch keine abschließende Bewertung, sondern nur eine Einführung und erste Hinweise zu datenschutzrechtlichen Fragestellungen enthalten.

Übrigens: Auch das Land Mecklenburg-Vorpommern hat nun die unübersehbaren Vorzüge einer Zusammenlegung der Datenschutzaufsicht im öffentlichen und im nicht-öffentlichen Bereich erkannt und wird diese Zusammenlegung demnächst vollziehen. Damit hat nun bereits das siebente Bundesland den zukunftsweisenden Schritt zu einer Datenschutzaufsicht „aus einer Hand“ getan. Es bleibt aus meiner Sicht dabei, dass nicht zuletzt aus verwaltungsökonomischer Sicht ein solcher Schritt auch für Baden-Württemberg längst überfällig wäre.

Abschließend ist der Vermögens- und Bauverwaltung des Landes dafür zu danken, dass sie die neue Unterbringung meiner Dienststelle in renovierten Räumen ermöglicht hat.

2. Teil: Öffentliche Sicherheit und Justiz

1. Abschnitt: Öffentliche Sicherheit

1. Volksfeste à la Oberschwaben – unter die Videolupe genommen

Volksfeste haben in Oberschwaben Tradition. In Biberach feiert man seit langem jedes Jahr im Sommer das Schützenfest, in Ravensburg das Rutenfest. Hier wie dort strömen jedes Jahr Zigtausende von Besuchern in die Stadt. Die Region wird damit ihrem Ruf gerecht, dass die dortige Bevölkerung ungebrochene wirtschaftliche Schaffenskraft durchaus mit barocker Lebensfreude in Übereinstimmung zu bringen weiß. Etwas überraschend kam dann doch die sicherheitspolitische Botschaft, Ordnung in das dortige Volksfesttreiben bringen zu wollen – und zwar mit einer Videoüberwachung. Hierzu muss man wissen, dass sogar bei größer dimensionierten Volksfesten, wie etwa dem Cannstatter Volksfest, eine Videoüberwachung durch Stadt oder Polizei nicht praktiziert wird – ohne erkennbaren Verlust an Sicherheit für die Volksfestbesucher. Jedenfalls titelten die Zeitungen im Frühsommer 2004: „Die Festbesucher in Biberach sollen künftig mit Kameras überwacht werden“ und „Von Videokameras bewachte Fröhlichkeit“. Damals hatten die Stadt und die Polizeidirektion Biberach ihr neues Sicherheitskonzept für das anstehende Schützenfest der Öffentlichkeit vorgestellt. Dabei beriefen sie sich auf die Polizeidirektion Ravensburg. Diese habe schon im Jahr zuvor das Rutenfest videoüberwacht.

Als wir nach den konkreten Gründen für die Videoüberwachung fragten und Näheres dazu wissen wollten, welche Videotechnik zum Einsatz kommen soll, bestätigten die Polizeidirektionen Biberach und Ravensburg, dass sie vorhaben, bestimmte Bereiche des Schützenfests bzw. des Rutenfests mit Videokameras zu überwachen, und gaben zunächst bereitwillig Auskunft dazu. Dass wir dann in unseren Stellungnahmen die beabsichtigte Videoüberwachung des Schützenfests als unzulässig bezeichneten und die geplante Videoüberwachung des Rutenfests mit diversen Fragezeichen versahen, war ihnen offenbar zu viel der Zuwendung. Die Polizeidirektion Biberach stellte den Schriftwechsel mit uns ein und ersuchte das Innenministerium um Schützenhilfe. Das Innenministerium sprang der Polizeidirektion Biberach bei. Es schob unsere Einwände zur Seite und ließ uns wissen, es halte mit der Polizeidirektion Biberach die geplante Videoüberwachung des Schützenfests für vom Polizeigesetz gedeckt. Unsere eingehende Replik und unsere Ankündigung einer förmlichen Beanstandung der Videoüberwachung schlug die Polizeidirektion Biberach in den Wind. Aus der Presse erfuhren wir kurz vor Beginn des Schützenfests, dass die Polizeidirektion Biberach und die Stadt Biberach an der Videoüberwachung festhalten. Zur Videoüberwachung kam es dann doch nicht. Auf Antrag eines Bürgers, der sich unsere Argumente zu Eigen gemacht hatte, gab das Verwaltungsgericht Sigmaringen mit Beschluss vom 2. Juli 2004, also einen Tag vor Festbeginn, der Stadt Biberach und der Polizeidirektion Biberach per einstweiliger Anordnung auf, die beabsichtigte Videoüberwachung des Schützenfests 2004 zu unterlassen.

Um unseren Fragen aus dem Weg zu gehen, verfiel man in Ravensburg auf folgende Idee: Die Polizeidirektion zog sich nach der Lektüre unserer Stellungnahme zu der von ihr beabsichtigten Videoüberwachung des Rutenfests zurück und überließ der Stadt Ravensburg das Feld. Auch dort ließ man unsere einige Zeit vor Durchführung des Rutenfests gestellten Fragen liegen. Die Stadt Ravensburg ordnete dann einen Tag vor Festbeginn die polizeiliche Videoüberwachung des „Grünen Platzes“ an. Darüber informierte uns tags darauf die Polizeidirektion Ravensburg per Telefon. Erst Tage nach dem Ende des Rutenfests übersandte uns die Stadt ihre Anordnung mit dem Bemerken, der bereits erwähnte Bürger habe, wohl angespornt durch seinen Erfolg in Biberach, auch in Ravensburg versucht, die Videoüberwachung per einstweiliger Anordnung zu Fall zu bringen. Diesmal habe sich das Verwaltungsgericht Sigmaringen mit Beschluss vom 23. Juli 2004 jedoch der Meinung der Polizeibehörden angeschlossen. Die Stadt Ravensburg unterschlug dabei die Fehler, die ihr gleichwohl bei der Anordnung der Videoüberwachung unterlaufen waren.

Keine Frage: Wäre es bei den beiden Videoüberwachungsvorhaben in Biberach und Ravensburg bloß um reine Übersichtsaufnahmen gegangen, auf denen die Festbesucher nicht zu identifizieren sind, wäre hier nicht viel Aufhebens zu machen. Um solche Übersichtsaufnahmen ging es bei der polizeilichen Videoüberwachung des Schützenfests und des Rutenfests jedoch gerade nicht. Vielmehr können mit den hochmodernen Videokameras, die in Biberach zum Einsatz kommen sollten und in Ravensburg zum Einsatz kamen, Festbesucher selbst über große Entfernungen so aufgenommen werden, dass sie auf den Bildern identifizierbar sind und auch bei schwierigen Lichtverhältnissen und sogar bei Nacht überwacht werden können. Zudem lassen sich die Videobilder mit Hilfe eingebauter Zoom-Objektive bis ins Detail vergrößern. Dabei werden von einer polizeilichen Videoüberwachung unterschiedslos sämtliche Festbesucher erfasst, die in den Bereich der Videokameras kommen; somit werden ganz überwiegend völlig unverdächtige Personen ins Visier genommen. Dabei wird nicht nur ihre Anwesenheit von der Polizei mit Hilfe der Videokameras beobachtet. Erfasst wird dabei vielmehr auch, wie sich die Festbesucher dabei geben, mit wem sie sich dort aufhalten, wie sie sich etwaigen Begleitern oder Begleiterinnen gegenüber verhalten und ob ihr Verhalten in ein bestimmtes Raster passt oder nicht. Deshalb gehen mit einer solchen Videoüberwachung gravierende Eingriffe in das Grundrecht auf informationelle Selbstbestimmung einher, das jedem Bürger die Befugnis gewährleistet, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Eine solche Videoüberwachung kann deshalb nur aufgrund einer entsprechenden gesetzlichen Regelung eingerichtet werden.

1.1 Biberach

Uns gegenüber berief sich die Polizeidirektion Biberach für die beabsichtigte Videoüberwachung des Schützenfests auf § 20 Abs. 2 des Polizeigesetzes (PolG). Auf diese Vorschrift ließ sich die Videoüberwachung jedoch nicht stützen.

– Zumindest fraglich ist bereits, ob diese Vorschrift hier überhaupt anwendbar ist. § 20 Abs. 2 PolG ist die allgemeine Ermächtigungsnorm für die Erhebung personenbezogener Daten durch die Polizei. Auf diese Vorschrift kann die Polizei nur zurückgreifen, soweit eine Maßnahme der Datenerhebung nicht in einer speziellen Vorschrift des Polizeigesetzes geregelt ist. In welchen Fällen die Polizei zum Mittel der Videoüberwachung greifen darf, hat aber der Gesetzgeber in § 21 PolG besonders geregelt. Danach darf eine polizeiliche Videoüberwachung – bei Vorliegen der weiteren Voraussetzungen dieser Vorschrift – nur bei bestimmten öffentlichen Veranstaltungen und Ansammlungen sowie an besonders gefährdeten Objekten und an Kriminalitätsbrennpunkten eingerichtet werden. Liegen die Voraussetzungen dieser besonderen Vorschrift für eine polizeiliche Videoüberwachung nicht vor – was bei der beabsichtigten Videoüberwachung des Biberacher Schützenfests auch von der Polizeidirektion Biberach und vom Innenministerium so gesehen wurde – und ließe man gleichwohl einen Rückgriff auf § 20 Abs. 2 PolG zu, wären die besonderen Voraussetzungen, an deren Vorliegen der Gesetzgeber die polizeiliche Videoüberwachung wegen der damit einhergehenden gravierenden Eingriffe in das Grundrecht auf informationelle Selbstbestimmung in § 21 PolG geknüpft hat, Makulatur.

– Selbst wenn man einen Rückgriff auf § 20 Abs. 2 PolG für möglich hält, vermochte diese Vorschrift die beabsichtigte Videoüberwachung des Schützenfests nicht zu tragen, weil die rechtlichen Voraussetzungen nicht erfüllt waren. Nach § 20 Abs. 2 PolG kann die Polizei Daten von Personen, durch deren Verhalten oder Sachen die öffentliche Sicherheit oder Ordnung bedroht wird, und von anderen Personen erheben, soweit dies zur Abwehr einer Gefahr oder zur Beseitigung einer Störung für die öffentliche Sicherheit oder Ordnung erforderlich ist. Voraussetzung für die Zulässigkeit einer Datenerhebung nach dieser Vorschrift ist das Vorliegen einer konkreten Gefahr. Eine solche Gefahr liegt jedoch nur vor, wenn ein bestimmter einzelner Sachverhalt, also eine konkrete Sachlage, bei ungehindertem Ablauf des ob-

jektiv zu erwartenden Geschehens mit hinreichender Wahrscheinlichkeit zu einem Schaden für die öffentliche Sicherheit oder Ordnung führen würde. Solche Umstände hatte die Polizeidirektion Biberach jedoch nicht dargetan; dafür war auch sonst nichts ersichtlich. Insbesondere vermochte ihr Hinweis, in den für die Videoüberwachung vorgesehenen Bereichen des Schützenfests komme es zu derart großen Ansammlungen insbesondere jugendlicher Festbesucher, dass ein Durchkommen kaum möglich sei, die Annahme einer konkreten Gefahr nicht zu rechtfertigen. Derartige Ansammlungen sind für solche Volksfeste vielmehr typisch und gehen mit der von den Veranstaltern des Biberacher Schützenfests durchaus angestrebten, ständig zunehmenden Anziehungskraft des Schützenfests geradezu zwangsläufig einher. Zwar kann auch eine bloße Menschenansammlung zu einer konkreten Gefahr werden, etwa wenn Panikreaktionen entstehen. Dass es dazu beim Schützenfest kommen könnte, hatte aber die Polizeidirektion Biberach selbst nicht behauptet. Im Gegenteil: Sie sah sich gar nicht aufgerufen, etwas an dem massenhaften Zustrom von Festbesuchern zu ändern. Ihr lag vielmehr daran, die gute Laune der Festbesucher nicht durch den Einsatz von Polizeikräften zu stören. Abgesehen davon war auch nicht ersichtlich, wie durch die Videoüberwachung der massenhafte Zustrom von Festbesuchern verhindert werden sollte. Ebenso blieb unklar, was die Videoüberwachung gegen den von der Polizeidirektion Biberach beobachteten zunehmenden Alkoholkonsum auf dem Schützenfest und dagegen bewirken sollte, dass bei dem Gedränge Gläser zu Bruch gehen und sich jemand an den Scherben verletzen könnte – dies aber war eine der Befürchtungen der Polizeidirektion, die sie im Zusammenhang mit der beabsichtigten Videoüberwachung geäußert hatte. Schließlich vermochten auch die Straftaten und Ordnungswidrigkeiten, die sich nach den Angaben der Polizeidirektion Biberach beim Schützenfest 2003 ereignet hatten (ein Diebstahl eines Rucksacks, zwei Körperverletzungen, zwei Verstöße gegen das Betäubungsmittelgesetz und eine Sachbeschädigung), die Annahme einer konkreten Gefahr der Straftatenbegehung beim Schützenfest 2004 schon deshalb nicht zu rechtfertigen, weil sich diese Vorfälle zum Teil ganz woanders zugetragen hatten und nicht den Schluss zuließen, dass sich im geplanten Überwachungsbereich regelmäßig Diebstähle oder Drogendelikte zutragen. Kurzum: Auf § 20 Abs. 2 PolG ließ sich die beabsichtigte Videoüberwachung des Schützenfests nicht stützen. Deshalb und weil sie auch von keiner anderen Vorschrift des Polizeigesetzes gedeckt war, war das Videoüberwachungsvorhaben der Stadt und der Polizeidirektion Biberach unzulässig, was ihnen das Verwaltungsgericht Sigmaringen schließlich auch bestätigte.

1.2 Ravensburg

Die Stadt und die Polizeidirektion Ravensburg haben sich für die Videoüberwachung des Rutenfests auf § 21 Abs. 3 PolG berufen. Nach dieser Vorschrift kann eine polizeiliche Videoüberwachung bei Vorliegen der weiteren Voraussetzungen dieser Vorschrift an Kriminalitätsbrennpunkten eingerichtet werden. Dass die Polizeidirektion und die Stadt Ravensburg unseren Fragen hierzu durch ihren spontanen „Rollentausch“ aus dem Weg gegangen sind und sich hinter den Beschluss des Verwaltungsgerichts Sigmaringen vom 23. Juli 2004 – auch wenn dieser lediglich im summarischen Verfahren ergangen ist – zurückgezogen haben, lässt sich nicht ändern. Nicht mehr akzeptabel, weil rechtswidrig, war die Vorgehensweise der Stadt Ravensburg bei der Anordnung der polizeilichen Videoüberwachung jedoch in folgenden Punkten:

– Statt in ihrer Anordnung vom 22. Juli 2004 die Videoüberwachung wenigstens auf die nach der Einschätzung der Polizeidirektion Ravensburg für die Begehung von Straftaten oder Ordnungswidrigkeiten relevanten Abend- und Nachtstunden zu beschränken, hat die Stadt Ravensburg die Überwachung des „Grünen Platzes“ mit zwei Videokameras während des gesamten Rutenfests, also rund um die

Uhr angeordnet. Eine so großzügige Anordnung der Videoüberwachung stand mit § 21 Abs. 3 PolG auf keinen Fall im Einklang. Danach muss eine polizeiliche Videoüberwachung auf die für die Begehung von Straftaten und Ordnungswidrigkeiten an der überwachten Örtlichkeit relevanten Zeiten beschränkt werden. Dieser Fehler war keine Lappalie, weil die Stadt Ravensburg dabei außer Acht gelassen hat, dass jede Stelle, die eine polizeiliche Videoüberwachung anordnet, von Anfang an darauf bedacht sein muss, dass dadurch nicht stärker als unausweichlich in die Grundrechte der mit einer solchen Videoüberwachung ins Visier genommenen Personen eingegriffen wird. Ihr nachträglicher Versuch, sich insoweit mit einem Hinweis auf die „Ravensburger Durchführungsvorschriften" zu exkulpieren, ging gründlich daneben. Hätte die Stadt einen Blick in ihre Vorschriften geworfen, hätte sie sehen können, dass darin ebenfalls stand, dass die Videoüberwachung für die Dauer des Rutenfests 2004 angeordnet wird, und nichts davon zu lesen war, dass die Videoüberwachung nur in den späten Abend- und Nachtstunden laufen soll.

- Zum anderen hat die Stadt Ravensburg dem Gebot der Offenheit der Videoüberwachung nach § 21 Abs. 3 PolG nicht hinreichend Rechnung getragen. Dieses Gebot verlangt, dass allen Personen klipp und klar vor dem Betreten der überwachten Örtlichkeit vor Augen geführt wird, dass sie dort einer Videoüberwachung ausgesetzt sind. Darauf ist durch Schilder hinzuweisen, die leicht verständlich und gut erkennbar sein müssen und in ausreichender Zahl anzubringen sind. Dazu hat die Stadt Ravensburg – was aber ihre Sache gewesen wäre – keinerlei Festlegungen getroffen.
- Schließlich hat die Stadt Ravensburg vor der Anordnung der Videoüberwachung die nach § 12 des Landesdatenschutzgesetzes (LDSG) gebotene Vorabkontrolle nicht durchgeführt. Eine solche Kontrolle soll sicherstellen, dass durch eine Videoüberwachung das Recht auf informationelle Selbstbestimmung der Betroffenen nicht gefährdet wird. Bei der dazu notwendigen Untersuchung sind die Risiken, die mit einer Videoüberwachung einhergehen, festzustellen und zu bewerten. Sie muss sich auch damit auseinander setzen, ob unter Berücksichtigung der technischen und organisatorischen Datenschutzmaßnahmen Gefahren für das Recht auf informationelle Selbstbestimmung angemessen verhindert werden. Das Ergebnis der Vorabkontrolle ist nach § 12 Abs. 2 LDSG schriftlich festzuhalten und dem behördlichen Datenschutzbeauftragten oder, wenn ein solcher nicht bestellt ist, unserem Amt zur Prüfung zuzuleiten. Erst wenn durch dieses Verfahren sichergestellt ist, dass besondere Gefahren für das Recht auf informationelle Selbstbestimmung nicht bestehen oder durch geeignete technische oder organisatorische Maßnahmen verhindert werden, darf mit einer Videoüberwachung begonnen werden. Hätte die Stadt Ravensburg eine solche Vorabkontrolle durchgeführt, wären ihr wenigstens die beschriebenen Datenschutzverstöße erspart geblieben.

Was ist das Fazit?

Die Videoüberwachung öffentlich zugänglicher (Fest-)Plätze darf nicht zur polizeilichen Standardmaßnahme werden, die zeitlich beliebig praktiziert werden kann und – wie das Innenministerium offenbar meint – bereits dann Platz greifen soll, wenn es sicherheitspolitisch wünschenswert oder notwendig erscheint. Zielrichtung von § 21 Abs. 3 PolG ist nämlich, gewachsene Schwerpunkte des Kriminalitätsgeschehens, also solche Örtlichkeiten einer polizeilichen Videoüberwachung unterziehen zu können, die aus sog. exogenen Ursachen ein überdurchschnittlich problematisches Kriminalitätslagebild aufweisen. Geht es dagegen um im weitesten Sinn von der Verwaltung selbst veranlasste oder sogar betriebene Veranstaltungen, ist das dort zu verzeichnende Kriminalitätsgeschehen endogen verursacht. Mit anderen Worten: Die von der Verwaltung (mit-)getragene Veranstaltung ist selbst mitursächlich für das Entstehen des Kriminalitätslagebilds. Entstehungsgeschichte sowie Sinn und Zweck der Vorschrift sprechen dafür, dass § 21 Abs. 3 PolG auf solche gesteuerten und temporär begrenzten Veranstaltun-

gen nicht anwendbar ist. Denn es wäre nur schwer verständlich, wenn – um es am Beispiel des vorliegenden Falles zu sagen – die Stadt und die Polizeidirektion Ravensburg, deren Aufgabe es eigentlich ist, Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren und gegen Störungen der öffentlichen Sicherheit oder Ordnung einzuschreiten, eine öffentliche Veranstaltung (mit-)veranstalten oder zumindest mittragen und damit solche Zustände schaffen oder zumindest nicht von vornherein verhindern, dass dort nach Einschätzung der Polizeidirektion Ravensburg von einem Kriminalitätsbrennpunkt gesprochen werden muss. Einzuräumen ist, dass das Verwaltungsgericht Sigmaringen in seiner das Rutenfest betreffenden Entscheidung – die ja im Eilverfahren ergangen ist – diese grundlegende rechtliche Fragestellung nicht weiter vertieft hat. Hier wäre eine abschließende Entscheidung im Hauptsacheverfahren wünschenswert gewesen, die aber vom Landesbeauftragten als nicht am Verfahren Beteiligten nicht herbeigeführt werden kann.

2. Ausschreibung von Ausländern im SIS und im INPOL

Im Jahr 1985 schlossen die Regierungen Frankreichs, der Benelux-Staaten und der Bundesrepublik Deutschland das erste Schengener Übereinkommen. Ziel war es, die Kontrollen des Personenverkehrs an den Binnengrenzen dieser Staaten zu beseitigen und den Warenverkehr zu erleichtern. Mit dem zweiten Schengener Abkommen vom Juni 1990 entstand ein umfangreiches Vertragswerk, das der Zusammenarbeit der Sicherheitsbehörden in Europa neue Möglichkeiten eröffnete. Kernstück dieses Abkommens ist das Schengener Informationssystem (SIS), das im März 1995 in Betrieb gegangen ist. Der Sache nach handelt es sich beim SIS um eine europaweite Fahndungsdatei, auf die u. a. auch alle baden-württembergischen Polizeidienststellen online zugreifen können. Mittlerweile sind praktisch alle europäischen Staaten an den SIS-Zentralrechner in Straßburg angeschlossen. Im SIS sind derzeit von deutschen Stellen 180 000 ausgewiesene oder abgeschobene Ausländer ausgeschrieben; 23 000 dieser Ausschreibungen stammen aus Baden-Württemberg. In der Personenfahndungsdatei des Informationssystems der Polizei (INPOL), an die ebenfalls alle Polizeidienststellen des Landes online angeschlossen sind, sind derzeit 480 000 ausgewiesene oder abgeschobene Ausländer ausgeschrieben, Zigtausende dieser Ausschreibungen stammen aus Baden-Württemberg.

Mit einer nach dem Zufallsprinzip gezogenen Stichprobe von 49 Personen, die auf Veranlassung baden-württembergischer Ausländerämter im SIS und zugleich im INPOL ausgeschrieben worden waren, befassten wir uns näher. Den Auftrag für diese Ausschreibungen hatten die Ausländerämter der Städte Aalen, Backnang, Böblingen, Ditzingen, Freiburg, Geislingen, Heilbronn, Karlsruhe, Konstanz, Ludwigsburg, Lörrach, Mannheim, Oberkirch, Offenburg, Rastatt, Ravensburg, Sindelfingen, Stuttgart, Vaihingen und Weingarten und der Landratsämter Alb-Donau-Kreis, Biberach, Esslingen, Göppingen, Karlsruhe, Ludwigsburg, Ortenaukreis, Rhein-Neckar-Kreis, Sigmaringen und Tübingen sowie die Bezirksstellen für Asyl der Regierungspräsidien Freiburg und Tübingen und die Landesaufnahmestelle für Flüchtlinge des Regierungspräsidiums Karlsruhe erteilt. Den Auftrag erledigten die Datenstationen der Polizeidirektionen Aalen, Biberach, Böblingen, Esslingen, Freiburg, Göppingen, Heidelberg, Heilbronn, Konstanz, Lörrach, Ludwigsburg, Offenburg, Rastatt, Ravensburg, Reutlingen, Sigmaringen, Tübingen, Ulm und Waiblingen sowie die Datenstationen der Polizeipräsidien Mannheim und Karlsruhe und der Landespolizeidirektion Stuttgart II über ihren Online-Anschluss an SIS und INPOL. Die Aufträge wurden den Datenstationen unter Verwendung des Vordrucks erteilt, den die Polizei beispielsweise für die Fahndung nach gesuchten Straftätern verwendet. Für unsere Prüfung zogen wir die Akten der Ausländerbehörden und der Datenstationen bei.

Um das Ergebnis vorwegzunehmen: Vieles war bei der Ausschreibung der 49 Ausländer im SIS und im INPOL nicht in Ordnung. So waren Ausländer im SIS ausgeschrieben, obwohl es dafür keine Rechtsgrundlage gab. In anderen Fällen waren Ausländer mit zu langen Ausschreibungsfristen im INPOL zur Personenfahndung ausgeschrieben. Selbst nach Ablauf der (zu langen) Ausschreibungsfristen wollen praktisch die Hälfte der Ausländer-

behörden die Ausschreibungen unbegrenzt fortbestehen lassen. Die allermeisten der 49 Ausländer waren im Auftrag der Ausländerämter im INPOL zur Festnahme ausgeschrieben worden, ohne dass eine richterliche Anordnung zur Festnahme vorlag. Ihre Ausschreibungsaufträge hatten die Ausländerämter recht lückenhaft ausgefüllt: Mal haben sie gar nicht angekreuzt, in welchem Fahndungssystem die Datenstationen den jeweiligen Ausländer zur Personenfahndung ausschreiben sollen, mal diese oder jene Kombination. In beinahe der Hälfte der überprüften Fälle haben die Ausländerbehörden in ihrem Ausschreibungsauftrag keinen Löschtermin für die SIS/INPOL-Ausschreibung eingetragen. In zwei Drittel der Fälle hatten die Ausländerbehörden dem Ausschreibungsauftrag ihre Ausweisungsverfügung oder den Bescheid, mit dem das Bundesamt für die Anerkennung ausländischer Flüchtlinge den Antrag des Ausländers auf Anerkennung als Asylberechtigter abgelehnt hatte, beigefügt und damit viel zu viele Daten an die Polizei weitergegeben. Es gab praktisch kaum einen Fall, der aus datenschutzrechtlicher Sicht ohne Fehler war.

2.1 Keine Drittausländer

Nicht in Ordnung war, dass unter den 49 im SIS ausgeschriebenen Personen Bürger aus den zehn Staaten waren, die am 1. Mai 2004 der Europäischen Union beigetreten sind. Nach Artikel 96 des Übereinkommens zur Durchführung des Schengener Übereinkommens (SDÜ) können unter den weiteren Voraussetzungen dieser Vorschrift nur Drittausländer im SIS zur Einreiseverweigerung ausgeschrieben werden. Drittausländer sind nach Artikel 1 SDÜ Personen, die nicht Staatsangehörige eines der Mitgliedstaaten der Europäischen Gemeinschaften sind. Bürger aus den zehn Staaten, die am 1. Mai 2004 der Europäischen Union beigetreten sind, durften demzufolge ab diesem Zeitpunkt nicht (mehr) im SIS zur Einreiseverweigerung ausgeschrieben sein. Tatsächlich waren solche Personen jedoch auch noch nach dem 1. Mai 2004 im SIS ausgeschrieben. So ging es beispielsweise einer Frau aus Tschechien. Sie hatte ein Ausländeramt aus Anlass ihrer Ausweisung und Abschiebung im November 1999 im SIS ausgeschrieben. Die Löschung ihrer Ausschreibung im SIS hat das Ausländeramt erst im Juni 2004, als wir es im Zuge unserer Prüfung darauf angesprochen haben, in die Wege geleitet.

2.2 Weder ausgewiesen noch abgeschoben und dennoch im SIS ausgeschrieben

Nach Artikel 96 Abs. 3 SDÜ können Ausländerämter Drittausländer bei Vorliegen der weiteren Voraussetzungen dieser Vorschrift im SIS zur Personenfahndung ausschreiben, wenn der Drittausländer ausgewiesen oder abgeschoben worden ist. Näheres dazu regeln die Allgemeinen Anwendungshinweise zum Schengener Durchführungsübereinkommen (AAH-SDÜ) und die Verwaltungsvorschrift des Innenministeriums, des Justizministeriums und des Sozialministeriums über die Ausweisung von Ausländern (VwV-Ausweisung). Nach Nr. 2.2.1.3 AAH-SDÜ bietet Artikel 96 Abs. 3 SDÜ keine Rechtsgrundlage für die Ausschreibung von Drittausländern im SIS zum Zweck der Aufenthaltsermittlung. Deshalb bestimmt Satz 2 dieser Regelung, dass beispielsweise ein abgelehnter Asylbewerber, der untergetaucht ist, nicht im SIS ausgeschrieben werden kann. Ebenfalls darf ein zurückgewiesener oder zurückgeschobener Drittausländer – so steht es in Nr. 2.2.1.4 AAH-SDÜ – nicht im SIS ausgeschrieben werden. Entgegen diesen klaren Regelungen hatten Ausländerämter sechs der 49 Ausländer im SIS zur Personenfahndung ausgeschrieben, sei es, dass sie nach der Ablehnung ihres Antrags auf Anerkennung als Asylberechtigte nach unbekannt verzogen oder unkontrolliert ausgereist oder zu ihrer Familie nach Österreich überstellt oder dass sie nach Frankreich, wo einer von ihnen ein Asylverfahren angestrengt hatte, zurückgeschoben worden waren. Bei diesen unzulässigen SIS-Ausschreibungen handelte es sich keineswegs bloß um eine Petitesse, denn sie können dazu führen, dass die so ausgeschriebenen Ausländer beim Versuch, in das Gebiet der Europäischen Union einzureisen, an den Außengrenzen zurückgewiesen oder von der

Polizei bei Personenkontrollen festgehalten werden. Von einer förmlichen Beanstandung dieser unzulässigen SIS-Ausschreibungen habe ich nur deshalb abgesehen, weil die Ausländerämter die sechs SIS-Ausschreibungen im Zuge unserer Prüfung umgehend gelöscht haben.

2.3 Ausschreibungsfristen im INPOL zu lang

Ausgewiesene und/oder abgeschobene Ausländer können auf Antrag der Ausländerbehörden im INPOL zur Personenfahndung ausgeschrieben werden, solange dies zur Erfüllung der Aufgaben der Ausländerbehörden erforderlich ist. Um den Ausländerbehörden die praktische Arbeit zu erleichtern, lassen sich aus den mit solchen Ausschreibungen verfolgten spezial- und generalpräventiven Zwecken Regelfristen ableiten, die sich am verwirklichten Ausweisungstatbestand orientieren. Es macht nämlich einen Unterschied, ob ein Ausländer ausgewiesen und abgeschoben worden ist, weil er beispielsweise schwere Straftaten begangen hat, oder ob er als Bürgerkriegsflüchtling aufgenommen wurde und dann später seiner Ausreisepflicht nicht nachgekommen ist. Entsprechend differenzierte Regelfristen haben das Innenministerium in der VwV-Ausweisung und das Landeskriminalamt in seiner Dienstanweisung für die Ausschreibung von Ausländern im INPOL getroffen. Danach beträgt die Ausschreibungsfrist – unbeschadet einer im Einzelfall möglichen Verlängerung – im Falle einer Ausweisung bzw. Abschiebung wegen besonderer Gefährlichkeit sechs Jahre und in den übrigen Fällen drei Jahre. Diese Ausschreibungsfristen haben die Ausländerbehörden und die Datenstationen der Polizei bei 41 der 49 ausgeschriebenen Ausländer ganz erheblich überschritten, sei es dass die Ausländerbehörden statt der angemessenen drei- oder sechsjährigen INPOL-Ausschreibungsfrist in ihrem Ausschreibungsauftrag eine zehnjährige Ausschreibungsfrist verfügt haben oder dass sie in ihrem Ausschreibungsauftrag keine Ausschreibungsfrist angegeben und die Datenstationen der Polizei von sich aus eine zehnjährige INPOL-Ausschreibungsfrist vergeben haben.

2.4 Ausschreibung im INPOL zur Festnahme oder: Wo ist das Recht der Ausländerbehörden zur Festnahme?

Bei 46 der 49 Ausländer kreuzten die Ausländerbehörden auf ihren Ausschreibungsaufträgen als Zweck der Ausschreibung „Festnahme“ an. Dementsprechend schrieben die Datenstationen die Ausländer im INPOL zur „Festnahme“ aus. Bei keiner der 46 INPOL-Ausschreibungen lag eine richterliche Haft- oder Festnahmeanordnung vor. Ist jemand zur Festnahme ausgeschrieben, so kann das für ihn gravierende Folgen haben. Trifft die Polizei ihn an, nimmt sie ihn – entsprechend dem von der jeweiligen Ausländerbehörde mit der INPOL-Ausschreibung erklärtermaßen verfolgten Zweck – fest. Wird der festgenommene Ausländer dabei allein infolge der von der Ausländerbehörde veranlassten INPOL-Ausschreibung zum Verbleiben auf der Polizeidienststelle gezwungen und wird dabei seine körperliche Bewegungsfreiheit für gewisse Dauer aufgehoben, wird man von einer Freiheitsentziehung sprechen müssen. Bei Freiheitsentziehungen gilt jedoch der Grundsatz der richterlichen Präventivkontrolle. Über Zulässigkeit und Fortdauer einer Freiheitsentziehung hat nach Artikel 104 Abs. 2 Satz 1 des Grundgesetzes (GG) nur der Richter zu entscheiden. Artikel 104 Abs. 2 Satz 2 GG verlangt eine unverzügliche Entscheidung des Richters bei jeder ohne richterliche Anordnung erfolgten Freiheitsentziehung. Eine Ermächtigung zur Festnahme ohne vorherige richterliche Entscheidung gibt Artikel 104 Abs. 2 GG jedoch nicht; er setzt eine solche gesetzliche Ermächtigung vielmehr voraus.

Aus dem Ausländergesetz ergibt sich keine Regelung, die die Ausländerbehörden dazu ermächtigt, ausgewiesene und abgeschobene Ausländer im Falle ihres Antreffens im Bundesgebiet von der Polizei festnehmen zu lassen. Nach § 42 Abs. 7 Satz 2 des Ausländergesetzes (AuslG) können Ausländerämter ausgewiesene und abgeschobene Ausländer für den Fall des Antreffens im Bundesgebiet zwar zur Festnahme im INPOL ausschreiben. Diese Vorschrift verleiht den Ausländerbehörden

jedoch keine Befugnis, solche Ausländer von der Polizei festnehmen zu lassen, sondern setzt vielmehr eine Festnahmeberechtigung voraus. Nach § 57 AuslG können Ausländer bei Vorliegen der weiteren Voraussetzungen dieser Vorschrift zur Vorbereitung oder zur Sicherung der Abschiebung in Haft genommen werden. Diese Vorschrift verlangt aber eine richterliche Anordnung der Abschiebungshaft; ohne richterliche Anordnung gestattet sie keine Freiheitsentziehung eines Ausländers, auch nicht zum Zwecke dessen Vorführung vor den Haftrichter, damit dieser über die von der Ausländerbehörde oder der Polizei beantragte Abschiebungshaft entscheidet. Schließlich verleiht auch § 49 AuslG den Ausländerbehörden kein Recht, ausgewiesene und abgeschobene (Dritt-)Ausländer von der Polizei festnehmen zu lassen. Nach dieser Vorschrift ist ein ausreisepflichtiger Ausländer abzuschieben, wenn die Ausreisepflicht vollziehbar ist und wenn ihre freiwillige Erfüllung nicht gesichert oder aus Gründen der öffentlichen Sicherheit und Ordnung eine Überwachung der Ausreise erforderlich erscheint. Zwar wird allein in der Durchführung der Abschiebung selbst unter Anwendung unmittelbaren Zwangs, die ohne vorherige richterliche Anordnung gestattet ist, keine freiheitsentziehende, sondern lediglich eine freiheitsbeschränkende Maßnahme gesehen. Maßnahmen des unmittelbaren Zwangs gegen Personen zur Durchsetzung eines Verhaltens, zu dem sie verpflichtet sind, werden nämlich nicht deshalb zu Freiheitsentziehungen, weil mit ihnen Eingriffe in die körperliche Bewegungsfreiheit verbunden sind. Dies gilt auch für die Abschiebung, mit der die Pflicht eines Ausländers, das Bundesgebiet zu verlassen, zwangsweise durchgesetzt wird. Diese Maßnahme ist nicht auf ein Festhalten des Ausländers gerichtet, sondern darauf, dass er sich außer Landes begibt oder dorthin befördert wird. Um solche Maßnahmen des unmittelbaren Zwangs geht es aber bei den im vorliegenden Zusammenhang in Rede stehenden Ausschreibungen von ausgewiesenen und abgeschobenen (Dritt-)Ausländern gerade nicht. Deren erklärter Zweck ist vielmehr sicherzustellen, dass ein trotz Ausweisung und Abschiebung erneut ins Bundesgebiet eingereister Ausländer festgenommen und festgehalten wird, bis das zuständige Ausländeramt die gebotenen ausländerrechtlichen Maßnahmen in die Wege geleitet oder getroffen hat. Nach alledem und weil auch sonst keine gesetzliche Vorschrift ersichtlich ist, die den Ausländerämtern eine Befugnis einräumt, ausgewiesene und abgeschobene Ausländer von der Polizei ohne richterliche Anordnung festnehmen zu lassen, fehlt es an einer tragfähigen Grundlage für die Ausschreibung solcher Ausländer im INPOL zur Festnahme. Deshalb bestimmt die VwV-Ausweisung zu Recht, dass ausgewiesene und abgeschobene Ausländer nicht zur Festnahme, sondern zur Einreiseverweigerung im INPOL ausgeschrieben werden.

2.5 Ausschreibungsaufträge unzureichend

Wollen Ausländerbehörden ausgewiesene oder abgeschobene Ausländer von den Datenstationen der Polizeidienststellen im SIS oder im INPOL zur Personenfahndung ausschreiben lassen, müssen sie den Datenstationen vollständige und zutreffende schriftliche Aufträge erteilen. So verlangt es § 7 LDSG. Schriftlich festlegen müssen die Ausländerbehörden danach in ihren Ausschreibungsaufträgen vor allem, in welchem polizeilichen Fahndungssystem der jeweilige Ausländer zu welchem Zweck ausgeschrieben und wann die Ausschreibung wieder gelöscht werden soll. Die Datenstationen müssen sich an diese Aufträge halten; sie dürfen sie nicht eigenmächtig abändern und bei der Ausschreibung nach eigenem Gusto verfahren. Diesen Anforderungen des Landesdatenschutzgesetzes an eine vorschriftsgemäße Datenverarbeitung im Auftrag haben die Ausländerbehörden und die Datenstationen nicht Rechnung getragen.

– Fahndungsmittel nicht oder nur unzureichend bestimmt

In 27 der überprüften 49 Fälle haben die Datenstationen die Ausländer nicht in dem von den Ausländerbehörden auf den Ausschreibungsanträgen angegebenen Fahndungssystem ausgeschrieben. Sie haben diese Ausländer jeweils im SIS und im INPOL zur Personen-

fahndung ausgeschrieben, obwohl die Ausländerämter in ihren Ausschreibungsaufträgen entweder gar kein Fahndungssystem angegeben oder nur „SIS“ oder nur „INPOL“ angekreuzt hatten. So eigenmächtig dürfen sich die Datenstationen aber nicht über Aufträge der Ausländerbehörden hinwegsetzen.

– Keine oder zu lange Ausschreibungsfrist

Ihrer Pflicht als Auftraggeber, die Frist für die INPOL- und die SIS-Ausschreibung in ihren Aufträgen korrekt festzulegen, sind die Ausländerbehörden in 41 der überprüften 49 Fälle nicht nachgekommen. In 22 Fällen haben sie in ihren Ausschreibungsaufträgen den Datenstationen gar keine Ausschreibungsfrist und in weiteren 19 Fällen viel zu lange Ausschreibungsfristen eingetragen. Dass die Datenstationen in den 22 Fällen, in denen die Ausländerbehörden in ihren Ausschreibungsaufträgen keine Ausschreibungsfrist eingetragen haben, aus eigener Entscheidung einfach eine zehnjährige Ausschreibungsfrist in die INPOL-Datensätze eingespeichert haben, entsprach ebenfalls nicht § 7 LDSG. Nach dieser Vorschrift ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer nur im Rahmen des Auftrags und der Weisungen des Auftraggebers zulässig. Fehlen solche Weisungen oder sind sie unvollständig, darf der Auftragnehmer nicht einfach nach eigenem Gutdünken verfahren, sondern muss eine Weisung des Auftraggebers einholen. Deshalb hätten die Datenstationen in diesen 22 Fällen bei den jeweiligen Ausländerbehörden nachfragen müssen, wie lange die Ausländer zur Personenfahndung ausgeschrieben werden sollen.

– Ausschreibungszweck unzutreffend

Bei einer Ausschreibung in polizeilichen Fahndungssystemen kommt es entscheidend darauf an, zu welchem Zweck jemand ausgeschrieben ist. Die ausgeschriebene Person muss nämlich im Falle ihres Antreffens durch die Polizei mit unterschiedlichen Maßnahmen rechnen, je nach dem, zu welchem Zweck sie ausgeschrieben ist. Zur Festnahme dürfen Ausländerbehörden ausgewiesene oder abgeschobene Ausländer nach dem oben Gesagten in polizeilichen Fahndungssystemen nur ausschreiben lassen, wenn ihnen ein Recht zur Festnahme der ausgeschriebenen Ausländer zur Seite steht. Da dies aber – wie oben erläutert – nicht der Fall war, hätten die Ausländerbehörden in ihren Ausschreibungsaufträgen den Datenstationen nicht vorgeben dürfen, dass die Ausländer im INPOL zur Festnahme auszuschreiben sind.

2.6 Zur Verlängerung der Ausschreibungen im SIS

Ist ein Drittausländer von einem Ausländeramt im SIS zur Einreiseverweigerung ausgeschrieben, hat das für ihn weit reichende Konsequenzen. Zum einen muss ihm die Einreise in das Hoheitsgebiet aller Vertragsstaaten verweigert werden. Zum anderen muss der Ausländer damit rechnen, dass ihm an den Außengrenzen der Europäischen Union die Einreise in das Gebiet der Vertragsstaaten verweigert wird. Drittausländer sind nämlich an den Außengrenzen einer eingehenden Kontrolle zu unterziehen. Diese umfasst nicht nur die Überprüfung seiner Grenzübertrittspapiere, sondern auch eine Abfrage des SIS. Ist er im SIS zur Einreiseverweigerung von einer Ausländerbehörde ausgeschrieben, wird er an den Außengrenzen zurückgewiesen. Eine solche SIS-Ausschreibung läuft damit praktisch auf eine Einreisesperre für das gesamte Gebiet der Europäischen Union hinaus. Wegen dieser weitreichenden Folgen dürfen Drittausländer nicht länger als erforderlich im SIS zur Einreiseverweigerung ausgeschrieben werden. Der Erforderlichkeitsgrundsatz ist in Nr. 2.2.2.1 AAH-SDÜ dahin gehend konkretisiert, dass die Ausschreibungsfristen – unbeschadet einer Verlängerung – drei oder sechs Jahre betragen, je nach dem, welchen Ausweisungstatbestand der Drittausländer verwirklicht hat. Dabei sind die SIS-Ausschreibungen nach Artikel 112 SDÜ spätestens drei Jahre nach ihrer Einspeicherung auf ihre Erforderlichkeit zu überprüfen.

Ist mit diesen Vorschriften die derzeitige Praxis, wonach nach Ablauf der dreijährigen Ausschreibungsfrist die SIS-Ausschreibung automatisch um weitere drei Jahre verlängert wird, schon schwer vereinbar, so ist es vollends bedenklich, dass die Hälfte der Ausländerbehörden die SIS-Ausschreibungsfrist an die Sperrwirkung nach § 8 AuslG koppeln will, der die Behörden eine dauerhafte und unbefristete Geltung beimessen. Dies würde in den Fällen, in denen von den betroffenen Drittausländern – was die Regel ist – kein Antrag auf Abkürzung der Sperrwirkung gestellt worden ist, dazu führen, dass die SIS-Ausschreibungen praktisch nie gelöscht werden, was auf eine ständige Einreisesperre für die betroffenen Drittausländer in das Gebiet der Europäischen Union hinausliefe. Dies dürfte nicht nur mit dem für solche Ausschreibungen nach Artikel 112 SDÜ geltenden Grundsatz der Erforderlichkeit, sondern auch mit dem Sinn und Zweck der Sperrwirkung kaum zu vereinbaren sein. Diese Sperrwirkung kann nämlich nur so lange Platz greifen, wie der mit ihr verfolgte spezial- oder generalpräventive Zweck Bestand hat. Die Frist ist so lange zu bemessen, bis dieser Zweck voraussichtlich erreicht sein wird. Hierfür ist eine Prognose unter Berücksichtigung und Abwägung aller Umstände des Einzelfalls, die für die Ausländerbehörde erkennbar sind, erforderlich. Welche Befristung der Sperrwirkung angemessen ist, kann danach von Fallgruppe zu Fallgruppe unterschiedlich sein. Dabei wird unter anderem nach der Art des Ausweisungstatbestands unter Berücksichtigung der Schwere des Ausweisungsgrunds zu differenzieren sein. Für die ausländerrechtliche Praxis lassen sich daraus Regelfristen für die Begrenzung der Sperrwirkung herleiten, an denen sich dann wiederum die SIS-Ausschreibungsfristen orientieren. Mit diesen Grundsätzen stünde die skizzierte Praxis der Ausländerbehörden nicht in Einklang, weil sie im Ergebnis dazu führen würde, dass ausgewiesene oder abgeschobene Drittausländer praktisch auf Dauer im SIS ausgeschrieben blieben. Dies würde auch den vom Innenministerium in Nr. 2.2.2.1 AAH-SDÜ und in Nr. 3 der VwV-Ausweisung für ausreichend gehaltenen drei- und sechsjährigen Regelspeicherfristen zuwiderlaufen.

2.7 Übersenden von Bescheiden unzulässig

Die Ausländerbehörden haben eine ausgesprochene Neigung, ihren Ausschreibungsaufträgen die Bescheide beizufügen, mit denen sie die jeweiligen Ausländer ausgewiesen haben oder mit denen das Bundesamt für die Anerkennung ausländischer Flüchtlinge ihren Antrag auf Anerkennung als Asylberechtigte abgelehnt hat. So sind die Ausländerbehörden in 38 der überprüften 49 Fälle verfahren. In diesen oft mehrere Seiten langen Bescheiden können die mit der Ausschreibung der betreffenden Ausländer zur Personenfahndung beauftragten Polizeidienststellen im Einzelnen nachlesen, aus welchen Gründen die Ausländer ausgewiesen worden sind oder ihr Antrag auf Anerkennung als Asylberechtigte abgelehnt worden ist. In einem Bescheid war beispielsweise in allen Einzelheiten geschildert, dass der betreffende Ausländer seine Anerkennung als Asylberechtigter beantragt hatte, weil er in seinem Heimatland bei einer Demonstration, die sich gegen die Misshandlungen seines Cousins durch die Polizei gerichtet habe, durch einen Schuss der Polizei verletzt worden sei und aus Furcht, wegen der Teilnahme an der Demonstration verfolgt zu werden, das Land habe verlassen müssen. Einem anderen Ausländer war in dem mit dem Ausschreibungsauftrag übersandten Bescheid vorgehalten worden, sich durch die Heirat mit einer namentlich genannten deutschen Bürgerin eine Aufenthaltserlaubnis erschlichen zu haben.

Die mit der Weitergabe solche Bescheide bewirkte Übermittlung sensibler personenbezogener Daten an die Polizeidienststellen war unzulässig, weil sie sich weder auf das Landesdatenschutzgesetz noch auf eine sonstige Vorschrift stützen ließ. Zur auftragsgemäßen Ausschreibung der Ausländer im SIS und im INPOL mussten die Polizeidienststellen nämlich nicht wissen, weswegen der betreffende Ausländer ausgewiesen oder sein Antrag auf Anerkennung als Asylberechtigter abgelehnt worden ist. Weil in den in Rede stehenden Fällen eine Hinterlegung der

den Ausweisungen zugrunde liegenden Bescheide beim Ausländerzentralregister vorgeschrieben war, konnten die Ausländerbehörden ihre großzügige Weitergabepraxis auch nicht auf die VwV-Ausweisung stützen. Danach können die Ausländerbehörden ihren Ausschreibungsaufträgen einen kurz gefassten Schriftsatz mit den für die Ausweisung maßgeblichen Rechtsvorschriften und Gründen nur in den Fällen beifügen, in denen die Ausweisungsverfügung nicht beim Ausländerzentralregister hinterlegt worden ist. Eine solche Hinterlegung war im vorliegenden Zusammenhang aber nach den dafür einschlägigen Vorschriften gerade vorgeschrieben.

Das Innenministerium leitete uns kurz vor Redaktionsschluss des Tätigkeitsberichts seine Stellungnahme zu. Es ist mit uns einig, dass die Ausschreibung von Staatsangehörigen der zehn Staaten, die am 1. Mai 2004 der Europäischen Union beigetreten sind, seitdem im SIS unzulässig ist und dass Ausschreibungen, die lediglich den Zweck der Aufenthaltsermittlung verfolgen, im SIS nichts zu suchen haben, also insbesondere Asylbewerber, die nach der Ablehnung ihres Antrags auf Anerkennung als Asylberechtigte nach unbekannt verzogen oder unkontrolliert ausgereist sind, nicht im SIS ausgeschrieben werden dürfen. Einigkeit besteht auch darin, dass die Ausländerbehörden beim Ausfüllen ihrer Ausschreibungsaufträge mehr Sorgfalt an den Tag legen und die Aufträge vollständig und präzise ausfüllen müssen und dass die Ausländerbehörden von ihrer Praxis, mit den Ausschreibungsaufträgen komplette Ausweisungsverfügungen und Bescheide über die Ablehnung von Asylanträgen an die Polizei weiterzugeben, Abstand nehmen müssen. Auch in Sachen INPOL-Ausschreibungsfrist stimmte das Innenministerium uns zu, was aber auch nicht verwunderlich ist, da wir doch nur gefordert hatten, dass sich die Ausländerbehörden hier an die Ausschreibungsfristen halten müssen, die das Innenministerium in der VwV-Ausweisung selbst festgelegt hat. Es konnte sich allerdings den Hinweis nicht verkneifen, seine nähere Befassung mit den INPOL-Ausschreibungsfristen aus Anlass unseres Prüfberichts habe die Frage aufgeworfen, ob die Fristen ausreichend sind oder überarbeitet werden müssen.

Was die SIS-Ausschreibungsfrist angeht, betonte das Innenministerium, dass die Ausländerbehörden nach Ablauf der drei- bzw. sechsjährigen SIS-Ausschreibungsfrist prüfen müssen, ob im Einzelfall eine Verlängerung der Ausschreibungsfrist erforderlich ist. So weit, so gut. Wonach aber soll sich die Prüfung richten? Das Innenministerium will dabei – wenn wir es recht verstehen – auf die Sperrwirkung des § 8 AuslG abstellen, die ein unbefristetes und dauerhaftes Einreiseverbot nach sich ziehe. Zwar räumt es ein, dass diese Wirkungen auf Antrag in der Regel zu befristen sind. Werde ein solcher Antrag nicht gestellt und komme ein solches Befristungsverfahren nicht in Gang, solle es bei der unbefristeten Sperrwirkung und infolge dessen bei der Ausschreibung des jeweiligen Drittausländers im SIS bleiben. Dies dürfte – so das Innenministerium – in der Regel sogar im Interesse des Drittausländers liegen, weil er so davor geschützt werde, sich durch eine illegale Einreise strafbar zu machen. Diese Fürsorge in Ehren – außer Acht bleibt dabei freilich, dass diese Sichtweise des Innenministeriums im Ergebnis dazu führt, dass die SIS-Ausschreibungen bis zum Sankt-Nimmerleins-Tag bestehen bleiben. Befristungsanträge werden nämlich schon deshalb recht selten gestellt, weil die Ausländer von ihrem Recht auf Befristung der Sperrwirkung gar nichts wissen. Wie solche SIS-Endlosspeicherungen mit dem Grundsatz der Verhältnismäßigkeit in Einklang zu bringen sind, lässt das Innenministerium offen. Deshalb kann hier das letzte Wort ebenso wenig gesprochen sein wie in der Frage der Ausschreibung von ausgewiesenen oder abgeschobenen Ausländern im INPOL zum Zweck der Festnahme. Unsere Auffassung in dieser Frage führt nämlich keineswegs – wie das Innenministerium aber meint – dazu, dass unter Verstoß gegen die Strafvorschriften des § 92 AuslG eingereiste Ausländer gar nicht mehr festgenommen werden können. Trifft die Polizei solche Ausländer an, kann sie sie unter den Voraussetzungen der Strafprozessordnung vorläufig festnehmen oder unter den Voraussetzungen des Polizeigesetzes in Gewahrsam nehmen. Um die Befugnisse der Polizei geht es hier jedoch gar nicht. Nicht die Polizei, sondern vielmehr die Ausländerbehörden schreiben die Ausländer im INPOL zur Festnahme aus. Deshalb müssen sie sich schon fragen lassen,

wo im Ausländergesetz eigentlich steht, dass die Ausländerbehörden – was sie mit ihren Ausschreibungen im INPOL zum Zweck der Festnahme in der Praxis bewirken – Ausländer ohne richterliche Anordnung festnehmen oder (von der Polizei) festnehmen lassen dürfen.

3. Datenschutzlücken bei der Beurteilung von Polizeibeamten

Polizeibeamte müssen alle zwei Jahre dienstlich beurteilt werden. Nähere Regelungen zur Ausführung der dafür einschlägigen Vorschriften des Landesbeamtengesetzes und des Landesdatenschutzgesetzes hat das Innenministerium in einer Verwaltungsvorschrift getroffen, die am 1. Januar 2004 in Kraft getreten ist. Danach gibt es jetzt bei der Beurteilung für Polizeibeamte keine Noten mehr nach schulischem Muster von eins bis sechs, sondern Punkte von eins (entspricht den Anforderungen nicht) bis fünf (übertrifft die Anforderungen in besonderem Maße). Das eigentliche Novum jedoch ist: Während es früher offenbar fast nur Spitzenpolizisten mit Noten zwischen der Bestnote und 1,5 gab, dürfen jetzt innerhalb einer Beurteilungsgruppe nur noch fünf Prozent mit 4,75 bis 5,00 Punkten und nur zehn Prozent mit 4,25 bis 4,50 Punkten und nur 15 Prozent mit 4,00 Punkten benotet werden. Die zu Beurteilern bestimmten vorgesetzten Polizeibeamten fertigen sog. vorläufige Beurteilungen. Der Leiter der Beurteilungskonferenz legt unter Berücksichtigung der für die einzelnen Notenbereiche festgelegten Quoten die endgültige Beurteilung im Einzelfall fest. Die Beurteilungen sollen nach der Verwaltungsvorschrift des Innenministeriums ein umfassendes Bild über die Eignung, Befähigung und fachliche Leistung geben und einen Eindruck von der Persönlichkeit des Beurteilten vermitteln. Sie schließt mit einer Gesamtnote ab. Diese ist aus den für alle 14 Submerkmale vergebenen Einzelbewertungen unter Berücksichtigung der Bedeutung der Submerkmale sowie der Gesamtpersönlichkeit des beurteilten Polizeibeamten zu bilden. Wer den umfangreichen Beschreibungskatalog für die Erläuterung der 14 Submerkmale gelesen hat und außerdem weiß, dass den dienstlichen Beurteilungen wichtige Bedeutung für die weitere berufliche Karriere eines Polizeibeamten zukommt, dem ist ohne weiteres klar, dass es sich bei den dienstlichen Beurteilungen von Polizeibeamten um außerordentlich sensible personenbezogene Personaldaten handelt und dass die mit den Beurteilungen befassten Stellen die dafür geltenden Datenschutzvorschriften penibel beachten müssen. Dies ist den beiden Polizeidienststellen, bei denen wir uns vor Ort angesehen haben, wie sie im Frühsommer 2004 bei der Beurteilung der Beamtinnen und Beamten des mittleren und gehobenen Polizeivollzugsdienst verfahren sind, nicht immer gelungen. Bei der einen Polizeidienststelle ist dieses, bei der anderen jenes schief gelaufen; mitunter passierte derselbe Fehler hier wie dort. Doch der Reihe nach:

3.1 Vorsicht beim Erstellen der vorläufigen Beurteilungen auf PC

Kein Polizeibeamter, der als Beurteiler vorläufige Beurteilungen erstellen muss, hat die Beurteilungsformulare handschriftlich auszufüllen. Natürlich darf er – wie es dem modernen Bild der Polizei entspricht – auch dafür die Segnungen der EDV nutzen und die vorläufigen Beurteilungen am PC erstellen. Wegen der damit einhergehenden Risiken ist dabei jedoch Vorsicht geboten. Auch dienstliche Beurteilungen von Polizeibeamten sind nämlich vertraulich zu behandeln. Erstellt ein Beurteiler solche Beurteilungen am PC, muss er die erhöhten datenschutzrechtlichen Anforderungen, die das Landesbeamtengesetz an die automatisierte Verarbeitung von Personaldaten stellt, beachten. Um diesen Anforderungen Genüge zu tun und das Recht auf informationelle Selbstbestimmung der Polizeibeamten bei der Erstellung von Beurteilungen nicht stärker als unerlässlich zu strapazieren, dürfen Beurteilungen – so steht es auch in der Verwaltungsvorschrift des Innenministeriums – nicht an vernetzten PC, sondern nur an Stand-alone-PC, also nur an vom Netz der Polizei und sonstigen Netzen abgekoppelten PC erstellt und dort nicht gespeichert werden, sondern müssen nach ihrer Fertigstellung ausgedruckt und sodann unverzüglich auf dem PC gelöscht werden. Ist nämlich der PC am Netz, ist die Vertraulichkeit der dienstlichen Beurteilungen nicht gewährleistet, weil nicht ausgeschlos-

sen werden kann, dass andere Netzteilnehmer von ihrem PC aus auf die Beurteilungen zugreifen können. Selbstverständlich dürfen die Beurteiler ihre Beurteilungen nicht offen per E-Mail der Personalstelle übersenden. Das Risiko, dass die Beurteilungen an die falsche Adresse geraten oder von anderen Netzteilnehmern ausgespäht werden können, ist viel zu groß.

Diesen Anforderungen haben die beiden Polizeidienststellen nicht Rechnung getragen:

– Bei einer der beiden Polizeidienststellen sind auf dem PC, den wir uns bei einer Probe aufs Exempel näher angesehen haben, dienstliche Beurteilungen erstellt worden, obwohl der PC an das Netz der Polizei angeschlossen war und ist. Die erstellten Beurteilungen sind zudem nach ihrem Ausdruck im Zuge des Beurteilungsverfahrens nicht gelöscht worden, sondern im Zeitpunkt unserer Kontrolle, also Monate nach dem Abschluss des Beurteilungsverfahrens, immer noch auf dem vernetzten PC gespeichert gewesen. Dies stand nicht nur mit den dafür einschlägigen Vorschriften des Landesbeamtengesetzes, sondern auch mit der bereits erwähnten Verwaltungsvorschrift des Innenministeriums nicht im Einklang. Darin hat das Innenministerium – zu Recht – bestimmt, dass Beurteilungen nur an vom Netz abgekoppelten PC erstellt und nicht gespeichert werden dürfen und nach dem Ausdruck auf Papier gelöscht werden müssen. Von einer förmlichen Beanstandung dieser gravierenden Verstöße haben wir nur deshalb abgesehen, weil die Polizeidienststelle uns noch während der Kontrolle zugesichert hat, die Beurteilungen auf dem PC zu löschen und alle übrigen Beurteiler in ihrem Bereich an ihre Löschverpflichtung zu erinnern.

  Dass die vom Innenministerium in der erwähnten Verwaltungsvorschrift getroffene Anordnung, dass Beurteilungen nur an vom Netz abgekoppelten PC erstellt werden dürfen, im Zuge des Beurteilungsverfahrens bei den Beurteilern zu Diskussionen geführt hat, ist uns wohl bekannt. Zu umständlich, lautete die mildeste Form der Kritik, mit der uns gegenüber die Regelung des Innenministeriums bedacht worden ist. Den Kritikern gegenüber konnten wir die Anordnung des Innenministeriums nur loben. Es scheint wirklich nicht zu viel verlangt zu sein, für die kurze Zeit, in der die Beurteilungen zu erstellen sind und ausgedruckt werden, am PC das Netzwerkkabel zu ziehen; soviel muss der Polizei das Persönlichkeitsrecht ihrer Beamten doch wohl wert sein. Dass dies geht, hatte sich bei der anderen Polizeidienststelle gezeigt. Bei ihr sind die Beurteilungen, ohne zu jammern und zu klagen, auf einem Stand-alone-PC erstellt worden. Will man an dieser Verfahrensweise etwas ändern, darf dies jedenfalls nicht auf Kosten des Datenschutzrechts der Polizeibeamten und der Vertraulichkeit der Beurteilungen gehen.

– Bei der anderen Polizeidienststelle haben Beurteiler Beurteilungsübersichten, die sie nach der erwähnten Verwaltungsvorschrift des Innenministeriums erstellen müssen und in denen sie praktisch alle von ihnen erstellten Beurteilungen in Listenform zusammengestellt haben, unverschlüsselt per E-Mail der Personalstelle zugeleitet. Dies hat die Polizeidienststelle dann unterbunden. Daran hat sie auch gut getan, weil sie mit der unverschlüsselten Übersendung von Beurteilungsübersichten dem Gebot der Vertraulichkeit dienstlicher Beurteilungen nicht Rechnung getragen und die beim Versand derart sensibler Daten gebotenen technischen Datenschutzmaßnahmen nicht getroffen hat, mit denen ein Zugriff Unbefugter verhindert werden kann.

3.2 Was bei der Personalstelle schief lief

Das soeben für die Behandlung der dienstlichen Beurteilungen durch die Beurteiler Gesagte gilt entsprechend für die Personalstellen der Polizeidienststellen. Sie dürfen (vorläufige) dienstliche Beurteilungen von Polizeibeamten auf PC nur speichern, soweit und so lange dies für Zwecke der Personalverwaltung oder Personalwirtschaft erforderlich

ist. Dabei müssen die Personalstellen die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um eine datenschutzgerechte Verarbeitung der Beurteilungen zu gewährleisten. Hierzu sind insbesondere Maßnahmen zu treffen, die geeignet sind zu verhindern, dass Unbefugte von den gespeicherten Beurteilungen Kenntnis erlangen und Daten unbefugt gelesen, kopiert, verändert oder entfernt werden können. Mit diesen Anforderungen stand die Vorgehensweise der Personalstelle einer der beiden Polizeidienstellen nicht im Einklang, weil bei ihr auf einem vernetzten PC selbst nach Abschluss des Beurteilungsverfahrens immer noch komplette Beurteilungsübersichten mit einer Vielzahl von (vorläufigen) Beurteilungen gespeichert gewesen sind, obwohl die Personalstelle diese Beurteilungsübersichten nach eigenem Bekunden zur Erfüllung ihrer Aufgaben schon seit geraumer Zeit nicht mehr gebraucht hat. Zusätzliche Brisanz hat dieses Manko dadurch erhalten, dass weder an diesem PC noch an dem Stand-alone-PC, auf dem die Personalstelle das Beurteilungsverfahren abgewickelt hat, ein Passwortschutz eingerichtet war und dass auf dem Stand-alone-PC ausgerechnet die Gesamtübersicht, die die Personalstelle aus den Hunderten von (vorläufigen) Beurteilungen erstellt hat und in der aufgelistet ist, welcher Polizeibeamte mit welcher Note beurteilt worden ist, im Klartext gespeichert war. Beide PC der Personalstelle wie alle übrigen PC der Polizeidienstelle, an denen ebenfalls kein Passwortschutz installiert war, ließen sich allein mit der von allen Mitarbeitern der Polizeidienststelle verwendeten einheitlichen Benutzerkennung starten, die lediglich aus vier Buchstaben bestand und auch noch leicht zu erraten war. So konnte jedermann, der Zutritt zu den Räumen der Personalstelle der Polizeidienststelle hatte oder sich verschaffen konnte, nach Eingabe der polizeidienststellenweit einheitlich verwendeten, trivialen Benutzerkennung auf die auf dem Stand-alone-PC gespeicherte Gesamtübersicht über alle Beurteilungen und zudem auf die auf dem anderen PC gespeicherten Beurteilungsübersichten zugreifen. Man muss kein Experte im Datenschutzrecht sein, um zu wissen, dass eine solche Gestaltung des Zugriffsverfahrens nun wirklich nicht dem Stand der Technik entspricht und deutlich in Widerspruch zu § 9 LDSG steht.

3.3 Wohin mit den Entwürfen, Notizen und Beurteilungsbeiträgen?

Geht der Leiter der Beurteilungskonferenz mit der vorläufigen Beurteilung des Beurteilers einig, wird sie dem beurteilten Polizeibeamten eröffnet und wird sodann als endgültige Beurteilung zu seiner Personalakte genommen. So steht es im Landesbeamtengesetz und in der Verwaltungsvorschrift des Innenministeriums. Wohin aber mit den Entwürfen, Notizen und Beurteilungsbeiträgen? Auch hier hilft ein Blick in die Verwaltungsvorschrift des Innenministeriums. Dort ist nachzulesen, dass nach der Aufnahme der Beurteilungen in die Personalakten die im Zuge der Erstellung der Beurteilungen angefallenen Entwürfe, Notizen und die herangezogenen Beurteilungsbeiträge in die Sachakten der Personalstelle aufzunehmen und nach einem Jahr zu vernichten sind. Recht so! Nur so lässt sich die Vertraulichkeit der dienstlichen Beurteilungen gewährleisten und ein Herumvagabundieren dieser sensiblen Personaldaten verhindern.

An diese klaren Regelungen haben sich die beiden Polizeidienststellen nicht gehalten. Hier wie dort haben Beurteiler eine Mehrfertigung der von ihnen erstellten Beurteilungen zurückbehalten. Wenn man diese Praxis sieht, fragt man sich schon, wie es dazu kommt, dass sich zu Beurteilern bestellte Polizeibeamte so salopp über die Regelungen des Innenministeriums hinwegsetzen, das diese ja nicht aus Jux und Tollerei, sondern deshalb in seine Verwaltungsvorschrift aufgenommen hat, weil die darin vorgeschriebene Verfahrensweise zur Gewährleistung der Vertraulichkeit der dienstlichen Beurteilungen geboten ist. Daran vermag auch der Einwand, ein Beurteiler müsse sich rechtfertigen können, wenn bei ihm ein beurteilter Polizeibeamter – was in der Praxis hin und wieder vorkomme – nach Abschluss des Beurteilungsverfahrens Beschwerde über seine Beurteilung führt, nichts zu ändern; sofern überhaupt eine Gedächtnisstütze in Anspruch genommen werden muss,

könnte in einem solchen Fall notfalls auf die Original-Beurteilungen zurückgegriffen werden. Dass eine der beiden Polizeidienststellen in ihrer Dienstanweisung für die Verfahrensweise bei den Beurteilungen bestimmt hat, dass Entwürfe, Notizen, Beurteilungsbeiträge und dgl. vom Beurteiler aufzubewahren sind, steht nicht nur in offenem Widerspruch zu der Verwaltungsvorschrift des Innenministeriums, sondern hat in der Praxis dazu geführt, dass bei ihr an vielerlei Orten außerhalb ihrer Personalstelle außerordentlich sensible Personaldaten gespeichert sind, wofür es aber keine Rechtsgrundlage gibt.

3.4 Die Beurteilungskonferenz

Die Beurteilungen, insbesondere beabsichtigte Abweichungen von der vorläufigen Beurteilung, sind mit den Beurteilern und ggf. den Beurteilungsberatern mit dem Ziel zu erörtern, leistungsgerecht abgestufte und untereinander vergleichbare Gesamturteile für den Zuständigkeitsbereich des Leiters der Beurteilungskonferenz zu erreichen. Der Leiter der Konferenz gewährleistet das einheitliche Vorgehen bei der Beurteilung. Er legt nach Vorliegen sämtlicher Beurteilungsübersichten unter Berücksichtigung der für die einzelnen Notenstufen vorgesehenen Quoten die endgültige Beurteilung im Einzelfall fest. Mehr steht in der Verwaltungsvorschrift des Innenministeriums über die Beurteilungskonferenz nicht. In der Praxis sind die beiden Polizeidienststellen bei der Beurteilungskonferenz so verfahren: Beide Polizeidienststellen haben eine Beurteilungskonferenz für die Polizeibeamten des mittleren Dienstes und eine eigene Konferenz für die Polizeibeamten des gehobenen Dienstes durchgeführt. Hier wie dort haben an den beiden Beurteilungskonferenzen alle Beurteiler teilgenommen, die die Polizeibeamten der jeweiligen Gruppe zu beurteilen hatten. Im Konferenzablauf sind die beiden Polizeidienstellen mit den Daten der beurteilten Polizeibeamten so unterschiedlich verfahren, wie es unterschiedlicher nicht sein kann. Die eine Polizeidienststelle hat in den beiden Beurteilungskonferenzen jeweils eine nach Beurteilungsgruppen und innerhalb der Beurteilungsgruppen nach der in der vorläufigen Beurteilung erzielten Gesamtpunktzahl geordnete Liste an die Wand projiziert, so dass jeder Beurteiler sehen konnte, mit welcher Gesamtnote die einzelnen Polizeibeamten des mittleren bzw. gehobenen Dienstes beurteilt worden sind und an welcher Stelle sie in der jeweiligen Vergleichsgruppe rangieren. Solche personenbezogenen Übersichten hat die andere Polizeidienststelle nicht in die Beurteilungskonferenzen eingeführt. Sie hat sich vielmehr auf Übersichten beschränkt, in denen für jede Vergleichsgruppe allein anhand von aggregierten Zahlenangaben gegenübergestellt war, wie viele Polizeibeamte jeweils rein rechnerisch auf die in der Verwaltungsvorschrift des Innenministeriums für die einzelnen Notenbereiche vorgegebenen Quoten entfallen dürfen und wie viele Polizeibeamte nach den vorläufigen Beurteilungen in den jeweiligen Notenbereichen rangieren. Weil mit dieser Vorgehensweise das Datenschutzrecht der beurteilten Polizeibeamten und die Vertraulichkeit dienstlicher Beurteilungen in der Beurteilungskonferenz am besten gewahrt werden kann, muss dieses Beispiel Schule machen.

3.5 Alte Beurteilungen gespeichert

Bei einer der beiden Polizeidienststellen waren auf zwei vernetzten PC auch noch Beurteilungen aus den Jahren 2002 und 2003 gespeichert. Einer von den PC war im Schreibzimmer installiert. Dieser PC wurde zudem von mehreren Mitarbeitern und Polizeibeamten gemeinsam benutzt mit der Folge, dass sie nachschauen konnten, wie die Kollegen beurteilt worden waren. Weil die Speicherung dieser alten Beurteilungen auf den beiden PC offensichtlich rechtswidrig war, hat die Polizeidienststelle, als wir sie beim Kontrollbesuch darauf angesprochen haben, die umgehende Löschung zugesagt.

Damit die bei den Polizeidienststellen angetroffenen Fehler gründlich und rasch behoben werden, haben wir unsere Feststellungen vor kurzem an das Innenministerium herangetragen. Seine Antwort steht noch aus.

4. Einzelfälle

Nach wie vor wenden sich gerade im Sicherheitsbereich viele Bürger mit Eingaben an unser Amt. Ihre Anliegen sind unterschiedlich. Die einen fragen sich, wie polizeiinterne Informationen über sie an Dritte gelangt sind. Andere wiederum befürchten, dass die Polizei Daten über sie speichert und wollen dies überprüft wissen.

4.1 Protokollierung von automatisierten Abrufen

Automatisierte Verfahren, die die Übermittlung personenbezogener Daten durch Online-Abruf ermöglichen, bergen erhebliche Risiken für den Datenschutz. Wer einen Online-Anschluss besitzt, muss weder die speichernde Stelle nach den gewünschten Daten fragen noch muss er seine Anfrage schriftlich oder mündlich begründen. Gewissermaßen auf Knopfdruck stehen ihm alle Daten zur Verfügung. Um wenigstens im Nachhinein erkennen zu können, welche Abrufe stattgefunden haben und ob sie berechtigt gewesen sind, gehören Protokollierungsverfahren bei solchen Abrufverfahren zum datenschutzrechtlichen Standard. Wohin es führt, wenn kein Protokollierungsverfahren eingerichtet ist oder wenn die Protokollierungsvorgaben nicht befolgt werden, zeigen folgende Fälle:

– Keine Protokollierung bei POLIS-BW

Eine geschiedene Frau war alkoholisiert und ohne Fahrerlaubnis Auto gefahren und dabei von der Polizei gestoppt worden. Bereits drei Tage später konnte sie in den Akten des Verfahrens, das ihr geschiedener Mann gegen sie vor Gericht wegen des Sorgerechts für ihr gemeinsames Kind führte, darüber lesen. Dessen Anwalt argumentierte mit diesem Vorfall in dem Sorgerechtsverfahren gegen die Eignung der Frau, für das gemeinsame Kind ordentlich sorgen zu können, und berief sich dabei für die vorgebrachten Einzelheiten der Trunkenheitsfahrt, die bis dahin eigentlich nur der Polizei bekannt waren, auf das Zeugnis eines Polizeibeamten. Weil dieser Polizeibeamte neben ihrem geschiedenen Mann wohnte und wohl von Zuhause aus bei seinen Kollegen angerufen und unter näheren Angaben zur Fahrtroute der Frau den Polizeieinsatz wegen der Trunkenheitsfahrt ausgelöst hatte, mutmaßte sie, der Anwalt habe sein Wissen um die Trunkenheitsfahrt von ihrem geschiedenen Mann und dieser sein Wissen wiederum von dem Polizeibeamten.

Um das Ergebnis gleich vorwegzusagen: Die Sache ließ sich mit den Befugnissen, die uns das Landesdatenschutzgesetz an die Hand gibt, nicht klären. Den geschiedenen Mann der Frau und dessen Anwalt konnten wir nicht fragen, woher sie von der besagten Trunkenheitsfahrt wussten, weil das Landesdatenschutzgesetz nur die Behörden und öffentlichen Stellen des Landes verpflichtet, mein Amt bei der Erfüllung seiner gesetzlichen Aufgaben zu unterstützen und Auskunft zu unseren Fragen zu geben. Der Polizeibeamte wies den Verdacht von sich. Die Polizeidirektion, in deren Bereich er Dienst tat, bestätigte uns, dass der Vorkommnisbericht über die Trunkenheitsfahrt und eine sog. Kurzinformation darüber zur fraglichen Zeit in ihrem Vorgangsbearbeitungssystem POLIS-BW gespeichert gewesen ist. Zugleich ließ sie uns wissen, dass auf die Kurzinformation und die Grunddaten des Vorkommnisberichts praktisch jeder Polizeibeamte der Polizeidirektion von seinem dienstlichen PC aus zugreifen konnte. Ob ein Polizeibeamter dies in der fraglichen Zeit überhaupt getan hat und, wenn ja, wozu, konnte uns die Polizeidirektion nicht sagen, weil Abfragen des POLIS-Systems nicht protokolliert werden.

– Unzureichende Angaben bei der ZEVIS-Protokollierung

Eine junge Frau, die aus einem anderen Bundesland, wo sie mit ihrem Vater unter einem Dach gewohnt hatte, nach Baden-Württemberg zugezogen war, staunte nicht schlecht, als sie mit einem an die Adresse ihres Vaters gerichteten Brief konfrontiert wurde. Der Brief

stammte von der Mutter einer verheirateten Frau. Darin teilte sie dem Vater der jungen Frau mit, seine Tochter lebe mit ihrem Schwiegersohn zusammen, leider wisse sie nicht wo. Weil sie ihren Schwiegersohn postalisch nicht mehr erreichen könne, bitte sie ihn, den Brief an seine Tochter weiterzugeben, damit diese ihn ihrem Schwiegersohn übergeben kann. Die junge Frau wies dieses Ansinnen von sich. Sie mutmaßte, dass die Briefschreiberin über ihr Kfz-Kennzeichen an die Adresse ihres Vaters gekommen sei und dass ihr dabei ein Polizeibeamter geholfen habe, der bei einer bestimmten Polizeidienststelle Dienst tue. Von dem wisse sie aber nur, wie er mit Vornamen heißt und dass er mit dem Sohn der Briefschreiberin gut bekannt ist. Ihr Auto sei nämlich noch an ihrem früheren Wohnsitz zugelassen; bei allen anderen Stellen sei sie seit ihrem Umzug mit ihrer baden-württembergischen Adresse gemeldet.

Wir fragten beim Kraftfahrt-Bundesamt nach, ob im fraglichen Zeitraum eine baden-württembergische Polizeidienststelle über das Zentrale Verkehrs-Informationssystem (ZEVIS), von dem alle baden-württembergischen Polizeidienststellen die Halter- und Fahrzeugdaten der in Deutschland zugelassenen Kraftfahrzeuge online abfragen können, das Zentrale Fahrzeugregister mit dem Kfz-Kennzeichen der jungen Frau nach deren Halterdaten abgefragt hatte. Das Kraftfahrt-Bundesamt wertete die ZEVIS-Protokolldaten aus und meldete uns drei Treffer. Zwei davon waren im vorliegenden Zusammenhang ohne Bedeutung. Die dritte Halterabfrage hatte tatsächlich ein Polizeibeamter durchgeführt, der mit Vornamen so hieß, wie uns die junge Frau gesagt hatte. Als Anlass für den Abruf hatte der Polizeibeamte den ZEVIS-Abfrageprotokollen zufolge „Verfolgung von Straftaten, Vorermittlungen“ angegeben. Dazu muss man wissen, dass das Kraftfahrt-Bundesamt bei jeder ZEVIS-Abfrage des Zentralen Fahrzeugregisters u. a. protokolliert, wann welcher Polizeibeamte welcher Polizeidienststelle die Abfrage aus welchem Anlass vorgenommen hat. Als wir die Polizeidienststelle, bei der der Polizeibeamte beschäftigt ist, fragten, was es mit dieser ZEVIS-Abfrage auf sich hat, ließ sie uns wissen, der Polizeibeamte könne sich an die ZEVIS-Abfrage nicht mehr erinnern. ZEVIS-Abfragen würden bisher in den Ermittlungsakten nicht vermerkt. Deshalb könnten die näheren Umstände der Abfrage nicht mehr nachvollzogen werden.

Die wesentliche Ursache dafür, dass alles im Dunkeln blieb, hatte der Polizeibeamte gesetzt, weil er bei seiner ZEVIS-Abfrage die für die Protokollierung solcher Abfragen einschlägigen Vorschriften nicht hinreichend beachtet hatte. Diese besagen nämlich, dass bei dem Abfrageanlass „Verfolgung von Straftaten“ in die ZEVIS-Protokollierungsmaske am Abfragebildschirm ein auf einen bestimmten Anlass bezogenes Aktenzeichen oder eine Tagebuchnummer einzutragen ist. Ist dies nicht möglich, ist in Kurzform die Art der Straftat einzugeben. Hätte der Polizeibeamte bei der Protokollierung das Aktenzeichen oder die Tagebuchnummer des der Abfrage zugrunde liegenden Vorgangs angegeben, hätte man die Akte ziehen und nach dem Grund der Abfrage schauen können. Selbst mit der bloßen Angabe der Art der Straftat wäre man der ZEVIS-Abfrage leichter auf die Spur gekommen als mit dem nichts sagenden Eintrag „Vorermittlungen“. Wer so nachlässig mit der Protokollierung umgeht, lässt nicht nur die einschlägigen Protokollierungsvorschriften, die dem Schutz des Datenschutzrechts der Betroffenen dienen, außer Acht, sondern muss auch bedenken, dass er sich der Möglichkeit begibt, aufkeimende Zweifel an der Rechtmäßigkeit seiner ZEVIS-Abfrage auszuräumen. So aber blieb ein schaler Nachgeschmack.

4.2 Benachrichtigung in einem Todesfall

Nimmt sich ein junger Mensch das Leben, ist dies vor allem für dessen Eltern ein harter Schicksalsschlag. Ihnen die Todesnachricht zu überbringen, ist bestimmt eine schwierige Aufgabe. Darum ist kein Polizeibeamter zu beneiden. Weil sich in der ganzen Nachbarschaft die Nachricht, dass und wie sich ihr Sohn an seinem Wohnort in einem anderen

Bundesland das Leben genommen hat, wie ein Lauffeuer verbreitet hatte, noch ehe sie selbst darüber benachrichtigt worden waren, wandten sich die in Baden-Württemberg wohnenden Eltern an uns mit der Bitte zu klären, wie es dazu kommen konnte. Ihnen konnten wir in ihrer Not nur teilweise helfen.

Das für den Wohnsitz der Eltern zuständige Polizeirevier war von der Polizei des anderen Bundeslandes über den Tod des jungen Mannes benachrichtigt worden. In der Nachricht waren die näheren Umstände geschildert, wie er zu Tode gekommen war und dass nach den bisherigen Ermittlungen von einem Suizid auszugehen sei. In seiner Wohnung habe die Polizei eine Adresse gefunden, bei der es sich höchstwahrscheinlich um diejenige seiner Eltern handele. Das Polizeirevier möge bitte die Anschrift überprüfen und, sofern es dort Angehörige antreffe, ihnen die Todesnachricht überbringen und sie zu eventuell geäußerten Selbsttötungsabsichten ihres Sohnes befragen. Ihrem Ersuchen hatte die Polizei des anderen Bundeslandes ein Infoblatt mit der Telefonnummer und der Anschrift seiner für die Ermittlungen in dem Todesfall zuständigen Polizeidienststelle beigefügt. Das hiesige Polizeirevier hat bei seinem ersten Versuch die Eltern des jungen Mannes nicht angetroffen. Bei seinem zweiten Versuch stieß es an der besagten Adresse auf eine Frau und einen Mann. Von dem Mann erfuhr es, dass die Eltern im Urlaub sind und wo sie sich wahrscheinlich aufhalten. Nach seinem erfolglosen Versuch, die Eltern an ihrem Urlaubsort zu erreichen, hat das Polizeirevier der mit den Todesermittlungen befassten Polizeidienststelle des anderen Bundeslandes telefonisch berichtet. Diese Polizeidienststelle hat das Polizeirevier gebeten, das erwähnte Infoblatt in dem Briefkasten der Eltern zu hinterlegen, was das Polizeirevier umgehend tat. Dass es dabei das Infoblatt in ein Kuvert hätte stecken müssen, bedachte das Polizeirevier nicht. Stattdessen warf es das Infoblatt offen in den Briefkasten der Eltern, obwohl es wusste, dass die Eltern eine dritte Person mit dem Leeren ihres Briefkastens während ihrer Urlaubsabwesenheit beauftragt hatten, und obwohl es sich darüber im Klaren gewesen sein musste, dass so außerordentlich sensible personenbezogene Daten wie die Todesnachricht nicht in die Hände Dritter gelangen dürfen. Die richtige Lehre aus dem Datenschutzverstoß, der ihrem Polizeirevier damit unterlaufen ist, hat die vorgesetzte Polizeidirektion sofort gezogen, als wir sie darauf ansprachen. Sie hat unverzüglich angeordnet, dass sämtliche Schreiben an Bürger, die in irgendeiner Weise personenbezogene Daten enthalten, entweder persönlich übergeben oder mit eindeutiger Adressierung ausschließlich kuvertiert und verschlossen in den Briefkasten geworfen werden.

Weil dem Polizeirevier diese Selbstverständlichkeit nicht in den Sinn gekommen war, kam es, wie es kommen musste: Als die damit betraute Nachbarin vormittags den Briefkasten der Eltern leerte, bekam dabei ein anderer Nachbar, dem sie – wie uns die Eltern geschrieben haben – nie und nimmer etwas vom Tod ihres Sohnes und erst recht nicht etwas davon gesagt hätten, dass und wie er sich das Leben genommen hat, das Infoblatt zu Gesicht. Spät abends rief dieser Nachbar die Eltern an, die bis dahin noch nichts von dem Suizid ihres Sohnes wussten, und erzählte ihnen, dass und wie sich ihr Sohn das Leben genommen hat. Woher er seine Informationen hatte, ließ sich bei unseren eingehenden Nachforschungen, in die wir auch unsere Kollegen des anderen Bundeslandes eingeschaltet haben, nicht klären. Aus dem Infoblatt konnte er sie nicht haben, weil dieses ganz neutral formuliert war und keinen Hinweis darauf enthielt, dass und wie sich der junge Mann das Leben genommen hat. Fest steht jedoch, dass der besagte Nachbar vor seinem Anruf bei den Eltern zweimal bei dem hiesigen Polizeirevier und einmal bei der Polizeidienststelle des anderen Bundeslandes wegen des – wie es in dem Infoblatt hieß – Todesfalles des jungen Mannes angerufen hat. Das hiesige Polizeirevier hat uns gegenüber dazu betont, dass es dem Nachbarn bei seinen Anrufen keine Auskunft über den Suizid gegeben hat. Die Polizeidienststelle des anderen Bundeslandes hat unseren Kollegen gegenüber versichert, dass sie dem Nachbar ebenfalls keine Informationen zu dem Todesfall des jungen Mannes gegeben hat.

Dies läuft auf das merkwürdige Ergebnis hinaus, dass keine der beiden Stellen, denen zum damaligen Zeitpunkt allein bekannt war, dass und wie sich der junge Mann das Leben genommen hat, dem besagten Nachbar davon etwas gesagt haben will und dass dieser doch alles gewusst hat. Die Tugend, zu begangenen Fehlern zu stehen, ist halt doch nicht so weit verbreitet.

4.3 Daten gelöscht

Ein junger Mann mit Hochschulabschluss schrieb uns, er habe von einem Bekannten bei der Polizei erfahren, dass er im Zusammenhang mit einem Ermittlungsverfahren, das von der Staatsanwaltschaft mangels hinreichenden Tatverdachts schon längst eingestellt worden ist, immer noch im Polizeicomputer erfasst sei. Registriert sei auch, dass er im Zuge des Ermittlungsverfahrens erkennungsdienstlich behandelt worden ist. Der Hinweis des Polizeibeamten traf zu. In der Tat war der junge Mann – wie sich bei unseren Nachforschungen rasch zeigte – in der Personenauskunftsdatei (PAD) der baden-württembergischen Polizei erfasst. Der registrierte Tatvorwurf lautete: Verstoß gegen das Sprengstoffgesetz. Was sich dahinter verbarg, mutete kurios an. Dem jungen Mann war bei seiner Rückkehr von einer Reise nach Thailand vom Zoll am Stuttgarter Flughafen zur Last gelegt worden, einem Mitreisenden bei der Einführung von 25 Kilogramm Feuerwerkskörpern geholfen zu haben. Das Zollfahndungsamt hatte deswegen den jungen Mann – man glaubt es kaum – mit dem Tatvorwurf eines Vergehens gegen das Sprengstoffgesetz im Informationssystem des Zolls (INZOLL) erfasst und das Bundeskriminalamt und die benachbarte Dienststelle der hiesigen Polizei unterrichtet. Das Bundeskriminalamt erfasste daraufhin den jungen Mann mit diesem Tatvorwurf im Informationssystem der Polizeien des Bundes und der Länder (INPOL); die baden-württembergische Polizeidienststelle registrierte ihn so in der PAD. Obwohl die Staatsanwaltschaft das Ermittlungsverfahren umgehend mangels hinreichenden Tatverdachts eingestellt hatte, war es bei der INZOLL-, INPOL- und PAD-Speicherung geblieben. Erst im Zuge unserer Nachforschungen drückten alle drei Stellen die Löschtaste.

2. Abschnitt: Justiz

1. Der Große Lauschangriff

Durch eine Grundgesetzänderung im Jahr 1998 wurden in Artikel 13 des Grundgesetzes (GG), in dem das Grundrecht der Unverletzlichkeit der Wohnung geregelt ist, die Absätze 3 bis 6 eingefügt. Mit dieser Grundgesetzänderung wollte der Gesetzgeber vor allem eine Möglichkeit zur Bekämpfung der organisierten Kriminalität schaffen. Nach Artikel 13 Abs. 3 GG ist seitdem die akustische Wohnraumüberwachung zum Zwecke der Strafverfolgung möglich (so genannter Großer Lauschangriff). Voraussetzung ist, dass bestimmte Tatsachen den Verdacht begründen, dass jemand eine durch Gesetz einzeln bestimmte besonders schwere Straftat begangen hat, sich der Beschuldigte vermutlich in der Wohnung aufhält und die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos ist.

Artikel 13 Abs. 3 GG wurde durch das Gesetz zur Verbesserung der Bekämpfung der organisierten Kriminalität vom 4. Mai 1998 (BGBl. I, S. 845) einfachgesetzlich ausgestaltet. Im Zentrum dieser Regelungen steht § 100 c Abs. 1 Nr. 3 der Strafprozessordnung (StPO). Nach dieser Vorschrift darf das in einer Wohnung nichtöffentlich gesprochene Wort eines Beschuldigten abgehört und aufgezeichnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass er eine der im Straftatenkatalog der Vorschrift genannte Straftat begangen hat. Weitere Vorschriften regeln u. a. die Zuständigkeit für die Anordnung der Abhörmaßnahmen, Beweiserhebungs- und Beweisverwertungsverbote, Pflichten zur Benachrichtigung der von der Maßnahme Betroffenen und inwiefern die Möglichkeit besteht, die Daten in weiteren Zusammenhängen zu verwenden.

1.1 Urteil des Bundesverfassungsgerichts zum Großen Lauschangriff vom 3. März 2004

Mit Urteil vom 3. März 2004 (1 BvR 2378/98 und 1 BvR 1084/99) hat der Erste Senat des Bundesverfassungsgerichts einen erheblichen Teil der durch das Gesetz zur Verbesserung der organisierten Kriminalität in die Strafprozessordnung eingefügten Vorschriften zur Durchführung der akustischen Wohnraumüberwachung für verfassungswidrig erklärt und dem Gesetzgeber aufgegeben, bis spätestens 30. Juni 2005 einen verfassungsgemäßen Zustand herzustellen.

1.1.1 Zulässigkeit der akustischen Wohnraumüberwachung

Das Bundesverfassungsgericht stellte in seiner Entscheidung klar, dass Artikel 13 Abs. 3 GG, der es dem Gesetzgeber ermöglicht, Ermächtigungen zur Wohnraumüberwachung zwecks Strafverfolgung zu schaffen, mit dem Grundgesetz vereinbar sei. Das Grundgesetz ermächtige jedoch nur eingeschränkt zu Überwachungsmaßnahmen, nämlich nur zu solchen, die die Menschenwürde wahren. In diesem Zusammenhang führte das Bundesverfassungsgericht aus, dass die Unverletzlichkeit der Wohnung einen engen Bezug zur Menschenwürde und zum verfassungsrechtlichen Gebot unbedingter Achtung einer Sphäre der ausschließlich privaten – „höchstpersönlichen“ – Entfaltung habe. Die vertrauliche Kommunikation benötige einen räumlichen Schutz, auf den die Bürger vertrauen können. Der Einzelne habe das Recht, in seinen privaten Wohnräumen in Ruhe gelassen zu werden, ohne Angst davor haben zu müssen, dass staatliche Stellen die Entfaltung seiner Persönlichkeit im Kernbereich privater Lebensgestaltung überwachen. In diesen unantastbaren Kernbereich privater Lebensgestaltung dürfe die akustische Wohnraumüberwachung nicht eingreifen. Dies gelte auch dann, wenn es um die Effektivität der Strafrechtspflege und die Erforschung der Wahrheit geht. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in den Kernbereich privater Lebensgestaltung nicht rechtfertigen. Das Bundesverfassungsgericht stellte auch klar, dass nicht jede akustische Wohnraumüberwachung die Menschenwürde verletze. So gehören Gespräche über begangene Straftaten ihrem Inhalt nach nicht zum absolut geschützten Kernbereich privater Lebensgestaltung.

Hieraus ergeben sich – laut Bundesverfassungsgericht – folgende generelle Anforderungen an gesetzliche Vorschriften zur akustischen Wohnraumüberwachung:

Artikel 13 Abs. 3 GG ermächtigt ausschließlich zum Erlass solcher gesetzlicher Regelungen, die gewährleisten, dass die akustische Wohnraumüberwachung nicht in den Kernbereich privater Lebensgestaltung eingreift. Eine auf Artikel 13 Abs. 3 GG gestützte Ermächtigung zur Durchführung der akustischen Wohnraumüberwachung muss daher so formuliert sein, dass das Risiko, durch die Abhörmaßnahmen die Menschenwürde zu verletzen, ausgeschlossen ist. Dies setzt voraus, dass die entsprechenden Vorschriften unter Beachtung des Grundsatzes der Normenklarheit nähere Sicherungen der Unantastbarkeit der Menschenwürde enthalten sowie den tatbestandlichen Voraussetzungen des Artikel 13 Abs. 3 GG und den übrigen Vorgaben der Verfassung entsprechen. Die Anforderungen an die Rechtmäßigkeit der Wohnraumüberwachung sind dabei umso strenger, je größer das Risiko ist, dass mit ihnen Gespräche höchstpersönlichen Inhalts erfasst werden. In Situationen, in denen Anhaltspunkte dafür bestehen, dass die Menschenwürde durch die Maßnahmen verletzt werden, müssen Abhörmaßnahmen daher von vornherein unterlassen werden. Führt eine Überwachung unerwartet zur Erhebung von absolut geschützten Informationen, muss sie sofort abgebrochen werden. Bereits erfolgte Aufzeichnungen müssen vernichtet werden. Jede Ver-

wendung solcher im Rahmen der Strafverfolgung erhobener absolut geschützter Daten ist untersagt.

Das Risiko, absolut geschützte Daten zu erfassen, besteht typischerweise beim Abhören von Gesprächen mit engsten Familienangehörigen sowie mit sonstigen engsten Vertrauten und Personen, zu denen ein besonderes Vertrauensverhältnis besteht (wie z. B. Pfarrern, Ärzten und Strafverteidigern). Bei diesem Personenkreis dürfen Überwachungsmaßnahmen daher nur ergriffen werden, wenn konkrete Anhaltspunkte dafür bestehen, dass die Gesprächsinhalte zwischen dem Beschuldigten und diesen Personen keinen absoluten Schutz erfordern, so bei einer Tatbeteiligung der das Gespräch führenden Personen. Anhaltspunkte dafür, dass die zu erwartenden Gespräche nach ihrem Inhalt einen unmittelbaren Bezug zu Straftaten aufweisen, müssen schon zum Zeitpunkt der Anordnung bestehen. Sie dürfen nicht erst durch eine akustische Wohnraumüberwachung begründet werden. Es besteht eine Vermutung dafür, dass Gespräche mit engsten Vertrauten in der Privatwohnung zum Kernbereich privater Lebensgestaltung gehören. Eine andere Bewertung kann hingegen erfolgen, wenn Gespräche in Betriebs- und Geschäftsräumen geführt werden. Diese nehmen zwar am Schutz des Artikels 13 Abs. 1 GG teil, betreffen bei einem fehlenden Bezug des konkreten Gesprächs zum Kernbereich privater Lebensgestaltung aber nicht den Menschenwürdegehalt des Grundrechts.

1.1.2 Auswirkungen des Urteils

Das Bundesverfassungsgericht hat in seinem Urteil zum Großen Lauschangriff festgestellt, dass die auf Artikel 13 Abs. 3 GG gestützte gesetzliche Ermächtigung zur Durchführung der akustischen Wohnraumüberwachung (§ 100 c Abs. 1 Nr. 3 StPO) und weitere damit verknüpfte Regelungen den vorgenannten verfassungsrechtlichen Anforderungen nicht genügen und daher in wesentlichen Teilen verfassungswidrig sind.

- So sind die in § 100 d Abs. 3 StPO genannten Erhebungs- und Verwertungsverbote nicht ausreichend konkretisiert. Der Gesetzgeber muss die Vorschrift so ausgestalten, dass Überwachungsmaßnahmen ausgeschlossen sind, wenn sich der Beschuldigte mit engsten Familienangehörigen oder engsten Vertrauten in der Wohnung aufhält und keine Anzeichen für deren Tatbeteiligung bestehen. In der Vorschrift fehlen außerdem hinreichende Vorkehrungen dafür, dass die Überwachung abgebrochen wird, wenn eine Situation eintritt, die dem unantastbaren Kernbereich privater Lebensgestaltung zuzurechnen ist. Weiter fehlen ein Verwertungsverbot und ein Gebot unverzüglicher Löschung rechtswidrig erhobener Informationen. Schließlich muss gesichert sein, dass rechtswidrig erhobene Daten, d. h. solche, die aus dem Kernbereich privater Lebensgestaltung stammen, weder im Hauptsacheverfahren verwertet noch Grundlage für weitere sich anschließende Ermittlungsmaßnahmen werden.
- Nach Artikel 13 Abs. 3 GG kommt eine Überwachung nur zur Ermittlung besonders schwerer, im Gesetz einzeln aufgeführter Straftaten in Betracht. Die besondere Schwere ist nur gegeben, wenn für die Straftat eine Höchststrafe von mehr als fünf Jahren Freiheitsstrafe vorgesehen ist. Einige der im Straftatenkatalog des § 100 c Abs. 1 Nr. 3 StPO genannten Taten erfüllen diese Anforderungen nicht. Sie scheiden deshalb als Anlass für eine Wohnraumüberwachung aus.
- Um das Grundrecht der Unverletzlichkeit der Wohnung auch verfahrensrechtlich zu sichern, hat das Bundesverfassungsgericht die Bedeutung des Richtervorbehalts – der besagt, dass für die Anordnung von Maßnahmen zur akustischen Wohnraumüberwachung Gerichte zuständig sind – herausgestellt

und die Anforderungen an den Inhalt und die schriftliche Begründung der gerichtlichen Anordnungen näher konkretisiert. Für den Fall der Verlängerung des ursprünglich festgesetzten Überwachungszeitraums stellte das Bundesverfassungsgericht fest, dass sowohl für die beantragende Staatsanwaltschaft als auch für das anordnende Gericht Prüfungs- und Begründungspflichten im Hinblick auf die bisherigen Ergebnisse der Maßnahme und die Erfolgsprognose bestehen.

– Die Regelungen über die Pflicht zur Benachrichtigung der Beteiligten (§ 101 Abs. 1 StPO) sind nur teilweise mit dem Grundgesetz vereinbar. Das Bundesverfassungsgericht verdeutlichte, dass der Begriff des Beteiligten im Sinne des § 101 Abs. 1 StPO weit auszulegen ist. Neben dem Beschuldigten sind daher die Inhaber und Bewohner einer Wohnung, in der Abhörmaßnahmen durchgeführt worden sind, zu benachrichtigen. Darüber hinaus sind auch solche Personen zu benachrichtigen, die sich als Gast oder sonst zufällig in einer überwachten Wohnung aufgehalten haben. Ausgenommen sind jedoch die Fälle, in denen die Benachrichtigung weiterer Beteiligter den Eingriff in das Persönlichkeitsrecht der Zielperson oder der sonstigen Beteiligten vertiefen würde. Dies ist dann der Fall, wenn die Überwachung keine verwertbaren Ergebnisse erbracht hat oder Nachforschungen zur Feststellung der Identität der Beteiligten erforderlich wären. Auch die in § 101 Abs. 1 Satz 1 StPO genannten Gründe für eine ausnahmsweise Zurückstellung der Benachrichtigung sind nur teilweise verfassungsgemäß. Die in der Vorschrift genannten Ausnahmen der Gefährdung der öffentlichen Sicherheit oder der Möglichkeit des weiteren Einsatzes eines nicht offen ermittelnden Beamten rechtfertigen die Zurückstellung der Benachrichtigung nicht. Auch die in § 101 Abs. 1 Satz 3 StPO enthaltene Zuständigkeitsregelung, wonach nach Erhebung der öffentlichen Klage das Prozessgericht über die Zurückstellung der Benachrichtigung entscheidet, ist nicht verfassungsgemäß, da sie mit dem Anspruch auf rechtliches Gehör (Artikel 103 Abs. 1 GG) nicht vereinbar ist. Denn damit erlangt das Prozessgericht Kenntnis über Tatsachen, die dem Angeklagten verborgen bleiben.

– Die Entscheidung stellte klar, dass aus einer akustischen Wohnraumüberwachung stammende Informationen nur zur Aufklärung anderer ähnlich gewichtiger Katalogtaten und zur Abwehr von im Einzelfall bestehenden Gefahren für hochrangige Rechtsgüter genutzt werden dürfen. Hierbei muss jedoch der Verwendungszweck mit dem ursprünglichen Zweck der Überwachung vereinbar sein. Soweit keine Pflicht zur Kennzeichnung der weitergegebenen Informationen besteht, genügen auch die Regelungen über die Verwendung personenbezogener Informationen in anderen Verfahren (§ 100 d Abs. 5 Satz 2 StPO und § 100 f Abs. 1 StPO) den verfassungsrechtlichen Vorgaben nicht.

– Die Vorschriften über die Datenvernichtung (§ 100 d Abs. 4 Satz 3 StPO, § 100 b Abs. 6 StPO) verstoßen gegen Artikel 19 Abs. 4 GG. Der Gesetzgeber hat die Interessen an der Vernichtung der Daten und das Gebot effektiven Rechtsschutzes gegenüber einer akustischen Wohnraumüberwachung nicht hinreichend aufeinander abgestimmt. Werden Daten noch benötigt – etwa deshalb, weil der Betroffene ein rechtlich begründetes Interesse an deren Nutzung hat – dürfen die Daten nicht gelöscht, sondern müssen gesperrt werden. Sie dürfen dann zu keinem anderen Zweck als dem zur Information des Betroffenen und zur gerichtlichen Kontrolle verwendet werden.

Die Entscheidung des Bundesverfassungsgerichts zum Großen Lauschangriff ist zu begrüßen. Das Urteil ist ein wichtiger Orientierungspunkt in der rechts- und rechtssicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staat-

lichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. In diesem Zusammenhang ist auch der Beschluss des Bundesverfassungsgerichts zum Außenwirtschaftsgesetz (AWG) von Bedeutung, der ebenso wie das Urteil zum Großen Lauschangriff vom 3. März 2004 stammt. In diesem Beschluss hat das Bundesverfassungsgericht die Regelungen in § 39 AWG zur Überwachung des Postverkehrs und der Telekommunikation im Bereich der Straftatenverhütung aus Gründen unzureichender Normenbestimmtheit und Normenklarheit für verfassungswidrig erklärt. Die Datenschutzbeauftragten des Bundes und der Länder haben diese beiden Entscheidungen zum Anlass genommen, in ihrer Entschließung vom 25./26. März 2004 (s. Anhang 1) zu fordern, auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung, aber auch die Polizei- und Verfassungsschutzgesetze der Länder auf den Prüfstand zu stellen und die einschlägigen Vorschriften zügig nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren.

1.2 Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung

Bereits am 24. Juni 2004 hat das Bundesjustizministerium einen Referentenentwurf für die „Neuregelung der akustischen Wohnraumüberwachung“ vorgelegt. Anders als es nach dem Urteil des Bundesverfassungsgerichts zum Großen Lauschangriff zu erwarten war, sah dieser jedoch nicht nur vor, den bisherigen Anwendungsbereich der akustischen Wohnraumüberwachung einzuschränken. In zwei Punkten sollte er sogar erweitert werden: Während es nach den bisherigen Vorschriften der Strafprozessordnung verboten ist, im Rahmen des Großen Lauschangriffs Gespräche mit Ärzten, Rechtsanwälten, Journalisten, Seelsorgern usw. abzuhören, wenn diese nicht selbst tatverdächtig sind, sah der Referentenentwurf im Hinblick auf Berufsgeheimnisträger weitaus großzügigere Abhörbefugnisse vor. Der andere Punkt betraf die im Referentenentwurf vorgesehene Anhebung des Höchstmaßes der Freiheitsstrafe für den besonders schweren Fall der Bildung krimineller Vereinigungen (§ 129 Abs. 4 des Strafgesetzbuchs) von fünf Jahren auf zehn Jahre. Das Bundesverfassungsgericht hat in seinem Urteil zum Großen Lauschangriff ausgeführt, dass die akustische Wohnraumüberwachung für Zwecke der Strafverfolgung nur zu rechtfertigen ist, wenn es um die Aufklärung besonders schwerer Straftaten geht. Diese besondere Schwere ist laut Bundesverfassungsgericht nur gegeben, wenn für die Straftat eine Höchststrafe von mehr als fünf Jahren vorgesehen ist, da diese Taten ein besonders schweres Tatunrecht aufweisen und damit den Bereich der mittleren Kriminalität eindeutig verlassen. Die im Referentenentwurf vorgesehene Anhebung des Strafrahmens für den besonders schweren Fall der Bildung krimineller Vereinigungen erfolgte offensichtlich gerade deshalb, um die vom Bundesverfassungsgericht gesetzten Hürden überwinden zu können, damit für dieses Delikt auch weiterhin das Instrument der akustischen Wohnraumüberwachung einsetzbar ist. Diese Vorgehensweise war sicher nicht im Sinne des Bundesverfassungsgerichts gewesen. Denn die bewusst vorgenommene Einschränkung auf besonders schwere Straftaten würde ihre verfassungsrechtliche Bedeutung verlieren, wenn der Gesetzgeber diese Einschränkung dadurch umgeht, dass er die Höchststrafe für die im derzeitigen Katalog verankerten Straftaten einfach anhebt und damit die Möglichkeit einer akustischen Wohnraumüberwachung für diese Straftatbestände weiterhin erhält.

Wegen der immensen Kritik an den beiden vorgenannten Punkten hat das Bundesjustizministerium auf diese Ausweitungen des Großen Lauschangriffs verzichtet und den Referentenentwurf entsprechend nachgebessert.

Den überarbeiteten Entwurf hat das Bundeskabinett am 22. September 2004 beschlossen. Dieser Entwurf der Bundesregierung ist zwar von dem Bemühen gekennzeichnet, die Vorgaben des Bundesverfassungsgerichts möglichst getreu zu erfüllen, was auch in weiten Teilen gelang. Allerdings enthält er auch Regelungen, die angesichts der ausführlichen und präzisen Vorgaben des Bundesverfassungsgerichts zu unklar und zu unbestimmt sind. So sind zentrale Punkte wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Personen „des persönlichen Vertrauens“ offen geblieben. Darüber hinaus drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwer wiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Außerdem wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr. Schließlich ist festzustellen, dass sich der Entwurf ausschließlich auf die akustische Wohnraumüberwachung bezieht und sich nicht mit den Auswirkungen des Bundesverfassungsgerichtsurteils zum Großen Lauschangriff auf andere heimliche Ermittlungsmaßnahmen befasst. Angesichts der engen zeitlichen Vorgaben des Bundesverfassungsgerichts, die rechtlichen Regelungen zur akustischen Wohnraumüberwachung bis zum 30. Juni 2005 den Anforderungen des Urteils anzupassen, ist es zwar durchaus verständlich, dass zunächst ausschließlich die Neuregelung des großen Lauschangriffs in Angriff genommen wurde. Ungeachtet dessen ist darauf hinzuweisen, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung unbedingt erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und auch der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Die Datenschutzbeauftragten des Bundes und der Länder haben daher ihre bereits in der Entschließung vom 25./26. März 2004 erhobene diesbezügliche Forderung in einer weiteren Entschließung vom 28./29. Oktober 2004 (s. Anhang 2) noch einmal bekräftigt.

2. Strafbarkeit unbefugter Bildaufnahmen

Durch die rasante Entwicklung des technischen Fortschritts hat das unbefugte Aufnehmen und Verbreiten von Bildaufnahmen erheblich zugenommen. Im Zeitalter des Internets, der Web-Kameras und Handys mit Kamerafunktion ist es möglich, Bilder von Menschen aufzunehmen und weltweit zu verbreiten, die unter Umständen tief in die Intimsphäre der Betroffenen eingreifen (z. B. durch heimliche Aufnahmen in Umkleidekabinen oder ärztlichen Behandlungsräumen). Es war daher dringend erforderlich, im Strafgesetzbuch eine Regelung zu schaffen, die das unbefugte Aufnehmen und Verbreiten von Bildern anderer Personen unter Strafe stellt. Denn während die Verletzung der Vertraulichkeit des Wortes, die Verletzung des Briefgeheimnisses, das unbefugte Ausspähen von Daten und die Verletzung von Privatgeheimnissen längst strafbar sind, war der höchstpersönliche Lebensbereich vor unbefugten Bildaufnahmen nicht hinreichend geschützt. Diese Strafbarkeitslücke sollte zwar bereits in der letzten Legislaturperiode geschlossen werden, das Vorhaben wurde seinerzeit jedoch nicht umgesetzt.

Erst durch das 36. Strafrechtsänderungsgesetz vom 30. Juli 2004 (Bundesgesetzblatt I, S. 2012) wurde ein neuer § 201 a in das Strafgesetzbuch (StGB) eingefügt. Nach Absatz 1 dieser Vorschrift macht sich strafbar, wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Ein-

blick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt. In § 201 a Abs. 2 StGB wird der strafrechtliche Schutz auf den Gebrauch und die Weitergabe von Aufnahmen erstreckt, die durch eine Tat nach Absatz 1 hergestellt worden sind. Nach Absatz 3 der Vorschrift wird bestraft, wer eine befugt hergestellte Aufnahme von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, wissentlich unbefugt einem Dritten zugänglich macht und dadurch den höchstpersönlichen Lebensbereich der betroffenen Person verletzt.

Anders als in früheren Gesetzentwürfen vorgesehen, werden von der Vorschrift somit nur Aufnahmen erfasst, die in einer Wohnung oder einem sonst besonders geschützten Raum gefertigt werden. Die Voraussetzung der „Nichtöffentlichkeit“ schränkt den räumlichen Schutzbereich der Strafvorschrift erheblich ein. Diese Einschränkung wird damit begründet, dass mit Bildaufnahmen, die in der Öffentlichkeit hergestellt werden, ein breites Spektrum von Alltagshandlungen unter Strafe gestellt werden würde. Ein Kriterium, mit dem solche Phänomene annähernd trennscharf ausgegrenzt werden könnten, sei nicht vorhanden. Ein Straftatbestand, der die unbefugte Abbildung in allen Lebensbereichen unter Strafe stelle, liefe Gefahr, das Übermaßverbot staatlichen Strafens sowie das strafrechtliche Bestimmtheitsgebot zu verletzen. Darüber hinaus erscheine die enge Tatbestandsfassung deshalb vertretbar, weil der Einzelne im öffentlichen Lebensraum damit rechnen müsse, auf Bildaufnahmen abgebildet zu werden.

Auch das Beobachten mit einem Bildaufnahmegerät oder anderen technischen Mitteln wird in der Vorschrift nicht unter Strafe gestellt. In der Bundestagsdrucksache 15/2466 (S. 6) ist hierzu ausgeführt, dass ein „frecher Blick“ in der Regel keine der Strafe würdige und bedürftige Rechtsgutsverletzung darstelle, sondern in erster Linie Gebote des Anstands verletze.

Die Argumentation des Gesetzgebers ist teilweise durchaus nachvollziehbar. So ist es zwar angemessen, dass beispielsweise Fotografien oder Filme, die in der Landschaft oder vor öffentlichen Bauwerken gefertigt und auf denen Personen lediglich „als Beiwerk“ in Situationen oder Zuständen mit abgebildet werden, nicht unter Strafe gestellt sind, auch wenn sie ihren höchstpersönlichen Lebensbereich tangieren. Andererseits werden durch die genannten Einschränkungen auch solche Bildaufnahmen nicht von der Vorschrift erfasst, die zwar an öffentlich zugänglichen Orten hergestellt werden, die die Intimsphäre der betroffenen Person jedoch gezielt verletzen.

Letztendlich bleibt abzuwarten, wie sich die Vorschrift in der Praxis bewährt.

3. ZStV-Auskunft einfach zur Akte genommen

Eine Beamtin, die in leitender Stellung bei einem Landratsamt außerhalb Baden-Württembergs beschäftigt ist, traute ihren Ohren kaum, als sie eine Frau aus dem Südbadischen anrief und ihr auf den Kopf zu sagte, dass sie wegen Nötigung im Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV) stehe. Die Beamtin informierte ihren Landrat. Der Landrat schrieb uns, die Tatsache, dass derart sensible Daten in die Hände einer Privatperson gelangen, sei für ihn umso ärgerlicher, als gerade Mitarbeiter des Bereichs seines Landratsamts, den die Beamtin leite, in Erfüllung ihrer gesetzlichen Aufgaben häufig persönlich mit unberechtigten Strafanzeigen überzogen werden. Gelangen dann, wie im Fall seiner Beamtin, Informationen über solche Ermittlungsverfahren auch noch in die Hände Privater, verstärke dies zusätzlich die Wirkung ungerechtfertigter Anzeigen gegen öffentlich Bedienstete. Zudem sei für ihn völlig unverständlich, dass seine Beamtin im ZStV erfasst ist, obwohl das Ermittlungsverfahren mangels Tatverdachts eingestellt worden ist.

Die Sache war rasch geklärt: Gegen die Anruferin war bei einer baden-württembergischen Staatsanwaltschaft ein Ermittlungsverfahren anhängig gewesen. Als die Staatsanwaltschaft dieses Ermittlungsverfahren im ZStV erfassen wollte, holte sie eine Auskunft aus dem ZStV ein, um zu prüfen, ob die Frau bereits erfasst ist. Weil die Frau einen sog. Allerweltsnamen hatte, beschränk-

te die Staatsanwaltschaft sich nicht auf eine Auskunft allein zu der Frau, sondern startete eine sog. Ähnlichenabfrage. Als Ergebnis bekam die Staatsanwaltschaft vom ZStV die Auskunft, dass zwar nicht die Frau, jedoch sieben andere Personen mit ähnlichem Namen – darunter die Beamtin des Landratsamts – erfasst sind. In dem seitenlangen Ausdruck konnte man die Namen und meist auch die Adressen dieser sieben Personen und zudem nachlesen, welche Staatsanwaltschaft gegen sie wegen welcher Straftat unter welchem Aktenzeichen ermittelt hatte und wie die Ermittlungsverfahren ausgegangen waren. Diese Auskunft nahm die Staatsanwaltschaft zu der Ermittlungsakte der Frau. Bei einer Akteneinsicht stieß die Frau auf die Ähnlichenauskunft. Weil im ZStV-Datensatz der Beamtin als Anschrift die Adresse des Landratsamts eingetragen war, hat die Frau sie dann dort angerufen.

Keine Frage: Die Staatsanwaltschaft hätte die Ähnlichenauskunft nicht einfach zu der Ermittlungsakte der Frau nehmen dürfen. Sie hätte vielmehr zunächst prüfen müssen, ob die darin aufgeführten Personen mit der Frau identisch sind. Hätte sie eine solche Prüfung vorgenommen, hätte sie gesehen, dass keine der in der Ähnlichenauskunft aufgeführten sieben Personen mit der besagten Frau, deren Ermittlungsverfahren die Staatsanwaltschaft im ZStV erfassen wollte, identisch ist. Bei diesem Befund hätte die Staatsanwaltschaft die Ähnlichenauskunft umgehend vernichten müssen. Zu welchen unzulässigen Datenübermittlungen es führt, wenn die Staatsanwaltschaft solche Ähnlichenauskünfte unbesehen zu ihren Ermittlungsakten nimmt, zeigt der vorliegende Fall exemplarisch. Als wir die Staatsanwaltschaft darauf ansprachen, nahm sie die Ähnlichenauskunft umgehend aus der Ermittlungsakte und vernichtete sie. Weil die Staatsanwaltschaft in einer internen Anordnung geregelt hatte, dass mit solchen Ähnlichenauskünften wie soeben beschrieben zu verfahren ist, haben wir von einer Beanstandung des ihr unterlaufenen Datenschutzverstoßes abgesehen.

Mit seiner Kritik an der Erfassung seiner Beamtin im ZStV hatte der Landrat ein Problem angesprochen, auf das mein Amt bereits hingewiesen hatte, als es um die Einführung des ZStV ging. Nachgehen konnten wir seiner Kritik jedoch nicht, weil seine Beamtin von einer Staatsanwaltschaft außerhalb Baden-Württembergs im ZStV erfasst worden war.

4. Geschäftsstatistik für Bewährungshelfer

Wie der folgende Fall zeigt, werden datenschutzwidrige Vorgehensweisen nicht immer erst auf Drängen unserer Dienststelle aufgegeben, sondern oftmals auch deshalb, weil die handelnde Behörde selbst erkennt, einen Fehler gemacht zu haben:

Die Verwaltungsabteilung eines Oberlandesgerichts hatte im Juni 2004 die Landgerichte des Bezirks aufgefordert, eine Geschäftsstatistik der Bewährungshelfer für das 1. Halbjahr des Geschäftsjahres 2004 vorzulegen. Hierzu sollten die den Landgerichten zugeordneten Bewährungshelfer einen Vordruck des Oberlandesgerichts ausfüllen, in dem – anders als für frühere Statistiken – nicht nur anonymisierte Angaben zu machen waren, sondern bei Vorliegen bestimmter Fallkonstellationen auch Name und Wohnort von Probanden angegeben werden sollten.

Die Weitergabe dieser Daten stellt eine Übermittlung personenbezogener Daten dar, die nur zulässig ist, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Im vorliegenden Fall war jedoch nicht erkennbar, dass eine dieser Voraussetzungen vorlag, weshalb wir uns an das Oberlandesgericht wandten. Dieses teilte auf unsere Nachfrage mit, in dem Erhebungsbogen sei vorgesehen gewesen, dass die einzelnen Bewährungshelfer diejenigen Probanden namentlich nennen, deren Bewährungszeit zum Stichtag 30. Juni 2004 bereits abgelaufen war. Außerdem sei für die Probanden, die ihre Wohnung außerhalb des Zuständigkeitsbereichs der Dienststelle verlegt hatten, neben der Angabe des Namens auch die des Wohnorts vorgesehen gewesen. Die Angaben sollten sicherstellen, dass diese Probanden in der Statistik nicht mehr erscheinen bzw. bei der Ermittlung der Probandenzahlen nicht mitberücksichtigt werden. Für die statistische Erhebung seien die personenbezogenen Daten der Probanden jedoch ohne Bedeutung. Das Oberlandesgericht teilte weiter mit, dass sich bereits die geschäftsführenden Bewährungs-

helfer gegen die Abfrage personenbezogener Daten ausgesprochen hatten. Deshalb habe es, bereits vor der Anfrage unserer Dienststelle, auf die personenbezogenen Angaben verzichtet. Es seien daher nahezu ausnahmslos anonymisierte Daten vorgelegt worden. Nur in wenigen Ausnahmefällen seien die Namen der Probanden in den Erhebungsvordrucken angegeben gewesen. Das Oberlandesgericht versicherte, dass personenbezogene Daten im Bereich der Bewährungshilfe künftig nicht mehr Gegenstand statistischer Erhebungen sein würden. Soweit auf den Vordrucken personenbezogene Daten gemacht worden waren, baten wir das Oberlandesgericht, diese unkenntlich zu machen.

5. Angaben im Sichtfenster von Briefen

5.1 Schreiben eines Gerichtsvollziehers

Niemand freut sich über Post vom Gerichtsvollzieher. Wenn dem Brief dann auch noch von außen zu entnehmen ist, dass der Adressat zu einem Termin erscheinen soll, ist es jedoch des Guten endgültig zu viel. So erging es einer Bürgerin. Im Sichtfenster eines von einem Gerichtsvollzieher stammenden Briefs war außer der Adressatenanschrift und dem Absender deutlich sichtbar angegeben: Termin 11. November 2002. Der Gerichtsvollzieher erklärte auf unsere Nachfrage, dass die Angabe des Termins deshalb im Sichtfenster erfolge, um zum einen auf die Wichtigkeit des Schreibens hinzuweisen. Zum anderen trage diese Vorgehensweise dazu bei, dass die Briefe überhaupt gelesen werden. Aus langjähriger Erfahrung wisse er, dass viele Briefe, die keine weiteren Angaben im Sichtfenster enthalten, ungeöffnet bleiben, Briefe mit einer Terminangabe im Sichtfenster aber gelesen werden.

Diese Vorgehensweise ist mit der Pflicht des Gerichtsvollziehers, zu verhindern, dass Dritten Informationen über laufende Zwangsvollstreckungsverfahren bekannt werden, nicht in Einklang zu bringen. Nach der Gerichtsvollzieherordnung hat der Gerichtsvollzieher zur Wahrung seiner Amtsverschwiegenheit insbesondere dafür zu sorgen, dass sein gesamtes Schriftgut vor dem Einblick und dem Zugriff Unberechtigter gesichert ist. Die Angabe eines Termins im Adressfeld entspricht diesen Anforderungen nicht.

Wir haben das Amtsgericht, in dessen Bezirk der Gerichtsvollzieher tätig ist, daher aufgefordert, den betroffenen Gerichtsvollzieher wie auch die anderen Gerichtsvollzieher des Sprengels über unsere Bewertung der Angelegenheit zu unterrichten.

5.2 Gerichtsschreiben

Auch auf der Post von Gerichten kann man Angaben finden, die einen Außenstehenden nichts angehen.

So hat uns beispielsweise ein Bürger, der bei einem Amtsgericht eine zivilrechtliche Forderung eingeklagt hatte, darüber informiert, dass er vom Amtsgericht Post erhalten habe, wobei im Sichtfenster des formlos zugestellten Briefs das Aktenzeichen des Verfahrens angegeben gewesen sei. Hierzu muss man wissen, dass die Aktenzeichen im Bereich der ordentlichen Gerichtsbarkeit, also der Zivil- und Strafgerichtsbarkeit, aber auch im Bereich der Sozialgerichtsbarkeit, Rückschlüsse auf den Rechtsbereich zulassen, auf den sich ein Verfahren bezieht. An den Aktenzeichen der ordentlichen Gerichtsbarkeit kann man beispielsweise erkennen, ob es sich um ein zivilrechtliches oder um ein strafrechtliches Verfahren handelt. Jeder, der einen Brief mit Aktenzeichenangabe zu Gesicht bekommt, kann daher herausfinden, ob der Adressat in einer Zivil- oder in einer Strafrechtsangelegenheit mit dem Gericht zu tun hat. Auch wenn damit noch nichts darüber ausgesagt wird, in welcher Funktion der Adressat in das Verfahren eingebunden ist, ob er Angeklagter, Kläger, Beklagter oder etwa nur Zeuge ist, handelt es sich bei der Angabe des Aktenzeichens im Sichtfenster oder auf dem Briefumschlag eines formlos zugestellten Schreibens um eine – wenn auch nicht sehr aussagekräftige – Information, die Dritte nichts angeht und die auch der Postbedienstete, der den Brief austrägt, nicht benötigt.

Vom Justizministerium, an das wir uns wegen des geschilderten Falls, aber auch wegen eines anderen ähnlich gelagerten Falls gewandt hatten, liegt zwar noch keine abschließende schriftliche Stellungnahme vor. Telefonisch wurden wir jedoch vorab davon unterrichtet, dass das Justizministerium zunächst bei sämtlichen Gerichtsbarkeiten Erkundigungen darüber eingezogen habe, bei welchen Gerichten Aktenzeichen im Sichtfenster von Briefen angegeben werden. Dort, wo dies der Fall ist, werde derzeit geprüft, mit welchem Aufwand das Layout der betroffenen Briefköpfe und Vordrucke so geändert werden kann, dass das Aktenzeichen nicht mehr im Sichtfenster erscheint.

3. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheit

Schon seit längerem steigen die Krankheitskosten nicht zuletzt auch aufgrund der Fortschritte im Bereich der Medizin stärker als die der allgemeinen Lebenshaltung. Diese problematische Entwicklung gehört daher schon seit geraumer Zeit zu den zentralen Handlungsschwerpunkten in der deutschen Gesundheitspolitik. Der Bundesgesetzgeber hat deshalb immer wieder versucht, durch entsprechende Reformmaßnahmen dem Kostenanstieg bei den Gesundheitsausgaben entgegenzusteuern.

Am 1. Januar 2004 trat das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung in Kraft (GMK) – wer erinnert sich nicht noch an die wochenlangen Unklarheiten und Diskussionen um Praxisgebühren und Zuzahlungen? Eine elektronische Gesundheitskarte soll im Jahr 2006 kommen, ebenfalls vor allem mit dem Ziel, den Anstieg der Gesundheitsausgaben möglichst einzudämmen. Allerdings scheint bereits heute der Zeitplan dafür zu wanken, weil sich Krankenkassen auf der einen und Ärzte, Zahnärzte, Apotheker, Kliniken und sonstige Leistungserbringer auf der anderen Seite nicht wie vorgesehen zum 1. Oktober dieses Jahres darauf einigen konnten, welche Aufgaben die neue Karte erfüllen soll und wie dies erreicht werden kann. Ebenso fällt einem zum Thema Gesundheitsreform der lange unionsinterne Streit darüber ein, ob nun das Modell „Kopfpauschale“ oder ein „einkommensabhängiges Stufenmodell“ oder eine Kompromisslösung dafür der beste Weg ist.

Es gab daher neben Hartz IV (Näheres dazu im nachfolgenden 3. Abschnitt) im zurückliegenden Jahr wohl kein Thema, über das in der Innenpolitik vergleichbar gestritten wurde und das ein so großes Medieninteresse genoss. Wen wundert es? Geht doch die Gesundheit jeden von uns etwas an.

Leider ist den wenigsten Bürgerinnen und Bürgern lebenslange Gesundheit beschieden. Dann führt der Weg in die Apotheke, in die Arztpraxis oder gar zur stationären Behandlung ins Krankenhaus – Kosten entstehen und müssen abgerechnet werden, wofür wiederum Patientendaten benötigt werden. Die Partner der Selbstverwaltung können dabei die ihnen zukommenden Aufgaben in aller Regel nicht ohne die Nutzung personenbezogener Daten erfüllen. Allerdings gehört es zu den wichtigen Aufgaben meiner Dienststelle, darauf zu achten, dass die Neugier der Akteure im Gesundheitsbereich nicht überhand nimmt und die Patienten und Versicherungsnehmer nicht zu „gläsernen“ Objekten werden. Dies gilt insbesondere auch in Zeiten knapper Kassen. Aber auch in schwierigen Zeiten darf der Zweck nicht jedes Mittel heiligen. Das aus dem allgemeinen Persönlichkeitsrecht des Artikels 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes vom Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. Dezember 1983 entwickelte informationelle Selbstbestimmungsrecht steht übermäßiger Wissbegier entgegen. So gilt gerade auch für den aus datenschutzrechtlicher Sicht äußerst sensiblen Gesundheitsbereich der Grundsatz, dass die Verarbeitung personenbezogener Daten so lange nicht erlaubt ist, wie eine besondere Rechtsgrundlage dies nicht ausdrücklich gestattet.

Dass der Gesundheits- und Sozialversicherungsbereich nicht zuletzt durch gesetzlich aufgegebene, aber auch von der Selbstverwaltung selbst verordnete Sparzwänge mehr denn je umkämpft war, bekam auch meine Dienststelle durch zahlreiche Eingaben zu spüren. Schlecht und nachteilig aus Bürgersicht, aber auch unter dem Aspekt der Nichtnutzung möglicher Synergieeffekte, erwies sich wiederum die zweigeteilte Kontrollzuständigkeit für den Datenschutz in Baden-Württemberg. Dass ein Weiterreichen von Petitionen infolge mangelnder Zuständigkeit meines Amtes für den sog. nicht-öffentlichen Bereich zwangsläufig zu vermeidbaren Zeitverlusten in der Bearbeitung führt, ist schon ärgerlich genug und stößt in der heutigen Zeit, in der Verschlankung der Verwaltung und sich daraus ergebende Einsparungen das Gebot der Stunde sind und von der Politik fast gebetsmühlenartig wiederholt werden, bei den Betroffenen auf wenig Verständnis. Dass dies ausgerechnet beim Datenschutz nicht gelten soll, ist Fachleuten kaum zu vermitteln – erst recht nicht unseren Bürgern, wenn sie sich mit Eingaben an meine Dienststelle wenden. Dadurch

werden ohne Not wertvolle Ressourcen meines Amts gebunden, zumal es im Krankenhausbereich aufgrund der eingangs beschriebenen Entwicklungen und der sich verändernden Rahmenbedingungen verstärkt zu Kooperationen oder gar Zusammenlegungen kommt, die nicht selten mit einer Änderung in der Rechtsform des Krankenhausbetriebs beispielsweise als GmbH einhergehen. Da trotz der „Flucht ins Privatrecht“ meist ein Landkreis oder eine Stadt zumindest (Mit-)Gesellschafter bleibt, lautet die Gretchenfrage am Anfang für den Datenschutz dann regelmäßig: Handelt es sich bei dieser Klinik in neuer Rechtsform nach wie vor um eine öffentliche Einrichtung, die Aufgaben im Bereich der gesundheitlichen Daseinsvorsorge wahrnimmt (mit Anwendung des Landesdatenschutzgesetzes) oder führt die Rechtsänderung dazu, dass das Krankenhaus zu einem echten Wettbewerbsunternehmen wird, das dann nicht mehr meiner Datenschutzkontrolle unterliegt? Dass die beteiligten Aufsichtsakteure – das Innenministerium für den nicht-öffentlichen und meine Dienststelle für den öffentlichen Bereich – sich unverdrossen um eine zeitnahe gemeinsame Erledigung der Aufgaben bemühen, ist selbstverständlich und wird durch die traditionell gute Zusammenarbeit auch erleichtert; dies ändert allerdings nichts daran, dass unnötigerweise viel Zeit und Kraft für die notwendigen Abstimmungsprozesse auf der Strecke bleibt.

Nachdem es im Gesundheits- und Sozialbereich bekanntlich sehr viele Akteure gibt, kann ein Tätigkeitsbericht gerade in diesem Betätigungsfeld des Datenschutzes niemals auch nur ein halbwegs komplettes Bild von dem liefern, womit sich die Dienststelle im Berichtszeitraum befassen musste. Insoweit können die nachfolgenden Ausführungen auch nur einen kleinen Ausschnitt aus der praktischen Arbeit meines Amtes liefern.

1. Das Landeskrebsregister – Wie geht es weiter?

So oder ähnlich lauteten bereits Überschriften in unseren früheren Tätigkeitsberichten. Im 14. Tätigkeitsbericht (LT-Drs. 11/2900, S. 81) stand zu lesen: „Kaum ein Thema beschäftigte mich ... so häufig wie das Krebsregister – nachzulesen in sieben der dreizehn Tätigkeitsberichte.“ Am 25. Februar 1994 trat das Landeskrebsregistergesetz für Baden-Württemberg als rechtliche Grundlage für das epidemiologische Krebsregister und als zweites Krebsregister bundesweit in Kraft. „Seitdem ist relative Ruhe eingekehrt“ – so nachzulesen im 22. Tätigkeitsbericht (LT-Drs. 13/520, S. 63). Wir haben dies vor allem darauf zurückgeführt, dass der Gesetzgeber seinerzeit aktiv geworden war und unter tatkräftiger Unterstützung meines Amts das o. g. Krebsregistergesetz erlassen hat. Grundprinzipien des Gesetzes waren unter anderem:

- Niemand war gezwungen, sich am Meldedienst zum Krebsregister zu beteiligen.
- Meldewillige Ärzte und Zahnärzte, insbesondere Krankenhäuser und Pathologen mit geeigneter EDV-Ausstattung, konnten die Identifizierungsdaten der Krebskranken rechnergestützt nach einer vorgegebenen Verschlüsselungsmethode vor Ort bereits verschlüsseln und diesen sog. Meldeschlüssel zusammen mit den bedeutsamen medizinischen Angaben der Registerstelle (Landesärztekammer) mitteilen. Ärzte und Zahnärzte ohne geeignete EDV-Ausstattung meldeten die Krebspatienten mit deren Einwilligung unter ihren unverschlüsselten Identifizierungsdaten direkt an die Registerstelle; dort erfolgte dann die Verschlüsselung der Identifizierungsdaten durch eine von der Registerstelle organisatorisch getrennte Verschlüsselungsstelle. Um die Anonymisierung zusätzlich zu sichern, nahm eine vom Krebsregister unabhängige Vertrauensstelle eine zweite Verschlüsselung der Identifizierungsdaten vor.

Aus Sicht des Datenschutzes war dieses Gesetz seinerzeit bemüht, die Persönlichkeitsrechte der im Krebsregister gespeicherten Krebskranken möglichst zu schonen.

Wie sich jedoch bereits wenige Jahre nach der Einführung des Landeskrebsregisters abzeichnen sollte, war diesem Gesetz nur wenig Erfolg beschieden. Ursächlich dafür waren ausweislich des Jahresberichts 2000 der Landesärztekammer zum Krebsgeschehen in Baden-Württemberg aber nicht datenschutzrechtliche Schwierigkeiten, sondern mangelnde Meldemoral und der

aus Sicht der Ärzte für sie fehlende unmittelbare Nutzen. Zehn Jahre nach Einführung des Krebsregisters und einer unter epidemiologischen Gesichtspunkten völlig unbefriedigenden Meldequote von nach wie vor unter fünfzig Prozent kam dann überraschend – für Insider eher weniger – das Fallbeil für das alte Projekt durch einen vom Sozialministerium herbeigeführten Kabinettsbeschluss vom 22. Juni 2004. Hier muss aus Sicht des Datenschutzes kritisch gefragt werden, ob das für die o. g. Zwecke über ein Jahrzehnt erfolgte Sammeln von höchst sensiblen Patientendaten – ohne das angestrebte Ziel auch nur annähernd zu erreichen – nicht von vornherein auf falschen Annahmen oder einem handwerklich fehlerhaften methodischen Ansatz beruhte. So stellt sich eigentlich zwangsläufig die Frage, wie sich ein solches Projekt mit den vom Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. Dezember 1983 aufgestellten Grundsätzen der Erforderlichkeit sowie der Datenvermeidung und -sparsamkeit vereinbaren lässt. Hätte man das heutige Wissen schon damals gehabt, so hätte das ganze Verfahren – zumindest aus Sicht des Datenschutzes – jedenfalls so nicht durchgeführt werden dürfen.

Nun soll ein neuer Anlauf für eine Krebsregistrierung in Baden-Württemberg auf der Basis der vom Ministerrat mit o. g. Beschluss verabschiedeten Eckpunkte des Sozialministeriums genommen werden und in ein neu gefasstes Landeskrebsregistergesetz münden. Die vom Ministerrat gebilligte Neukonzeption der Krebsregistrierung sieht als zentrales Strukturprinzip die Verbindung von klinischer und epidemiologischer Krebsregistrierung vor. Damit das neue Verfahren nicht das gleiche Schicksal erleidet wie das Vorgängerprojekt, soll das künftige epidemiologische Krebsregister auf einer einheitlichen klinischen Krebsregistrierung insbesondere an den Tumorzentren und Onkologischen Schwerpunkten des Landes aufbauen.

Es sollen dazu fünf regionale (klinische) Krebsregister eingerichtet werden, an die Ärzte, Zahnärzte und Kliniken in einem jeweils definierten Einzugsgebiet mit etwa gleicher Einwohnerzahl Krebsneuerkrankungen melden. Diese regionalen Krebsregister sollen die eingehenden Meldungen für Qualitätssicherungszwecke auswerten und nach der Überprüfung auf Plausibilität und Doppelmeldungen den anonymisierten epidemiologischen Datensatz dem künftigen epidemiologischen Krebsregister zuleiten. Die Verknüpfung von epidemiologischem und klinischem Krebsregister entfalte dabei nach Auffassung des Sozialministeriums für beide Register „optimale Synergieeffekte“, da der Datensatz eines epidemiologischen Krebsregisters bereits in dem für ein klinisches Krebsregister erforderlichen Datensatz enthalten sei und aus diesem „einfach exportiert“ werden könne. So nachzulesen in der Stellungnahme der Landesregierung (LT-Drs. 13/3542 vom 13. September 2004) zu einem Antrag zur Frage der Zukunft des Krebsregisters in Baden-Württemberg. Wie dort weiter zu lesen ist, sollen durch die neuen regionalen Krebsregister Rückmeldungen an die behandelnden Ärzte und Kliniken erfolgen, um eine Verlaufs- und Erfolgskontrolle von Krebstherapien zu ermöglichen; unter anderem soll dabei eine gesetzliche Meldepflicht den unabdingbaren Erfassungsgrad von neunzig Prozent herbeiführen. Wer sich noch näher über dieses Thema informieren möchte, kann dies in der o. g. Landtagsdrucksache nachlesen.

Nachdem das Sozialministerium sowohl meine Dienststelle als auch das für den Datenschutz im nicht-öffentlichen Bereich zuständige Innenministerium darüber informiert hatte, dass es durch Ministerratsbeschluss vom 22. Juni 2004 beauftragt worden sei, die dem Kabinett vorgestellten Eckpunkte zur Neuordnung der Krebsregistrierung im Land weiter zu konkretisieren und auf dieser Grundlage einen Gesetzentwurf zu erarbeiten, fanden zur Klärung der damit im Zusammenhang stehenden schwierigen datenschutzrechtlichen Fragen bereits mehrere Abstimmungsgespräche mit dem Fachressort statt. Dass hier von Seiten des Sozialministeriums unaufgefordert und rechtzeitig unser Rat gesucht wurde, ist sehr zu begrüßen. Ist es doch wichtig, dass angesichts des noch vorhandenen Abklärungsbedarfs im Grundsätzlichen wie auch zu offenen Fragestellungen im Detail eine abgestimmte Position zu diesem sensiblen Thema gefunden werden kann.

Aus heutiger Sicht lässt sich allein so viel sagen, dass das Krebsregistergesetz (neu) zu einer grundlegenden Änderung der früheren Krebsregistrierung

in Baden-Württemberg führen soll. Deshalb muss gerade angesichts des Flops mit dem früheren Krebsregister Baden-Württemberg von Seiten des Datenschutzes in besonderem Maße und sehr sorgfältig darauf geachtet werden, dass der Wille der Krebspatienten, darüber zu bestimmen, was letztlich mit ihren personenbezogenen Krankendaten geschehen soll, im neuen Gesetz einen ausreichenden und datenschutzkonformen Niederschlag findet. Mag auch der Druck nach dem kurzfristigen „Aus“ für das alte Krebsregister sehr groß sein, eine möglichst rasche Ersatzlösung präsentieren zu können, so darf dies nicht zu Lasten der Qualität einer neuen Regelung gehen.

Es ist im Augenblick zunächst Sache des Sozialministeriums, die für uns derzeit noch offenen Fragen zu beantworten, um dann auf einer gesicherten Faktengrundlage zu einer auch aus Sicht des Datenschutzes akzeptablen Lösung zu kommen.

2. Mammographie-Screening

Auf der Grundlage des Beschlusses des Bundesausschusses der Ärzte und Krankenkassen zur Änderung der Krebsfrüherkennungs-Richtlinie vom 1. Dezember 2003 sowie der weiteren Beschlüsse der Partner der Bundesmantelverträge wurde das Mammographie-Screening gemäß der Regelung des § 92 Fünftes Buch des Sozialgesetzbuchs (SGB V) als neue ärztliche Leistung in die vertragsärztliche Versorgung für Frauen im Alter von 50 bis 69 Jahren aufgenommen. Dabei ist eine „Zentrale Stelle“ für die Durchführung der Einladung der daran Teilnahmeberechtigten vorgesehen, um auch alle in Frage kommenden Frauen zu erreichen.

Fachlich unbestritten ist, dass der nach langer Diskussion gefasste Beschluss zur Einführung eines flächendeckenden Systems zur Früherkennung von Brustkrebs – zukünftig auf hohem europaweit geltenden Qualitätsniveau – zu einer Verbesserung der Krebsvorsorge in diesem Bereich in Deutschland führen wird. Dementsprechend finden die derzeit laufenden Anstrengungen der Selbstverwaltung zur Umsetzung dieses Früherkennungsprogramms die Unterstützung sowohl der betroffenen Fachministerien im Land (Sozialministerium federführend; Innenministerium) als auch meiner Dienststelle, damit ein Verfahren entwickelt werden kann, das sowohl praktischen wie auch den datenschutz- bzw. melderechtlichen Anforderungen Rechnung trägt.

Eine erste Erkenntnis bei der Umsetzung des Projekts in Baden-Württemberg war, dass die Vorgaben des Bundesausschusses für das Umfeld der eigentlichen Mammographie-Leistung (z. B. Einladung unter Einschaltung des Melderegisters, Evaluation etc.) nicht optimal, zum Teil sogar realitätsfern und unnötig kompliziert waren und auch der dafür erforderliche Rechtsrahmen erst noch geschaffen bzw. geändert werden müsste.

So ist es aus Sicht des Datenschutzes nur wenig einsichtig, warum bei der Einladung der teilnahmeberechtigten Frauen nicht auf die bei den gesetzlichen und privaten Krankenversicherungen vorhandenen Daten der Versicherten zurückgegriffen werden soll, mit deren Hilfe laut Aussagen des Sozialministeriums über 99 % der betroffenen Frauen erreicht werden könnten. Dies auch deshalb, weil durch das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung seit 1. Januar 2004 auch alle Sozialhilfeempfängerinnen mit laufender Leistung zum Lebensunterhalt nach § 264 SGB V in die gesetzliche Krankenversicherung einbezogen sind. Die Krankenversicherungen könnten auf die erforderlichen Daten auf einer gesicherten rechtlichen Grundlage zurückgreifen, ohne dass dabei grundsätzliche datenschutzrechtliche Probleme auftreten könnten. Außerdem ist es selbstverständlich, dass die Krankenversicherungen die bei ihnen versicherten Frauen über das neue Angebot der Mammographie-Leistung jeweils individuell informieren dürfen. Ein Rückgriff auf die Melderegisterdaten, die darüber hinaus auch noch weniger valide sein dürften als die Daten der Krankenversicherungen, wäre demgegenüber erst nach Änderung der landesrechtlichen Bestimmungen zum Melderecht in den meisten der 16 Bundesländer möglich. Diese gemeinsame Auffassung der beteiligten Ministerien sowie meiner Dienststelle hat der seinerzeitige baden-württembergische Sozialminister in einem Schreiben vom 14. Mai 2004 an die Bundesministerin für Gesundheit und Soziale Sicherung daher auch verdeutlicht.

Unabhängig hiervon hat die Gesundheitsministerkonferenz auf ihrer 77. Sitzung den Beschluss gefasst, dass die Länder bereit sind, sich den mit der Einführung des Mammographie-Screenings verbundenen Aufgaben zu stellen; dies umfasst auch eventuell notwendige Anpassungen der Meldegesetze oder der Meldeverordnungen im Hinblick auf ein bundeseinheitliches bevölkerungsbezogenes Einladungswesen für die Früherkennung von Brustkrebs. Im Interesse der Sache würde sich mein Amt dem nicht widersetzen, obwohl es – wie ausgeführt – unseres Erachtens bessere Lösungen gibt. Unverzichtbar ist selbstverständlich in jedem Fall, dass etwa fehlende Rechtsgrundlagen noch geschaffen werden.

Insoweit ist es zu begrüßen, dass im Anschluss an eine Besprechung Ende Juli 2004, an der neben den Partnern der Selbstverwaltung auch das Innenministerium und meine Dienststelle vertreten waren, das Sozialministerium in einem weiteren Schreiben an die Bundesgesundheitsministerin einen nochmaligen Vorstoß unternommen hat, die erforderlichen Rechtsänderungen von Bundesseite einzufordern. Nach unserer gemeinsamen Rechtsauffassung ist außer den Melderechtsänderungen, die Ländersache sind, eine spezielle gesetzliche Grundlage für die Einrichtung der vorgesehenen Zentralen Stelle für das Einladungswesen erforderlich, die u. a. die Anforderungen an eine öffentliche Stelle im Sinne von § 18 des Melderechtsrahmengesetzes erfüllt. Da die Zentrale Stelle nicht nur die Meldedaten der gesetzlich krankenversicherten, sondern auch der privat krankenversicherten Frauen erhalten soll, reicht die Schaffung einer Arbeitsgemeinschaft der gesetzlichen Krankenversicherungen und der Kassenärztlichen Vereinigung auf der Grundlage von § 219 Abs. 2 SGB V hierfür allein nicht aus. Für privat Versicherte fehlt es an der gesetzlichen Zuständigkeit. Es muss daher zunächst eine für alle Bundesländer und Versicherten gleichermaßen geltende Rechtsgrundlage geschaffen werden, um eine solche gemeinsame Zentrale Stelle überhaupt aufbauen zu können; die Gesetzgebungskompetenz hierfür liegt beim Bund.

Bei Drucklegung dieses Tätigkeitsberichts lag noch keine Rückäußerung von Bundesseite vor. Wir werden das Projekt auch weiterhin in beratender Funktion konstruktiv begleiten.

3. Datenschutz im Krankenhaus

3.1 Der Kontrollbesuch

Auf die schwierige finanzielle Situation im Gesundheitswesen und den sich daraus ergebenden Kosten- und Reformdruck habe ich bereits eingangs hingewiesen. Dies gilt in besonderem Maße auch für den Krankenhausbereich. In Gesprächen mit Krankenhausleitungen und Klinikärzten wird hierüber oft ebenso geklagt wie über die zunehmende Komplexität datenschutzrechtlicher Fragestellungen im Gesundheitsbereich. Man mag daher ein gewisses Verständnis dafür haben, wenn im Spannungsbogen des täglichen Klinikbetriebs einerseits und den Datenschutzbestimmungen und hier vor allem der ärztlichen Schweigepflicht andererseits nicht alles nach der reinen Lehre abläuft. Andererseits ist aber darauf zu achten, dass die vom Gesetzgeber bewusst gesetzten hohen Hürden im Umgang mit sensiblen Patientendaten nicht allein aus Kostengründen (ein-)gerissen werden. Die unmittelbar betroffenen Patienten hätten dafür zu Recht nur wenig Verständnis.

Ein Kontrollbesuch führte in diesem Jahr in ein Krankenhaus eines Landkreises, dem im Jahre 2001 bereits ein Kontrollbesuch in einem anderen Kreiskrankenhaus gegolten hatte (22. Tätigkeitsbericht, LT-Drs. 13/520, S. 51 ff.). Nachdem wir seinerzeit zum Teil gravierende Mängel im Umgang mit Patientendaten feststellen mussten, war für uns interessant zu sehen, ob man vor Ort auf Ebene des Landkreises daraus auch Lehren gezogen hat. Dies nicht zuletzt auch deshalb, weil alle drei Krankenhäuser des Landkreises über ein gemeinsames Krankenhaus-Rechenzentrum verfügen, dessen Krankenhausinformationssystem ebenfalls von den beiden von uns aktuell nicht überprüften Kreiskliniken mitbenutzt wird. Erfreulich war dabei zu sehen, dass es gegenüber dem ersten Kontrollbesuch zu einer Steigerung des Problembewusst-

seins und damit einhergehend auch zu einem sensibleren Umgang mit Patientendaten gekommen ist. Allerdings gab es dennoch einiges zu verbessern. Folgendes ist dabei erwähnenswert:

3.1.1 Datenschutzbeauftragte im Krankenhaus

Nach § 51 Abs. 1 des Landeskrankenhausgesetzes (LKHG) hat der Krankenhausträger für das Krankenhaus einen Beauftragten für den Datenschutz schriftlich zu bestellen. Zwar hat das von uns kontrollierte Krankenhaus seit 1993 eine Mitarbeiterin zur Datenschutzbeauftragten bestellt. Die Bestellung erfolgte allerdings formlos und kann von ihr nur neben ihrer hauptamtlichen Tätigkeit als Leiterin der allgemeinen Verwaltung bei einer Bettenkapazität von immerhin rd. 470 Betten erledigt werden. Dass dabei für die Aufgaben als behördliche Datenschutzbeauftragte nur wenig Zeit bleibt – uns wurden ca. 3 Stunden im Monatsdurchschnitt genannt – verwundert nicht. Folge davon ist, dass für sie zwar die Möglichkeit besteht, an datenschutzrechtlichen Fortbildungsmaßnahmen teilzunehmen; das tatsächliche Engagement für Aufgaben des innerbetrieblichen Datenschutzes muss aufgrund des verbleibenden schmalen Zeitbudgets zwangsläufig jedoch weitgehend graue Theorie bleiben. Ganz zu schweigen davon, dass es nicht nur um die eigene Fortbildung geht, sondern ein interner Datenschutzbeauftragter u. a. auch als Multiplikator und Berater in Datenschutzfragen für die Krankenhausbediensteten Zeit haben sollte.

Bei der Größe des o. g. Krankenhauses, der zunehmenden Komplexität der datenschutzrechtlichen Fragestellungen sowie der Sensibilität von Patientendaten darf die Bestellung eines Beauftragten für den Datenschutz keine Alibibestellung sein, um formal den Anforderungen des § 51 LKHG Rechnung zu tragen. Die erforderliche schriftliche Bestellung ist schon allein deshalb wichtig, damit sich der Krankenhausträger im Zusammenhang mit der Arbeitsplatzbeschreibung bewusst wird, dass eine sachgerechte Ausübung des Amts eines innerbetrieblichen Datenschützers Arbeitskapazität bindet. Insoweit stellt das Schriftformerfordernis auch keine schlichte bürokratische Formalie dar, sondern verpflichtet die Krankenhausleitung darüber hinaus, sich zusätzlich Gedanken darüber zu machen, ob bei der für diese Funktion vorgesehenen Person bei der Aufgabenwahrnehmung kein Interessenkonflikt mit dem ausgeübten Hauptamt besteht. In diesem Zusammenhang ist auf § 51 Abs. 3 LKHG in Verbindung mit §§ 4 f, 4 g des Bundesdatenschutzgesetzes sowie auf die Ausführungen im gemeinsamen Merkblatt des Innenministeriums Baden-Württemberg und des Landesbeauftragten für den Datenschutz vom Januar 2001 („Behördlicher Datenschutzbeauftragter“) hinzuweisen. Danach gehört es beispielsweise auch zu den Aufgaben eines behördlichen Datenschutzbeauftragten, die Bediensteten über die datenschutzrechtlichen Vorschriften in geeigneter Weise zu unterrichten oder – soweit Datenverarbeitung im Auftrag erfolgt (z. B. Schreibarbeiten, Aktenvernichtung) – vor Ort sich selbst ein Bild darüber zu machen, ob bei den Vertragspartnern des Krankenhauses die erforderlichen technisch-organisatorischen Vorkehrungen zum Schutz der personenbezogenen Daten in ausreichendem Maße berücksichtigt wurden.

Dass dies bei noch nicht einem halben Tag zur Verfügung stehender Zeit pro Monat für einen Datenschutzbeauftragten faktisch nicht leistbar ist, braucht nicht näher ausgeführt zu werden. Wir halten es daher für dringend geboten, dass in diesem Bereich die aufgezeigten Mängel behoben und dem innerbetrieblichen Datenschutz durch konkrete Veränderungen auch zeitlich mehr Beachtung geschenkt wird. Dies gilt im Übrigen unabhängig davon, in welcher Rechtsform die Krankenhäuser des betreffenden Landkreises betrieben werden.

Im konkreten Fall zeigte sich der Krankenhausträger sehr aufgeschlossen und hat mitgeteilt, dass er noch in diesem Jahr eine Stelle eigens für den Datenschutzbereich einrichten werde. Diese 70-Prozent-Teilzeitstelle soll dabei ausschließlich der Funktion des Datenschutzbeauftragten dienen, wobei der Stelleninhaber dann für alle drei Krankenhäuser zuständig sein soll. Wir meinen, dass damit eine akzeptable Lösung gefunden wurde, die durchaus zur Nachahmung empfohlen werden kann.

3.1.2 Patientenaufnahme

Wie wir vor Ort feststellen mussten, erfolgt die reguläre Patientenaufnahme in einem ausschließlich dafür vorgesehenen Büroraum mit drei eingerichteten Aufnahmeplätzen. Die Datenerhebung geschieht im Dialog zwischen Patient und Aufnahmekraft, wobei die erfragten Angaben unmittelbar in das EDV-System eingegeben werden. Allerdings besteht nach unseren Feststellungen zwischen den drei Aufnahmeplätzen nur ein kleiner mobiler Sichtschutz, der keinerlei akustische Abschirmung gewährleistet. Nach Angaben des Krankenhauses soll dies im Zuge der anstehenden Umbaumaßnahmen durch die Einrichtung von Einzelkabinen verbessert werden. Es bleibt zu hoffen, dass dies möglichst bald geschieht. Wie uns inzwischen mitgeteilt wurde, soll mit den entsprechenden Maßnahmen im Frühjahr 2005 begonnen werden.

Unabhängig davon stellten wir fest, dass das Krankenhaus mehr Daten erhebt bzw. in mehr Daten Einblick nimmt, als es dürfte.

Jede Form der Datenverarbeitung personenbezogener Daten greift in das Grundrecht der betroffenen Person auf Datenschutz ein und darf deshalb nur unter gesetzlich bestimmten Voraussetzungen erfolgen. Die vom Krankenhaus hierbei zu beachtenden Datenschutzbestimmungen ergeben sich vorwiegend aus dem 7. Abschnitt des Landeskrankenhausgesetzes. § 45 Abs. 1 Satz 1 LKHG bestimmt die Zwecke, für die das Krankenhaus Patientendaten verarbeiten darf. Es geht dabei zum einen um die Patientenversorgung, zum anderen um die verwaltungsmäßige Abwicklung des Behandlungsverhältnisses, insbesondere um die Leistungsabrechnung. Weiter wird vorausgesetzt, dass Patientendaten für diese Zwecke nur verarbeitet werden, soweit dies auch tatsächlich erforderlich ist.

Bei der Aufnahme eines Patienten geht es in erster Linie darum, die für die verwaltungsmäßige Abwicklung des Behandlungsverhältnisses erforderlichen Daten zu erheben (§ 45 Abs. 1 Satz 1 Nr. 2 LKHG). Die medizinischen Daten werden in aller Regel erst durch die behandelnden Ärzte, deren Station der Patient zugewiesen wird, erfasst.

Folgende Angaben bei der Aufnahme bzw. folgende Einsichtsmöglichkeiten durch dort tätige Beschäftigte erscheinen danach nicht erforderlich:

- Die Patientenaufnahme hat Zugriff auf eine Maske, aus der sie Diagnoseschlüssel für die Erstellung von Aufenthaltsbescheinigungen entnimmt, die für Patienten auf deren Wunsch erstellt und von diesen beispielsweise als Nachweis gegenüber ihrer Krankenversicherung verwendet werden. In dieser Maske waren neben dem Diagnoseschlüssel auch eine verbale Beschreibung der Diagnose sowie etwaige Nebendiagnosen sichtbar. Nach unseren Feststellungen benötigt die Patientenaufnahme für den genannten Zweck weder Kenntnis von der verbalen Beschreibung der Diagnose noch von den Nebendiagnosen.
- Bei der Aufnahme wird auch die telefonische Erreichbarkeit von Angehörigen erfragt. Hierfür reichen Nachname und Telefonnummer aus. Das Verwandtschaftsverhältnis zum Patienten ist insoweit ohne Belang und darf bei der Aufnahme nicht erfragt werden.

– In einem für die Aufnahme von Schwangeren vorgesehenen Modul konnte die Patientenaufnahme erkennen, ob besondere Schwangerschaftsrisiken bestehen. In einem konkreten Fall war auf diese Weise ersichtlich, dass die betreffende Frau drogenabhängig war.

– Im Zusammenhang mit der Entlassung eines Kindes konnte die Patientenaufnahme zudem erfahren, ob eine Erkrankung oder Fehlbildung des Kindes vorlag.

Um diese Mängel zu abzustellen, muss das Krankenhaus die Gestaltung der Masken und die damit verbundenen Zugriffsberechtigungen mit dem Ziel überarbeiten, dass die Patientenaufnahme nur solche Daten lesen und ändern kann, die sie für die Erfüllung ihrer Aufgaben benötigt.

Hinsichtlich der Einsichtsmöglichkeit in die Diagnosetexte wird derzeit die Software geändert, so dass nach erfolgter Umprogrammierung grundsätzlich kein lesender Zugriff für die Mitarbeiter in der Patientenaufnahme mehr möglich ist. Die weiteren von uns für erforderlich gehaltenen Änderungen wurden zwischenzeitlich nach Angaben des Krankenhauses bereits teilweise realisiert.

3.1.3 Krankenhausseelsorge

Die Religionszugehörigkeit wird über besondere Formulare bei der Aufnahme miterfasst. Im Krankenhaus gibt es eine evangelische und eine römisch-katholische Seelsorge. Die Formulare erfassen folgerichtig nur die evangelische oder katholische Religionszugehörigkeit und nicht, wie man es leider zum Teil immer noch erlebt, auch Religionszugehörigkeiten, für die es im Krankenhaus gar keine seelsorgerische Betreuung gibt.

Die Krankenhausverwaltung separiert danach die beiden genannten Religionszugehörigkeiten und leitet dem jeweiligen Seelsorger nur die Angaben derjenigen Patienten zu, für die er seelsorgerische Aufgaben übernommen hat. Allerdings werden den Seelsorgern die kompletten Wohnadressen, das Geburtsdatum und das Geschlecht der aufgenommenen Patienten übermittelt. Es war sogar möglich, frühere Patienten aufzurufen, die – glücklicherweise – längst, nämlich vor sechs Jahren und vielleicht auch schon früher, das Krankenhaus verlassen hatten.

Hier müssen die Verfahrensabläufe dringend geändert werden. Nach unserer Auffassung hat die sog. Pfarrerliste ihre Aufgabe mit der Patientenentlassung erfüllt. Im Übrigen werden auch keine zwingenden Gründe gesehen, weshalb in der Information an den Seelsorger die Wohnanschrift und weitere personenbezogene Daten übermittelt werden. Sinn und Zweck der in diesem Zusammenhang bei der Aufnahme erhobenen und weitergemeldeten Informationen an den Krankenhauspfarrer erschöpfen sich nämlich darin, eine seelsorgerische Betreuung durch eine vom Patienten gewünschte Kontaktaufnahme mit dem Geistlichen zu ermöglichen. Die anderen Dinge können – so es der Patient denn wünscht – dem Pfarrer dann immer noch im direkten Kontakt am Krankenbett mitgeteilt werden.

Seitens der Krankenhausverwaltung hat man rasch reagiert und den geschilderten Anliegen bereits Rechnung getragen.

3.1.4 Behandlungsvertrag

Das uns vorliegende aktuell geltende Formular des Behandlungsvertrags sieht vor, dass der Patient zunächst durch seine Unterschrift den eigentlichen Behandlungsvertrag abschließt. Daneben – ohne dass dies textlich besonders hervorgehoben wird – willigt er durch weitere Unterschrift darin ein, dass seine im Zusammenhang mit dem Krankenhausaufenthalt aufgenommenen personenbezogenen Daten an externe Schreibbüros weitergeleitet werden

dürfen, soweit dies zum Schreiben von Arztbriefen erforderlich ist. Positiv ist dabei anzumerken, dass die Patienten darauf hingewiesen werden, dass sie diese Einwilligung jederzeit ohne nachteilige Folgen widerrufen können.

Zu bemängeln ist allerdings, dass diese Erklärung gesetzlichen Formerfordernissen widerspricht. So ist nach § 43 Abs. 5 LKHG in Verbindung mit § 4 Abs. 3 Satz 2 LDSG eine Einwilligungserklärung, die zusammen mit anderen Erklärungen schriftlich erteilt werden soll, bereits im äußeren Erscheinungsbild besonders hervorzuheben.

Eine entsprechende Neugestaltung der Vordrucke wurde uns zugesagt.

3.1.5 Archiv

Uns liegt es fern, nur zu kritisieren. Deshalb zunächst das Lob: Positiv anzumerken ist, dass eine Archivordnung vorhanden war, die derjenigen entspricht, die seinerzeit aufgrund unserer Beanstandung anlässlich unseres Kontrollbesuchs im Jahre 2001 in einem anderen Krankenhaus des Landkreises neu erstellt wurde.

Eingehende Post wird durch Mitarbeiter der Registratur im Krankenhaus verteilt. Soweit die Eingangspost adressiert ist, wird sie ungeöffnet direkt an den Adressaten weitergeleitet. Nicht persönlich zuordenbare Post – wie beispielsweise nur an das Kreiskrankenhaus adressierte Schreiben – werden an das Sekretariat des Verwaltungsdirektors weitergeleitet, dort geöffnet und in den Postlauf gegeben. Die Ausgangspost des Krankenhauses kommt bereits in verschlossenen Umschlägen ins Archiv und wird dort lediglich noch frankiert.

Das sich im ersten Untergeschoss des Krankenhauskomplexes befindliche Archiv ist über Treppen, Aufzüge und Flure für jedermann problemlos zu erreichen. Der Zutritt in die Archivräume selbst ist allerdings nur nach vorheriger Anmeldung über eine Klingel und Gegensprechanlage möglich. Dies ist auch gut so. Leider mussten wir feststellen, dass außerhalb des gegen unbefugten Zutritt geschützten Archivbereichs in den allgemein zugänglichen Fluren mehrere Karteikartenschränke aufgestellt waren. Dies allein ist schon nicht unproblematisch. Leichtfertig wird das Ganze dann, wenn – wie wir leider feststellen mussten – die Schränke unverschlossen sind. Sie enthielten Karteikarten mit Angaben über aktuelle und frühere Patienten, wobei den älteren Karteikarten u. a. Angaben über Staatsangehörigkeit, Telefonnummern, Adressen, einweisenden Arzt, Hausarzt und vieles andere mehr zu entnehmen waren. Dass diese Datenerhebung erkennbar nicht dem Grundsatz der „Erforderlichkeit“ im Sinne des § 45 Abs. 1 Satz 1 LKHG genügt, bedarf hier keiner näheren Ausführung. Nachdem sich allerdings bei unseren Stichproben auf Karteikarten jüngeren Datums keine vergleichbar umfangreichen (Vorrats-)Datensammlungen feststellen ließen, gehen wir davon aus, dass die seinerzeit zu diesem Thema gewonnenen Erkenntnisse aus unserem Kontrollbesuch im Jahr 2001 in einem anderen Krankenhaus desselben Landkreises auch hier bereits umgesetzt worden sind.

Dass in der heutigen Zeit überhaupt noch mit doppelter Absicherung (konventionelle Karteikarten und EDV-Einsatz) und damit doppelter Datenmenge in der Praxis gearbeitet wird, erklärte man uns damit, dass man auf der sicheren Seite sein wolle, falls es mit dem EDV-Patienteninformationssystem einmal Probleme geben sollte. Dagegen lässt sich wenig sagen.

Inakzeptabel und mit dem Persönlichkeitsrecht des Patienten auf Schutz seiner Patientendaten im Sinne von § 44 LKHG sowie § 43 Abs. 5 LKHG in Verbindung mit § 9 Abs. 2 LDSG unvereinbar ist jedoch, dass die Karteikartenschränke nicht verschlossen angetroffen wurden.

Dass dies aus Unvorsichtigkeit versehentlich geschah – wie man erklärend versicherte – muss aber wohl bezweifelt werden. So wurden im Flurbereich weitere unverschlossene Schränke angetroffen, in denen ebenfalls Patientenakten abgelegt waren. Uns wurde erklärt, dass es sich hier nicht um Krankenhausakten handele, sondern um Patientenakten aus der Privatambulanz des Chefarzts. Da diese Flächen lediglich in Form eines Mietvertrags durch das Krankenhaus dem betreffenden Arzt überlassen worden seien, trage dieses für den Datenschutzverstoß keine Verantwortung. Diese Einlassung – selbst wenn sie richtig wäre – macht das Ganze nicht unproblematischer, auch wenn mir hier die Kontrollbefugnis infolge mangelnder Zuständigkeitszuweisung nach dem Landesdatenschutzgesetz bedauerlicherweise fehlt. Es verstärkt vielmehr – zuständig oder nicht – den Eindruck, dass in diesem Teilbereich der Archivverwaltung sehr sorglos mit Patientendaten umgegangen wird und die einschlägigen Bestimmungen des Datenschutzrechts nicht die notwendige Beachtung finden.

Auch dies zumindest stichprobenweise zu überprüfen und Missstände anzusprechen, wäre Aufgabe eines betriebsinternen Datenschutzbeauftragten, wenn diesem denn ausreichend Zeit zur Verfügung stünde (siehe oben Nr. 3.1.1).

Dazu, dass die Karteikartenschränke bei unserem Kontrollbesuch zum Teil nicht verschließbar waren, hat uns das Krankenhaus mittlerweile berichtet, dass damals die Schlüssel fehlten und auch nicht auffindbar waren. Inzwischen habe man aber die Technik beauftragt, neue Schlösser einzubauen. Allerdings hätte man auf diese Lösung wohl doch früher und auch ohne unsere Hinweise kommen können.

3.1.6 Pforte

Nach unseren Feststellungen gibt es durch den Pfortendienst keine Zugriffe auf sog. historische Patientendaten. Entlassene Patienten werden im Verzeichnis spätestens fünf Tage nach der Entlassung gelöscht. Dass diese Datenangaben nicht unverzüglich nach der Entlassung gelöscht werden, wurde u. a. damit begründet, dass dies zur technischen Abwicklung der Telefonabrechnung erforderlich sei.

Daneben konnte von der Pforte aus auf Informationen aus dem Labor zugegriffen werden. Zur Erklärung und Rechtfertigung wurde gesagt, dass während der sog. Nachtschicht mit weniger Publikumskontakt die an der Pforte Dienst tuenden Mitarbeiter Kontrollaufgaben in diesem Bereich wahrzunehmen hätten. Hier sehen wir von Seiten des Krankenhauses noch weiteren Aufklärungsbedarf. Insbesondere bedarf es näherer Angaben, um welche konkrete Kontrolltätigkeit es sich handelt, wie oft diese Tätigkeiten anfallen und ob das Pfortenpersonal überhaupt die dafür erforderliche Ausbildung besitzt. Unabhängig davon ist dies keine Erklärung dafür, dass auch die sog. Tagesschicht an der Pforte dieselben, ganz offensichtlich von ihr nicht benötigten Zugriffsrechte besitzt. Insoweit müssten hier die Berechtigungen eingeschränkt werden.

Mittlerweile wurde eine datenschutzkonforme Lösung dadurch erreicht, dass die genannten Kontrollaufgaben automatisch softwaregesteuert wahrgenommen werden; die Zugriffsberechtigung für den Pfortendienst konnte deshalb zurückgenommen werden.

3.2 Entlassbericht in falsche Hände

Ein betagter Bürger hatte sich an mein Amt gewandt, nachdem er nach einem stationären Krankenhausaufenthalt zu Hause in Ruhe die ihm bei der Entlassung ausgehändigten Unterlagen näher betrachten konnte. Er musste feststellen, dass ihm zusammen mit weiteren Entlasspapieren

ein Pflegebericht über einen Patienten ausgehändigt worden war, den er überhaupt nicht kannte und bei dem weder vom Namen, Alter, Wohnort auch nur ansatzweise Verwechslungsgefahren mit seinen eigenen Daten bestand. Erklärt wurde uns dieser Fehler auf Nachfrage in der Klinik damit, dass man irrtümlich wegen (angeblich) ähnlicher Namensgebung das falsche Patienten-Etikett manuell auf den für die Person des Petenten bestimmten Entlassbericht geklebt habe. Von der Klinik gelobte man Besserung und bedauerte den Fehler – zumindest uns gegenüber. Ferner sollen künftig Formulare entwickelt und auch eingesetzt werden, auf denen die Patientendaten direkt aus dem EDV-System des Krankenhauses auf die Vordrucke übernommen werden, um solche manuellen Fehlerquellen von vornherein auszuschalten.

So gut, so schlecht. Derselbe Mann wurde nach seiner sich an den Krankenhausaufenthalt anschließenden Behandlung in einer Reha-Klinik erneut Opfer einer Verwechslung. Dort händigte man ihm sogar den Entlassbericht einer Patientin aus; schon wegen des unterschiedlichen Geschlechts hätte eigentlich kaum eine Verwechslungsgefahr bestehen können. Der Petent verstand die Welt nicht mehr. Wir konnten ihm leider nur im ersten Fall weiterhelfen, nicht dagegen hinsichtlich der Vorgänge in der Reha-Klinik, da diese in privater Rechtsform betrieben wird und daher nicht der Datenschutzaufsicht des Landesdatenschutzbeauftragten unterliegt. Hoffentlich wurde dadurch das Weltbild dieses Bürgers nicht zusätzlich erschüttert.

3.3 Patientenverwechslung bei der Aufnahme

In einem städtischen Klinikum wurden zwei verschiedene Personen zu verschiedenen Zeitpunkten und mit unterschiedlichen Erkrankungen in der Notaufnahme unter dem Namen des Petenten behandelt, der zu diesem Zeitpunkt davon noch nichts wusste. Als der Petent selbst später in dieses Krankenhaus stationär aufgenommen werden musste, war sein Erstaunen groß, als man ihm mitteilte, dass es über ihn bereits eine Krankenakte gebe. Besonders pikant wurde die Angelegenheit noch dadurch, dass die beiden ersten Notaufnahmen jeweils im Zusammenhang mit Verletzungen infolge übermäßigen Alkoholgenusses standen. Er wandte sich Hilfe suchend an mein Amt. Wir baten daraufhin das Klinikum um Auskunft, so wie es das Landesdatenschutzgesetz in seinem § 29 auch vorsieht.

Erstaunlicherweise hat das Klinikum erst nach zähem Nachhaken durch uns u. a. eingeräumt, dass es sich bei den nicht dem Petenten zuzurechnenden früheren Notaufnahmefällen nicht um ein und dieselbe Person gehandelt hat, sondern um zwei verschiedene. Man habe – so teilte man uns weiter mit – inzwischen den Datenschutzbeauftragten des Klinikums eingeschaltet und unter dessen Mitwirkung eine Lösung gefunden, wonach in den Stammdaten des Petenten hinterlegt wird, dass bei einem erneuten Klinikaufenthalt einer sich unter dessen Namen ausgebenden Person eine genauere Überprüfung der Personalien (z. B. durch Vorlage eines geeigneten mit einem Lichtbild versehenen Identifikationspapiers) zu erfolgen habe. Einen vergleichbaren Fall habe es im Klinikum – soweit man sich erinnern könne – noch nicht gegeben. Fast mag man diese Aussage glauben, so kurios dieser Fall gelagert ist.

Andererseits stimmt der Fall bedenklich, wenn man berücksichtigt, dass die erforderlichen technisch-organisatorischen Datenschutzmaßnahmen nach § 43 Abs. 5 LKHG in Verbindung mit § 9 LDSG erst mit erheblichem Zeitverzug und nur deshalb getroffen wurden, weil der Petent unglücklicherweise – oder sollte man lieber glücklicherweise sagen – selbst in die Klinik eingeliefert werden musste. Auch stellt sich die Frage, was passiert wäre, wenn der Petent sich nicht an uns gewandt hätte. Verräterisch ist in diesem Zusammenhang die Aussage des Klinikums zu der vom Petenten beim zuständigen Polizeirevier gegen Unbekannt erstatteten Anzeige: „Wir haben uns der Klage nicht angeschlossen, da der Schaden im Gegensatz zum Aufwand unerheblich ist“. So kann man es zwar sehen – sollte es aber nicht.

Immerhin hat sich die Klinik inzwischen beim Petenten entschuldigt. Ob dadurch allerdings das einmal zerstörte Vertrauen wieder hergestellt werden konnte und dieser ohne Not noch mal dasselbe Krankenhaus aufsuchen würde, entzieht sich unserer Kenntnis. Zweifel scheinen angebracht.

3.4 Abrechnung durch Chefarztgattin

In einem Kreiskrankenhaus sollen nach einem Hinweis an uns aus der Klinik die Abrechnungen über die Privatpatienten des Chefarztes von dessen Gattin zu Hause erstellt werden. Man bat uns in diesem Zusammenhang lediglich um eine allgemeine Rechtsauskunft, weil eine Rückfrage in der Klinik, bei der wir selbstverständlich nicht den Namen unserer Informationsquelle offen gelegt hätten, ausdrücklich nicht gewünscht wurde.

Die Absicht, sich sinnvoll zu beschäftigen und Kosten im Gesundheitswesen zu sparen, verdient Anerkennung. Allerdings sollte man sich vorher schon Gedanken darüber machen, ob dies überhaupt rechtlich zulässig ist. Immerhin geht es um sensible Patientendaten und -akten. Um die uns geschilderte Abrechnungspraxis durchführen zu können, müssen nämlich zunächst sensitive Daten und Unterlagen aus dem Krankenhaus heraus in das private Wohnumfeld der Chefarztgattin verbracht werden. Die Daten werden dabei Personen überlassen, die weder dem Personalkörper des Krankenhauses zuzurechnen sind noch zum behandelnden Ärzte- oder Schwesternteam gehören. Das Offenbaren von Patientengeheimnissen stellt eine Durchbrechung der durch § 203 des Strafgesetzbuchs (StGB) geschützten ärztlichen Schweigepflicht dar, die nur zulässig ist, wenn entweder eine Entbindung von der Schweigepflicht durch den Patienten vorliegt oder eine Rechtsvorschrift die Weitergabe ausdrücklich gestattet. In Ermangelung einer solchen besonderen Regelung im Landeskrankenhausgesetz Baden-Württemberg hätten sich die Patienten ausdrücklich mit dieser Art der Rechnungserstellung einverstanden erklären müssen. Die Einwilligung ist dabei aus guten Gründen an bestimmte Formerfordernisse gebunden; sie bedarf insbesondere nach § 50 LKHG der Schriftform. Dass eine solche eingeholt worden wäre, wurde uns nicht berichtet.

Der Vollständigkeit halber sei noch erwähnt, dass derjenige, welcher unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm u. a. als Arzt anvertraut worden oder sonst bekannt geworden ist, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft wird.

4. Einzelfälle

4.1 Weitergabe des vertraulichen Teils der Todesbescheinigung an Pharmakonzern

Ein Gesundheitsamt wandte sich Rat suchend an uns, nachdem ein Pharmakonzern dort um die Übermittlung des vertraulichen Teils des Leichenschauscheins eines früheren Firmenmitarbeiters gebeten hatte. Dabei muss man wissen, dass der amtlich vorgesehene und vom Arzt bei einem Todesfall auszufüllende Formularsatz aus mehreren Durchschreibesätzen besteht. So gibt es u. a. auch einen vertraulichen Teil der Todesbescheinigung, der für das jeweils zuständige Gesundheitsamt bestimmt ist und in den besonders sensible medizinische Angaben, etwa die Todesursache oder klinische Befunde, eingetragen werden. Diese Angaben benötigt das Gesundheitsamt zur Erfüllung seiner gesetzlichen Aufgaben.

Dass nun eine Firma der Chemieindustrie Interesse an einer solchen Todesbescheinigung zeigte, machte sowohl das Gesundheitsamt als auch uns hellhörig, zumal von Firmenseite zur Begründung ausgeführt wurde, dass sie im Rahmen ihrer werkärztlichen Aufgaben nach § 3 des Gesetzes über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (ASiG) verpflichtet sei, Ursachen von ar-

beitsbedingten Erkrankungen zu untersuchen, diese Untersuchungen zu erfassen und auszuwerten und Maßnahmen zur Verhütung dieser Erkrankungen vorzuschlagen. Dazu sei auch die Durchführung epidemiologischer Untersuchungen erforderlich, wofür auch Leichenschauscheine (vertraulicher Teil) von verstorbenen Mitarbeitern ausgewertet werden müssten.

Zusammen mit der Anfrage wurde dem Gesundheitsamt auch eine von dem Konzern vorbereitete formularmäßige Einverständniserklärung übermittelt, die von der Ehefrau des Verstorbenen bereits unterschrieben und von ihr noch durch weiter erbetene handschriftliche Angaben ergänzt worden war. Nach dem Motto „Wenn schon – denn schon!“ ließ sich die Firma von der Witwe den Hausarzt und das Krankenhaus, in dem ihr Mann verstorben war, benennen. Eine Entbindungserklärung von der ärztlichen Schweigepflicht war damit ebenso verbunden wie ihre Zustimmung zur Übersendung der über ihren verstorbenen Mann angefallenen Krankenunterlagen.

Wir vermuteten, dass hinter einem solchen Vorgehen Methode steckt und haben deshalb das zuständige Fachministerium sowie die anderen Datenschutzbeauftragten in Bund und Ländern informiert. Eine Nachfrage bei den übrigen Gesundheitsämtern in Baden-Württemberg förderte zu Tage, dass entsprechende Anfragen allein bei neun von insgesamt 38 Ämtern vorlagen und zum Teil schon positiv beantwortet worden waren.

Ich war daher froh, dass meine Dienststelle von einem Gesundheitsamt auf diese Fälle aufmerksam gemacht worden war, weil wir aus Datenschutzgründen dringend von der Erteilung solcher Auskünfte an die Firma abraten mussten. Das Sozialministerium baten wir, für eine einheitliche und restriktivere Handhabung dieser und vergleichbarer Fälle im Rahmen seiner Fachaufsicht zu sorgen.

Wir beurteilen die Rechtslage dabei wie folgt: Für die Frage der Zulässigkeit der Übermittlung des vertraulichen Teils der Todesbescheinigung ist § 22 Abs. 5 des Bestattungsgesetzes einschlägig, wonach das Gesundheitsamt auf Antrag Einsicht in den Leichenschauschein gewähren oder Auskünfte daraus erteilen kann, wenn der Antragsteller ein rechtliches Interesse an der Kenntnis über die Todesumstände des namentlich bezeichneten Verstorbenen glaubhaft macht und kein Grund zu der Annahme besteht, dass durch die Offenbarung schutzwürdige Belange des Verstorbenen oder der Hinterbliebenen beeinträchtigt werden. Ein lediglich berechtigtes Interesse genügt hier gerade nicht. Der Verweis der Firma auf ihre sich aus § 3 ASiG ergebenden werkärztlichen Aufgaben und einem sich daraus ableitenden Anspruch auf Einsicht in den vertraulichen Teil einer Todesbescheinigung beruht auf einer falschen Gesetzesinterpretation, wie uns das Sozialministerium als zuständiges Fachressort im Übrigen auf Anfrage zuvor bestätigt hatte.

Zur Frage, ob die Einverständniserklärung der Witwe die Übermittlung einer Kopie des Leichschauscheins (vertraulicher Teil) sowie der sonstigen Krankenunterlagen rechtfertigt, ist zunächst darauf hinzuweisen, dass Ärzte nach § 203 StGB (strafrechtlich) sowie nach § 9 der Ärztlichen Berufsordnung (berufsrechtlich) der ärztlichen Schweigepflicht unterliegen. Das strafrechtliche Schweigegebot schließt nach seinem Schutzzweck auch Feststellungen ein, die der Arzt am Körper eines Toten trifft. Die ärztliche Schweigepflicht bezieht sich dabei von ihrem Schutzzweck her auf die verfassungsrechtlich verankerte Geheim- und Individualsphäre des Einzelnen (Artikel 1 Abs. 1 und Artikel 2 Abs. 1 des Grundgesetzes) sowie auf das öffentliche Interesse an der Funktionsfähigkeit des Arztberufes, weil nur ein allgemeines Vertrauen in die Verschwiegenheit des Arztes eine effiziente Gesundheitsversorgung gewährleistet.

Die Schweigepflicht des Arztes gilt in vollem Umfang auch nach dem Tod des Patienten. Entbindet der Patient den Arzt zu Lebzeiten von seiner Schweigepflicht – was vorliegend gerade nicht der Fall war –, wirkt diese Erklärung über seinen Tod hinaus. Hat der Patient eine solche Er-

klärung hingegen nicht abgegeben, kann der Arzt zur Offenlegung befugt sein, wenn der Patient darin mutmaßlich eingewilligt hätte. Wegen ihres höchstpersönlichen Charakters geht die Befugnis zur Entbindung von der Schweigepflicht nicht auf die Erben oder nächsten Angehörigen über. Der mutmaßliche Wille des Verstorbenen ist im Einzelfall aus den persönlichen Umständen des Betroffenen, seinen individuellen Interessen, Bedürfnissen und Wertvorstellungen zu ermitteln. Es ist hierbei ein restriktiver und strenger Maßstab anzulegen. Die abgegebene Einverständniserklärung eines Angehörigen kann hier allenfalls ein (Hilfs-) Indiz sein.

Aufgrund der vorliegenden Gesamtumstände und nachdem sich bei einem solch umfänglichen Datentransfer an einen früheren Arbeitgeber die möglichen Weiterungen bzw. Nutzungsmöglichkeiten von vornherein nicht überblicken lassen, hätte der Verstorbene vernünftigerweise zu Lebzeiten dieser pauschalen und indifferenten Datenweitergabe wohl kaum zugestimmt. Dass dabei das von der Weltfirma verwendete Einwilligungsformular nicht einmal ansatzweise den formellen und materiellen Voraussetzungen entsprach, die an eine sog. informierte Einwilligungserklärung nach § 4 Abs. 2 LDSG bzw. § 4 a des Bundesdatenschutzgesetzes zu stellen sind, überrascht denn doch.

4.2 Kostentragung bei sexuell übertragbaren Krankheiten und Tuberkulose

Nachdem am 12. September 2003 die Verordnung des Sozialministeriums über die Erstattung von Kosten bei sexuell übertragbaren Krankheiten im Gesetzblatt verkündet worden war (GBl. S. 521), mussten wir zweierlei feststellen:

Zum einen war versäumt worden, meine Dienststelle bei der Ausarbeitung dieser Rechtsverordnung zu beteiligen, obwohl sich eine entsprechende Verpflichtung hierzu aus § 31 Abs. 3 LDSG ergibt. Hierfür hat sich das Sozialministerium bereits entschuldigt. In der Sache hatte das Ganze aber insoweit Auswirkungen, als infolge dieses Versäumnisses eine datenschutzfreundlichere Regelung zunächst unterblieben ist. Nach einer nachträglichen Beratung sagte das Sozialministerium zu, bei einer anstehenden Änderung dieser Verordnung unsere Vorschläge zu übernehmen.

Worum ging es? Zum Personenkreis, an den sich die genannte Verordnung in erster Linie richtet, gehören Prostituierte und Obdachlose. Suchen diese mit entsprechendem Krankheitsbild einen Arzt auf, soll mit den medizinisch erforderlichen Maßnahmen unverzüglich begonnen werden, ohne dass zu diesem Zeitpunkt genau feststellbar wäre, wer die Behandlungskosten am Ende zu tragen hat. Hierüber kann danach verwaltungsmäßig entschieden werden. Materieller Anknüpfungs- und Kritikpunkt für den Datenschutz war dabei, dass die Verordnung ein Formblatt vorsieht, mit dem der behandelnde niedergelassene Arzt beim örtlich zuständigen Gesundheitsamt einen Antrag auf Kostenübernahme stellt und diesem für die dort vorzunehmende Prüfung personenbezogene Patientendaten (z. B. die versicherungsmäßigen, fürsorgerischen und wirtschaftlichen Verhältnisse der Patienten) übermitteln muss. Dabei war aus Sicht des Datenschutzes zu bemängeln, dass diese Mitteilung des Arztes von Anfang an und immer personenbezogen zu erfolgen hat, obwohl die Anfrage wegen der besonderen Sensibilität dieser Angaben und der durch das Gesundheitsamt zu erwartenden Ablehnungsfälle zunächst auch in pseudonymisierter Form hätte erfolgen können.

Bei der nächsten Änderung der Verordnung wird das Sozialministerium deshalb § 1 Abs. 1 Satz 1 der Rechtsverordnung dahin gehend ändern, dass der behandelnde Arzt den Antrag an das Gesundheitsamt auf Übernahme der Behandlungskosten nur dann personenbezogen stellt, wenn der Betroffene hierzu das Einverständnis nach entsprechender Aufklärung erklärt hat. Es ist zu hoffen, dass das Sozialministerium diese Änderung möglichst rasch umsetzt. Wir werden uns jedenfalls zu gegebener Zeit nach dem Umsetzungsstand erkundigen.

2. Abschnitt: Die gesetzliche Krankenversicherung

1. Zeitverzug bei Auszahlung von Krankengeld

Eine Bürgerin wandte sich Rat suchend an uns, nachdem eine AOK-Bezirksdirektion sich zunächst geweigert hatte, ihr das Krankengeld in voller Höhe für einen Zeitraum von mehreren Monaten auszubezahlen.

Die Krankenkasse rechtfertigte ihr Verhalten damit, dass die Petentin über ihren Rentenversicherungsträger eine stationäre Reha-Maßnahme begonnen habe, die sie schon nach wenigen Tagen wieder abbrach. Wegen des Übergangs der Zuständigkeit für die Gewährung von Sozialleistungen auf den Rentenversicherungsträger während des Reha-Bewilligungszeitraums habe die Krankenkasse bei ihr bzw. beim behandelnden Arzt in der Reha-Einrichtung rückfragen müssen. Es sollte dadurch abgeklärt werden, ob die AOK trotz des Abbruchs der Behandlung die Gewährung der Sozialleistungen wieder übernehmen müsse. Die Petentin habe der Krankenkasse aber weder die Gründe für den Abbruch der Reha-Maßnahme genannt noch den betreffenden Arzt von seiner Schweigepflicht entbunden. Daraufhin sei sie von Seiten der Krankenkasse mündlich darüber informiert worden, dass sie nach § 60 des Ersten Buchs des Sozialgesetzbuchs (SGB I) eine gesetzliche Mitwirkungspflicht zur Auskunftserteilung habe und man im Falle weiter fehlender Mitwirkung die Zahlung des Krankengeldes einstellen werde. Da gleichwohl keine schriftliche Rückmeldung durch die Versicherte erfolgte, habe man die Zahlungen – wie angekündigt – gemäß § 66 SGB I eingestellt.

Dass der Bürgerin – nachdem sie sich an uns gewandt hatte – dennoch das Geld von der Krankenkasse in voller Höhe nachträglich ausbezahlt wurde, hat die AOK damit begründet, dass sie es versäumt habe, die Petentin rechtzeitig schriftlich auf die geschilderten Rechtsfolgen nach dem SGB I hinzuweisen.

Diese Eigenerkenntnis der Krankenkasse konnten wir nur begrüßen. Zwar war die AOK aufgrund der unterschiedlichen Verantwortlichkeiten für die Bezahlung der Sozialleistungen während des Zeitraums der Reha-Maßnahme (Rentenversicherungsträger) und außerhalb dieses Zeitraums (Krankenkasse) nach § 2 Abs. 4 des Fünften Buchs des Sozialgesetzbuchs (SGB V) in Verbindung mit § 60 SGB I durchaus berechtigt, nach den Gründen für den Abbruch der Reha-Maßnahme zu fragen. § 2 Abs. 4 SGB V verpflichtet die Krankenkassen u. a., wirtschaftlich zu arbeiten, wozu auch die Prüfung gehört, ob sie selbst oder ein anderer Sozialleistungsträger zur Zahlung verpflichtet ist. Allerdings hätte die AOK-Bezirksdirektion von Anfang an formal ordnungsgemäß vorgehen und bei der Bürgerin schriftlich anfragen müssen; ebenso hätte sie schriftlich auf die etwaigen Folgen mangelnder Mitwirkung hinweisen müssen.

Dies ist aus Sicht des Datenschutzes auch keine lässliche Sünde. Der Bürger kann bei nur mündlich erbetenen Auskünften häufig nicht genau abschätzen und erkennen, ob die erbetenen Auskünfte tatsächlich zur Sachentscheidung erforderlich sind, und gibt unter Umständen Dinge unreflektiert preis, die er so bei einer schriftlichen Anfrage nicht mitgeteilt hätte – von der Frage einer späteren Überprüfbarkeit und Nachvollziehbarkeit der von der Krankenkasse getroffenen Verwaltungsentscheidung einmal ganz abgesehen. Auch hier bestätigt sich wieder der Grundsatz: Sorgfalt geht vor Schnelligkeit.

2. Hausarztmodell

Das inzwischen als Pilotprojekt in einer ersten Stufe auf Vertragsgrundlage zwischen der Kassenärztlichen Vereinigung Nordbaden, dem Ärztenetz Qualinet (Mannheim) und der AOK Baden-Württemberg eingeführte Qualitäts- und Kooperationsmodell in der hausärztlichen Versorgung Rhein-Neckar (sog. Hausarztmodell) soll durch neue Formen der Zusammenarbeit der Vertragspartner dazu beitragen, die Qualität und Wirtschaftlichkeit der Versorgung im Gesundheitswesen zu verbessern. Eine externe wissenschaftliche Projektbegleitung dient zur Kontrolle dieses Modellvorhabens. Als Anreiz für die freiwillige Teilnahme der Versicherten wurde diesen von Kassenseite angeboten, die seit Anfang 2004 durch das Gesetz zur Moder-

nisierung der gesetzlichen Krankenversicherung (GKV) eingeführte Praxisgebühr zu übernehmen.

Vereinfacht ausgedrückt soll bei dem Projekt der Hausarzt in seiner Funktion als erster Ansprechpartner, Lotse und Koordinator bei gesundheitlichen Problemen seiner Patienten gefördert und gestärkt werden.

Es handelt sich dabei um ein Modellvorhaben auf der Grundlage des § 63 SGB V, so dass trotz der durch das GKV-Modernisierungsgesetz vorgenommenen Änderung des § 284 Abs. 1 Satz 1 Nr. 13, Abs. 3 SGB V nach Auffassung meines Amts die Betroffenen nach wie vor offen und vollständig darüber aufgeklärt werden müssen, wie im Rahmen des Hausarztmodells mit ihren Daten umgegangen wird. Die Datenhoheit der Betroffenen manifestiert sich deshalb auch darin, dass diese schriftlich einwilligen müssen und jederzeit aus dem Projekt durch entsprechende Widerrufserklärung gegenüber dem Hausarzt oder der AOK-Bezirksdirektion Rhein-Neckar aussteigen können. Unsere mit dem Bundesbeauftragten für den Datenschutz abgestimmte rechtliche Bewertung wurde inzwischen auch von der Krankenversicherung akzeptiert.

Insoweit ist es zu begrüßen, dass die AOK Baden-Württemberg wegen der anspruchsvollen datenschutzrechtlichen Fragestellungen im Zusammenhang mit diesem Modellvorhaben frühzeitig um die Beratung durch den Landesbeauftragten für des Datenschutz gebeten hat (§ 31 Abs. 3 LDSG) und es dadurch möglich wurde, den Anforderungen des Datenschutzes gerecht werdende Merkblätter und Vordrucke für die Teilnahmeerklärung der Versicherten zu entwickeln.

Die AOK hat im Übrigen zugesagt, uns auch während der nächsten Projektphasen rechtzeitig zu beteiligen.

3. Einrichtung von Telearbeitsplätzen bei Krankenkassen

Äußerer Anlass, sich erneut und noch intensiver mit dem Thema zu befassen, war für uns die Mitteilung eines Kollegen aus einem anderen Bundesland, wonach sich die dortige AOK wegen der beabsichtigten Einrichtung von Teleheimarbeitsplätzen mit der Bitte um Beratung an ihn gewandt hatte.

Da es bei der Telearbeit im Vergleich zum Büroarbeitsplatz unter datenschutzrechtlichen Aspekten latente Schwachstellen gibt und wir in der Vergangenheit die AOK Baden-Württemberg hierzu bereits beraten hatten, sahen wir uns veranlasst, diese nach dem aktuellen Sachstand zu fragen.

Wie uns berichtet wurde, sind dort seither etwa 140 Heimarbeitsplätze mit PC-Anschluss eingerichtet worden; zuvor waren auf der Grundlage des § 286 SGB V in Verbindung mit § 78 a des Zehnten Buchs des Sozialgesetzbuchs (SGB X) und dessen Anlagen sowie nach Beratung durch meine Dienststelle die organisatorischen Maßnahmen für die Bereitstellung und Nutzung von Telearbeitsplätzen durch verschiedene Dienstanweisungen des Vorstands der AOK definiert worden. Dabei ging es insbesondere auch um die Anforderungen an die Telearbeiter selbst und um die explizite schriftliche Verpflichtung, im Rahmen der Telearbeit zu Hause die datenschutzrechtlichen Anforderungen einzuhalten.

Bei der Überprüfung der uns übermittelten Unterlagen konnten wir feststellen, dass aus technisch-organisatorischer Sicht die von der Krankenkasse getroffenen Maßnahmen ausreichend sind. Einige weitere Fragen zur Ausgestaltung des Telearbeitsprojekts erschienen uns hingegen erörterungsbedürftig. Diese bezogen sich in erster Linie darauf, ob und welche Tätigkeiten sich für die Telearbeit bei einer gesetzlichen Krankenversicherung überhaupt eignen und ob bei der Entscheidung über die Zulassung eines solchen Arbeitsplatzes auch die Art der dabei zu bearbeitenden Daten angemessen berücksichtigt und welche Kriterien dafür herangezogen werden.

In der Besprechung mit der AOK Baden-Württemberg haben wir darauf hingewiesen, dass eine Verarbeitung von personenbezogenen Daten, welche einem Berufs- oder besonderen Amtsgeheimnis unterliegen, grundsätzlich nicht im Wege der Telearbeit vorgenommen werden sollte. Dies bedeutet, dass Telearbeit in besonders sensiblen Bereichen nicht die Regel sein darf

und daher Ausnahmen nur in besonders zu begründenden Einzelfällen zugelassen werden können. Es erscheint im Übrigen auch nur möglich, eine Telearbeitseignung einzelfallbezogen festzustellen und dafür eine Arbeitsplatzbeschreibung zusammen mit einer Prüfung der konkreten Verhältnisse vor Ort zugrunde zu legen. Es bestand mit der AOK Einvernehmen, dass wegen der Sensibilität der Sozialdaten Telearbeit als Ausnahmetatbestand grundsätzlich nur dann datenschutzrechtlich hinnehmbar ist, wenn die folgenden Kriterien berücksichtigt werden, die bereits vom Landesdatenschutzbeauftragten eines benachbarten Bundeslandes für die dortige AOK entwickelt worden waren:

– Eine anonymisierte oder pseudonymisierte Datenverarbeitung am Telearbeitsplatz ist nicht möglich.

– Die betroffenen Mitarbeiter können auch nicht anderweitig mit der Verarbeitung weniger sensibler Daten beschäftigt werden.

– Den technisch-organisatorischen Anforderungen wird in besonderem Maße Rechnung getragen.

– Auf der Basis einer Individualvereinbarung werden Zutrittsrechte des behördlichen Datenschutzbeauftragten sowie der Mitarbeiter der Landesbeauftragten für den Datenschutz vertraglich vereinbart, mit der Maßgabe, dass im Falle des Widerrufs oder einer Zutrittsverweigerung die Telearbeit – soweit personenbezogene Daten betroffen sind – mit sofortiger Wirkung beendet ist.

– Der behördliche Datenschutzbeauftragte sowie der Personalrat sind ordnungsgemäß zu beteiligen.

Hinsichtlich der oben genannten Kriterien erklärte der interne Datenschutzbeauftragte der AOK, dass diese in Baden-Württemberg bereits heute weitgehend realisiert sind. Für künftig zu beantragende bzw. einzurichtende Telearbeitsplätze werde man aber noch zusätzliche Regelungen treffen bzw. bestehende weiter präzisieren. Insbesondere soll eine betriebliche Verfahrensanweisung für die datenschutzrechtliche Einzelfallprüfung für jeden beantragten Telearbeitsplatz erstellt werden. Dabei ist u. a. zu prüfen, ob die Zuweisung von Tätigkeiten möglich ist, die keinen Umgang mit schutzwürdigen bzw. besonders schutzwürdigen Daten erfordern, ob die Tätigkeit auch mit anonymisierten bzw. pseudonymisierten Daten ausgeübt werden kann und ob die räumlichen Voraussetzungen so sind, dass Datenschutzrisiken massiv eingeschränkt werden können (insbesondere separat abschließbarer Raum). Nach Abschluss einer solchen Einzelfallprüfung ist deren Ergebnis zu dokumentieren. Ferner wird die Verpflichtungserklärung der Telearbeiter an folgenden Punkten noch erweitert bzw. präzisiert:

– Es wird explizit darauf hingewiesen, dass in den Fällen, in denen während der Arbeit am Teleheimarbeitsplatz ein Dritter den Raum betritt, sofort die Funktion „Computer sperren“ zu aktivieren ist und Papier- und sonstige Unterlagen vor einer möglichen Einsichtnahme durch Unbefugte zu schützen sind.

– Die Kontrollbefugnisse am Telearbeitsplatz werden dahin gehend erweitert, dass auch dem Amt des Landesbeauftragten für den Datenschutz ein solches Kontrollrecht eingeräumt wird, wenn am Telearbeitsplatz personenbezogene Daten verarbeitet werden. Ergänzend wird für solche Telearbeitsplätze der Hinweis aufgenommen, dass bei einer Zutrittsverweigerung gegenüber dem Datenschutzbeauftragten der AOK Baden-Württemberg oder dem Amt des Landesbeauftragten für den Datenschutz die Telearbeit sofort beendet ist.

3. Abschnitt: Soziales

Dass es sich bei der Bezeichnung Hartz IV nicht um die Fortsetzung einer mehr oder weniger beliebten Film- oder Fernsehserie handelt, sondern vielmehr um den Namen einer gesetzgeberischen Arbeitsmarktreform, ist mittlerweile allen klar. Dieses Vierte Gesetz für moderne Dienstleistungen am Arbeitsmarkt bewegt wie selten zuvor ein anderes Gesetzesvorhaben die Gemüter

in der Republik und hat auch den Datenschutz auf den Plan gerufen. Sozusagen im Windschatten jenes Reformgesetzes ist dem Grundrecht auf Datenschutz im Sozialbereich allerdings auch von anderer Seite auf die Pelle gerückt worden.

„Leistungsmissbrauch“ ist häufig das Startsignal für entsprechende Gesetzesmaßnahmen, „automatisierter Datenabgleich“ die als adäquat empfundene Lösung der Probleme. Das neue Zwölfte Buch des Sozialgesetzbuchs (SGB XII) wird das seitherige Bundessozialhilfegesetz ersetzen. Bei der Eingliederung dieses alten Leistungssystems in das umfassende Sozialgesetzbuch wurde die Übertragung der erprobten Datenabgleichsregelung selbstverständlich nicht vergessen. Über diese Vorschrift zur automatisierten Datenerhebung bei anderen öffentlichen Stellen haben wir bereits wiederholt berichtet (19. Tätigkeitsbericht, LT-Drs. 12/3480, S. 13 f.; 20. Tätigkeitsbericht, LT-Drs. 12/4600, S. 63 ff.; 22. Tätigkeitsbericht, LT-Drs. 13/520, S. 76 f.). Selbstredend darf die Bundesagentur für Arbeit im Rahmen der genannten Arbeitsmarktreform von ihr festgestellte Daten in gleicher Weise u. a. mit jenen der Träger der gesetzlichen Unfall- oder Rentenversicherung sowie mit dem Bundesamt für Finanzen abgleichen. Aber auch die Wohngeldstellen sollen nicht länger zurückstehen müssen. Nach einem Gesetzentwurf der Bundesregierung erhalten diese Behörden – über die bereits bestehenden Abgleichsgelegenheiten hinaus – ebenfalls die automatisierte Möglichkeit zur Überprüfung „entscheidungsrelevanter Angaben der Antragsteller“ – genauer des Bezugs von Sozialleistungen anderer Träger, die einen Wohnkostenanteil bezuschussen, und von Einnahmen aus Kapitalvermögen. Aber damit nicht genug: Nach einem Gesetzentwurf des Bundesrats zur Änderung des Sozialgesetzbuchs – Entwurf eines Gesetzes zur Entlastung der Kommunen im sozialen Bereich – soll die Erhebung von Sozialdaten über den Betroffenen bei Dritten erleichtert werden. Datenerhebungen zur Bekämpfung von Leistungsmissbrauch sollen nicht mehr von einem sog. Anfangsverdacht abhängig sein – nach unserer Meinung eine unangemessene Regelung.

Das – bereits verkündete – Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003, welches in Teilen am 1. April 2005 in Kraft treten soll, hält den einen oder anderen überraschenden Kniff bereit. So könnte danach beispielsweise ein Sozialamt mit Hilfe der Finanzbehörde und des Bundesamts für Finanzen sog. Kontostammdaten (also keine Kontostände oder Kontobewegungen) eines Hilfesuchenden in Erfahrung bringen (vgl. auch 4. Teil, 4. Abschnitt, Nr. 1).

Über eine geplante Neuerung mit dem Ziel, einen automatisierten Datenabgleich zu erreichen, können wir uns dagegen nicht beschweren. Vielmehr wurde diese Bestimmung von uns sogar gefordert. In unserem letzten Tätigkeitsbericht berichteten wir über den Datenabgleich der Ämter für Ausbildungsförderung mit dem Bundesamt für Finanzen (LT-Drs. 13/2650, S. 51 f.). Nach unserer Ansicht erfolgte diese Maßnahme, bei der es um die tatsächlich in Anspruch genommenen Freistellungsaufträge und damit um die Zinseinkünfte Auszubildender aus vorhandenem Kapitalvermögen ging, ohne ausreichende rechtliche Grundlage. Diese soll nun mit dem Gesetzentwurf der Bundesregierung zur Änderung des Bundesausbildungsförderungsgesetzes endlich geschaffen werden (s. weiter unten Nr. 2).

Eine Fülle an Berichtenswertem also, was die anschließende Auswahl verdeutlichen wird.

1. Hartz IV

Es gibt kaum ein Thema der jüngsten Zeit, um das mit einer solchen Schärfe gestritten wurde und das mit so vielen Emotionen befrachtet war und ist, wie das Projekt Hartz IV. Was die Bürger beschäftigte und viele sogar auf die Straße trieb, waren zunächst die zu erwartenden Leistungen des Zweiten Buchs des Sozialgesetzbuchs, insbesondere das Arbeitslosengeld II, war möglicherweise die veränderte Zumutbarkeit angebotener Arbeiten, war ganz sicher aber auch – und hier kommt der Datenschutz mit ins Spiel – der Umfang des Erhebungsbogens und die damit verbundene umfassende Datensammlung, die, nebenbei bemerkt, so gar nicht zu den Bestrebungen des von staatlicher Seite immer wieder angekündigten Bürokratieabbaus passen will.

Aber der Reihe nach: Die Kommission „Moderne Dienstleistungen am Arbeitsmarkt“, auch kurz „Hartz-Kommission“ genannt, legte im Jahr 2002 ihr Gesamtkonzept zur Modernisierung der Arbeitsmarktpolitik vor. „Die Schaffung des rechtlichen Rahmens einer neuen Ordnung am Arbeitsmarkt erfolgt in mehreren aufeinander bezogenen Gesetzgebungsverfahren“, heißt es an einer Stelle der Begründung des Gesetzentwurfs. Ein Teil der Vorschläge und Empfehlungen der Kommission floss zunächst ein in das Erste und Zweite Gesetz für moderne Dienstleistungen am Arbeitsmarkt, in Kraft getreten zum 1. Januar 2003. Ziele waren u. a. die Verbesserung der Arbeitsvermittlung und die stärkere Gewichtung des Dienstleistungscharakters der damaligen Bundesanstalt für Arbeit. Diese mehr oder weniger tief greifenden Veränderungen in die dortigen Strukturen wurden mit dem Dritten Gesetz für moderne Dienstleistungen am Arbeitsmarkt vom 23. Dezember 2003 fortgesetzt. Dieses sorgte u. a. für den weiteren „Umbau (der Bundesanstalt) zu einer leistungsfähigen Serviceeinrichtung“, vollzogen mit einer Umbenennung der Anstalt in die „Bundesagentur für Arbeit“ und mit deren Gliederung in eine Zentrale, in Regionaldirektionen sowie in Agenturen für Arbeit auf der örtlichen Verwaltungsebene. Die einschneidendste Veränderung widerfährt dem seitherigen System aber erst durch das Vierte Gesetz für moderne Dienstleistungen am Arbeitsmarkt vom 24. Dezember 2003, welches in einem wesentlichen Teil am 1. Januar 2005 in Kraft tritt. Für den Außenstehenden ist der Kern dieser Reform, die auch die Gründung von sog. Job-Centern als einheitliche Anlaufstelle für alle Arbeitsuchenden vorsieht, die Zusammenführung von Arbeitslosenhilfe und Sozialhilfe für erwerbsfähige Hilfebedürftige. Damit werden alle erwerbsfähigen hilfebedürftigen Empfänger der genannten Transferleistungen in das neue sog. Arbeitslosengeld II einbezogen. Geregelt ist das wiederum im Zweiten Buch des Sozialgesetzbuchs.

Eine solche Zusammenlegung oder doch zumindest eine Harmonisierung der beiden „Fürsorgeleistungen“ wurde in der Vergangenheit mehrfach gefordert. Beide Transferleistungen sind steuerfinanziert, beide sind vom Gesetzgeber bedarfsabhängig ausgestaltet. Beide können sich in der Leistungshöhe dennoch unterscheiden und sind zudem uneinheitlich geregelt, was den Nachweis und die Überprüfung der Bedürftigkeit anbelangt. Hinzu kommt, dass viele Empfänger von Arbeitslosenhilfe ergänzende Hilfen nach dem Bundessozialhilfegesetz beziehen und bezogen haben und somit bei verschiedenen Leistungsträgern vorsprechen müssen. Und natürlich: Ein Datenaustausch zwischen der Arbeitsverwaltung einerseits und den Sozialämtern andererseits war bislang regelmäßig nur nach den Erlaubnisnormen des Sozialgesetzbuchs zulässig.

Erwerbsfähige Hilfebedürftige erhalten nun im neuen Jahr als zentrale Leistung zur Sicherung des Lebensunterhalts das Arbeitslosengeld II, die nicht erwerbsfähigen Mitglieder ihrer Bedarfsgemeinschaft daneben das sog. Sozialgeld; jeder Person, die Leistungen nach diesem Gesetz bezieht, wird einmalig eine eindeutige Kundennummer zugeteilt. Arbeitslosengeld II umfasst auch die angemessenen Kosten für Unterkunft und Heizung. Fallen damit erwerbsfähige Hilfebedürftige demnächst aus dem System der Sozialhilfe heraus, ergeben sich zwangsläufig auch Änderungen im Sozialhilferecht. Auf das neue Zwölfte Buch des Sozialgesetzbuchs haben wir oben bereits hingewiesen. Das Normengeflecht, das die Nachfolge des Bundessozialhilfegesetzes antritt, betrifft nun, vereinfacht ausgedrückt, nicht oder nicht mehr erwerbsfähige Hilfebedürftige. Während hier klar ist, dass das Sozialamt der Ansprechpartner bleibt, stellt sich für die erwerbsfähigen Hilfesuchenden durchaus die Frage, wer ihnen denn nun die benötigte materielle Hilfe gewährt. Vorgesehen war die Zusammenführung der beiden Systeme unter einheitlicher Trägerschaft. Träger der Leistungen der Grundsicherung für Arbeitsuchende ist daher die Bundesagentur, sind aber auch kommunale Träger, das heißt die Stadt- und Landkreise. Letztere haben danach beispielsweise die Schuldner- und Suchtberatung sowie die Leistungen für Unterkunft und Heizung zu übernehmen. Nun könnte ein Sozialhilfeträger, der seither vielleicht im Rahmen seiner Bemühungen um Hilfe zur Arbeit ganz erfolgreich war, auf die Idee kommen, die neuen gesetzlichen Aufgaben an Stelle der Agenturen für Arbeit gänzlich übernehmen zu wollen. Auch diesem Wunsch wurde vom Gesetzgeber, wenn auch in begrenztem Umfang,

entsprochen. Zur Erprobung, wie es heißt, ließ das Bundesministerium für Wirtschaft und Arbeit durch Rechtsverordnung kommunale Träger an Stelle der Agenturen für Arbeit als Leistungsträger zu. Diese Zulassung erfolgt durch Rechtsverordnung, ist bundesweit auf 69 kommunale Träger begrenzt, antragsbedürftig und an die Zustimmung der zuständigen obersten Landesbehörde gebunden. In Baden-Württemberg wurde den Landkreisen Biberach, Tuttlingen, Waldshut sowie dem Bodenseekreis und dem Ortenaukreis diese Stellung eingeräumt.

Damit nicht genug: Zur einheitlichen Wahrnehmung ihrer Aufgaben sollen die genannten Leistungsträger nicht länger nebeneinanderher arbeiten, sondern, sofern keine Zulassung kommunaler Träger vorliegt, Arbeitsgemeinschaften bilden, die wiederum an die Stelle der Agentur für Arbeit rücken. Auch solche Organisationseinheiten wird es in Baden-Württemberg geben. Womöglich wird sich aber ein weiteres Modell ausbreiten, wonach die Träger zwar miteinander kooperieren, zu diesem Zweck aber (noch) nicht die gesetzliche vorgesehene Arbeitsgemeinschaft aufbauen, sondern ihre Zusammenarbeit allein auf vertragliche Füße stellen. Gerade in diesen Fällen ist zu beachten, dass der Bürger stets wissen muss, mit welcher Stelle er es eigentlich zu tun hat. Es ist also vorab zu klären, wie und in welcher Form die an der Zusammenarbeit beteiligten Träger den Hilfesuchenden gegenübertreten bzw. für welche Stelle die Mitarbeiter der Träger handeln und Verwaltungsakte erlassen sollen. Auf jeden Fall zu bestimmen ist daher die für die Datenverarbeitung verantwortliche Stelle. Gegen sie richten sich nämlich u. a. die datenschutzrechtlichen Ansprüche wie der Auskunftsanspruch des Betroffenen sowie dessen Ansprüche auf Berichtigung, Löschung und Sperrung von Daten. Ist zudem die Weitergabe von personenbezogenen Informationen an den jeweiligen Kooperationspartner vorgesehen, sind für derartige Datenübermittlungen die entsprechenden Befugnisnormen zu berücksichtigen.

Aber nicht nur die unterschiedliche Erscheinungsform des zuständigen Leistungsträgers kann zur Verwirrung des Bürgers beitragen, auch die Art und Weise des Vorgehens bei der Datenerhebung sorgte für reichlich Gesprächsstoff. Nach ihrem gesetzlichen Auftrag sollten die Träger ab 1. Oktober 2004 bei den in Betracht kommenden erwerbsfähigen Hilfebedürftigen und den mit ihnen in einer Bedarfsgemeinschaft lebenden Personen die zur Gewährung der Leistung zur Sicherung des Lebensunterhalts erforderlichen Angaben feststellen. Ab diesem Zeitpunkt bestand somit eine entsprechende Obliegenheit zur Mitwirkung der Antragsteller. Tatsächlich durften diese Daten, wenn auch nur auf freiwilliger Basis, bereits ab 1. August 2004 erhoben werden. Zu diesem Zweck verteilte die Bundesagentur kurz zuvor Erhebungsvordrucke, die dann zum Stein des öffentlichen Anstoßes wurden. Offensichtlich ging die Bundesagentur davon aus, dass die Leistungsempfänger zufrieden sein werden, wenn sie ab 1. Januar 2005 das Arbeitslosengeld II erhalten und deshalb den Inhalt des umfassenden Vordrucks nicht weiter hinterfragen. Das Gegenteil war der Fall: Es hagelte Kritik von allen Seiten. Dabei hätte sich die Arbeitsverwaltung viel Ärger ersparen können, hätte sie die Datenschutzbeauftragten des Bundes und der Länder vor der Ausgabe des Vordrucks angemessen an der Erstellung der Unterlage beteiligt. So sollten mit dem Grundbogen allgemeine Daten des Antragstellers, dessen persönliche Verhältnisse, die Verhältnisse der mit ihm in einem Haushalt lebenden weiteren Personen sowie Einkommen und Vermögen der genannten Personen festgestellt, mit weiteren Zusatzblättern die angemessenen Kosten für Unterkunft und Heizung, weitere Angehörige, ausführliche Angaben zu Einkommen und Vermögen bezeichnet und zusätzlich Bescheinigungen des Arbeitgebers zum Arbeitsentgelt vorgelegt werden. In den folgenden Monaten rangen die Datenschützer heftig mit der Bundesagentur für Arbeit um die datenschutzgerechte Gestaltung des Erhebungsvordrucks. Unsere Fragen, Kritikpunkte und Änderungswünsche reichten von der Angabe von Telefonnummer und E-Mail-Adresse des Antragstellers, von Daten des Vermieters, der Verwendung eines Mutterpasses, der Notwendigkeit zur Vorlage von Bescheinigungen durch die Arbeitgeber für Antragsteller und Angehörige bis hin zur umfassenden Feststellung von Informationen über Haushaltsangehörige. Nicht in allen Punkten waren allerdings die Bemühungen von Erfolg gekrönt. So besteht die Bun-

desagentur weiter darauf, dass für die Vorlage einer Bescheinigung, mit der der Arbeitgeber Art und Dauer der Erwerbstätigkeit sowie die Höhe des Arbeitsentgelts bestätigt, der gesetzlich legitimierte Vordruck verwendet wird. Inzwischen handelt es sich dabei immerhin aber um ein isoliertes Zusatzblatt, ohne umseitige Angaben, welches nun auch seine Druckkennung („BA“) verlieren soll und dann nicht mehr zuordenbar wäre. Fragen, die sich an die Kernfamilie, die sog. Bedarfsgemeinschaft richten, dürfen nun nicht mehr auf andere Haushaltsangehörige bezogen werden. Leider aber können Änderungen am Vordruck selbst erst bei dessen anstehender Neuauflage berücksichtigt werden. Bis dahin müssen sich alle Beteiligten mit einer Ausfüllhilfe behelfen, die seit Wochen erhältlich ist *(www.arbeitsagentur.de)* und die auch datenschutzrechtliche Fragen behandelt. Diese Hilfestellung zum Antragsvordruck wurde auf Wunsch und mit Unterstützung der Datenschutzbeauftragten durch die Bundesagentur erarbeitet; sie dient nicht nur der Information der Antragsteller, sondern ist auch eine Hilfe für die Mitarbeiter der Leistungsträger. Insgesamt ist sicherzustellen, dass „Überschussinformationen“, die aus vorherigen Anträgen resultieren, gelöscht werden.

Konnte diese Klippe durch nachträgliches Manövrieren somit gerade noch umschifft werden, so droht dem Grundrecht auf Datenschutz schon die nächste Havarie: Zur Berechnung der auszuzahlenden Geldleistung setzt die Bundesagentur ein Datenbanksystem (A2LL) ein. Schon früh wurde deutlich, dass dieses System über keine sog. Zugriffsberechtigungsverwaltung verfügt, d. h. Zugriffsbeschränkungen auf einzelne Verantwortungsbereiche konnten noch nicht realisiert werden. Wird den Kommunen, die bislang nicht mit der Arbeitsverwaltung elektronisch verzahnt waren, nun im Rahmen einer Kooperation auch die Mitnutzung dieser Leistungsberechnungs-Software, welche durch die Bundesagentur betrieben und bereitgestellt wird, gestattet, so könnten auch die Kommunen plötzlich in den Genuss eines bundesweiten Zugriffs auf Daten derjenigen Hilfesuchenden kommen, die von dem Verfahren erfasst sind. Dass diese Überlegung tatsächlich zutraf, davon konnten wir uns anlässlich eines Besuchs bei einem Sozialamt überzeugen. Dieser Leistungsträger, der gemeinsam mit der Bundesagentur eine Arbeitsgemeinschaft errichten und damit seine Kompetenzen in eine gemeinsame, noch zu bildende öffentliche Stelle einbringen wird, nutzte bereits die genannte Software. Dankenswerterweise gewährte uns die Behörde kurzfristig einen Einblick. Die Nutzer des Verfahrens konnten nicht nur auf die vom Sozialamt erfassten Daten der Antragsteller auf Arbeitslosengeld II und weiterer in den Anträgen genannter Personen zugreifen, sondern vielmehr bundesweit auf alle mit dem Verfahren erfassten Personen. Zu einer Suche genügte dabei bereits die Eingabe der ersten drei Buchstaben des Nachnamens sowie eines weiteren Kriteriums (z. B. Wohnort: „Berlin“). Die Zugriffsmöglichkeiten umfassten dabei nicht nur die Stammdaten der Antragsteller, sondern sämtliche zur Bearbeitung automatisiert erfassten personenbezogenen Informationen, die sich auch auf andere Personen, beispielsweise Familienangehörige des Antragstellers, beziehen können. So wäre es etwa möglich gewesen, auf die medizinischen Ursachen zuzugreifen, die Anlass für einen bewilligten Mehrbedarf etwa infolge kostenaufwändiger Ernährung waren. Hinzu kam, dass neben dem lesenden offenbar sogar ein schreibender Zugriff möglich war.

Die Bereitstellung dienstlich nicht erforderlicher Zugriffsmöglichkeiten stellt einen erheblichen datenschutzrechtlichen Mangel dar. Bei dem Besuch konnten wir nämlich keine Gründe feststellen, die einen derartig umfassenden Zugriff auf andernorts erfasste und bearbeitete Leistungsfälle rechtfertigen würden. Dabei fällt neben dem besonderen Schutzbedarf der Sozialdaten der Betroffenen vor allem ins Gewicht, dass mit dem Verfahren A2LL möglicherweise die Daten Millionen Betroffener verarbeitet werden, das Sozialamt hiervon jedoch den weit überwiegenden Teil dieser Informationen für seine Aufgaben nicht benötigt. Wir halten es daher für dringend geboten, dass die Zugriffsmöglichkeiten auf das dienstlich notwendige Maß beschränkt werden und haben dies auch den beteiligten Stellen mitgeteilt. Hiervon nicht direkt betroffen sind die im Land als Leistungsträger eigens zugelassenen Landkreise, die offensichtlich nicht mit dieser Software versorgt werden sollen. Tatsächlich haben drei Landkreise, die ab 1. Januar 2005 insoweit die Rechte und Pflichten der Agentur für Arbeit übernehmen,

mitgeteilt, dass sie sich für die automatisierte Datenverarbeitung anderer spezieller Verfahren bedienen werden. Derzeit ein glücklicher Umstand, könnte man meinen.

Die bundesweite Brisanz dieses Themas spiegelt sich auch in einer von den Datenschutzbeauftragten des Bundes und der Länder gefassten Entschließung, die insgesamt erhebliche Datenschutzmängel bei der Umsetzung des Gesetzeswerks aufzeigt (s. Anhang 4). Mit der Entschließung wird die Bundesagentur aufgefordert, die notwendigen Schritte zur Beseitigung der datenschutzrechtlichen Mängel des Verfahrens A2LL unverzüglich einzuleiten. Aber damit nicht genug: Inzwischen hat der Bundesbeauftragte für den Datenschutz die seinen Forderungen zum Trotz unveränderte Verwendung der Software A2LL gegenüber dem Vorstand der Bundesagentur für Arbeit förmlich beanstandet.

2. Verarbeitung von BAföG-Daten im Auftrag durch das ZfI

In unserem letzten Tätigkeitsbericht hatten wir berichtet, dass das Zentrum für Informationstechnik bei der Oberfinanzdirektion Stuttgart (ZfI) unter anderem die Daten der Empfänger von Leistungen nach dem Bundesausbildungsförderungsgesetz im Auftrag der BAföG-Ämter verarbeitet. Wir hatten damals bemängelt, dass diese Datenverarbeitung noch immer ohne das vom Gesetzgeber in einem solchen Fall geforderte schriftliche Auftragsverhältnis erfolgt. Die Schriftlichkeit der Auftragserteilung hat sehr wohl ihren Sinn und ist keine bloße Förmlichkeit, denn in diesem Vertrag sind auch die getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit festzustellen und zu bezeichnen, und erst durch die schriftliche Festschreibung dieser Anforderungen wird die Datenverarbeitung auf eine verlässliche und jederzeit nachvollziehbare Grundlage gestellt.

Wir schlossen unseren damaligen Bericht in der Hoffnung, dass die BAföG-Ämter die Aufträge über die Verarbeitung „ihrer“ Daten durch das ZfI bald erteilen würden. Mut machte uns dabei die Tatsache, dass sich das von uns in diesem Zusammenhang ebenfalls kritisierte Wissenschaftsministerium nun mächtig ins Zeug legte. Die Behörde sagte sogar zu, dass ein neuerlicher vom Bundesforschungsministerium geforderter Datenabgleich erst dann durchgeführt werde, wenn, ja wenn die „Vereinbarungen über die Auftragsdatenverarbeitung zwischen den Ausbildungsämtern und dem ZfI unterschrieben vorliegen“. Eine kühne Aussage fürwahr, die sich in der Folgezeit jedoch als schwere Hypothek erweisen sollte. Dabei erschien doch alles sehr einfach: Das Ministerium empfahl, in der angestrebten Vereinbarung schlicht auf die beim ZfI vorliegenden Beschreibungen zur Datensicherheit zu verweisen. Schließlich, so das Ministerium, führe das ZfI „für die Landesverwaltung eine erhebliche Anzahl von Verfahren im Auftrag durch“ und müsste daher doch „entsprechend ausreichende Beschreibungen zur Datensicherheit“ vorhalten. Dieser Erwartung kann man eigentlich nur zustimmen. Doch leider gab es diese Dokumente, auf die man ohne weiteres hätte verweisen können, gar nicht. Nahezu am gleichen Tag ging uns nämlich ein Vereinbarungsentwurf des ZfI zu. Dieser Entwurf bezog sich auf mehrere Konzepte, die erst noch zu erstellen waren oder deren Erstellung erst noch abzuschließen war. Der mehrfache Hinweis auf noch zu erarbeitende Unterlagen machte deutlich, dass zu diesem Zeitpunkt selbst aus der Sicht des ZfI dort gerade keine geeigneten Dokumentationen vorlagen. Das ZfI ließ uns nun wissen, dass auch nach dortiger Auffassung ein derartiger Verweis nur berechtigt ist, wenn solche Konzepte auch in Schriftform vorliegen und präsentierte zu deren Erstellung einen Zeitplan. Die Fertigstellung der erforderlichen Dokumentationen war darin in drei Schritten mit dem 31. Oktober 2004 als Endtermin vorgesehen. Um es deutlich zu machen: Es handelt sich hierbei keineswegs um überzogene Forderungen des Datenschutzes, sondern die schriftliche Fixierung der zu treffenden und tatsächlich vorgenommenen Maßnahmen zur Datensicherheit sollte zum Standardrepertoire eines Auftragsdatenverarbeiters gehören.

Der Rest der Geschichte ist schnell erzählt: Das Ministerium ließ den vom Bund verlangten Datenabgleich durchführen, das in Aussicht gestellte Sicherheitskonzept, verstanden als Beschreibung der zur Wahrung des Da-

tenschutzes erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen, liegt noch immer nicht vor und der gesetzlich geforderte schriftliche Auftrag wurde demzufolge auch noch nicht erteilt. Auf diesen Mangel haben wir zum wiederholten Mal hingewiesen. Nun bleibt zu hoffen, dass die Angelegenheit demnächst doch ein datenschutzgerechtes Ende findet.

3. Begleitende Untersuchung zur Einführung und Umsetzung des Gesetzes über eine bedarfsorientierte Grundsicherung im Alter und bei Erwerbslosigkeit

Wissenschaftliche Begleituntersuchungen zu den Auswirkungen von Leistungsgesetzen im Sozialbereich können eine ganz eigene Gefahr für das informationelle Selbstbestimmungsrecht der betroffenen Leistungsempfänger begründen; diese Erfahrung musste unsere Dienststelle schon einmal machen. Hierüber hatten wir ausführlich in unserem 24. Tätigkeitsbericht (LT-Drs. 13/2650, S. 55 f.) berichtet. Damals mussten wir feststellen, dass ein Sozialhilfeträger ohne ausreichenden Rechtsgrund Daten einer großen Anzahl von Hilfeempfängern an das mit der Begleitforschung beauftragte Institut weitergegeben hatte. Dass sich Geschichte wiederholen kann, lehrte uns die Beschäftigung mit einem weiteren Untersuchungsprojekt.

Schon im Jahr 2002 erreichte den Bundesbeauftragten für den Datenschutz ein Schreiben des Bundesministeriums für Arbeit und Sozialordnung, welches an die Landesbeauftragten weitergegeben wurde. Darin warb das Ministerium um „Unterstützung für ein sozialpolitisch außerordentlich wichtiges Forschungsvorhaben“. Gegenstand sollte das Gesetz über eine bedarfsorientierte Grundsicherung im Alter und bei Erwerbsminderung (GSiG) sein. Das Gesetz trat zum 1. Januar 2003 in Kraft. Es schuf bundesweit ein neues Sozialleistungssystem zur Sicherung des Lebensunterhalts für über 65-Jährige sowie für über 18-Jährige mit voller Erwerbsminderung. Ein wesentliches Ziel der Gesetzgebung war somit der Abbau und die Verhinderung einer sog. „verschämten Armut“, deren Ursache in den Zugangsschwellen für den Erhalt von Sozialhilfeleistungen gesehen wurde. Im Rahmen des Forschungsvorhabens sollten u. a. Fragen des Zugangs zu diesem neuen Leistungssystem, der Häufigkeit der Inanspruchnahme, der Geeignetheit des Systems zur Zielerreichung sowie der Akzeptanz einzelner Regelungsbereiche bei den Bürgern untersucht werden. Beauftragt mit der so umrissenen wissenschaftlichen Begleitung des Grundsicherungsrechts wurde das Institut für angewandte Sozialwissenschaft GmbH (infas). Infas sollte zu diesem Zweck Leistungsbezieher gezielt telefonisch befragen. Für diese Vorgehensweise benötigte das Institut jedoch Sozialdaten der potenziellen Gesprächspartner.

Im Jahr 2003 erteilte das Sozialministerium fünf Landkreisen und einem Stadtkreis die Genehmigung zur Übermittlung personenbezogener Daten (Name, Anschrift, Telefonnummer, Geschlecht sowie Alter) von jeweils 270 Grundsicherungsberechtigten. Die Genehmigung wurde u. a. mit dem Hinweis verknüpft, dass die mitwirkende Behörde die Betroffenen zunächst über die beabsichtigte Übermittlung, den Zweck des Forschungsvorhabens sowie ein Widerspruchsrecht schriftlich zu unterrichten habe. Mit diesem Hinweis hatte das Sozialministerium einer entsprechenden Forderung des Landesbeauftragten für den Datenschutz Rechnung getragen. Ende des Jahres 2003 wandten wir uns an die Leistungsträger mit der Bitte, über die Mitwirkung an der Untersuchung zu berichten. Ein Kontakt mit infas ergab, dass bis zu diesem Zeitpunkt vier der Träger die gewünschten Informationen an den wissenschaftlichen Begleiter weitergegeben hatten. Leider stellte sich heraus, dass zwei Kreise die genannte Auflage nicht beachtet und Sozialdaten somit in großem Umfang ohne Berücksichtigung der geschilderten „Widerspruchslösung“ weitergegeben hatten. Während eine Behörde dieses Versäumnis einräumte, war dies bei der anderen zunächst nicht der Fall. Erst auf nochmaliges Nachfassen gestand das Sozialamt die Nichtbeachtung des Verfahrens ein und ging dabei anscheinend davon aus, den Datenschutzverstoß durch eine Abrede mit infas über die Verwendung der übermittelten Daten sowie durch eine Nachholung des Verfahrens beseitigen zu können.

Wir sahen zwar von einer Beanstandung der Verstöße ab, baten das Sozialministerium aber um Wahrnehmung seiner Kontrollpflichten hinsichtlich des Ablaufs solcher von ihm genehmigter wissenschaftlicher Untersuchungen.

4. Datenerhebung durch das Studentenwerk bei Dritten

Darf das Amt für Ausbildungsförderung das Einkommen des Vaters einer Studentin beim Finanzamt erfragen, wenn der Vater sich weigert, die entsprechenden Auskünfte zu geben? Eher ja, möchte man zögerlich antworten, denn sicher ist man sich da nicht. Vor allem, wenn der Vater durch seine anwaltlichen Vertreter auch noch vortragen lässt, seine Tochter sei zwischenzeitlich verheiratet gewesen und somit sei doch wohl der frühere Ehegatte vorrangig zum Unterhalt verpflichtet und er (der Vater) prozessiere derzeit mit seiner Tochter über Grund und Höhe eines solchen Unterhaltsanspruchs und gebe schon deshalb bis zum Abschluss des gerichtlichen Verfahrens keine Erklärungen ab. Im Ergebnis mussten wir aber doch die Befugnis für eine derartige Nachfrage und die Zulässigkeit entsprechender Auskünfte durch die Finanzbehörde bejahen.

Die Ausbildungsförderung wird nach den Vorschriften des Bundesausbildungsförderungsgesetzes (BAföG) für den Lebensunterhalt und die Ausbildung geleistet. Auf den Bedarf des Leistungsempfängers sind jedoch dessen Einkommen und Vermögen sowie das Einkommen des nicht dauernd getrennt lebenden Ehegatten und schließlich das Einkommen seiner Eltern in eben dieser Reihenfolge anzurechnen. Im vorliegenden Fall schied somit ein Rückgriff auf den Ex-Ehemann, der zudem leistungsunfähig war, bereits von vornherein aus. Da die gesetzlichen Ausnahmegründe, nach denen auch das Einkommen der Eltern außer Betracht bleiben kann (z. B. wenn die Auszubildende bei Beginn des Ausbildungsabschnitts bereits das 30. Lebensjahr vollendet hat), nicht vorlagen, konnte die Leistung nur elternabhängig gewährt werden. Die Eltern sind dann aber auch gehalten, bei der Ermittlung ihrer Einkommensverhältnisse mitzuwirken. Sie trifft somit per Gesetz eine verfahrensrechtliche Obliegenheit, ihr Einkommen gegenüber dem Amt für Ausbildungsförderung zu offenbaren. Gleichzeitig wird dem Leistungsträger vom Gesetz die Befugnis eingeräumt, dem Nachweispflichtigen eine angemessene Frist zur Mitwirkung zu setzen.

Die Ämter für Ausbildungsförderung (in unserem Fall ein Studentenwerk) können sich ausnahmsweise die notwendigen Informationen auch bei anderen Stellen als beim Nachweispflichtigen selbst beschaffen. Dies ist ihnen selbstverständlich dann erlaubt, wenn eine Rechtsvorschrift eine derartige Vorgehensweise ausdrücklich gestattet. Eine solche Bestimmung, die eine solche Dritt- oder Fremderhebung, also eine Feststellung von Umständen nicht beim Betroffenen selbst, zulässt, ist § 21 Abs. 4 des Zehnten Buchs des Sozialgesetzbuchs (SGB X). Danach haben die Finanzbehörden dem Sozialleistungsträger u. a. Auskunft über die ihnen bekannten Einkommens- und Vermögensverhältnisse des (potenziell) Unterhaltsverpflichteten zu erteilen; dies gilt allerdings nur insoweit, als eine solche Auskunft in dem Verwaltungsverfahren nach dem Bundesausbildungsförderungsgesetz auch erforderlich ist. Nach dem bürgerlich-rechtlichen Unterhaltsrecht sind die Eltern unter bestimmten Voraussetzungen grundsätzlich auch zur Finanzierung einer Berufsausbildung des Kindes verpflichtet. Das Studentenwerk ging mit guten Gründen von einer bestehenden Unterhaltsverpflichtung aus, da es sich bei dem Studium der Tochter um eine „erste angemessene Ausbildung“ handele. Nach der Äußerung des Vaters, keinerlei Erklärungen in dieser Sache abzugeben, mit anderen Worten, jegliche verfahrensrechtliche Mitwirkung gegenüber dem Studentenwerk zu verweigern, durfte sich das Amt für Ausbildungsförderung demzufolge an das zuständige Finanzamt wenden und die Finanzbehörde durfte diesem Ersuchen auch nachkommen. Dass sich die Beteiligten gleichzeitig vor Gericht stritten, stand der behördlichen Informationsbeschaffung auf dem (Um-)Weg über die Finanzverwaltung nicht entgegen.

5. Aus der Praxis verschiedener Sozialämter

5.1 Intimes zur Feststellung einer nichtehelichen Lebensgemeinschaft

Hilfe zum Lebensunterhalt ist nach dem Bundessozialhilfegesetz (BSHG) nur dem zu gewähren, der seinen notwendigen Lebensunterhalt nicht oder nicht ausreichend aus eigenen Kräften oder Mitteln, vor allem aus seinem Einkommen und Vermögen, bestreiten kann. Zudem ist das Sozialamt gehalten, bei nicht getrennt lebenden Ehegatten im Rahmen der Bedarfsprüfung Einkommen und Vermögen beider Ehegatten zu berücksichtigen.

Wie aber sieht es bei der sog. eheähnlichen Gemeinschaft zwischen Mann und Frau aus? § 122 BSHG will eine annähernde Gleichstellung beider Lebensformen erreichen; dort ist geregelt, dass die Personen, die in eheähnlicher Gemeinschaft leben, sowohl hinsichtlich der Voraussetzungen als auch hinsichtlich des Umfangs der Sozialhilfe nicht besser gestellt werden dürfen als Ehegatten. Im Klartext heißt das: In einer eheähnlichen Gemeinschaft sind Einkommen und Vermögen des Partners zu berücksichtigen. Die Hilfe zum Lebensunterhalt ist somit dann zu versagen, wenn das Einkommen (und/oder Vermögen) des einen Partners geeignet ist, die Bedürftigkeit des anderen zu beseitigen. Die Bestimmung soll vor allem verhindern, dass sich Partner einer eheähnlichen Gemeinschaft sozialhilferechtliche Vorteile verschaffen. Damit ist klar, dass sich die Sozialämter um Aufklärung zu bemühen haben, ob eine solche Gemeinschaft vorliegt. Mehr noch: Sie sind für das Vorliegen einer solchen sogar nachweispflichtig, was gleichzeitig die Pflicht zu weiteren Nachforschungen auslöst. Ergeben sich aus den Angaben eines Antragstellers offenkundige Hinweise auf eine gemeinsame Haushaltsführung, so ist damit an einer entsprechenden Datenerhebungsbefugnis der Sozialbehörden nicht zu rütteln. Die kritische Frage ist allerdings, wodurch sich eine solche eheähnliche Gemeinschaft auszeichnet und wie das Sozialamt zweifelsfrei feststellen kann, ob sie vorliegt, sofern diese nicht zu Beginn des Verfahrens von Seiten der Betroffenen eingeräumt wird. Nach der Rechtsprechung des Bundesverfassungsgerichts muss es sich hierbei um eine Lebensgemeinschaft zwischen einem Mann und einer Frau handeln, die auf Dauer angelegt ist, daneben keine Lebensgemeinschaft gleicher Art zulässt und sich durch innere Bindungen auszeichnet, die ein gegenseitiges Einstehen der Partner füreinander begründen. Die reine Haushalts- oder Wirtschaftsgemeinschaft reicht somit nicht aus, vielmehr muss das Gefühl gegenseitiger Verantwortung so weit gehen, dass die Partner zunächst den gemeinsamen Lebensunterhalt sicherstellen, bevor sie ihre Mittel zur Befriedigung eigener Bedürfnisse einsetzen. Ob dies der Fall ist, kann die Behörde regelmäßig nur anhand von Indizien feststellen. Sie ist dabei auf äußere objektive Merkmale angewiesen, hat damit aber auch, so ihr Dilemma, subjektive Elemente nachzuweisen.

Zuweilen verwenden Sozialämter hierfür einen Vordruck, der beispielsweise Fragen zur gemeinsamen Nutzung von Wohnraum enthält, denn wichtigstes Kriterium ist eine tatsächliche Wohngemeinschaft; gefragt wird aber auch nach der gemeinsamen Zubereitung von Mahlzeiten und weiteren Gemeinsamkeiten bei hauswirtschaftlichen Verrichtungen, nach einer etwaigen gemeinsamen Kontoführung, nach gemeinsamer Nutzung eines Pkw, gemeinsamen Kindern, aber auch nach gemeinsamen Urlauben, gemeinsamer Freizeitgestaltung und etwaiger wechselseitiger Unterstützung bei der Tilgung eines Kredits. Diese Kriterien sind je für sich genommen zwar noch kein Nachweis für das Vorliegen einer eheähnlichen Gemeinschaft; gleichwohl haben wir insoweit eine Obliegenheit zur Mitwirkung der Betroffenen, also zur Beantwortung dieser Fragen bejaht, wollen die Antragsteller nicht Gefahr laufen, ihren Anspruch zu verlieren. Das mussten wir auch einer Bürgerin mitteilen, die die Beantwortung ablehnte. In einem Punkt ging der vorgelegte Fragebogen aber doch zu weit. Die Behörde wollte nämlich wissen, ob die Frau intime Beziehungen unterhielt.

Damit hat der Leistungsträger eindeutig über das Ziel hinausgeschossen. Zwar haben die Gerichte keinen Zweifel daran gelassen, dass intime Beziehungen zwischen den Partnern ein gewichtiges Indiz für das Vorliegen einer eheähnlichen Gemeinschaft sein können, aber das Bundesverwaltungsgericht hat dies auf die Fallgestaltung beschränkt, dass solche Beziehungen „bekannt“ sind. Gleiches gilt, sollten diese Beziehungen offenkundig sein. Das Gericht hat zudem deutlich gemacht, „dass behördliche Nachforschungen in der Intimsphäre der Partner unzulässig sind.“ Das muss nach unserem Dafürhalten auch für Fragen nach solchen Beziehungen gelten, wenn von deren Beantwortung die Weiterbearbeitung des Antrags abhängig gemacht wird. Hier endet die verfahrensrechtliche Mitwirkungspflicht.

Noch deutlicher wurde der vergleichbare Fragebogen eines anderen Landratsamts, der uns im Rahmen eines Kontrollbesuchs in die Hände fiel. Darin fand sich die Frage: „Bestehen intime Beziehungen mit einer der ... genannten Personen? Falls ja, mit welcher dieser Personen?“ Der Vordruck schloss mit den Hinweisen, dass falsche Angaben zu einer Strafanzeige wegen Betrugs führen werden und dass der Antragsteller darüber belehrt wurde, dass seine Angaben erforderlichenfalls auch durch persönlichen Augenschein überprüft werden können. Die Einvernahme durch Augenschein ist zwar ein Beweismittel, auf welches die Behörde verfahrensrechtlich grundsätzlich zurückgreifen darf; in dem dargestellten Zusammenhang ist ein solcher Hinweis aber völlig fehl am Platz. Zudem hielten wir es für angezeigt, das Landratsamt darauf hinzuweisen, dass die Wohnungen der Antragsteller nach wie vor nur mit deren Zustimmung betreten werden dürfen.

5.2 Pauschale Ermächtigung zur Einholung einer Bankauskunft

Die sog. Bankvollmacht, genauer die von Sozialbehörden den Hilfesuchenden abverlangte Ermächtigung zur Einholung von Bankauskünften, ist ein stets wiederkehrendes datenschutzrechtliches Thema. Bereits im Jahr 1999 hat sich unsere Dienststelle in ihrem 20. Tätigkeitsbericht mit jener verbreiteten Praxis der Sozialämter befasst und die Anforderungen an eine wirksame Einwilligung der Betroffenen näher beschrieben. Damals kamen wir zu dem Ergebnis, dass die meisten der abgegebenen Erklärungen unwirksam sind, weil sie den Anforderungen an eine wirksame Einwilligungserklärung gerade nicht Rechnung getragen hatten. Zwar trifft den Antragsteller die grundsätzliche Obliegenheit, auf Verlangen des Leistungsträgers auch der Erteilung erforderlicher Auskünfte durch Dritte zuzustimmen. Diese Zustimmung darf jedoch keine Blanko-Vollmacht beinhalten; sie muss vielmehr den gesetzlichen Voraussetzungen an eine wirksame datenschutzrechtliche Einwilligung genügen. Zu unbestimmt ist diese beispielsweise, wenn die Bank oder Sparkasse, die zur Auskunftserteilung an die Behörde ermächtigt werden soll, dem Einwilligenden gegenüber nicht benannt wird.

Nachdem wir auch in den folgenden Jahren immer wieder rechtlich fehlerhafte Einwilligungserklärungen kritisiert haben (21. Tätigkeitsbericht, LT-Drs. 12/5740, S. 42 f.; 23. Tätigkeitsbericht, LT-Drs. 13/1500, S. 42 ff.), sind wir nun erneut auf einen erwähnenswerten Fall gestoßen:

Ein städtisches Amt für Grundsicherung forderte im Jahr 2003 von den Hilfesuchenden bei der Antragstellung sowohl die Vorlage von Kontoauszügen als auch die Abgabe einer Ermächtigungserklärung zur Einholung einer Bankauskunft. Die hierzu erforderliche Einwilligungserklärung befand sich in einem Vordruck „Befreiung vom Bankgeheimnis und Ermächtigung zur Auskunft“. Die Petentin wurde aufgefordert, diese Erklärung zu unterschreiben, jedoch auf dem Vordruck keinesfalls weitere Eintragungen vorzunehmen. Nach den Einlassungen der Stadt trug diese nachträglich das entsprechende Kreditinstitut ein, dann wurde die „Bankanfrage ... in der Regel an die vom Antragsteller angegebene Bank versandt.“ Wir rügten diese Vorgehensweise und baten darum, den Antragstellern eine Einwilligung erst abzuverlangen, wenn die gleichfalls vorgelegten Kontoauszüge zum Nachweis nicht aus-

reichen. Zudem macht diese Art der Blanko-Ermächtigung die erklärte Einwilligung unwirksam. Grundsätzliche Voraussetzung für eine wirksame Einwilligungserklärung ist, dass der Einwilligende weiß, worauf er sich mit seiner Erklärung einlässt. Das ist hier gerade nicht der Fall. Hinzu kommt, dass eine solche Erklärung einzelfallbezogen und inhaltlich bestimmt sein muss. Blanko-Einwilligungen oder Pauschalermächtigungen sind somit rechtlich ausgeschlossen. Naturgemäß kann dann auch keine Verpflichtung bestehen, eine entsprechende Erklärung zu unterzeichnen.

Die Stadt versprach, künftig eine Ermächtigung zur Einholung einer Bankauskunft nur noch in begründeten Einzelfällen zu verlangen und dabei Bankanfragen vorzulegen, auf denen die anzufragenden Bankinstitute namentlich aufgeführt sind. „An andere Geldinstitute werden wir Anfragen nicht richten." Deutliche Worte, die das Thema eigentlich im Sinne des Datenschutzes und im Interesse der betroffenen Bürger abgeschlossen haben sollten.

Kurz darauf – ebenfalls noch im Jahr 2003 – erreichte uns eine Eingabe, mit der ein Bürger, der bei derselben Stadt Leistungen der Sozialhilfe beantragte, den gleichen Sachverhalt vortrug. Der Vorgang bedurfte überraschenderweise nochmals einer eingehenden rechtlichen Betreuung. Die Stadt berief sich zwar auf das Vorliegen eines begründeten Einzelfalles – dass sie sich mit ihrem Verlangen der Abgabe einer solchen Pauschalermächtigung in Widerspruch zu der uns seinerzeit gegebenen Zusage gesetzt hatte, thematisierte sie jedoch nicht. Im Gegenteil: Der Vertreter der Kommune führte unverdrossen aus, dass die Vorlage eines Blanko-Vordrucks zur Unterschrift durch den Antragsteller datenschutzrechtlich unbedenklich sei. Keinesfalls sei beabsichtigt gewesen, diese Bankanfrage breit gestreut zu versenden. Diese Rechtsposition war bereits angesichts der geschilderten Vorgeschichte unverständlich. Der Vertreter der Stadt, der nach wie vor an dieser Meinung festhält, betont nun die datenschutzrechtliche „Unschädlichkeit" dieser Maßnahme, hat inzwischen aber wenigstens versprochen, solche Erklärungen nicht mehr zu verlangen.

5.3 Übermittlung von Sozialdaten an das Bundesamt für die Anerkennung ausländischer Flüchtlinge

Die Landkreise müssen – wie andere öffentliche Stellen auch – beständig darum bemüht sein, ihre Ausgaben nach Möglichkeit zu begrenzen; das gilt auch für die Kosten der Sozialhilfe. Vor diesem Hintergrund ist es verständlich, dass ein Landratsamt folgenden Sachverhalt mit der Bitte um datenschutzrechtliche Bewertung an uns herantrug:

Der Landkreis leiste in nicht unerheblichem Umfang Sozialhilfe auch an Asylberechtigte. In diesem Kreis der Leistungsempfänger befänden sich auch Personen, in deren Herkunftsländern sich zwischenzeitlich die politischen Verhältnisse geändert hätten. Möglicherweise seien damit auch die Gründe, die zur Anerkennung als Asylberechtigte geführt hätten, weggefallen. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge könne die Anerkennung in diesen Fällen widerrufen und das zuständige Ausländeramt dann den Aufenthalt wegen des Bezugs von Sozialhilfeleistungen beenden. Die Behörde fragte, ob sie zum Zweck, „das Bundesamt um eine Überprüfung des Asylstatus zu bitten", dieses oder das Ausländeramt über jene Bleibeberechtigten und deren Sozialhilfebezug unterrichten dürfe. Dabei hatte die Behörde bereits erkannt, dass die Bestimmungen des Sozialdatenschutzes eine solche Datenübermittlung kaum zulassen würden. Sie sollte Recht behalten.

Die Regelungen sehen zwar spezielle Übermittlungsbefugnisse der Sozialleistungsträger gerade an die Ausländerbehörden vor. Voraussetzung für eine Übermittlung ist jedoch entweder ein entsprechendes Ersuchen der Ausländerverwaltung, welches nicht vorlag, oder eine gesetzliche Mitteilungspflicht. Eine solche besteht nach dem Ausländergesetz für öffentliche Stellen, wenn sie von einem Ausweisungsgrund Kenntnis erhalten hat. Ein derartiger Grund liegt vor, wenn ein Ausländer Sozialhilfeleistungen in Anspruch nimmt. Anerkannte Asylberech-

tigte genießen jedoch einen besonderen Ausweisungsschutz und können nur aus „schwerwiegenden Gründen der öffentlichen Sicherheit und Ordnung“ ausgewiesen werden (§ 48 des Ausländergesetzes). Eine – im Übrigen berechtigte – Inanspruchnahme von Sozialhilfeleistungen erfüllt diese rechtlichen Voraussetzungen nicht. Deshalb hätte eine entsprechende Mitteilung des Sozialleistungsträgers nicht zu einer Ausweisung der Asylberechtigten führen können und wäre in den hier in Rede stehenden Fällen nicht erforderlich gewesen.

Somit kam als gesetzliche Erlaubnis zur Übermittlung der Sozialdaten nur noch die Bestimmung in Betracht, wonach die Datenweitergabe für die Aufgabenerfüllung des Sozialhilfeträgers erforderlich sein muss. Dabei ist der Kreis der Datenempfänger gesetzlich nicht eingeschränkt, so dass hier grundsätzlich auch das Bundesamt Adressat sein könnte. Es kann auch durchaus als gesetzliche Aufgabe des Sozialamts angesehen werden, dafür Sorge zu tragen, dass nur derjenige die staatlichen Leistungen erhalten soll, dem sie auch tatsächlich zustehen. Auf den ersten Blick schien diese Norm also einen Datentransfer an die öffentliche Stelle des Bundes zu ermöglichen. Bei genauerer Betrachtung zeigte sich aber, dass dem nicht so war. Die ins Auge gefassten Hilfeempfänger erhielten ihre Leistungen nämlich völlig zu Recht. Erkenntnisse über einen Leistungsmissbrauch oder wenigstens der Verdacht eines Leistungsmissbrauchs lagen damit gerade nicht vor, so dass eine Nachfrage beim Bundesamt dem Landratsamt bei seiner Aufgabenerfüllung gar nicht weiterhelfen konnte. Fazit: Das bloße Bemühen eines Leistungsträgers, solche Hilfeempfänger, die Leistungen zu Recht beziehen, kassenwirksam aus dem Kreis der Anspruchsberechtigten zu „entfernen“, legitimiert keine mit Sozialdaten versehenen Informationen an das Bundesamt oder an die Ausländerbehörde.

5.4 Verdacht von Straftaten oder Ordnungswidrigkeiten im Rahmen der Sozialhilfesachbearbeitung

Das Fehlen einer datenschutzrechtlichen Übermittlungsbefugnis mussten wir auch in einem weiteren Fall feststellen. Wiederum hatte ein Sozialhilfeträger unsere Dienststelle um Rat gebeten und hierbei folgenden Sachverhalt vorgetragen: Das zuständige Sozialamt hatte bei einer Unterhaltsprüfung festgestellt, dass der Unterhaltspflichtige, der eine Eigenheimzulage als Einnahme eingeräumt hatte, anscheinend zu Unrecht zusätzlich eine Kinderzulage nach dem Eigenheimzulagengesetz bezog. Zu Unrecht deshalb, weil nach den Feststellungen der Behörde die Kinder des Betroffenen im Förderzeitraum nicht dessen Haushalt angehörten. Das Sozialamt wollte nun wissen, ob es die Berechtigung oder gar Verpflichtung habe, seinen Verdacht, von dem das Finanzamt nichts ahnte, diesem mitzuteilen. Dies war im konkreten Fall zu verneinen.

Zwar haben wir im 24. Tätigkeitsbericht (LT-Drs. 13/2650, S. 61) die Zulässigkeit der Weitergabe von Tatsachen, die einen Missbrauchsverdacht begründen, bejaht. Dies aber deshalb, weil das Sozialgesetzbuch derartige Datentransfers beispielsweise erlaubt, wenn der Datenempfänger ein Sozialleistungsträger ist. Zu diesem Empfängerkreis zählt das Finanzamt jedoch nicht. Da die Verhinderung einer etwaigen missbräuchlichen Inanspruchnahme der Eigenheimzulage auch nicht zu den eigenen Aufgaben des Sozialamts gehört, kam als Rechtsgrundlage für eine Datenübermittlung nur noch die gesetzliche Mitteilungspflicht zur Sicherung des Steueraufkommens in Betracht. Die Eigenheimzulage ist nämlich aus den Einnahmen aus der Einkommensteuer auszuzahlen. Dabei hat jede Behörde Tatsachen, die sie dienstlich erfahren hat und die den Verdacht einer Steuerstraftat begründen, der zuständigen Finanzbehörde mitzuteilen. Die gesetzliche Mitteilungspflicht nach § 116 der Abgabenordnung zur Anzeige des Verdachts einer Steuerstraftat löst aber nur dann eine entsprechende Übermittlungsbefugnis nach dem Sozialgesetzbuch aus, wenn die Vorschriften der Abgabenordnung unmittelbar anwendbar sind. Beim Verfahren nach dem Eigenheimzulagengesetz sind Bestimmungen der Abgabenordnung jedoch nur entsprechend, somit ergänzend und damit gerade nicht unmittelbar anwendbar. Eine Übermittlungsbefugnis unter Rückgriff auf eine etwaige

Mitteilungspflicht an das Finanzamt schied damit ebenfalls aus. Deshalb hatte die Mitteilung in diesem speziellen Fall zu unterbleiben.

6. Datenschutz bei den Jugendämtern

6.1 Gemeindebezogene Erhebung von Klientendaten bei Beratungsstellen

Vom Landeswohlfahrtsverband Württemberg-Hohenzollern erfuhren wir, dass verschiedene Jugendämter im Zuständigkeitsbereich dieses Verbands mit dem Aufbau eines Konzepts zur örtlichen Jugendhilfeberichterstattung beschäftigt waren. Dies geschah vor dem Hintergrund, dass die Träger der öffentlichen Jugendhilfe gesetzlich u. a. auch zur Jugendhilfeplanung verpflichtet sind. Zu diesem Zweck führten die Jugendämter Erhebungen bei Beratungsstellen durch, um planungsrelevante Informationen darüber zu erhalten, wie die Hilfeleistung der Erziehungsberatung umgesetzt wird. Um den Bedarf an Einrichtungen ermitteln zu können, sollte die Erhebung möglichst kleinräumig, d. h. gemeinde- bzw. stadtteilbezogen, durchgeführt werden. Dabei sollten einzelne Beratungsstellen den Jugendämtern aus ihren Beratungsfällen die Klientenmerkmale „Wohnort/Alter/Geschlecht/deutsch/nicht-deutsch“ übermitteln. Das Landesjugendamt unterstützte die Jugendämter bei der Erarbeitung dieses Konzepts örtlicher Berichterstattung. Die Bedenken, die von anderer Seite wegen dieser örtlich spezifizierten Erhebung an uns herangetragen wurden, gingen dahin, dass bei einer Verknüpfung dieser Angaben mit einem vorhandenen oder beschaffbaren Zusatzwissen in Einzelfällen eine Identifizierung von beratenen Personen möglich sein könnte. Diese Gefahr, die vor allem aus der Benennung des Wohnorts abgeleitet wurde, war umso mehr gegeben, je kleiner die Gemeinde oder der Stadtteil war. Dies hätte zur Folge, dass dann zugleich die gesetzliche Schweigepflicht der Berater berührt gewesen wäre. Diese Bedenken waren auch nach unserem Dafürhalten nicht von der Hand zu weisen.

Mit der Strafvorschrift des § 203 des Strafgesetzbuchs hat der Gesetzgeber Angehörigen verschiedener Berufsgruppen unter Strafandrohung verboten, die ihnen anvertrauten Geheimnisse ihrer Klienten unbefugt zu offenbaren. Das gilt gleichermaßen für Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung, für staatlich anerkannte Sozialarbeiter oder staatlich anerkannte Sozialpädagogen wie auch für Ehe-, Familien-, Erziehungs- oder Jugendberater in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist (vgl. auch 21. Tätigkeitsbericht, LT-Drs. 12/5740, S. 50; 23. Tätigkeitsbericht, LT-Drs. 13/1500, S. 48 f.; 24. Tätigkeitsbericht, LT-Drs. 13/2650, S. 60). Eine Befugnis zur Offenbarung und damit eine straflose, weil gerechtfertigte Durchbrechung der Schweigepflicht kann sich aus speziellen Rechtsvorschriften, den allgemeinen Rechtfertigungsgründen (insbesondere dem Notstand) oder der Einwilligung des Betroffenen ergeben. Solche Befugnisse lagen hier nicht vor. Somit durften die Angaben, sollten sie an die örtlichen Jugendhilfeträger weitergegeben werden, keinerlei Personenbezug mehr aufweisen. Von einer danach notwendigen Anonymisierung kann ausgegangen werden, wenn Einzelangaben nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren Person zugeordnet werden können. Eine solche Zuordnungsmöglichkeit ist dann anzunehmen, wenn das Jugendamt etwa auch unter Zuhilfenahme von Zusatzwissen diesen Personenbezug herstellen könnte. Dass in Einzelfällen eine Identifizierung tatsächlich erfolgen konnte, war nicht auszuschließen. Um eine solche Identifizierung einzelner Klienten und damit eine Kollision mit der strafgesetzlichen Schweigepflicht auch in Ausnahmefällen mit Sicherheit auszuschließen, schlugen wir vor, auf die Angabe des Wohnorts jedenfalls dann zu verzichten, wenn die Wohnortgemeinde oder der Stadtteil nicht eine bestimmte Mindesteinwohnerzahl aufweist. Dem schloss sich das Landesjugendamt an. Im Ergebnis sind nun durch die Beratungsstellen die genannten Daten nur dann gemeinde- oder stadtteilspezifisch zu übermitteln, wenn die Einwohnerzahl größer als 2 500 ist.

6.2 Weitergabe von Daten durch das Jugendamt auf Anfrage des Vormundschaftsgerichts

Ein Jugendamt hat uns bei der rechtlichen Bewertung folgenden Sachverhalts um Beratung gebeten:

Ein Vormundschaftsgericht wandte sich an das Jugendamt und teilte diesem mit, dass dem Gericht in einer bestimmten Strafsache nun das verkündete Urteil vorliege. Darin wurde eine Frau wegen Misshandlung Schutzbefohlener bestraft. Das Gericht wollte wissen, ob die Verurteilte weiterhin als Pflegemutter Kinder oder andere Personen betreue und ob aus der Sicht des Jugendamts weitere gerichtliche Maßnahmen erforderlich erscheinen. Begründet wurde diese Anfrage nicht. Die Strafsache war dem Jugendamt bekannt.

Auch in diesem Fall galt: Das Jugendamt benötigt für die Weitergabe personenbezogener Daten an das Vormundschaftsgericht eine gesetzliche Ermächtigung. In Betracht kam eine sozialgesetzliche Erlaubnisvorschrift, wonach die Übermittlung von Daten durch die Sozialleistungsträger zulässig ist, wenn zur Durchführung eines gerichtlichen Verfahrens erforderlich. Nach dem Inhalt des Auskunftsersuchens war davon auszugehen, dass es sich lediglich um eine allgemeine Anfrage handelte, mit der Informationen zum Sachstand beschafft werden sollten. Die Durchführung eines gerichtlichen Verfahrens stand offensichtlich gar nicht zur Diskussion. Vielmehr sollte lediglich in Erfahrung gebracht werden, ob das Jugendamt über ein solches Verfahren vielleicht bereits nachgedacht hatte. Von der Erforderlichkeit einer Datenübermittlung für die Durchführung eines gerichtlichen Verfahrens kann dann nicht ausgegangen werden, da es nicht Sinn der Befugnisnorm ist, die Möglichkeit ständiger Sachstandsanfragen zu eröffnen; ein derartiges Kontrollinstrument sollte nach dem Zweck der Vorschrift den Gerichten nicht an die Hand gegeben werden.

Dem Jugendamt obliegt es auch, das zuständige Vormundschaftsgericht bei allen Maßnahmen, die die Sorge für die Person von Kindern und Jugendlichen betreffen, zu unterstützen und in bestimmten Verfahren vor dem Familien- und Vormundschaftsgericht mitzuwirken. Eine solche Unterstützung soll nach dem Willen des Gesetzgebers auch in gerichtlichen Verfahren oder bei Maßnahmen erfolgen, wenn das Gericht hierbei aufgrund des Amtsermittlungsgrundsatzes tätig wird. Hätte in diesem Fall also eine entsprechende Maßnahme zur Regelung der Personensorge bestimmter Kinder oder Jugendlicher konkret in Rede gestanden (z. B. Übertragung der elterlichen Sorge), wäre die Behörde zur Weitergabe befugt gewesen. Eine von einem solchen konkreten Anlass losgelöste allgemeine Anfrage „zum Stand der Dinge“ vermochte diese Befugnis jedoch nicht zu begründen. Es ist dabei auch zu berücksichtigen, dass das Jugendamt bereits per Gesetz und somit auch ohne gerichtliche Anfragen gehalten ist, das Gericht anzurufen, wenn es zur Abwendung einer Gefährdung für das Wohl des Kindes oder Jugendlichen ein Tätigwerden der Justiz für erforderlich hält. Das Jugendamt durfte somit im konkreten Fall der Anfrage des Gerichts nicht entsprechen.

4. Teil: Kommunales und anderes

1. Abschnitt: Kommunales

1. Die begehrten Einwohner

Durch eine Bürgereingabe wurden wir auf folgenden Sachverhalt aufmerksam:

Eine ältere Frau ist in derselben Großen Kreisstadt, in der auch ihre Tochter wohnt, mit Nebenwohnung gemeldet. Ihre Hauptwohnung befindet sich in ihrer Heimatgemeinde, wo sie ein eigenes Haus besitzt. Ohne zeitlichen Zusammenhang mit ihrer Anmeldung in der Großen Kreisstadt forderte das städtische Einwohnermeldeamt die Betroffene auf, exakt aufzulisten, zu welchem Zweck und an welchen Wochentagen sie sich in den vergangenen drei Monaten in der Stadt aufgehalten hat. Die Betroffene versicherte der Stadt, sie halte sich in der Regel nur an zwei bis drei Tagen im Monat in der Großen Kreisstadt auf, weshalb ihre dortige Wohnung Nebenwohnung und die Wohnung in ihrer Heimatgemeinde Hauptwohnung bleiben solle. Damit gab sich das Einwohnermeldeamt aber nicht zufrieden. Es beharrte weiterhin auf einer exakten Aufstellung der Aufenthaltszeiten. Aber nicht genug damit: Das Einwohnermeldeamt drohte auch gleich noch eine Geldbuße an.

Die von uns eingeholte Stellungnahme der Stadt förderte Überraschendes zu Tage. Die Stadt hatte nämlich nach sage und schreibe 21 Jahren festgestellt, dass Bundes- und Landesgesetzgeber 1983 einen „neuen“ objektivierten Hauptwohnungsbegriff im Melderecht eingeführt hatten. Seither können Einwohner mit mehr als einer Wohnung nicht mehr frei darüber bestimmen, welche Wohnung ihre Hauptwohnung und welche ihre Nebenwohnung ist. Vielmehr richtet sich der Wohnungsstatus seither nach objektiven Kriterien. Bei unverheirateten Einwohnern – wie im vorliegenden Fall – ist die Hauptwohnung in der Gemeinde, in der sich der Betroffene vorwiegend, d. h. zeitlich überwiegend aufhält. Außerdem stellte sich heraus, dass die Stadt nicht nur die Petentin, sondern alle dort mit Nebenwohnung gemeldeten Personen angeschrieben hatte, ohne dass ein Anhaltspunkt für die Unrichtigkeit des Melderegisters vorlag. Als Rechtsgrundlage für ihre Aktion nannte uns die Stadt § 12 Abs. 1 des Meldegesetzes (MG). Nach dieser Vorschrift hat die Meldebehörde das Melderegister von Amts wegen oder auf Antrag des Betroffenen zu berichtigen oder zu ergänzen, wenn es unrichtig oder unvollständig ist. Im konkreten Einzelfall verwies die Stadt hinsichtlich ihrer Zweifel an der Richtigkeit des Melderegisters auch auf das hohe Alter der betroffenen Person. Offenbar ging die Stadt davon aus, dass die betagte Mutter ihre Hauptwohnung nur an dem Ort haben kann, wo ihre Tochter wohnt.

Wir wunderten uns zwar darüber, wieso die Stadt „nur“ hinsichtlich der Nebenwohnungsinhaber einen Bereinigungsbedarf für ihr Melderegister sah. Hängt dies vielleicht damit zusammen, dass die Gemeinden vor allem dann Interesse an der Korrektheit des Melderegisters haben, wenn es der „positiven“ Bereinigung der Einwohnerzahl, die ja Anknüpfungspunkt für manche Transferleistung an die Kommunen ist, zugute kommt? Einerlei: Es ist nicht unsere Aufgabe, Motivforschung zu betreiben. Vielmehr hatten wir die Datenerhebung durch die Stadt ausschließlich datenschutzrechtlich zu beurteilen. Dabei kamen wir zu folgendem Ergebnis:

In der Anlage 1 zur Meldeverordnung (Anmeldung) ist festgelegt, welche Daten bei den Meldepflichtigen zu erheben sind. Hierzu gehören auch die für die Bestimmung des Wohnungsstatus notwendigen Angaben (bei Nichtverheirateten: Welche Wohnung wird vorwiegend benutzt?). Die Erläuterungen für das Ausfüllen des Meldescheins enthalten hierzu nähere Hinweise für die Meldepflichtigen. Die Stadt durfte deshalb nicht unterstellen, dass alle bei ihr aktuell mit Nebenwohnung gemeldeten Personen früher falsche Angaben gemacht oder sich deren Verhältnisse inzwischen geändert haben. Nach der Begründung zur ursprünglichen Gesetzesfassung sind die Meldebehörden selbst bei der Anmeldung nur in Zweifelsfällen veranlasst, Nachforschungen über die wahren Wohnverhältnisse anzustellen. Der Anwendungsbereich des § 20 Abs. 1 MG ist zwar im Jahr 2000 insoweit erwei-

tert worden, als der Meldepflichtige seither der Meldebehörde auf deren Verlangen nicht nur die zur „Meldung“, sondern die zur „ordnungsgemäßen Führung des Melderegisters“ erforderlichen Auskünfte erteilen muss. Nach der Begründung zu dieser Rechtsänderung hat sich aber nichts daran geändert, dass tatsächliche Anhaltspunkte zu Zweifeln an den Angaben des Meldepflichtigen oder an der Richtigkeit der Melderegisterdaten Anlass geben müssen. Nur bei Vorliegen dieser Voraussetzung darf die Meldebehörde auch einer Berichtigung des Melderegisters (§ 12 Abs. 1 MG) näher treten. Selbst § 4 a Abs. 2 des Melderechtsrahmengesetzes, den der Landesgesetzgeber noch nicht in Landesrecht umgesetzt hat, ließe es nicht zu, die Meldeverhältnisse aller mit Nebenwohnung gemeldeten Personen zu überprüfen. Nach der einschlägigen Kommentarliteratur müssen konkrete Anhaltspunkte für die Unrichtigkeit des Melderegisters vorliegen. Die auf gesicherten und langjährigen Erkenntnissen der Meldebehörden beruhende Vermutung, dass das Meldeverhalten der Inhaber von mehreren Wohnungen überdurchschnittlich nachlässig ist, reicht als Anhaltspunkt nicht aus.

Der Vollständigkeit halber sei noch erwähnt, dass das Land die Umstellung der Eintragungen im Melderegister auf den neuen Hauptwohnungsbegriff seinerzeit nur auf Antrag der Betroffenen für zulässig erklärt hat (vgl. Zweite gemeinsame Verwaltungsvorschrift des Finanzministeriums und des Innenministeriums über die Fortschreibung des Bevölkerungsstandes der Gemeinden und die Bestimmung der Hauptwohnung im Sinne des § 17 Abs. 2 des Meldegesetzes vom 15. März 1984).

Die Stadt hätte demnach nicht alle mit Nebenwohnung gemeldeten Personen anschreiben und nach ihren Aufenthaltszeiten usw. fragen dürfen. Auch den Fall der Petentin hätte die Stadt deshalb in diesem Zusammenhang nicht aufgreifen dürfen. Im Übrigen lässt das Alter einer Einwohnerin keine Rückschlüsse darauf zu, welche von ihren beiden Wohnungen sie vorwiegend benutzt.

Das wurde der Stadt mitgeteilt. Den Datenschutzverstoß beanstandete ich gegenüber dem Oberbürgermeister und bat ihn, dafür Sorge zu tragen, dass die datenschutzrechtlichen Vorschriften durch die Stadtverwaltung künftig beachtet werden.

2. Bürgermeister sucht Bewerber für die Gemeinderatswahl

Durch eine Landtags-Drucksache wurde uns bekannt, dass sich der Bürgermeister einer Kleinstadt vor den Kommunalwahlen am 13. Juni 2004 offenbar auf Kandidatensuche für die Gemeinderatswahl begeben hat. Hierzu um Stellungnahme gebeten, bestätigte uns der Bürgermeister, eine Liste mit möglichen Wahlbewerbern erstellt und an die Fraktionsvorsitzenden im Gemeinderat sowie an eine neue Wählervereinigung weitergegeben zu haben. Die Liste enthielt neben den Vor- und Familiennamen sowie den Anschriften der Betroffenen deren Telefonnummer und Beruf.

Wir haben dem Bürgermeister, der von einem Personenbezug all dieser Daten und damit auch von einer datenschutzrechtlichen Relevanz des Sachverhalts nichts wissen wollte, die Rechtslage verdeutlicht:

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 LDSG). Demnach sind alle in der Liste zu den einzelnen Personen in Verbindung mit deren Namen gemachten Angaben (Anschrift, Beruf und Telefonnummer) als personenbezogene Daten zu qualifizieren. Das gilt auch für die in der Überschrift der Liste zum Ausdruck kommende Wertung „Mögliche Kandidaten für den Gemeinderat ...“. Aus § 4 Abs. 1 LDSG ergibt sich, dass die Verarbeitung personenbezogener Daten nur zulässig ist, wenn das Landesdatenschutzgesetz selbst oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Nachdem die Betroffenen in die Verarbeitung ihrer Daten nicht eingewilligt hatten, hätte die Stadt diese nach § 13 Abs. 1 LDSG nur erheben dürfen, wenn die Kenntnis der Daten zur Erfüllung städtischer Aufgaben erforderlich gewesen wäre. Es gehört aber nicht zu den Aufgaben einer Stadt und ihres Bürgermeisters, potenzielle Bewerber für die Gemeinderatswahlen ausfindig zu machen. Die Erstellung der Liste war demnach unzulässig. Das

gilt auch für die Weitergabe der Liste, da weder die Übermittlungsvoraussetzungen des § 18 Abs. 1 LDSG vorlagen noch eine sonstige einschlägige Rechtsgrundlage ersichtlich ist. An dieser rechtlichen Bewertung ändert auch die Tatsache nichts, dass die Stadt die herausgegebenen Unterlagen als vertraulich bezeichnet hatte, weil im Zeitpunkt des Zugangs der Liste bei den Empfängern die rechtswidrige Datenübermittlung bereits vollzogen war.

Das Innenministerium hat in seiner Stellungnahme zu dem Landtagsantrag die Handlungsweise des Bürgermeisters datenschutzrechtlich genauso beurteilt.

Ich habe den Datenschutzverstoß beanstandet und den Bürgermeister gebeten, die datenschutzrechtlichen Vorschriften künftig zu beachten. Der Bürgermeister hat zugesagt, die personenbezogenen Daten zu löschen, sobald ein laufendes Wahlanfechtungsverfahren abgeschlossen ist.

3. Probleme mit der Zweitwohnungssteuer

Ein Wohnungseigentümer, den die Stadt A. rückwirkend für die Jahre 1999 bis 2003 zur Zweitwohnungssteuer veranlagt hatte, wandte sich Hilfe suchend an uns. Er fühlte sich von der Stadt ungerecht behandelt. Der Petent meinte, bei seiner Wohnung in A. handle es sich nicht um eine steuerpflichtige Zweitwohnung im Sinne der städtischen Zweitwohnungssteuersatzung, sondern um eine steuerfreie Kapitalanlage. Die Wohnung sei nämlich als künftiger Altersruhesitz für ihn und seine Ehefrau, die in B. wohnt, angeschafft worden. Im fraglichen Zeitraum habe er die Wohnung insgesamt nur wenige Wochen im Jahr ausschließlich zu „Inspektionszwecken“ aufgesucht. Datenschutzrechtlich monierte der Petent, dass die Stadt ihn zur Feststellung der „Familienwohnung“ aufgefordert habe, die Strom- und Wasserverbrauchswerte der Wohnungen in A. und B. anzugeben. Nachdem er das abgelehnt habe, habe das Steueramt sich die entsprechenden Daten beim städtischen Eigenbetrieb Stadtwerke beschafft.

Mehrere Stellungnahmen der Stadt versetzten uns nicht in die Lage, den Sachverhalt datenschutzrechtlich abschließend zu beurteilen. Wir baten die Stadt deshalb um Übersendung von Kopien der vollständigen Akten. Das lehnte die Stadt rundweg ab, was zu einer Beanstandung führte.

Erst jetzt war die Stadt bereit, uns die Akten zur Verfügung zu stellen.

Unsere Prüfung führte schließlich zu dem Ergebnis, dass die Erhebung der Verbrauchswerte schon zur Beantwortung der Vorfrage, ob es sich bei der Wohnung in A. überhaupt um eine Zweitwohnung – und nicht um die Hauptwohnung des Petenten – handelt, nicht erforderlich war. Auch zur Abgrenzung zwischen steuerpflichtiger Zweitwohnung im Sinne der städtischen Satzung und steuerfreier Kapitalanlage im Sinne der Rechtsprechung konnte die Erhebung der Verbrauchswerte nichts beitragen und war damit unzulässig:

Nach § 2 der städtischen Satzung zur Erhebung der Zweitwohnungssteuer ist Steuerschuldner, wer im Stadtgebiet für einen nicht nur vorübergehenden Zeitraum eine Zweitwohnung innehat. Eine Zweitwohnung ist u. a. jede Wohnung, die jemand neben seiner Hauptwohnung zu Zwecken des sonstigen persönlichen Lebensbedarfs im Stadtgebiet innehat. Nach der einschlägigen Rechtsprechung, insbesondere des Bundesverfassungsgerichts, des Bundesverwaltungsgerichts und des Verwaltungsgerichtshofs Baden-Württemberg, unterliegt eine Zweitwohnung unabhängig davon der Steuerpflicht, ob der Inhaber sie tatsächlich nutzt. Es genügt, dass er die Wohnung für Zwecke seines persönlichen Lebensbedarfs vorhält. Als nicht steuerpflichtig sieht die Rechtsprechung allerdings Wohnungen an, die als reine Kapitalanlage der Gewinnerzielung dienen. Diese Voraussetzung ist erfüllt, wenn eine Wohnung vermietet ist und der Vermieter sich die Eigennutzung der Wohnung nicht vorbehalten hat. Das Vorliegen dieser Ausnahmevoraussetzung hat der Petent gegenüber der Stadt nicht geltend gemacht.

Unabhängig davon, ob man mangels eigenständiger Definition des Begriffs „Hauptwohnung“ (und auch des Begriffs „Zweitwohnung“) in der o. g. Satzung – wie wir – § 17 Abs. 2 MG für entsprechend anwendbar hält oder wie

die Stadt den Schwerpunkt der Lebensbeziehungen des Wohnungsinhabers als maßgebend ansieht, kommt man zu dem Ergebnis, dass der Petent im fraglichen Zeitraum seine Hauptwohnung in B. und damit seine Zweitwohnung in A. hatte. Er hat nämlich gegenüber der Stadt mehrmals geäußert, er halte sich in A. insgesamt höchstens vier Wochen im Jahr auf. Nachdem der Petent zudem nie vorgebracht hat, seine Ehefrau wohne nicht nur in B., sondern auch oder gar vorwiegend in A., lag es auf der Hand, dass die Wohnung in B. die von der Familie vorwiegend benutzte Wohnung im Sinne von § 17 Abs. 2 MG und damit die Hauptwohnung des Petenten war. Dass dieser seinerzeit in B. nicht gemeldet war, konnte steuerrechtlich nicht zu einem für ihn günstigeren Ergebnis führen.

Die Stadt hätte sich deshalb, ehe sie den Zweitwohnungssteuerbescheid erließ, beim Petenten allenfalls über den Umfang der Benutzungszeiten der beiden Wohnungen durch ihn und seine Ehefrau vergewissern dürfen, wie sie es bereits 1989 in dem Steuererklärungsvordruck angekündigt hatte. Die Stadt hätte aber weder den Petenten um Auskunft zum Strom- und Wasserverbrauch ersuchen noch die Verbrauchsdaten ihres Eigenbetriebs Stadtwerke für Steuerzwecke nutzen dürfen, weil die Kenntnis dieser Daten zur Feststellung eines für die Besteuerung erheblichen Sachverhalts (§ 3 Abs. 1 Nr. 3 Buchst. a des Kommunalabgabengesetzes in Verbindung mit § 93 Abs. 1 der Abgabenordnung) nicht erforderlich war.

Von einer förmlichen Beanstandung dieses Datenschutzverstoßes habe ich aus verschiedenen Gründen, u. a. wegen der Komplexität des Sachverhalts, abgesehen. Ich habe aber die Stadt A. gebeten, die datenschutzrechtlichen Vorschriften künftig zu beachten.

4. Bekanntgabe von Kaufverträgen im Gemeinderatsausschuss bei Ausübung des gemeindlichen Vorkaufsrechts

Soll im Gemeindegebiet in Bereichen, die nach den Festsetzungen eines Bebauungsplans vorwiegend mit Wohngebäuden bebaut werden können, ein unbebautes Grundstück veräußert werden, so steht der Gemeinde nach dem Baugesetzbuch (BauGB) hieran ein Vorkaufsrecht zu. Dies ist nur einer der Fälle, in denen die Gemeinde dieses gesetzliche Vorrecht genießt. Weitere Beispiele sind Verkäufe von Grundstücken in einem Umlegungs- oder in einem förmlich festgelegten Sanierungsgebiet. Die Gemeinde darf ihr Vorkaufsrecht allerdings nur ausüben, wenn das Wohl der Allgemeinheit dies rechtfertigt. Die Entscheidung über die Geltendmachung dieses Rechts ist nach der wohl herrschenden Meinung durch die Gemeindevertretung zu treffen.

Ein Landratsamt ist als Rechtsaufsichtsbehörde an unsere Dienststelle herangetreten und hat um datenschutzrechtliche Würdigung folgenden Vorgangs gebeten: Bei einer Stadt herrschte die Praxis vor, alle privaten Grundstücksverkäufe im Verwaltungsausschuss des Gemeinderats der Stadt bekannt zu geben. Dabei wurden in allen Fällen die Personen der Vertragsparteien, die Flurstücksnummer des zu verkaufenden Grundstücks, dessen Größe, die vorhandene Bebauung sowie das Datum des Kaufvertrags bezeichnet. Nach einer Information von dritter Seite galt dies auch für die jeweilige Kaufpreissumme. Bei dieser Bekanntgabe wurde aber keine Rücksicht darauf genommen, ob überhaupt ein Fall vorlag, in dem die Gemeinde das gesetzliche Vorkaufsrecht in Anspruch nehmen durfte. Die Stadt begründete die Bekanntgabe aller Vorgänge, unabhängig von den gesetzlichen Voraussetzungen eines gemeindlichen Vorkaufsrechts, mit der Bedeutung für die Kommune, generell über Grundstücksgeschäfte informiert zu sein.

Besteht ein Vorkaufsrecht aus Rechtsgründen nicht, bedarf es zur Eintragung des Käufers als Eigentümer in das Grundbuch eines entsprechenden Nachweises. Das Grundbuchamt darf bei Kaufverträgen den Käufer nämlich nur dann als Eigentümer eintragen, wenn ihm die Nichtausübung oder das Nichtbestehen des Vorkaufsrechts nachgewiesen ist. Dieser Nachweis, ein sog. Negativattest, ist auf Antrag auszustellen. Aus den Bestimmungen des Baugesetzbuchs folgt nun nicht, dass die Gemeindevertretung bzw. ein Ausschuss auch in diesen Fällen zwingend über das auszustellende Zeugnis und vor allem die zugrunde liegenden Kaufverträge personenbezogen zu unterrichten ist. Deshalb hat die Verwaltung bei ihrer Unterrichtung des zu-

ständigen Ausschusses über solche Erwerbsvorgänge die Bestimmungen des Landesdatenschutzgesetzes zu beachten. Danach ist die Nutzung personenbezogener Daten zulässig, wenn dies zur Aufgabenerfüllung der Gemeinde erforderlich ist und die Daten dabei zweckentsprechend verwendet werden. Selbst wenn man unterstellt, dass es im Interesse der Kommune liegt, wenn der Gemeinderat über die Bewegungen auf dem Grundstücksmarkt unterrichtet wird, so ist es dennoch nicht erforderlich, diese Unterrichtung stets personenbezogen vorzunehmen. Es war für uns jedenfalls nicht ersichtlich, warum es für die Unterrichtung über Verkaufsfälle außerhalb des gemeindlichen Vorkaufsrechts regelmäßig schon von vornherein auf die Kaufvertragsparteien, die genaue Lage des Grundstücks und den Kaufpreis ankam. Wir schlugen daher vor, die Information des Ausschusses zunächst auf die Tatsache eines Kaufvertrags über ein Grundstück bestimmter Größe einschließlich einer ungefähren örtlichen Einordnung desselben (Straße, Gebiet) sowie auf die Schilderung der aktuellen Grundstückssituation (vorhandene Bebauung) zu beschränken. Für den Gemeinderat und dessen Mitglieder bedeutet diese Lösung auch keinen wesentlichen Informationsverlust. Machen die Mitglieder des Gemeinderats nämlich ein besonderes Interesse auch an den übrigen Angaben geltend, so haben sie nach der Gemeindeordnung gegenüber der Verwaltung immer noch das Recht, entsprechend informiert zu werden. Ein solches besonderes Interesse kann aber nicht regelmäßig von vornherein unterstellt werden.

Die Aufsichtsbehörde schloss sich dieser Ansicht an und instruierte die Stadt entsprechend.

5. Führung der Kaufpreissammlung durch Dritte

Eine wesentliche Aufgabe nach dem Baugesetzbuch ist die Ermittlung von Grundstückswerten. Dies vollzieht sich auf der Ebene der Gemeinden durch die Gutachterausschüsse. Die Ausschüsse üben ihre behördliche Tätigkeit selbstständig und unabhängig aus. Ein Instrument der von den Ausschüssen vorzunehmenden Wertermittlung ist die sog. Kaufpreissammlung. Sie wird vom Gutachterausschuss bzw. von dessen Geschäftsstelle betrieben und soll dem Ausschuss einen möglichst vollständigen Überblick über die örtlichen Grundstückspreise verschaffen. Die Auswertung dieser Sammlung führt wiederum zur Ermittlung der sog. Bodenrichtwerte. Das sind gemeindescharfe „durchschnittliche Lagewerte für den Boden unter Berücksichtigung des unterschiedlichen Entwicklungszustands“ (§ 196 BauGB). Die Kaufpreissammlung kann aber nur entstehen, wenn dem Gutachterausschuss auch die abgeschlossenen Kaufverträge zugeleitet werden. Deshalb „ist jeder Vertrag, durch den sich jemand verpflichtet, Eigentum an einem Grundstück gegen Entgelt, auch im Wege des Tausches zu übertragen oder ein Erbbaurecht zu begründen, von der beurkundenden Stelle in Abschrift dem Gutachterausschuss zu übersenden“ (§ 195 BauGB).

Drei Diplom-Sachverständige kamen auf die Idee, verschiedenen Gemeinden anzubieten, in deren Auftrag die Kaufpreissammlung zu führen und die eingehenden Kaufverträge einzusehen, auszuwerten und anonymisiert in die Sammlung aufzunehmen. Zuvor baten sie unsere Dienststelle um eine datenschutzrechtliche Bewertung des geplanten Unterfangens.

Die Zulässigkeit des Vorhabens hängt ganz entscheidend davon ab, ob es sich bei der dazu notwendigen Weitergabe der Kaufverträge (bzw. deren Abschrift) zum Zwecke der Einsichtnahme und Auswertung durch die Sachverständigen um eine Datenverarbeitung im Auftrag des jeweiligen Gutachterausschusses handelt oder um eine Datenübermittlung. Diese Weichenstellung ist bedeutsam, da die Datenübermittlung nur unter engen gesetzlichen Voraussetzungen zulässig ist, wohingegen die Auftragsdatenverarbeitung eine Form der Datennutzung durch die verantwortliche Stelle selbst darstellt und im Wesentlichen (lediglich) verlangt, dass der – sorgfältig ausgewählte – Auftragnehmer vertraglich zu datenschutzkonformem und den Weisungen des Auftraggebers unterliegendem Verhalten verpflichtet wird. Eine Auftragsdatenverarbeitung konnte angesichts des Umfangs des Vorhabens hier nicht angenommen werden. Denn die Sachverständigen hatten angeboten, die eingehenden – personenbezogenen – Kaufverträge zu sichten, auszuwerten und die zur Wertermittlung notwendigen Zahlen abzu-

leiten, um eine unabhängige und qualifizierte Auswertung der Informationen des örtlichen Grundstücksmarktes zu ermöglichen. Damit wollten die Sachverständigen nicht mehr nur eine unselbstständige Hilfeleistung für den Gutachterausschuss erbringen, sondern hatten im Auge, selbst eine umfassende Bewertung vorzunehmen. Dann spricht man datenschutzrechtlich nicht mehr von einer Auftragsdatenverarbeitung, sondern von einer Funktionsübertragung. Damit konnte die beabsichtigte Überlassung personenbezogener Angaben durch den Gutachterausschuss oder dessen Geschäftsstelle an die Sachverständigen aber nicht mehr als Datennutzung durch den Gutachterausschuss selbst angesehen werden, sondern war vielmehr als Datenübermittlung zu werten. Dann aber bedurfte es einer ausdrücklichen gesetzlichen Ermächtigung zur Weitergabe derartiger Informationen. Das Baugesetzbuch regelt in Verbindung mit der Gutachterausschussverordnung den Zugang zur Kaufpreissammlung abschließend. Auch die Weitergabe der Kaufverträge zur Sichtung und Auswertung ist damit allenfalls unter den dort genannten Voraussetzungen zulässig. Nach § 195 BauGB darf die Kaufpreissammlung aber nur dem zuständigen Finanzamt für Zwecke der Besteuerung übermittelt werden. Darüber hinaus soll die Sammlung auch bei gerichtlichen Auseinandersetzungen zugänglich sein. Im Übrigen besteht kein Recht auf Einsichtnahme, sondern ausschließlich auf Auskunft aus der Kaufpreissammlung, sofern ein hierauf gerichtetes berechtigtes Interesse vorliegt und schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Aber selbst dann dürfen Name und Anschrift des Eigentümers oder sonstiger berechtigter Personen nicht mitgeteilt werden. Mit uns kam auch das Innenministerium zu dem Ergebnis, dass die begehrte Weitergabe von Kaufverträgen und damit die Umsetzung des Vorhabens rechtswidrig gewesen wäre.

2. Abschnitt: Personalwesen

1. Neue Steuerungsinstrumente

Auch in diesem Jahr waren die Neuen Steuerungsinstrumente (NSI) Gegenstand unserer Prüfung. U. a. gingen wir der Frage nach, ob Störungsmeldungen datenschutzgerecht bearbeitet werden, kontrollierten den Einsatz von NSI-Programmen und befassten uns mit der kostenträgerorientierten Zeit- und Mengenerfassung bei Offline-Dienststellen.

1.1 Der Umgang mit Störungsmeldungen

Die Landesbehörden, die das NSI-System anwenden, haben ein privates Unternehmen beauftragt, Störungsmeldungen zu bearbeiten und sich um Fragen von Anwendern des NSI-Systems zu kümmern. Das Unternehmen hat dazu ein „User Help Desk“ (UHD) eingerichtet, an das sich die Anwender (d. h. die Beschäftigten der Landesbehörden, die mit dem System arbeiten) wenden können. Ein Ministerium sowie der Lenkungsausschuss NSI baten uns, die UHD-bezogenen Datenschutzkonzepte mit Blick auf den Schutz der personenbezogenen Daten der Beschäftigten des Landes zu überprüfen. Mein Amt bat daraufhin um Übersendung der entsprechenden Datenschutzkonzepte des Unternehmens. Dieses lehnte das jedoch ab, weil es eigene Konzepte nicht aus seinem Einflussbereich herausgeben wolle und es als privates Unternehmen nicht der Zuständigkeit meines Amts unterstehe. Letzteres trifft zwar zu, doch bearbeitet das Unternehmen die Störungsmeldungen lediglich als Auftragnehmer der meiner Kontrolle unterliegenden Landesbehörden. Daher sind diese dafür verantwortlich, dass das Unternehmen als Auftragnehmer die Vorschriften über den Datenschutz einhält. Zudem setzt eine verantwortungsvolle Nachprüfung der genannten Konzepte durch mein Amt grundsätzlich deren Überlassung voraus, weil es uns regelmäßig nur dann möglich ist, diese in der gebotenen Gründlichkeit zu überprüfen. In Anbetracht dessen wurde vereinbart, dass mein Amt diese Konzepte bei dem Unternehmen vor Ort einsehe und die als besonders wichtig erachteten Teile der Konzepte in Kopie erhalte. Letzteres geschah dann schließlich bei einem zweiten Termin. Bei einem weiteren Termin besprachen wir mit dem Unternehmen die

Punkte, die uns bei der Durchsicht der Konzepte aufgefallen waren. Wir verblieben so, dass unsere Hinweise geprüft und die Konzepte gegebenenfalls fortgeschrieben werden. Eine abschließende Bewertung der Angelegenheit steht noch aus.

1.2 Kontrolle bei einer Dienststelle

Schon mehrfach hatten wir Gelegenheit, uns das NSI-System vorführen zu lassen. Bei diesen Vorführungen hatte schon ausreichend Anlass bestanden, Verbesserungsvorschläge hinsichtlich einer datenschutzfreundlicheren Gestaltung zu machen. Nachdem das System im Berichtszeitraum bei einer Vielzahl von Behörden und Ämtern eingerichtet und produktiv genutzt wurde, hielten wir es für angebracht, den Einsatz des NSI-Systems vor Ort bei einer Dienststelle des Landes zu kontrollieren. Mit der im vergangenen Jahr von der damals kontrollierten Behörde strapazierten Generalentschuldigungsklausel, man sei eine Pilotdienststelle und noch im Testbetrieb, im Wirkbetrieb seien die datenschutzrechtlichen Mängel behoben, konnte diese Dienststelle nicht mehr arbeiten – und dies hat sie auch nicht getan. Im Einzelnen hat sich bei der Kontrolle Folgendes ergeben:

– Freitextfelder

Der Umgang mit Freitextfeldern ist offensichtlich nicht ohne Probleme. Denn meine Mitarbeiter machten bei ihrer Kontrolle Freitextfelder ausfindig, die nicht in den entsprechenden Datenschutzkonzepten genannt werden. Um es klar zu sagen: Ein Datenschutzkonzept, das nicht alle Freitextfelder – und damit Risikopotenziale für die unzulässige Speicherung von personenbezogenen Daten – benennt, ist nicht vollständig und muss nachgebessert werden. Zudem sind Freitextfelder, die nicht benötigt werden, zu deaktivieren – eine Funktionalität, die ein datenschutzfreundliches EDV-Verfahren zu leisten im Stande sein sollte. Des Weiteren ist klar zu regeln, welche Art von Daten in den Freitextfeldern eingegeben werden dürfen. Es ist dafür Sorge zu tragen, dass die zulässige Speicherdauer der in Freitextfeldern einzugebenden Daten nicht die Speicherdauer der Daten, mit denen das Freitextfeld assoziiert ist, unterschreitet, da die Löschung dann meist erheblich komplizierter ist oder sogar unterbleibt.

– Rollengenerator

Innerhalb des Systems können differenzierte Zugriffsrechte für einzelne Konten vergeben werden. Die aus datenschutzrechtlicher Sicht notwendige Kontrolle, wem welche Zugriffsrechte eingeräumt wurden, kann theoretisch anhand von Auflistungen der Zugriffsrechte gewonnen werden. Theoretisch deshalb, weil zum Verständnis dieser Auflistungen, die aus „mnemonischen Transaktionskennungen“ bestehen, eine profunde technische Kenntnis über die internen Abläufe des Systems notwendig ist, über die im Allgemeinen nur Experten verfügen. Dem NSI-Projekt war klar, nicht nur dafür sorgen zu müssen, dass nur derjenige Zugriff auf die im System gespeicherten personenbezogenen Daten hat, die er für die Sachbearbeitung braucht, sondern es muss auch sichergestellt sein, dass die als erforderlich gemeldeten Berechtigungen mit den tatsächlich im System eingestellten Berechtigungen abgeglichen werden können. Das Zauberwort zur Lösung dieses Problems hieß „Rollengenerator“; dieser wurde im Auftrag des NSI-Projekts entwickelt und soll es ohne eingehende Systemkenntnis ermöglichen, die Berechtigungen in verständlicher Form aus dem System zu extrahieren. Bei der Kontrolle wollten sich meine Mitarbeiter auch ein Bild von den Informationen machen, die durch den Einsatz des Rollengenerators, der im Februar 2004 freigegeben wurde, gewonnen wurden. Die Enttäuschung war dementsprechend groß, als sich herausstellte, dass die Dienststelle erst eine Woche vor dem Kontrollbesuch den Rollengenerator zur Verfügung gestellt bekommen und erst einen Versuch unternommen hatte, die Berechtigungen zu prüfen. Dies bedeutet nichts anderes, als dass es Dienststellen im Land gibt, die schon seit eineinviertel Jahren mit

dem System arbeiten, wobei erst jetzt die datenschutzrechtlich Verantwortlichen überprüfen konnten, ob die von ihnen mitgeteilten Berechtigungen auch korrekt im System konfiguriert wurden oder ob nicht etwa Unbefugten Zugriffsmöglichkeiten auf personenbezogene Daten eingeräumt worden waren.

Die beim Aufruf des Rollengenerators festzustellenden Ergebnisse waren unvollständig und daher nur eingeschränkt für Prüfungszwecke zu gebrauchen. Obwohl aus den Gesamtumständen klar war, dass es Benutzerbetreuer geben musste, die unter ihrer Benutzerkennung auf die Daten der Dienststelle zugreifen können, erschienen diese Benutzerkennungen nicht in den Ergebnissen des Rollengenerators. Aus den Schilderungen des Ablaufs eines Zahlungsvorgangs durch die Mitarbeiter der Dienststelle und nach Einsicht in zufällig ausgewählte Einzelbelege ergab sich weiterhin, dass es auch bei der Landesoberkasse Baden-Württemberg Benutzer geben musste, die Buchungen auf die Konten der kontrollierten Behörde durchführen und damit Kenntnis personenbezogener Daten erlangen können. Die vom Rollengenerator generierten Listen mit Zugriffsberechtigungen führten dennoch keine Benutzer der Landesoberkasse auf. Lediglich Benutzer der übergeordneten Dienststellen und des zuständigen Ministeriums sowie des Finanzministeriums waren in der Liste genannt. Ob neben den bisher genannten weitere SAP-Benutzer (beispielsweise SAP_ALL, SAP_NEW) zugriffsberechtigt waren, ging aus den Aufstellungen ebenfalls nicht hervor.

Wir empfahlen der Dienststelle, als verantwortliche Stelle nach § 3 Abs. 3 LDSG gegenüber dem NSI-Betreiber darauf zu drängen, dass mit dem Rollengenerator alle Benutzerkennungen, die auf Datenobjekte der Dienststelle zugreifen können, angezeigt werden. Zumindest muss erkennbar sein, von welchen anderen Stellen aus ein Zugriff auf diese Datenobjekte möglich ist.

Zum Rollengenerator war weiter festzustellen, dass die Ergebnisse eine Aufschlüsselung nur bis zur Ebene der Finanzstelle zuließen. So konnte zwar festgestellt werden, auf welche Finanzstellen ein Benutzer zugreifen kann. Es kann aber sein, dass auf der Ebene der Finanzpositionen weitere Einschränkungen im Zugriff sachgerecht sind. Um hinreichende Aussagekraft hinsichtlich der erlaubten Zugriffsberechtigungen zu haben, sind die derzeitigen Ergebnislisten des Rollengenerators, so wie er bei der Dienststelle eingesetzt wird, jedenfalls unzureichend.

Für die Kontrolle der Berechtigungen wurde den Dienststellen des Landes ein handhabbares Werkzeug versprochen. Wenn das NSI-Projekt der Auffassung ist, dass sie es mit dem Rollengenerator bekommen haben, dann muss das Projekt durch Schulung dafür sorgen, dass dieses Werkzeug auch sachgerecht und effizient eingesetzt werden kann.

– Berechtigungserteilung

Das so genannte NSI-CC, eine Stelle, die die Benutzerbetreuung wahrnimmt, war unser Ansprechpartner, als es darum ging, die für den Zugriff auf die Konten der Dienststelle Berechtigten in Erfahrung zu bringen. Nach Rückfrage bei der Dienststelle teilte diese mit, dass sie keine Mitarbeiter für den Zugriff auf ihre Konten berechtigt habe, die nicht Mitarbeiter der Dienststelle sind. Wie im vorangehenden Spiegelstrich dargestellt, gab es aber bei der Dienststelle mehr als genug solcher Zugriffsberechtigter. Das heißt, dass es bei der Berechtigungsvergabe möglich war, dass Berechtigungen an Mitarbeiter des zuständigen Ministeriums und des Finanzministeriums vergeben wurden, obwohl die Dienststelle selbst davon keine Kenntnis hatte. Zwar wurde in einem Rahmenkonzept für die Berechtigungsvergabe detailliert vorgegeben, wie eine Berechtigung zu vergeben ist; daran scheint man sich aber nicht unbedingt gehalten zu haben.

Wir haben der Dienststelle empfohlen, von den Ministerien Klärung darüber zu verlangen, warum und zu welchem Zweck eine nicht unbeträchtliche Anzahl von Mitarbeitern der Ministerien Zugriff auf die Konten der Dienststelle haben muss. Es darf auch nicht sein, dass hinter dem Rücken der Behörde als verantwortlicher Stelle weiteren Behörden Zugriffsrechte eingeräumt werden.

– Zugriff auf Belege

Ein wesentlicher Kritikpunkt, der sich über die gesamte Entwicklung des Systems erstreckte, bestand darin, dass Benutzer übergeordneter Behörden, deren Aufgabe nicht in der Bearbeitung von Einzelfällen besteht, sondern die beispielsweise für die Mittelbewirtschaftung verantwortlich zeichnen, trotzdem Zugriff auf die Einzelbelege hatten. Dies war dann festzustellen, wenn diesen Benutzern übergeordneter Behörden die Berechtigung für den lesenden Zugriff auf die Konten eingeräumt wurde, denen die Einzelbelege zugeordnet sind. So wäre es beispielsweise Mitarbeitern des Kultusministeriums möglich gewesen, Einzelbelege über die Gewährung von BAföG-Leistungen, die von den Regierungspräsidien festgesetzt werden, einzusehen. Dies deshalb, weil das Kultusministerium die BAföG-Mittel bewirtschaftet. Aus gutem Grund lehnten die Verantwortlichen des Regierungspräsidiums einen Zugriff des Ministeriums auf die Konten ab.

Wann immer diese Problematik – nicht nur von meinen Mitarbeitern, sondern auch von Haushältern insbesondere bei ressortübergreifenden Zugriffen – gegenüber dem Projekt und dem Betreiber zur Sprache gebracht wurde, erhielten wir die stereotype Aussage, die von uns für erforderlich gehaltene Berechtigungsvergabe, dass nur die Sachbearbeiter „vor Ort“ Zugriff auf die Belege eines Kontos haben dürfen, sei mit dem SAP-System nicht machbar. Dass ein System, das über ein so reichhaltiges und feinkörniges Berechtigungssystem verfügt, derartige Zugriffsberechtigungen nicht modellieren können soll, konnten wir nicht nachvollziehen. Die angebliche Unmöglichkeit, solche differenzierten Zugriffsrechte vergeben zu können, hat dann etwa zur Folge, dass in der Praxis eine Reihe von externen Mitarbeitern auf so sensible Daten wie die Konten und Belege zur Einnahme von Geldern aus Disziplinarmaßnahmen bei der kontrollierten Dienststelle zugreifen kann. In den Belegen werden regelmäßig die Namen der Betroffenen erwähnt. Wir haben auch dieser Dienststelle empfohlen, gegenüber dem Betreiber darauf zu drängen, dass Zugriffe auf Belege nur für Mitarbeiter der Dienststelle möglich sein dürfen.

Nunmehr teilt uns der NSI-Betreiber mit, dass Zugriffsberechtigungen entwickelt wurden, die den Zugriff nur auf die Konten und nicht gleichzeitig auf die Belege erlauben. Man wolle diese Profile in der Produktivumgebung austesten. Wenn die Tests erfolgreich verlaufen, wäre damit ein großer Schritt hin zu einem wesentlich datenschutzfreundlicheren Betrieb des Systems gemacht.

1.3 Kostenträgerorientierte Zeit- und Mengenerfassung bei Offline-Dienststellen

Die Aussagekraft einer Kosten- und Leistungsrechnung steht und fällt mit der Genauigkeit, mit der die anfallenden Kosten den Produkten zugeordnet werden. Um ein Höchstmaß an Aussagekraft zu erreichen, soll die Arbeitszeit jedes Mitarbeiters bezogen auf die für ein Produkt aufgewendete Zeit erfasst werden. Für diese Erfassung wird beim NSI-Projekt das SAP-Verfahren CATS (Cross Application Time Sheet) verwendet. Mit dem Programm kann jeder Mitarbeiter seine Arbeitszeit auf die Produkte, bei deren Herstellung er mitwirkt, buchen. Die Erfassung geschieht normalerweise derart, dass die über ein Clientprogramm eingegebenen Daten über ein Netzwerk auf einem CATS-Server in einer Datenbank gespeichert werden.

Vielfach gibt es Dienststellen im Land, die noch nicht über die entsprechende technische Infrastruktur verfügen, um die Anbindung an

den CATS-Server beim Rechenzentrum so vorzunehmen, dass die Zeiterfassung effizient durchgeführt werden kann. Daher hat man sich im Projekt darauf zurückgezogen, dass Mitarbeiter dieser Dienststellen – sog. Offline-Dienststellen – die Arbeitszeit nicht über den Zugriff auf den CATS-Server verbuchen, sondern ihre Arbeitszeit mit einem Tabellenkalkulationsprogramm in Tabellen produktbezogen erfassen. Die Tabellen werden an wenigen zentralen Stellen ressortweit gesammelt, geprüft, konvertiert, an das Service-Rechenzentrum übertragen und dort automatisch in den CATS-Server eingegeben. Ab diesem Zeitpunkt verläuft die weitere Verarbeitung der Daten wie in den Fällen, in denen die Daten von Mitarbeitern direkt mit dem Clientprogramm ein- und freigegeben werden.

Aus der Beschreibung wird deutlich, dass die personenbezogenen Daten der Mitarbeiter von Offline-Dienststellen durch viele Hände laufen. Dass dabei der Datenschutz gewahrt werden muss, versteht sich bei der Sensibilität dieser Daten von selbst, könnten die Daten doch von Unbefugten zu einer zumindest stichprobenweisen Leistungskontrolle der Mitarbeiter herangezogen werden. Eine Leistungskontrolle ist aber nach Aussage des Betreibers des NSI-Systems nicht beabsichtigt und soll auch nicht allgemein ermöglicht werden. Unter anderem zur Gewährleistung des Datenschutzes hat das Projekt ein Handbuch verteilt, in dem beschrieben wird, wie Installation und Ablauf der Erfassung und Verarbeitung zu erfolgen haben und welche Maßnahmen zur Gewährleistung des Datenschutzes ergriffen werden müssen. Die Polizei Baden-Württemberg hat diese dort beschriebene Vorgehensweise auf ihre Bedürfnisse angepasst, beide Beschreibungen vorgelegt und um beratende Äußerung gebeten. Wir haben nach der Prüfung der Konzepte unter anderem Folgendes empfohlen:

– Verschlüsselung

  Die Tabellen mit den verbrauchten Zeiten eines Mitarbeiters sind personenbezogene Daten, die des besonderen Schutzes bedürfen. Es ist daher erforderlich, folgende Maßnahmen zu ergreifen:

  • Speicherkontrolle

    Die Tabelle mit den verbrauchten Zeiten je Produktart muss von den Mitarbeitern an einem nur von ihnen zugreifbaren Speicherort gespeichert werden. Wenn ein derartiger Speicherplatz nicht zur Verfügung gestellt werden kann, dann muss es dem Mitarbeiter möglich sein, seine Daten in verschlüsselter Form zu speichern. Es muss durch entsprechende Maßnahmen sichergestellt werden, dass temporäre Dateien, die möglicherweise in ungeschützten Speicherbereichen angelegt werden, gelöscht werden. Ansonsten ist nicht mit Sicherheit auszuschließen, dass Unbefugte Kenntnis vom Inhalt temporärer Dateien erlangen könnten.

  • Transportkontrolle

    Bei der Übertragung der Tabellen und beim Transport von Datenträgern, auf denen die Tabellen gespeichert sind, müssen die Tabellen verschlüsselt sein. Nur dann kann mit hoher Sicherheit ausgeschlossen werden, dass Unbefugte die Daten lesen können. Selbst wenn in dem NSI-Projekt eine Infrastruktur zur asymmetrischen Verschlüsselung von Dokumenten besteht, können die Offline-Dienststellen diese aus oben erwähntem Grund nicht nutzen. Daher bleibt nur der Weg, die Tabellen symmetrisch zu verschlüsseln und den Schlüssel auf einem anderen Kommunikationsweg als die Tabellen an die empfangende Stelle zu übermitteln.

– Authentifizierung

  Die Zeiten werden in CATS auf eine verfahrensspezifische Personalnummer – CATS-Personalnummer – gebucht. Damit Benutzer nicht versehentlich Zeiten falsch verbuchen, müssen technische Vorkehrungen zur Authentifizierung getroffen werden. Zur Gewährleistung

der Zugriffskontrolle ist ein Authentifizierungsmechanismus erforderlich, der sicherstellt, dass der Eingebende auch derjenige ist, auf dessen CATS-Konto die Zeiten gebucht werden.

Das Problem besteht nun darin, einen zuverlässigen Authentifizierungsmechanismus in einem Tabellenkalkulationsprogramm zu realisieren, das Authentifizierungsmechanismen nicht vorsieht. Daraus ergibt sich die Anforderung, Kennworte in der Tabelle so zu speichern, dass sie von Benutzern nicht eingesehen und verändert werden können, obwohl ihnen lesender und schreibender Zugriff auf die Tabelle eingeräumt werden muss. Auch ist sicherzustellen, dass die Algorithmen, nach denen die Authentifizierung erfolgt und die bei Tabellenkalkulationsprogrammen als sog. Makros gespeichert werden, nicht durch Benutzer verändert werden können, da sonst die Authentifizierung praktisch ausgehebelt wäre. Die wesentlichen Unterschiede zu Authentifizierungssystemen, wie sie normalerweise eingesetzt werden, besteht nämlich darin, dass bei diesen Systemen die Benutzer nicht auf die Speicherbereiche zugreifen können, in denen die Kennwörter gespeichert werden, und sie die Authentifizierungsalgorithmen nicht verändern können.

Deshalb hat man sich Folgendes ausgedacht: In einer Tabelle wird von den NSI-Controllern eine Prüfsumme, der so genannte Hash-Wert, gespeichert, die aus der CATS-Personalnummer und dem zugehörigen Namen des Mitarbeiters einer Organisationseinheit mit einem mathematischen Verfahren gebildet wird. Diese Tabelle wird so geschützt, dass sie für die Benutzer nicht sichtbar ist. Der Benutzer gibt bei der Erfassung seinen Namen und ein Kennwort ein, das seiner CATS-Personalnummer entspricht. Daraus wird der Hash-Wert berechnet und mit dem gespeicherten Hash-Wert verglichen. Stimmen die Werte überein, dann kann man einigermaßen sicher sein, dass der Eingebende auch derjenige ist, auf dessen CATS-Konto die eingegebenen Daten gebucht werden. Die Makros, mit denen die Verarbeitung erfolgt, sollen durch ein Passwort geschützt werden. Hierzu ist zu sagen:

- Das Kennwort ist nicht änderbar, da es der CATS-Personalnummer entspricht. Was geschieht, wenn Dritte Kenntnis einer CATS-Personalnummer und eines Namens erhalten, bleibt unklar.
- Die Sichtbarkeit des Mitarbeiterblatts wird über eine Systemeinstellung gesteuert. Es muss sichergestellt werden, dass normale Benutzer diese Systemeinstellung nicht verändern können.
- Ob die unsichtbar gemachten Teile der Tabelle und die passwortgeschützten Makros nicht doch von normalen Benutzern sichtbar gemacht bzw. verändert werden können, ist fraglich.
- Hinsichtlich des Hash-Werts muss sichergestellt werden, dass der Abbildungsbereich groß genug ist und Kollisionen ausgeschlossen werden können.

Wir haben uns kritisch zur Vorgehensweise bei der Authentifizierung geäußert. Als hochgradig sicher darf man die geplante Vorgehensweise auf jeden Fall nicht bezeichnen. Andererseits bietet das Vorgehen Schutz vor unbeabsichtigter Fehleingabe – insoweit ist die Zielrichtung des Vorgehens auch zu begrüßen. Man sieht an diesem Verfahren aber auch deutlich: Wenn ein Programm für Zwecke eingesetzt wird, für die es nicht geschaffen ist, kommen häufig Lösungen zu Stande, die nicht in jeder Hinsicht zu überzeugen vermögen.

– Anonymisierung

In den übersandten Unterlagen wurde ausgeführt, bei der Datenüberleitung vom Erfassungs-System in das Programmmodul zur Kosten- und Leistungsrechnung würden die Daten auf Zeiten je Kostenstelle, Leistungsart und Kostenträger zusammengefasst und anonymisiert. Wie bereits an anderer Stelle wiesen wir hierzu u. a. darauf hin, dass personenbezogene Daten nur dann anonymisiert sind, wenn die

Daten einer bestimmten oder bestimmbaren natürlichen Person nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können (vgl. § 3 Abs. 6 LDSG). Ob dies in jedem Fall so ist (insbesondere bei Kostenstellen, denen nur wenige Beschäftigte zugeordnet sind, oder bei Kostenträgern bzw. Produkten, für die nur wenige Beschäftigte tätig sind), war anhand der uns übersandten Unterlagen nicht festzustellen. Damit die betroffenen Beschäftigten nicht unzutreffend über den Umfang der Verarbeitung ihrer personenbezogenen Daten unterrichtet werden, darf von Anonymisieren nur dann die Rede sein, wenn dessen Voraussetzungen in jedem einzelnen Fall tatsächlich vorliegen. Zudem ist in diesem Zusammenhang zu berücksichtigen, dass auch anonymisierte Daten personenbezogen sein können: Dies ist nur dann nicht der Fall, wenn sie einer bestimmten oder bestimmbaren natürlichen Person nicht zugeordnet werden können; ist eine solche Zuordnung jedoch möglich (wenngleich bei anonymisierten Daten nur mit unverhältnismäßig großem Aufwand), liegen personenbezogene Daten vor. Wir baten um Erläuterung der entsprechenden Ausführungen oder um deren Änderung.

Zwischenzeitlich liegt uns eine Äußerung der Polizei vor, die wir noch auswerten müssen, bevor wir eine abschließende Beurteilung abgeben können.

2. Arbeitsschutz und Datenschutz

Keine Frage: Um Arbeitsunfälle innerbehördlich bzw. innerbetrieblich aufarbeiten und um hieraus Lehren für die Zukunft ziehen zu können, dürfen Daten des Betroffenen – im Rahmen der datenschutzrechtlichen Bestimmungen – verarbeitet werden.

Ein als Eigenbetrieb geführtes Klinikum wandte sich an unsere Dienststelle mit der Frage, ob eine „Interne Unfallmeldung“, die es selbst entworfen hatte und mit der Angaben zum Unfall erfasst werden sollen (z. B. Verletzter, Unfallort und -zeit, Unfallhergang, Arbeitsunterbrechung: ja/nein), in Kopie an die Sicherheitsbeauftragten der einzelnen Bereiche weitergegeben werden dürfen.

Hierfür sahen wir jedoch keine gesetzliche Grundlage. Bei den auf dem Formular erhobenen Daten über Dienstunfälle handelt es sich um Personalaktendaten. Für diese gilt das Personalaktengeheimnis: Sie dürfen nur für Zwecke der Personalverwaltung oder -wirtschaft verwendet werden, es sei denn, der Beschäftigte willigt in die anderweitige Verwendung ein; Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Verarbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalwirtschaft erforderlich ist. Eine (generelle) Weitergabe von Kopien der jeweiligen „Internen Unfallmeldung“ ist nicht zulässig:

- Während Betriebsärzte u. a. die Aufgabe haben, den Arbeitnehmer zu untersuchen, arbeitsmedizinisch zu beurteilen und zu beraten sowie die Untersuchungsergebnisse zu erfassen und auszuwerten, und es zu den Aufgaben der Fachkräfte für Arbeitssicherheit gehört, Ursachen von Arbeitsunfällen zu untersuchen (vgl. §§ 3 und 6 des Gesetzes über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit), gibt es eine entsprechende (auf Arbeitsunfälle bezogene) Aufgabenzuweisung für die Sicherheitsbeauftragten nicht. Diese haben den Unternehmer vielmehr bei der Durchführung der Maßnahmen zur Verhütung von Arbeitsunfällen und Berufskrankheiten zu unterstützen, insbesondere sich von dem Vorhandensein und der ordnungsgemäßen Benutzung der vorgeschriebenen Schutzeinrichtungen und persönlichen Schutzausrüstungen zu überzeugen und auf Unfall- und Gesundheitsgefahren aufmerksam zu machen (vgl. § 22 Abs. 2 des Siebten Buchs des Sozialgesetzbuchs).
- Auch die in § 16 Abs. 1 des Arbeitsschutzgesetzes angesprochenen Unterstützungspflichten der Beschäftigten führen nicht dazu, dass der Arbeitgeber generell Kopien der Unfallmeldung an den Sicherheitsbeauftragten weiterleiten darf: Der Beschäftigte hat danach die Pflicht, (ledig-

lich) dem Arbeitgeber oder dem zuständigen Vorgesetzten jede von ihm festgestellte unmittelbare erhebliche Gefahr für die Sicherheit und Gesundheit sowie jeden an den Schutzsystemen festgestellten Defekt zu melden. Zudem „soll“ der Beschäftigte von ihm festgestellte Gefahren für die Sicherheit und Gesundheit sowie Mängel an den Schutzsystemen auch der Fachkraft für Arbeitssicherheit, dem Betriebsarzt oder dem Sicherheitsbeauftragten mitteilen. Auch diese an den Beschäftigten gerichtete Soll-Vorschrift begründet keine Befugnis des Arbeitgebers, personenbezogene Daten des Beschäftigten an den Sicherheitsbeauftragten weiterzugeben, zumal der Beschäftigte sich nicht an diesen wenden muss, sondern stattdessen an die Fachkraft für Arbeitssicherheit oder den Betriebsarzt herantreten kann.

Eine generelle Weitergabe von Kopien der „Internen Unfallmeldung“ an Sicherheitsbeauftragte ist damit ohne Einwilligung des Beschäftigten unzulässig und wäre im Übrigen auch nicht notwendig, um dem Anliegen des Arbeitsschutzes Rechnung zu tragen: Der Sicherheitsbeauftragte kann regelmäßig seine gesetzlichen Aufgaben erfüllen, wenn er insoweit ausschließlich über den Unfall und dessen Ursache bzw. den Geschehensablauf ohne personenbezogene Daten des Beschäftigten informiert wird, zumal es ausdrücklich zu den Aufgaben der Fachkräfte für Arbeitssicherheit – und nicht der Sicherheitsbeauftragten – gehört, die Ursachen der Arbeitsunfälle zu untersuchen. Wir haben dies dem Klinikum mitgeteilt.

3. Herr Peter Werner und die persönliche Post für Herrn Werner Peter

Herr Werner (die wirklichen Namen des Beschwerdeführers und des mitbetroffenen Kollegen waren natürlich andere) rügte gegenüber meinem Amt, dass für ihn bestimmte Mitteilungen über die Zusammensetzung seiner Bezüge, Beihilfebescheide und andere Schreiben seinem Kollegen Herrn Peter vorgelegt würden, der bei derselben Behörde wie er beschäftigt sei. Im Gegenzug erhalte er, Herr Werner, solche an Herrn Peter gerichteten Sendungen. Wurzel des Übels sei die Adressierung dieser Schreiben: Dort werde der Nachname vor dem Vornamen aufgeführt, also sein, Herrn Werners, Name mit „Werner Peter“ und Herrn Peters Name mit „Peter Werner“ angegeben.

Eine solche Adressierung (ein Voranstellen des Nachnamens, zumal wenn dieser nicht als solcher erkennbar ist, etwa durch Großbuchstaben oder ein nachgestelltes Komma) leistet einer Verwechslung der Adressaten in der Tat Vorschub. Deshalb ist es geboten, die Adressierung zu ändern – ganz abgesehen von der Schutzbedürftigkeit der Daten, die in den Sendungen enthalten sind. Auf unsere Anfrage hin kündigte die für diese Schreiben verantwortliche Stelle an, dass die Adressierung im Rahmen der Neugestaltung des EDV-Programms geändert werde und ab Mai 2003 Schreiben mithilfe des neuen Programmmoduls erstellt würden. Die verantwortliche Stelle unterbrach jedoch die entsprechenden Programmierarbeiten, um u. a. Gesetze, Tarifverträge, Verordnungen und Verwaltungsvorschriften mit kurzzeitigem Wirkungszeitpunkt vorrangig programmtechnisch umsetzen zu können. Sie strebte daraufhin an, die ersten Schreiben mit den neu gestalteten Adressfeldern bis Ende des Jahres 2003 zu versenden. Unseren Vorschlag, dem vorangestellten Nachnamen zunächst wenigstens ein Komma anzufügen, um ihn so als solchen kenntlich zu machen, lehnte die verantwortliche Stelle aus wirtschaftlichen Gründen ab. Wie wir feststellen konnten, waren die Mitteilungen über die Zusammensetzung der Bezüge im Dezember 2003 „neu“ adressiert: In der Anschrift erschien der Vorname vor dem Nachnamen. Auf unseren Hinweis, dass bei Beihilfebescheiden noch im Juni 2004 die „alte“ Adressierung verwendet werde, erklärte die verantwortliche Stelle unter Verweis auf die Einsparungen bei den dortigen Personalstellen, sie werde die entsprechenden Programme sukzessive auf die „neue“ Adressierung umstellen und gehe davon aus, dass diese in allen Fällen mit Beginn des Jahres 2005 verwendet werde. Nun bleibt zu hoffen, dass dieses Ziel erreicht wird und dann auch das Nebeneinander der „alten“ und der „neuen“ Adressierung endet, denn dieses hat zur Folge, dass für Herrn Werner bestimmte Besoldungsmitteilungen gleich adressiert sind wie für Herrn Peter bestimmte Beihilfebescheide (nämlich mit der Namensbe-

zeichnung „Peter Werner“ – oder doch umgekehrt?). Wirtschaftliche Überlegungen bei Umprogrammierungsmaßnahmen sind schön und gut – der Datenschutz darf deshalb aber nicht auf Dauer auf der Strecke bleiben. Meine Dienststelle wird diese Frage deshalb weiter im Blick behalten.

3. Abschnitt: Schul- und Hochschulwesen

1. Evaluation an den Hochschulen

Das Wissenschaftsministerium hat uns an einem Gesetzgebungsverfahren zu einer umfassenden Hochschulreform beteiligt. Mit einem Zweiten Gesetz zur Änderung hochschulrechtlicher Vorschriften sollen u. a. die bisher bestehenden vier Hochschulgesetze, nämlich das Universitätsgesetz, das Fachhochschulgesetz, das Gesetz über die Pädagogischen Hochschulen und das Kunsthochschulgesetz, zu einem verschlankten und deregulierten Landeshochschulgesetz zusammengefasst werden.

Wir haben uns insbesondere mit den in § 5 des Entwurfs eines Landeshochschulgesetzes (LHG-E) vorgesehenen Regelungen über die Evaluation befasst. Die hierzu beabsichtigte Neuregelung ist aus datenschutzrechtlicher Sicht schon deshalb zu begrüßen, weil damit die in den bisherigen Hochschulgesetzen jeweils verstreuten Regelungen in einem einzigen Paragraphen zusammengefasst werden. Die Neuregelung „aus einem Guss“ dient nicht nur dem Komfort der Leser, die bislang durch entsprechendes Hin- und Herblättern in Gesetzestexten strapaziert werden. Sie dient auch der Rechtsklarheit. So ist es etwa zur datenschutzrechtlichen Beurteilung universitärer Evaluationen bislang unter Umständen erforderlich, neben den grundlegenden Regelungen des § 4 a Abs. 2 und 3 des Universitätsgesetzes (UG) auch die Vorschriften des § 125 a Abs. 4 UG für Lehrveranstaltungsevaluationen ins Auge zu fassen. Dabei muss man sich eventuell mit der Frage befassen, in welchem Verhältnis diese Regelungen zueinander stehen und was es bedeutet, wenn nach § 4 a Abs. 2 Satz 4 UG der § 125 a Abs. 4 UG „unberührt“ bleibt. Mit der vom Wissenschaftsministerium vorgesehenen Neuregelung würde es möglich, ohne einen solchen Aufwand und ohne die damit verbundenen Anwendungsschwierigkeiten die für eine Evaluation maßgeblichen Regelungen einem einzigen, klar gegliederten Paragraphen zu entnehmen. Unserer Stellungnahme, in der wir einige Fragen zum Datenschutz aufgeworfen hatten, folgte eine weitere, durchaus konstruktive Abstimmung mit dem Wissenschaftsministerium. So konnten letztlich alle datenschutzrechtlichen Problemstellungen durch entsprechende Änderungen des vorgesehenen Gesetzestextes und Anpassungen der Gesetzesbegründung bereinigt werden. Im Einzelnen:

Nach § 5 Abs. 1 Satz 5 LHG-E sollen die Ergebnisse einer Evaluation veröffentlicht werden. Bei diesen zur Veröffentlichung vorgesehenen Ergebnissen handelt es sich nicht um personenbezogene Daten. Es kann also beispielsweise nicht Gegenstand einer solchen Veröffentlichung sein, welche bestimmten oder bestimmbaren Personen im Rahmen einer Evaluation welche Bewertungen abgegeben (etwa Studierende) oder erfahren (etwa Hochschullehrer) haben. Dies ergibt sich zwar nicht unmittelbar aus dem Text des § 5 Abs. 1 Satz 5 LHG-E. Es ist aber der mit dem Wissenschaftsministerium abgestimmten Gesetzesbegründung zu entnehmen, dass diese Veröffentlichung „keine personenbezogenen Daten im Sinne des Datenschutzrechts“ enthält. Nach § 5 Abs. 2 Satz 4 LHG-E soll es den Hochschulen überlassen sein, in ihren jeweiligen, für die Durchführung einer Evaluation erforderlichen Satzungen u. a. zu bestimmen, in welchem Umfang und in welcher Form personenbezogene Daten innerhalb und außerhalb der Hochschule veröffentlicht werden. Demnach können im Rahmen einer Evaluation personenbezogene Daten nur veröffentlicht werden, wenn und soweit dies in einer entsprechenden Hochschulsatzung vorgesehen ist. Es ist aus datenschutzrechtlicher Sicht hinnehmbar, dass der Gesetzestext keine ins Einzelne gehenden Vorgaben darüber enthält, unter welchen Voraussetzungen und in welchem Umfang eine Hochschule durch entsprechende satzungsrechtliche Regelungen die Möglichkeit zur Veröffentlichung personenbezogener Daten eröffnen darf. Dabei war insbesondere das legitime Ziel der Hochschulrechtsnovelle zu berücksichtigen, dass insgesamt eine

Erweiterung des Verantwortungsbereichs der Hochschulen vorgesehen ist. Eine aus datenschutzrechtlicher Sicht ausreichende Konkretisierung ergibt sich aus der mit dem Wissenschaftsministerium abgestimmten Gesetzesbegründung. Danach gilt: Je unbestimmter und weiter der Adressatenkreis, je größer der Umfang der veröffentlichten Daten, je detaillierter der Bericht, desto stärker muss die Legitimation für eine solchermaßen gestaltete Veröffentlichung sein. Darüber hinaus sind die allgemeinen datenschutzrechtlichen Grundsätze, etwa der Erforderlichkeit, zu beachten.

2. Die multifunktionale Schülerindividualdatei: ein Projekt mit vielen Fragezeichen

Das Kultusministerium hat ein komplexes EDV-Verfahren zur Verarbeitung einer Vielzahl personenbezogener Daten von Schülerinnen und Schülern, deren Erziehungsberechtigten sowie Lehrerinnen und Lehrern entwickelt. Das Projekt nennt sich E-Stat (ein Kürzel für „Elektronische Statistik“). Danach ist unter anderem vorgesehen, Individualdaten aller Schüler an öffentlichen Schulen in Baden-Württemberg zukünftig zentral zu erfassen und deren Nutzung für Statistik- und verschiedene Verwaltungszwecke zu ermöglichen. Die hierzu vorgesehenen weitreichenden Änderungen hinsichtlich der Verarbeitung personenbezogener Daten von Schülern begegnen grundlegenden datenschutzrechtlichen Bedenken. Wir haben das Kultusministerium daher gebeten, eine über den bisherigen Umfang der Schulstatistik hinausgehende Verarbeitung personenbezogener Daten erst dann vorzunehmen oder zu veranlassen, wenn diese Bedenken ausgeräumt sind. Zunächst bleibt das Ergebnis der weiteren Prüfung durch das Kultusministerium abzuwarten. Die im Rahmen des Projekts vorgesehenen Änderungen bei der Verarbeitung personenbezogener Daten von Lehrern werden von uns derzeit noch geprüft.

Im Einzelnen geht es um Folgendes:

Mit E-Stat ist vom Kultusministerium – im Rahmen des Vorhabens SVN (Schulverwaltung am Netz) – die Einführung und Nutzung einer landesweiten EDV-Infrastrukur vorgesehen, mit der sich auf allen Ebenen der Kultusverwaltung und der Schulen verschiedene Vorgänge der Schüler- und Lehrerverwaltung dienststellenübergreifend bearbeiten lassen. Ein wesentlicher Bestandteil dieser EDV-Infrastruktur soll die zentrale Schülerindividualdatei sein, in der für jeden Schüler an einer öffentlichen Schule in Baden-Württemberg ein personenbezogener Datensatz angelegt wird, der neben Namen, Vornamen und Geburtsdatum eine Vielzahl von weiteren Angaben enthält: zum Beispiel das Geburtsland, die Muttersprache, das Übersiedlungsjahr, das Datum der Abmeldung vom Religionsunterricht, Angaben über eine Behinderung und die Teilnahme an Betreuungsangeboten der Schule, die Notwendigkeit der Sprachförderung, die Fremdsprachenfolge sowie die Zuordnung der Schüler zu Unterrichtselementen, die ihrerseits wiederum durch zahlreiche Merkmale konkretisiert werden.

Die Schulen sollen diese personenbezogenen Daten an das Kultusministerium übermitteln, welches sie in einer zentral verwalteten Datenbank, einer sog. operativen Datenbank, speichert. Die operative Datenbank soll von den Schulen für verschiedene Verwaltungszwecke genutzt werden:

- Schulen, die über kein Schulverwaltungsprogramm verfügen, sollen das Verfahren E-Stat auch als Schulverwaltungsprogramm nutzen können.
- Zudem sollen Schulen im Rahmen von schulübergreifenden Unterrichtsformen und Kooperationen (z. B. für gemeinsame Neigungskurse benachbarter Gymnasien oder bei Außenklassen von Sonderschulen an allgemeinen Schulen) die in der zentralen Schülerindividualdatei gespeicherten Daten von Schülern einer anderen Schule für die Unterrichtsorganisation nutzen können (z. B. zur Erstellung einer namentlichen Klassenliste für den Klassenlehrer oder zur Pflege des Kontakts mit den Schülern).
- Wenn Schüler die Schule wechseln, soll die aufnehmende Schule deren Stammdaten der operativen Datenbank entnehmen können.
- Berufliche Vollzeitschulen sollen mit Hilfe von E-Stat Mehrfachbewerbungen von Schülern erkennen können.

Zur statistischen Auswertung sollen die Schülerdatensätze, ohne Angabe von Namen, Vornamen, Geburtstag, Geburtsort und Straße, dafür aber unter Verwendung einer landesweit eindeutigen Schüler-Identifikationsnummer (Schüler-ID), in eine so genannte Auswertungsdatenbank übernommen werden. Diese soll zudem Daten für ein Führungsinformationssystem der Kultusverwaltung bereitstellen.

In mehreren Eingaben wurde meine Dienststelle gebeten, das Projekt E-Stat in datenschutzrechtlicher Hinsicht zu prüfen. Von einer Seite wurde u. a. die Befürchtung geäußert, dass mit diesem Verfahren der „gläserne Schüler“ möglich gemacht werde. Als diese Eingaben bei uns eingingen, war uns das Verfahren E-Stat zwar nicht völlig unbekannt. Aufgrund der bis dahin vom Kultusministerium zur Verfügung gestellten Informationen gingen wir allerdings seinerzeit noch davon aus, dass es bei dem Projekt E-Stat im Wesentlichen darum gehe, die bislang papiergebundene Schulstatistik in ihrem bisherigen – durch entsprechende Regelungen im Schulgesetz und in einer Verordnung des Kultusministeriums über statistische Erhebungen an Schulen definierten – Umfang durch die Eröffnung elektronischer Übermittlungswege zu modernisieren. Aus der Stellungnahme des daraufhin befragten Kultusministeriums ergab sich allerdings, dass es diesem nicht mehr nur darum, sondern um die Einführung erheblich ausgeweiteter Datenverarbeitungsvorgänge geht. Die vom Kultusministerium übersandten Unterlagen von über 1 000 Seiten ließen schon gewichtsmäßig ahnen, dass mit E-Stat wohl eine Fülle von personenbezogenen Daten von Schülern verarbeitet und in einer zentralen Schülerindividualdatei gespeichert werden sollten, die bislang im Rahmen der amtlichen Schulstatistik keine Verwendung finden. Derzeit zählen beispielsweise die Namen, Vornamen, Adressen und Telekommunikationsdaten nicht zum Kreis der Erhebungsmerkmale für Schüler in der amtlichen Schulstatistik. Hinzu kommt, dass die Daten künftig nicht mehr nur für die amtliche Schulstatistik, sondern in vielfältiger Weise auch für Verwaltungszwecke verarbeitet werden sollen.

Da vom Kultusministerium vorgesehen ist, die im Rahmen von E-Stat vorgesehene Verarbeitung personenbezogener Daten von Schülern durch eine Änderung des Schulgesetzes abzudecken, haben wir uns zunächst vorrangig mit den Aspekten der Verarbeitung dieser Daten befasst. Nicht zuletzt wegen der Komplexität von E-Stat war die datenschutzrechtliche Beurteilung der vorgesehenen Änderungen des Schulgesetzes mit äußergewöhnlichem Aufwand verbunden. Auf unsere erste Stellungnahme zu einem – gleichfalls ersten – Gesetzentwurf präsentierte uns das Kultusministerium einen zweiten – deutlich geänderten – Entwurfstext. Eine Besprechung des geänderten Entwurfs mit dem Kultusministerium führte dazu, dass das Kultusministerium einen dritten – wiederum deutlich geänderten – Gesetzentwurf erarbeitete. Danach soll das Schulgesetz um die Regelung ergänzt werden, dass die Schulen dem Kultusministerium zu statistischen Zwecken personenbezogene Daten von Schülern im Rahmen einer zentralen Schülerindividualdatei nach Maßgabe einer Rechtsverordnung übermitteln können und die Schülerindividualdatei für die statistischen Auswertungen pseudonymisiert wird. Zudem soll im Schulgesetz geregelt werden, dass „von den ... im Rahmen der zentralen Schülerindividualdatei gespeicherten Daten ... über die statistischen Zwecke hinaus für Schulen die dort zu Verwaltungszwecken erforderlichen personenbezogenen Daten zur Verarbeitung bereitgehalten werden“ können.

In unserer Stellungnahme mussten wir dem Kultusministerium mitteilen, dass sowohl die Darstellung der Verarbeitungsabläufe in der Begründung zum Gesetzentwurf als auch der Gesetzentwurf selbst noch grundlegende datenschutzrechtliche Unzulänglichkeiten aufweisen:

Grundsätzlich spricht aus datenschutzrechtlicher Sicht natürlich nichts dagegen, dass Schulen dem Kultusministerium personenbezogene Daten von Schülern übermitteln, soweit diese für die Erfüllung der Aufgaben des Kultusministeriums bei der Schulstatistik erforderlich sind. Die Unterlagen, die das Kultusministerium uns bislang zugänglich machte, ließen aber nicht erkennen, ob und weshalb alle zur Übermittlung an das Kultusministerium vorgesehenen personenbezogenen Daten jeweils statistischen Zwecken im Sinne des Gesetzentwurfs dienen. Es war auffällig, dass in der Begründung

des Gesetzentwurfs beispielsweise die Telekommunikationsdaten von Schülern als „statistisch nicht relevant“ bezeichnet werden, diese Daten aber gleichwohl zur Übermittlung von den Schulen an das Kultusministerium vorgesehen sind (wohlgemerkt im Zusammenhang mit einer geplanten gesetzlichen Regelung, nach der es den Schulen ausdrücklich möglich sein soll, die zu statistischen – und nicht auch zu sonstigen – Zwecken erforderlichen personenbezogenen Daten von Schülern dem Kultusministerium zu übermitteln). Wir haben das Kultusministerium daher gebeten, hinsichtlich der einzelnen zur Übermittlung vorgesehenen personenbezogenen Daten jeweils konkret darzustellen, ob und weshalb diese Daten statistisch relevant sind bzw. deren Übermittlung statistischen Zwecken im Sinne des Gesetzentwurfs dient. Diese Darstellung könnte etwa im Rahmen einer sowieso erforderlichen Änderung der Verordnung des Kultusministeriums über statistische Erhebungen an Schulen erfolgen. Die Übersendung des Entwurfs einer Änderungsverordnung bleibt deshalb zunächst abzuwarten.

Unabhängig von der demnach noch zu klärenden Frage, welche personenbezogenen Daten von Schülern letztlich überhaupt von den Schulen dem Kultusministerium zu statistischen Zwecken übermittelt werden dürfen und somit Eingang in eine zentrale Schülerindividualdatei finden können, ist es aus datenschutzrechtlicher Sicht insbesondere bedenklich, wenn die oben angesprochene Datennutzung der einzelnen Schulen für Verwaltungszwecke auf dem „Umweg“ über das Kultusministerium und dessen zentrale Schülerindividualdatei realisiert werden soll. Denn nach der uns bekannten Konzeption sollen die Daten der Schüler vom Kultusministerium als verantwortliche Stelle im Sinne des § 3 Abs. 3 LDSG gespeichert und für Schulen zur Verarbeitung bereitgehalten werden. Das Kultusministerium auf diese Weise zum „Herrn der Daten“ zu machen, ist aber zur Erreichung dieser Verwaltungszwecke nicht erforderlich. Vielmehr ist stattdessen die Datenverarbeitung im Auftrag ein nahe liegendes und nach unserem Dafürhalten passendes Instrumentarium, mit dem die verfolgten Zwecke praxis- und datenschutzgerecht erreicht werden können. So ist beispielsweise nicht erkennbar, warum – zur Übermittlung personenbezogener Daten zwischen zwei Schulen im Falle des Schulwechsels eines Schülers – das Kultusministerium in den Übermittlungsprozess als datenschutzrechtlich verantwortliche Stelle eingeschaltet werden müsste. Die Übermittlung der erforderlichen Daten kann vielmehr unmittelbar zwischen den betroffenen Schulen als den dafür verantwortlichen Stellen erfolgen. Dies schließt keineswegs aus, dass dazu vom Kultusministerium die erforderliche technische Infrastruktur zur Verfügung gestellt wird (z. B. die auf einem zentralen Server betriebene E-Stat-Software). Entscheidend aber ist, dass dabei die Schulen die für die Verarbeitung verantwortlichen Stellen bleiben und das Kultusministerium für diese lediglich als Auftragnehmer nach § 7 LDSG tätig wird.

Die abschließende Abstimmung mit dem Kultusministerium steht noch aus.

3. Datenschutz an Schulen: noch „ausreichend“?

Der Gesetzgeber hat es in klare Worte gefasst: Nach dem Landesdatenschutzgesetz melden die öffentlichen Stellen, die keinen behördlichen Datenschutzbeauftragten bestellt haben, von zwei Ausnahmen abgesehen, meiner Dienststelle den Einsatz und die wesentliche Änderung eines automatisierten Verfahrens (vgl. § 32 Abs. 1 LDSG). Was in diesem Fall gemeldet werden soll, ist ebenfalls in verständlicher Sprache ausgedrückt: Sozusagen eine „10-Punkte-Checkliste“ ist es, an die es sich dabei zu halten gilt. Es handelt sich um diejenigen Angaben, die in das Verfahrensverzeichnis einzutragen sind (vgl. § 32 Abs. 2, § 11 Abs. 2 LDSG). Ein solches Verzeichnis der automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, muss nach § 11 Abs. 1 Satz 1 LDSG jede öffentliche Stelle ohnehin führen. Der Aufwand für die oben angesprochene Meldung müsste sich für die öffentlichen Stellen deshalb in – wie wir meinen – überschaubaren Grenzen halten: Grundsätzlich genügt es, das ohnehin vorhandene Verfahrensverzeichnis zu kopieren und mit einem kurzen Begleitschreiben an den Landesbeauftragten für den Datenschutz zu schicken. Zudem hat meine Dienststelle Hinweise zum Verfahrensverzeichnis herausgegeben, die über unsere Internetseite (www.baden-wuerttemberg.datenschutz.de) abgerufen werden können und die das Kultusministerium zudem seiner

Verwaltungsvorschrift „Verarbeitung personenbezogener Daten von Schülerinnen und Schülern sowie von deren Erziehungsberechtigten durch öffentliche Schulen“ vom 18. September 2003 (Kultus und Unterricht S. 382) als Anlage beigefügt hat.

In der jüngeren Vergangenheit gingen von verschiedenen Schulen zahlreiche Meldungen dieser Art ein, wobei sich die Schulen dabei jeweils eines gleichen Vordrucks bedient hatten. Nun ist die Gestaltung der Meldung nicht vorgeschrieben, sondern nur deren Inhalt, und es bleibt somit den Stellen selbst überlassen, wie sie die Meldung einreichen. Verwenden die Stellen dafür einen Vordruck, kann dies von Vorteil sein, da eine gewisse Systematik den Schulen und auch uns die Handhabung der Meldung erleichtern kann. Der Nutzen des besagten Vordrucks war jedoch gering: Auch wenn eine Schule den Vordruck vollständig ausgefüllt an uns schickte, gab sie damit eine ungenügende Meldung ab, da der Vordruck selbst fehlerhaft bzw. unvollständig war. Beispielsweise sah der Vordruck keine Angaben zu den technischen und organisatorischen Maßnahmen zum Datenschutz vor, die in das Verfahrensverzeichnis einzutragen und meinem Amt mitzuteilen sind (vgl. § 11 Abs. 2 Nr. 10, § 9 LDSG). Weiter enthielt der Vordruck zur Art der gespeicherten Daten die Mitteilung: „Es werden nur Merkmale gespeichert, die in der Verwaltungsvorschrift aufgeführt sind (s. Erläuterung)“. Um welche Verwaltungsvorschrift es sich dabei handelte, war jedoch dem Vordruck nicht zu entnehmen; auch enthielten die ausgefüllten Vordrucke keine entsprechenden Erläuterungen, so dass die Art der verarbeiteten personenbezogenen Daten nicht festzustellen war. Wenn gerade von ausgefüllten Vordrucken die Rede war, so darf daraus leider keineswegs geschlossen werden, dass die unzureichenden Vordrucke wenigstens vollständig ausgefüllt waren. Von den hierher übersandten Varianten nur teilweise ausgefüllter Vordrucke sei allein auf das inhaltliche Schlusslicht eingegangen: Dort waren lediglich Name und Anschrift der Schule sowie das Datum eingetragen; die Erklärung, eine Verhaltens- oder Leistungskontrolle der Beschäftigten mittels EDV finde nicht statt, war angekreuzt und die Unterschrift der Schulleitung mit Datum war beigefügt. Weder angekreuzt noch ergänzt waren die im Vordruck vorgesehenen Angaben, ob Gegenstand der Meldung die Einführung, Anwendung, wesentliche Änderung oder wesentliche Erweiterung der automatisierten Verarbeitung personenbezogener Daten von Beschäftigten ist, zur Erfüllung welcher Aufgaben die Daten verarbeitet werden, auf welchen Rechtsgrundlagen die Verarbeitung beruht, welcher Art die gespeicherten Daten sind, welche Personen zugriffsberechtigt sind sowie welche Hardware und Software eingesetzt wird.

Damit die Schulen nicht weiter von diesem Vordruck Gebrauch machen – denn ihre Zahl riss nicht ab – übersandten wir ein (anonymisiertes) Musterexemplar hiervon dem Kultusministerium, teilten diesem mit, dass der verwendete Vordruck den gesetzlichen Anforderungen nicht entspreche und er zudem teilweise unvollständig ausgefüllt werde, und baten es, sich der Angelegenheit nochmals anzunehmen. (Nochmals, weil sich meine Dienststelle bereits im Jahr 2002 nach mehreren „Falschmeldungen“ von Schulen, und zwar zum bereits im Jahr 2000 abgeschafften „Datenschutzregister“, an das Kultusministerium gewandt hatte, das daraufhin die Oberschulämter auf die aktuelle Rechtslage hinwies und sie bat, auch die Schulen darüber zu informieren.)

Das Kultusministerium übersandte daraufhin unser Schreiben unter Hinweis auf die Rechtslage an die Oberschulämter (ohne den von uns bemängelten Vordruck, den die Schulen ja nicht verwenden sollen), von dort gelangte es zu den Schulen. Das, was dann folgte, hatten wir uns so aber nicht vorgestellt: Unsere Telefone liefen heiß. Am Apparat: zumeist Rat suchende Schulleiter und Beschäftigte der Schulverwaltung mit Fragen, was denn mit der Meldung, mit einem Verfahrensverzeichnis sowie mit einem automatisierten Verfahren gemeint sei und was unser Schreiben denn überhaupt zu bedeuten habe. Kämpferische Rektoren erklärten, dass sie „das alles nicht einsehen“ wollten, sich sogar einfach nur untätig und trotzig „auf den Hosenboden setzen“ wollten (obwohl stattdessen „Nachsitzen“ angesagt wäre), und räumten ein, man könne in der Schule mit unserem Schreiben nichts anfangen und/oder unseren Forderungen wegen der notwendigen Aufrechterhaltung des Lehrbetriebs nicht nachkommen. Und immer wieder die Bitte,

der Schule doch freundlicherweise den in unserem Schreiben erwähnten Vordruck zur Verfügung zu stellen, da man ihn dort leider nicht habe. Viele Schulen wandten sich auch schriftlich an meine Dienststelle, oft mit Fragen, doch auch mit „Meldungen“ wie: „An unserer Schule werden die notwendigen und üblichen Daten verwendet“ (bis auf den Briefkopf und die Grußformeln vollständig wiedergegeben) sowie etlichen weiteren unvollständigen Meldungen fast jeder Art – auch mit dem von uns bemängeltem Vordruck. Wir wiesen daraufhin die Schulen nochmals schriftlich auf die gesetzlichen Anforderungen und unsere Hinweise zum Verfahrensverzeichnis (mit der WWW-Adresse des Dokuments) hin. Doch auch dies half nicht (immer), wie bei der Schule, deren erneute Meldung unklar und unvollständig war und u. a. die Angabe der Rechtsgrundlage der Datenverarbeitung vermissen ließ, obwohl diese Angabe ausdrücklich vorgeschrieben ist (vgl. § 11 Abs. 2 Nr. 3 LDSG). Ebenfalls in unserer Post: an das Kultusministerium adressierte Schreiben und Telefaxe, die jedoch an unsere Postfachadresse bzw. Telefaxnummer geschickt wurden. Zudem erhielten wir noch immer Meldungen zum inzwischen längst abgeschafften „Datenschutzregister“ (s. o.) oder Meldungen, die auf eine Verwaltungsvorschrift des Kultusministeriums Bezug nahmen, welche zum Zeitpunkt der Meldung bereits rund ein Jahr außer Kraft getreten und durch eine neue Verwaltungsvorschrift ersetzt worden war. Kurios auch die Mitteilung einer Schule, wonach sie „den beigefügten Vordruck leider nicht erhalten“ habe und darum um dessen Zusendung bitte, und zuletzt sogar die telefonische Frage einer Schule an uns, wie sie es denn vermeiden könne, weitere Schreiben des Oberschulamts in dieser Sache zugesandt zu bekommen. Mehrere hierdurch beschäftigte Mitarbeiter meiner Dienststelle können bestätigen: Eigentlich war alles Mögliche und vor allem Unmögliche dabei.

Zu all dem kann Folgendes gesagt werden: Das Echo der Schulen auf unsere Initiative hin hat gezeigt, dass dort – jedenfalls aus der Sicht des Datenschutzes – viel Nachholbedarf zu bestehen scheint und die Irritation um die Meldepflicht quasi nur „die Spitze eines Eisbergs“ sein könnte. Die Probleme mancher Schulen, eine vollständige und inhaltlich korrekte Meldung anzufertigen, deuten darauf hin, dass dort darüber hinaus Unklarheiten über das bereits angesprochene Verfahrensverzeichnis bestehen sowie möglicherweise auch über sonstige datenschutzrechtliche Vorschriften. Soweit Schulen jedoch die für sie geltenden datenschutzrechtlichen Vorschriften nicht kennen, bleibt es dem Zufall überlassen, ob diesen im Ergebnis entsprochen wird oder ob diese Schulen Schüler, deren Erziehungsberechtigte oder Lehrer in ihrem Recht auf informationelle Selbstbestimmung verletzen. Solchen Rechtsverstößen können die Schulen gerade auch dadurch vorbeugen, dass sie das gesetzlich vorgeschriebene Verfahrensverzeichnis erstellen. Dazu müssen sie zunächst feststellen und sodann dokumentieren, welche personenbezogenen Daten sie auf welchen Rechtsgrundlagen mit Hilfe welcher automatisierten Verfahren auf welche Weise verarbeiten und welche Datenschutzmaßnahmen sie dazu getroffen haben. Ein solcher Überblick über die Datenverarbeitung ermöglicht eine effektive datenschutzrechtliche Eigenkontrolle, denn so kann und muss die Schule etwa prüfen, auf welchen Rechtsgrundlagen sie die personenbezogenen Daten jeweils verarbeiten darf. Nachholbedarf beim Datenschutz dürfte allerdings nicht nur bei Schulen festzustellen sein. Dafür spricht eine Meldung, die eine Schule an ein Staatliches Schulamt adressiert hatte: Sie enthielt nur einen Bruchteil der vorgeschriebenen Angaben, nämlich die Art der gespeicherten (Schüler-, Eltern- und Lehrer-)Daten, und kein Wort zu den anderen Angaben, sie entsprach also nicht annähernd den gesetzlichen Vorgaben. Gleichwohl wies das Staatliche Schulamt (soweit von hier aus nachzuvollziehen) die Schule nicht auf diesen Mangel hin, sondern beschränkte sich darauf, die handschriftlich auf der Meldung notierte Frage zu beantworten, wer diese bekomme, nämlich der Landesdatenschutzbeauftragte.

Naturgemäß erfahren wir es seltener, wenn eine Stelle sich datenschutzgerecht verhält. Die Schulen, die sich nicht Hilfe und Rat suchend hierher wenden mussten und deren Meldungen ordnungsgemäß sind, sollen daher nicht unter den Tisch fallen. Dem gegenüber steht jedoch eine viel zu große Zahl von Schulen, die Mängel bei der Beachtung des Datenschutzes erkennen lassen. Aus diesem Grund haben wir uns in dieser Sache nochmals an

das Kultusministerium gewandt mit der Bitte, das Thema Datenschutz bei den Schulen noch mehr ins Bewusstsein zu rücken.

Wie bereits erwähnt, sind unsere Hinweise zur Meldepflicht und zum Verfahrensverzeichnis immerhin Anlage einer Verwaltungsvorschrift des Kultusministeriums zur Verarbeitung personenbezogener Daten durch öffentliche Schulen. Es ist zu hoffen, dass in den Schulen diesen Vorschriften und Hinweisen zum Datenschutz künftig mehr Beachtung geschenkt wird und vor allem, dass sie in die Tat umgesetzt werden. Auch für die öffentlichen Schulen dürfte dabei von Interesse sein, dass sie bestimmte Angaben des Verfahrensverzeichnisses (unter anderem zu Zweckbestimmung und Rechtsgrundlage der Verarbeitung, zur Art der gespeicherten Daten, zum Kreis der Betroffenen und zu den Empfängern der Daten) auf Antrag jedermann in geeigneter Weise verfügbar zu machen haben (vgl. § 11 Abs. 4 Satz 1 LDSG).

Noch länger in Erinnerung bleiben wird uns das Telefongespräch mit einer Schule. Der Beschäftigte der Schule teilte in unerschütterlicher Überzeugung mit: „Sie brauchen sich aber auch keine Sorgen zu machen. Bei uns sind nur Beamte mit diesen Aufgaben betraut, die Rechtmäßigkeit ist also gewährleistet“. Na dann ...

4. Die Filterung von E-Mails durch eine Universität

Aufgrund einer Eingabe befassten wir uns mit datenschutzrechtlichen Aspekten der Filterung von E-Mails. Der Beschwerdeführer teilte mit, dass eine Universität in Baden-Württemberg auf den E-Mail-Systemen einer ihrer Fakultäten alle E-Mails blockiere, in deren Kopf – also zum Beispiel unter „Absender“, „Empfänger“, „Cc“ und „Betreff“ – der Name des Beschwerdeführers vorkommt. Dabei würden sowohl die E-Mails blockiert, die der Beschwerdeführer an die Universität sendet, als auch diejenigen, die von dort an ihn gesandt werden sollen. Meine Dienststelle hat die Universität dazu um Stellungnahme gebeten. Einer ersten Äußerung der Universität war zu entnehmen, dass die E-Mail-Server der Fakultät aufgrund eines an den Beschwerdeführer gerichteten Schreibens des Dekans der Fakultät tatsächlich solche E-Mails zurückweisen, die in ihrem Kopf den Namen des Betroffenen enthalten. Da eine abschließende Stellungnahme der Universität noch aussteht, war uns eine vollständige datenschutzrechtliche Prüfung dieser Angelegenheit leider noch nicht möglich. Die Beschwerde gibt jedoch Anlass – ohne das Ergebnis einer eingehenden Prüfung vorwegnehmen zu wollen – in allgemeiner Form auf einige datenschutzrechtliche Aspekte der Filterung von E-Mails einzugehen:

Öffentliche Stellen, die durch entsprechende technische Vorkehrungen beim Betrieb ihrer E-Mail-Server an sie gerichtete oder von dort zu versendende E-Mails hinsichtlich des Namens von Personen durchsuchen, um die herausgefilterten E-Mails zu blockieren oder in sonstiger Weise selektiv zu behandeln, verarbeiten damit personenbezogene Daten der betroffenen Namensträger. Um die E-Mails auf das Vorkommen des Namens einer bestimmten Person zu durchsuchen, muss dieser Name – bei dem es sich zweifellos um ein personenbezogenes Datum im Sinne des Landesdatenschutzgesetzes handelt – im EDV-System gespeichert sein. Bei dieser Speicherung und der Nutzung zur Filterung handelt es sich um Erscheinungsformen der Verarbeitung personenbezogener Daten nach der Begriffsbestimmung des § 3 Abs. 2 Satz 1 LDSG. Für eine solche Speicherung und Nutzung gelten die allgemeinen Anforderungen des § 4 Abs. 1 LDSG: Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Als weitere Rechtsvorschriften, die je nach Fallkonstellation hierbei zu berücksichtigen sind, kommen insbesondere das Telekommunikationsgesetz und dessen Regelungen zu Inhalt und Anwendungsbereich des Fernmeldegeheimnisses in Frage. Eine öffentliche Stelle hat danach in jedem Einzelfall vor dem Beginn einer entsprechenden Verarbeitung personenbezogener Daten zu prüfen, ob eine solche Verarbeitung durch Rechtsvorschriften erlaubt ist oder, wenn das nicht der Fall ist, eine entsprechende Einwilligung des Betroffenen vorliegt. Zudem muss in die Prüfung einbezogen werden, ob darüber hinaus personenbezogene Daten des Namensträgers verarbeitet werden, etwa im Rahmen einer elektronischen

Dokumentation von Filterungsvorgängen, in welcher eventuell im Zusammenhang mit dem zur Filterung verwendeten Namen die Anzahl der gefilterten E-Mails, die Zeitpunkte der Filterung oder weitere Einzelheiten (z. B. der jeweilige „Betreff“ der gefilterten E-Mails – welcher in der Regel Rückschlüsse auf den Inhalt der E-Mails erlaubt) gespeichert werden. Von einer solchen weiteren Speicherung zum Zweck der Dokumentation können neben dem Namensträger, dessen Name für die Filterung von E-Mails gespeichert wurde, auch andere Personen hinsichtlich ihrer personenbezogenen Daten betroffen sein. Das wäre beispielsweise dann der Fall, wenn auch die Namen der Personen gespeichert werden, die per E-Mail den Namensträger anschreiben wollten oder von diesem angeschrieben werden sollten. Wie man sieht, ist die Filterung von E-Mails jedenfalls nicht ohne datenschutzrechtliche Tücken.

4. Abschnitt: Sonstiges

1. Steuerehrlichkeit: Ja, aber nicht ohne ausreichenden Datenschutz!

Das Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003, dessen Amnestieregelungen für Schwarzgeldsünder bereits ein breites Echo gefunden hatten, steht erneut im Blickpunkt des öffentlichen Interesses. Diesmal geht es um die in diesem Gesetz ebenfalls vorgesehenen weit reichenden Möglichkeiten für Behörden und Gerichte, durch den automatisierten Abruf von Kontoinformationen bei Kreditinstituten auf Bankdaten zuzugreifen. Die neuen gesetzlichen Vorschriften des § 93 Abs. 7, 8 und des § 93 b der Abgabenordnung (AO) sollen am 1. April 2005 in Kraft treten. Danach ist vorgesehen, dass Finanzbehörden und eine Vielzahl anderer Behörden und Gerichte aufgrund automatisierter Abrufe Kontoinformationen erhalten können, die von den Kreditinstituten nach § 24 c des Kreditwesengesetzes bislang nur zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung zum automatisierten Abruf bereitgehalten werden; diese Regelung war seinerzeit eine der Konsequenzen aus den Ereignissen des 11. September 2001. Bei diesen Kontoinformationen handelt es sich neben den Kontonummern oder Nummern eines Depots insbesondere um die Namen und Geburtsdaten der Konto- und Depotinhaber und der Verfügungsberechtigten sowie um die Namen und Anschriften der sonst wirtschaftlich Berechtigten. Die Kontostände sind nicht Bestandteil der Kontoinformationen, können aber unter Umständen im Rahmen weiterer Überprüfungen erhoben werden.

Die vorgesehenen Regelungen begegnen in zweifacher Hinsicht datenschutzrechtlichen Bedenken: Zum einen ist nicht sichergestellt, dass die Betroffenen von einem automatisierten Abruf ihrer Daten überhaupt etwas erfahren. Nach den bislang bekannt gewordenen Vorstellungen der Finanzverwaltung sollen die Betroffenen von einer automatisierten Abfrage ihrer Daten nur dann etwas erfahren, wenn diese Abfrage zu einer Diskrepanz zwischen den dabei erhobenen Daten und früheren Angaben der Betroffenen führt und die Betroffenen von der zuständigen Behörde mit diesem Umstand konfrontiert werden. Angesichts des verfassungsrechtlichen Transparenzgebots und der Rechtsschutzgarantie des Artikels 19 Abs. 4 GG kann es nicht von diesen Voraussetzungen und den damit eventuell verbundenen Zufälligkeiten abhängen, ob Betroffene über den Umstand eines automatisierten Abrufs ihrer Daten informiert werden. Es ist für die Betroffenen zur Erlangung effektiven Rechtsschutzes unabdingbar, dass sie über einen automatisierten Abruf ihrer Daten informiert werden.

Ein weiteres datenschutzrechtliches Problem besteht darin, dass neben den Finanzbehörden eine unbestimmte Vielzahl weiterer Behörden Zugriff auf die Bankdaten erhalten soll. Nach § 93 Abs. 8 AO sollen Behörden auf ein entsprechendes, an Finanzbehörden gerichtetes Ersuchen im Wege eines automatisierten Abrufs Kontodaten erhalten können, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Angesichts der Vielzahl von Begriffen im Einkommensteuergesetz und aufgrund

der nach dem Wortsinn sehr weit reichenden und nur schwer abgrenzbaren Voraussetzung des Anknüpfens an solche Begriffe, bleibt letztlich unklar, welche Behörden unter welchen Voraussetzungen berechtigt sind, solche Ersuchen an die Finanzbehörden zu richten und daraufhin Kontoinformationen zu erhalten. Um dem verfassungsrechtlichen Gebot der Normenklarheit gerecht zu werden, muss diese Unbestimmtheit der gesetzlichen Regelung ausgeräumt werden.

Zusammen mit den anderen Landesbeauftragten unterstütze ich den für die Bundesgesetzgebung zuständigen Bundesbeauftragten für den Datenschutz dabei, den Gesetzgeber zu veranlassen, diese Regelungen mit dem Ziel zu überarbeiten, dem Recht auf informationelle Selbstbestimmung den gebotenen Stellenwert zukommen zu lassen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 26. November 2004 hierzu eine entsprechende Entschließung gefasst (s. Anhang 10). Um Probleme bei der Rechtsanwendung zu vermeiden, die sich unter Umständen auch im Rahmen meiner Zuständigkeit ergeben können, wäre es dringend zu begrüßen, wenn die geforderte Gesetzesänderung noch vor dem Inkrafttreten der oben dargestellten Regelungen realisiert wird.

2. Datenschutz im Verfahren nach dem Landesenteignungsgesetz

Mit dem Landesmessegesetz vom 15. Dezember 1998 war es sozusagen amtlich: „Als Maßnahme zur Stärkung der wirtschaftlichen Infrastruktur wird für das Land Baden-Württemberg eine Landesmesse errichtet. Standort, Größe und Ausstattung der Landesmesse sollen den Bedürfnissen überregionaler und internationaler Messen und Ausstellungen entsprechen, insbesondere der Präsentation für ein nationales und internationales Publikum und der Veranstaltung von Kongressen und Tagungen.“ So lautet § 1 Abs. 1 des Landesmessegesetzes. Vom Gesetzesbeschluss bis zur Realisierung des Landesprojekts ist es allerdings ein langer und beschwerlicher Weg. Notfalls können derartige Projekte auch nur gegen den Widerstand der Betroffenen durchgesetzt werden. Der Gesetzgeber hat daher in den §§ 7 und 8 des Landesmessegesetzes Folgendes bestimmt: „Für Zwecke des Baues und des Betriebes der Messe ist die Enteignung zugunsten des Trägers des Vorhabens zulässig, soweit sie zur Ausführung eines ... festgestellten und vollziehbaren Plans notwendig ist ... Ist der sofortige Beginn von Bauarbeiten geboten und weigert sich der Eigentümer oder Besitzer, den Besitz eines für die Baumaßnahme benötigten Grundstücks ... zu überlassen, so hat die Enteignungsbehörde den Träger des Vorhabens auf Antrag nach Feststellung des Plans in den Besitz einzuweisen“. So kam es dann auch. Nach dem Scheitern der Grunderwerbsverhandlungen beantragte die Projektgesellschaft Neue Messe GmbH & Co. KG, das Verfahren zur Enteignung durchzuführen und den Projektträger vorzeitig in den Besitz der Flächen einzuweisen. Zuständige Enteignungsbehörde war das Regierungspräsidium Stuttgart, dem diese knifflige und emotionsgeladene Aufgabe auf der Grundlage des Enteignungsgesetzes zufiel.

Einmal beantragt, gingen die Enteignungsverfahren ihren Gang. Zu diesem Zweck ist die Gemeinde, in deren Gebiet sich das zu enteignende Grundstück befindet, gesetzlich gehalten, das Enteignungsverfahren mindestens zwei Wochen vor dem ersten Termin zur mündlichen Verhandlung öffentlich bekannt zu machen. So war unter anderem im Amtsblatt der Stadt Leinfelden-Echterdingen eine solche Bekanntmachung des Regierungspräsidiums zu lesen, in welcher die Person des zu enteignenden Grundstückseigentümers mit Name und Anschrift bezeichnet war. Daneben war u. a. auch das entsprechende Flurstück sowie dessen Größe angegeben. Zu viel der Information, wie wir meinten, denn für eine solch umfangreiche öffentliche Bekanntmachung fehlt der Enteignungsbehörde die gesetzliche Erlaubnis. Das Regierungspräsidium sah dies anders. Erst die Namensangabe des Eigentümers ermögliche es Dritten, das Grundstück hinreichend sicher zu identifizieren, um damit etwaige Rechte noch geltend machen zu können. Zur Konkretisierung des Enteignungsgegenstands sei die Angabe des Eigentümers somit zwingend erforderlich. Dies mag so sein oder auch nicht. Tatsache jedenfalls ist, dass bereits das Bundesverfassungsgericht feststellte: Eine Bekanntmachung ist die „intensivste Form einer Übermittlung personenbezogener Daten“. Für einen solchen Grundrechtseingriff be-

darf es aber einer gesetzlichen Grundlage. Der Bundesgesetzgeber hat diese beispielsweise für Enteignungen nach dem Baugesetzbuch geschaffen, in dem er die Nennung der im Grundbuch eingetragenen Eigentümer für die öffentliche Bekanntmachung dort ausdrücklich vorschreibt. Anders dagegen das Enteignungsgesetz des Landes: Hier fehlt eine entsprechende ausdrückliche Regelung. Den Gesetzesmaterialien war vielmehr zu entnehmen, dass der notwendige Inhalt der Bekanntmachung eindeutig festgelegt ist, und dies ohne Bezeichnung des Eigentümers, so jedenfalls die Ansicht des Innenministeriums im Rahmen des Gesetzgebungsverfahrens.

Das angesprochene Regierungspräsidium reagierte prompt. Die Enteignungsbehörde werde unsere Hinweise künftig beachten, hieß es in einer eiligst verfassten Pressemitteilung. So weit, so gut. Das Präsidium konnte es sich allerdings nicht verkneifen, nochmals „nachzutreten“ und erklärte öffentlich und unverzagt, gleichwohl rechtmäßig gehandelt zu haben. Es übersah dabei, dass eine gesetzliche Ermächtigung für eine so weit gehende öffentliche Bekanntmachung im Landesenteignungsgesetz nach wie vor fehlt. Auch der Hinweis des Regierungspräsidiums, dass die vorgenommene Bekanntmachung schon deshalb datenschutzrechtlich zu akzeptieren sei, weil die Namen und Anschriften der betroffenen Grundstückseigentümer mit den Planunterlagen bereits im vorausgegangenen Planfeststellungsverfahren öffentlich ausgelegen hatten, kann nicht dazu führen, dass die Daten der durch die Enteignungsmaßnahmen Betroffenen nicht mehr schutzwürdig sind. Denn die Information darüber, dass ein Grundstückseigentümer nach den Vorstellungen des Antragstellers zu einem bestimmten Zweck enteignet werden soll, hat einen ganz anderen Aussagegehalt als die bloße Tatsache, dass ein Grundstück im Planungsbereich eines Vorhabens liegt.

Darüber hinaus musste die Praxis des Regierungspräsidiums aber auch in weiteren Punkten gerügt werden: In einem Schreiben zur Anhörung sowie zur Ladung eines Betroffenen zur mündlichen Verhandlung wurden auch andere, von weiteren Enteignungsverfahren betroffene Eigentümer aufgeführt und deren Verhandlungstermine mitgeteilt. Einer anderen Betroffenen wurde ein Auszug aus dem Grunderwerbsverzeichnis mitgeliefert, der weitere Grundstücke sowie die zugeordneten Daten der jeweiligen Eigentümer auswies; außerdem enthielten ihre Unterlagen Sammel-Einlieferungsbelege der Deutschen Post, aus denen sich weitere Empfänger von Einschreiben ergaben.

3. Pressearbeit bei der Auszeichnung von Lebensrettern – so nicht!

Tue Gutes und rede darüber, so lautet eine Grundregel der Öffentlichkeitsarbeit. Gilt sie immer, oder ist es manchmal nicht doch besser, nichts in die Öffentlichkeit zu tragen? Diese Frage stellt sich bei der Auszeichnung von Lebensrettern, die beherzt eingegriffen und jemand davor bewahrt haben, sich das Leben zu nehmen. Natürlich gehören auch sie wie alle Lebensretter geehrt. Sie haben es wirklich verdient. Aber müssen dabei in aller Öffentlichkeit Umstände der guten Tat zur Sprache gebracht werden, so dass sie anderntags in der Zeitung stehen? Der Zeitungsleser, mag man einwenden, kann ja sowieso nicht ahnen, um wen es dabei geht, wenn nur der Name der geretteten Person aus dem Spiel bleibt. Wie mag sich aber die gerettete Person fühlen, wenn sie durch die Berichterstattung über die öffentlich inszenierte Auszeichnung der Lebensretter ihren Versuch, sich das Leben zu nehmen, nochmals vor Augen geführt bekommt? Doch nicht darum geht es hier, sondern um die Gedankenlosigkeit, mit der die Pressestelle der Landesregierung bei der Auszeichnung dreier Lebensretter den Namen der geretteten Person und die näheren Umstände, wie diese sich das Leben nehmen wollte, an anwesende Journalisten herausgegeben hat.

Zu der Auszeichnung der drei Lebensretter hatte die Pressestelle der Landesregierung die Damen und Herren der Presse, des Hörfunks und der Fernsehredaktionen eingeladen. Für die anstehende Auszeichnung brachte ein Mitarbeiter der Pressestelle einige Informationen zu Papier. In diesem Schriftstück war die gerettete Person mit Vor- und Familiennamen und ihrem Alter genannt. Ferner war erwähnt, an welchem Tag und zu welcher Tageszeit es in welcher Straße zu dem Suizidversuch gekommen war. Nach dem Gesamtzusammenhang erschloss sich daraus auch, in welcher Stadt

sich der Vorfall abgespielt hatte. Schließlich konnte man in dem Schriftstück Näheres dazu lesen, wie sich die gerettete Person den drei Lebensrettern gegenüber verhalten hatte und von welcher Statur sie war. Bei diesem Schriftstück hat es sich nach den Angaben der Pressestelle der Landesregierung um einen internen Vermerk gehandelt, der allein zur Information der Mitarbeiter, die zur Betreuung der geladenen Journalisten eingeteilt waren, gedient habe. Von diesem Schriftstück sind auf Anordnung der Leitung der Pressestelle bei der Auszeichnung der drei Lebensretter etwa 20 Kopien gefertigt und auf entsprechende Bitte an Journalisten verteilt worden. Dazu habe sie sich infolge von Nachfragen anwesender Journalisten nach schriftlichen Informationen veranlasst gesehen. Der genaue Inhalt des Schriftstücks sei ihr dabei nicht bekannt gewesen. Dass in dem Vermerk der Name der geretteten Person und weitere Angaben über sie gestanden haben, sei für sie nicht vorhersehbar gewesen, weil solche Angaben – wie die Pressestelle der Landesregierung uns gegenüber betonte – von ihr, auch in internen Vermerken, grundsätzlich nicht gemacht würden.

Man muss kein Experte im Datenschutzrecht sein um zu wissen, dass solche außerordentlich sensiblen Daten nicht an Dritte gelangen dürfen. Solches darf auch nicht versehentlich passieren, weil das Bekanntwerden dieser Daten in den Kernbereich der Persönlichkeit der geretteten Person eingreift. Dass es bei der Auszeichnung der drei Lebensretter gleichwohl dazu gekommen ist, hatte mehrere Ursachen: Der Kardinalfehler war, dass die Pressestelle der Landesregierung den Namen der geretteten Person und weitere personenbezogene Daten über sie überhaupt in den internen Vermerk geschrieben hat, anstatt diesen Vermerk zu anonymisieren. Sodann hätte die Pressestelle den Vermerk mit dem Namen der geretteten Person nicht ihren Mitarbeitern, die zur Betreuung der Journalisten eingeteilt waren, aushändigen dürfen. Auf keinen Fall hätte die Leitung der Pressestelle – wie aber bei der Auszeichnung geschehen – praktisch unbesehen die Weisung geben dürfen, den Vermerk zu kopieren und auf entsprechende Bitte an die Journalisten zu verteilen. Gerade weil ihr der Inhalt des Vermerks nicht bekannt war und weil es nach ihrer Darstellung nur grundsätzlich, mithin nicht in jedem Fall ausgeschlossen war, dass in internen Vermerken personenbezogene Daten enthalten sind, hätte vielmehr Anlass bestanden sicherzustellen, dass keine personenbezogenen Daten der geretteten Person, und schon gar nicht deren Name, an Journalisten gelangen. Deshalb hätte die Leitung der Pressestelle der Landesregierung den Vermerk auf darin enthaltene personenbezogene Daten der geretteten Person durchsehen und vor dem Kopieren den Namen und alle anderen Angaben, die auf die gerettete Person schließen ließen, schwärzen lassen müssen. Dass die Pressestelle der Landesregierung all dies nicht beachtet hat, hat dazu geführt, dass sie unzulässigerweise in dem Vermerk Daten über die gerettete Person gespeichert und die Daten unbefugt genutzt und schließlich mit der Verteilung der Kopien außerordentlich sensible personenbezogene Daten an Journalisten weitergegeben hat. Auf unsere Beanstandung dieser gravierenden Datenschutzverstöße ließ uns das Staatsministerium wissen, es habe aus Anlass dieses Falles die Mitarbeiterinnen und Mitarbeiter der Pressestelle der Landesregierung auf die strenge Einhaltung der Bestimmungen des Datenschutzes hingewiesen.

4. Weitergabe von Einwenderdaten im immissionsschutzrechtlichen Genehmigungsverfahren

Durch eine Bürgereingabe wurden wir auf folgenden Fall aufmerksam gemacht: Die Petenten hatten im Rahmen eines immissionsschutzrechtlichen Genehmigungsverfahrens nach § 16 des Bundesimmissionsschutzgesetzes beim Landratsamt als der zuständigen unteren Immissionsschutzbehörde Einwendungen gegen ein Vorhaben erhoben. In ihrem Schreiben baten die Petenten, ihren Namen sowie ihre Anschrift vor der Weitergabe ihrer Einwendungen unkenntlich zu machen. § 12 Abs. 2 Satz 3 der 9. Bundesimmissionsschutzverordnung sieht diese Möglichkeit vor. Nach dieser Vorschrift sollen Namen und Anschrift auf Verlangen unkenntlich gemacht werden, wenn diese Daten zur ordnungsgemäßen Durchführung des Genehmigungsverfahrens nicht erforderlich sind. Das Landratsamt kam dem Wunsch der Petenten zunächst so weit als möglich nach. Vor Weiterleitung der Einwen-

dungen an den Antragsteller und die beteiligten Behörden schwärzte es die Namen und die Hausnummern der Petenten. Die Orts- und Straßenangaben wurden dagegen nicht unkenntlich gemacht. Letzteres ist datenschutzrechtlich nicht zu beanstanden, da für die sachliche Prüfung einer in einem immissionsschutzrechtlichen Verfahren eingelegten Einwendung ein Ortsbezug notwendig ist. Außerdem wird das Interesse des Einwenders, nicht bekannt zu werden, durch diese Vorgehensweise regelmäßig gewahrt.

In der Genehmigung des Vorhabens gab das Landratsamt die Namen und die Anschrift der Petenten dagegen vollständig an. Das Landratsamt stützte diese Vorgehensweise auf ein Urteil des Verwaltungsgerichtshofs Baden-Württemberg aus dem Jahr 1989, das sich auf ein Planfeststellungsverfahren bezog. In diesem ist ausgeführt, dass ein Planfeststellungsbeschluss unvollständig ist, wenn die Einwenderangaben nur in anonymisierter Form enthalten sind. Das Landratsamt übersah dabei, dass für Planfeststellungsverfahren keine dem § 12 Abs. 2 Satz 3 der 9. Bundesimmissionsschutzverordnung entsprechende Vorschrift existiert, die in Planfeststellungsverfahren zu beachtenden Verfahrensvorschriften somit von den im vorliegenden Fall anzuwendenden Vorschriften abweichen. Das Urteil des Verwaltungsgerichtshofs konnte daher keineswegs auf die Genehmigung nach § 16 des Bundesimmissionsschutzgesetzes übertragen werden. Auch aus der Tatsache, dass sich die Einwender während des öffentlichen Erörterungstermins zu Wort gemeldet hatten, lässt sich nicht der Schluss ziehen, dass sie ihr Verlangen nach Anonymität aufgegeben haben. Denn aus einer Äußerung während eines Erörterungstermins lässt sich nicht ohne weiteres schließen, dass der Sprecher Einwendungen erhoben hatte.

Die Aufhebung der Anonymität der Petenten wäre daher nur zulässig gewesen, wenn die Namens- und die vollständigen Adressangaben zur ordnungsgemäßen Durchführung des Genehmigungsverfahrens erforderlich gewesen wären oder wenn ein schutzwürdiges Interesse des Antragstellers an der Bekanntmachung der Einwender vorgelegen hätte, das dem informationellen Selbstbestimmungsrecht der Einwender vorging. Beides war jedoch nicht der Fall. Das Landratsamt war daher nicht berechtigt, Namen und vollständige Anschrift der Petenten in der Genehmigung zu nennen.

Wir haben das Landratsamt gebeten, unsere Rechtsauffassung künftig in vergleichbaren Fällen zu beachten.

5. Schornsteinfeger als Datenquelle?

Der Gemeinderat einer Stadt hatte beschlossen, zum Zwecke der Reduzierung von CO_2-Emissionen ein städtisches Klimaschutzkonzept zu erstellen. Um die Emissionen, die größtenteils durch Gebäudeheizungen und Warmwasserbereitungen entstehen, möglichst genau erfassen zu können, wollte die Stadt zunächst die jeweiligen Gebäudedaten und die Daten über die Art der Befeuerung ermitteln. Da sich die Stadt den Arbeits- und Kostenaufwand einer eigenen, gesonderten Datenerhebung ersparen wollte, wandte sie sich kurzerhand an die Bezirksschornsteinfegermeister und bat diese, ihr die Daten zu den Feuerungsanlagen der einzelnen Gebäudeeigentümer zu übermitteln. Die Schornsteinfeger lehnten die Herausgabe der erbetenen Daten jedoch unter Hinweis auf den Datenschutz ab. Die Stadt erhoffte sich nun, dass wir ihr bei der Bereitstellung der Schornsteinfegerdaten behilflich sind und die Daten sozusagen „freigeben“. Wir konnten der Stadt hier jedoch nicht weiterhelfen, da es keine Rechtsgrundlage gibt, die es den Schornsteinfegern erlauben würde, der Stadt ein Verzeichnis mit den Daten sämtlicher Feuerungsanlagen zu übermitteln.

Nach § 19 Abs. 3 des Gesetzes über das Schornsteinfegerwesen darf der Bezirksschornsteinfegermeister zwar personenbezogene Angaben aus seinen Aufzeichnungen, zu denen auch ein Verzeichnis der Feuerungsanlagen gehört, an öffentliche Stellen übermitteln, soweit das für die Erfüllung seiner Aufgaben, die Bekämpfung der Luft-, Boden- und Gewässerverschmutzung, die rationelle Energieverwendung, die Bauaufsicht oder die Brandbekämpfung erforderlich ist. Im vorliegenden Fall konnte jedoch dahingestellt bleiben, ob es zu den Aufgaben der Stadt gehörte, ein Klimaschutzkonzept zu erstellen und Gebäudeeigentümer zum Thema „rationelle Energieverwendung“ zu beraten. Denn selbst wenn man dies angenommen hätte,

wären die von der Stadt gewünschten Daten zur Erfüllung dieser Aufgaben nicht erforderlich gewesen. Zum einen kann ein Klimaschutzkonzept auch ohne die Kenntnis der Daten der einzelnen Feuerungsanlagen erstellt werden; zum anderen sind Gebäudeeigentümer nicht verpflichtet, eine städtische Energieberatung in Anspruch zu nehmen.

Wir haben der Stadt deshalb mitgeteilt, dass sie die Daten gegebenenfalls direkt bei den Betroffenen erheben müsste (vgl. § 13 Abs. 2 LDSG), auch wenn dies mit einem Mehraufwand an Arbeit und Kosten verbunden ist. Denkbar wäre beispielsweise, die Gebäudeeigentümer im städtischen Mitteilungsblatt auf die städtische Energieberatung aufmerksam zu machen. Datenschutzrechtlich unbedenklich wäre es auch, wenn die Stadt die Betroffenen in einem entsprechenden Informationsschreiben auf die Energieberatung aufmerksam machen und dieses Schreiben zusammen mit den Grundsteuerbescheiden verschicken würde. In einem solchen Schreiben sollten die Betroffenen auf die Freiwilligkeit der Teilnahme an der Beratung hingewiesen werden. Diejenigen Gebäudeeigentümer, die eine Beratung wünschen, können sich dann mit der Stadt in Verbindung setzen und ihr gegebenenfalls die Daten zukommen lassen.

5. Teil: Technik und Organisation

1. Sensible Daten auf dem Präsentierteller

Die Vernetzung dienstlicher Arbeitsplatzcomputer ist in den vergangenen Jahren immer weiter vorangeschritten. Mittlerweile gibt es kaum noch einen Computer, der nicht Teil eines lokalen oder überregionalen Verwaltungsnetzes ist. Neben vielfältigen nützlichen Funktionen birgt diese zunehmende Vernetzung erhebliche Sicherheitsrisiken. Unzulängliche Sicherheitsmaßnahmen können in einer vernetzten Umgebung dazu führen, dass eine Vielzahl von Personen auf Daten zugreifen kann, die nicht für sie bestimmt sind. Gleich mehrere in diesem Jahr durchgeführte Kontrollen offenbarten eklatante Netzwerkmängel in Bereichen, in denen besonders schutzbedürftige Daten verarbeitet werden: Unter anderem waren medizinische Daten, Justizdaten, Personaldaten sowie Daten eines Gesundheitsamts, eines Sozialamts und einer Psychologischen Beratungsstelle nur unzulänglich vor unberechtigten Zugriffen geschützt. Folgende Mängel stellten wir bei unseren Kontrollen in einer Justizvollzugsanstalt, in zwei Landratsämtern sowie in einem Staatlichen Schulamt fest:

1.1 Mängel im Netz der Justizvollzugsanstalten

Bei einer Kontrolle einer Justizvollzugsanstalt stellte sich heraus, dass die dortigen Bediensteten auf zahlreiche Dokumente zugreifen konnten, die auf Computern anderer Justizvollzugsanstalten gespeichert waren, ohne dass dafür eine dienstliche Notwendigkeit bestand. Unter anderem war es ohne weiteres möglich, von Computern der Justizvollzugsanstalt aus auf folgende Dokumente zuzugreifen:

– Dokumente des Justizvollzugskrankenhauses

  • Über 3 100 jeweils mit Vor- und Nachnamen sowie zum Teil auch mit dem Geburtsdatum versehene Fotos von Gefangenen.

  • Bis zu sechs Jahre alte Protokolle von Teamsitzungen. Darin war beispielsweise notiert, welcher Gefangene welchen Geldbetrag für einen Einkauf bei einem Versandhaus verwenden darf, oder wann, aus welchem Anlass und in Begleitung welcher Personen welcher Gefangene Ausgang erhält.

  • Mehrere, jeweils auf ein Quartal bezogene tabellarische Übersichten über die Ergebnisse von Urinkontrollen bei Gefangenen. Darin waren jeweils unter anderem Vorname, Name und Geburtsdatum der Gefangenen, die Häuser und Bereiche, in denen sie untergebracht waren sowie das Datum der Kontrollen genannt. Ferner war angegeben, wer die Kontrollen angeordnet hatte und ob die Tests auf Kokain, Amphetamine sowie andere Substanzen jeweils positiv oder negativ ausgefallen waren.

  • Eine Personalliste, der sich Namen, Vornamen und Geburtsdaten der Beschäftigten entnehmen ließen.

Mit der Zugriffsberechtigung eines lokalen Administrators der Justizvollzugsanstalt ließen sich darüber hinaus weitere Dokumente mit sensiblen personenbezogenen Daten öffnen, beispielsweise

  • ein Schreiben des Justizvollzugskrankenhauses in Sachen eines darin mit Namen und Geburtsdatum genannten Gefangenen. Darin hieß es unter anderem über den Gefangenen:

    „Herr X ist zum körperlichen Drogenentzug ... im Justizvollzugskrankenhaus. ... Herr X hat ... wegen gefährlicher Körperverletzung eine dreimonatige Strafe zu verbüßen. ... Wegen familiärer Probleme habe er begonnen, Heroin zu konsumieren. ... Nach Auskunft des ihn betreuenden Pflegepersonals kommt es hier zu sozialen Unverträglichkeiten mit Mitgefangenen“.

  • ein Schreiben des Justizvollzugskrankenhauses an ein Notariat unter dem Betreff „Anregung einer Betreuung gemäß § 896 BGB“.

Darin ist zu einem durch Namen, Geburtsdatum und Geburtsort bezeichneten Gefangenen ausgeführt:

„Wegen einer geistig-seelischen Störung ist er nicht in der Lage, seine Angelegenheiten zu besorgen. Wir regen daher für Herrn X eine Betreuungsbeiordnung an. Die Betreuung sollte die Gesundheits- und Vermögensfürsorge sowie die Bestimmung des Aufenthalts umfassen.“

– Dokumente einer anderen Justizvollzugsanstalt

  • Eine Übersicht der Vollzugsbediensteten dieser Justizvollzugsanstalt mit Angabe ihrer Vor- und Nachnamen, privater Anschriften sowie Telefonnummern.

  • Ein mit „Schießausbildung“ überschriebenes Dokument, das für mehrere namentlich genannte Bedienstete die Teilnahme am Übungsschießen anordnet.

  • Angaben über die Durchführung der Briefkontrolle bei Untersuchungshäftlingen. Neben den Namen der Häftlinge war daraus zu entnehmen, welcher Stelle die Briefe zur Kontrolle vorzulegen sind und welches Aktenzeichen dabei jeweils anzugeben ist.

– Dokumente einer weiteren Justizvollzugsanstalt

  Es war möglich, die auf den Arbeitsplatzcomputern dieser Justizvollzugsanstalt gespeicherten Benutzerprofile namentlich genannter Anwender einzusehen und dabei auch Informationen über Internet-Angebote zu erhalten, die diese Nutzer in Anspruch genommen haben.

Die hier erwähnten Dokumente stellen nur einen Teil der zahlreichen Dokumente anderer Justizvollzugsanstalten dar, auf die von Arbeitsplatz-PC der kontrollierten Justizvollzugsanstalt aus zugegriffen werden konnte. Die Zugriffsberechtigungen waren dabei zudem vielfach so gestaltet, dass diese Dokumente nicht nur hätten gelesen, sondern auch verändert werden können. Eine entsprechende Konfiguration der lokalen Arbeitsplatz-PC vorausgesetzt, bestanden die genannten Zugriffsmöglichkeiten nicht nur für Bedienstete dieser Justizvollzugsanstalt, sondern auch für Bedienstete anderer Justizvollzugsanstalten.

1.2 Mängel im Netz eines Landratsamts

Das Landratsamt betreibt in seiner Hauptstelle sowie in mehreren Außenstellen mehrere hundert Arbeitsplatz-PC sowie mehrere von diesen PC aus zugängliche Server. Bei einer an einem Arbeitsplatz des Sozialamts in der Hauptstelle durchgeführten stichprobenweisen Überprüfung ergab sich, dass von diesem PC aus eine Vielzahl personenbezogener Dokumente anderer Organisationseinheiten ohne weiteres gelesen und vielfach auch geändert werden konnte, ohne dass dies dienstlich erforderlich war. Im Einzelnen waren beispielsweise folgende Zugriffe möglich:

– Zugriff auf Dokumente einer Psychologischen Beratungsstelle des Landratsamts

  • Eine Aktennotiz, in der über einen namentlich genannten Klienten unter anderem ausgeführt war, dass dieser wegen Vergewaltigung im Wiederholungsfall in einem Zentrum für Psychiatrie untergebracht ist und in der beschrieben wird, wie er nach der Haftentlassung betreut werden kann. Die Aktennotiz enthielt ferner eine Darstellung der Schwierigkeiten, die im Zusammenhang mit der Entlassung des Klienten aus dem Zentrum für Psychiatrie und dessen Aufnahme in eine Einrichtung der ambulanten Betreuung bislang aufgetreten waren.

  • Ein an eine Stellenbewerberin adressiertes Schreiben, in dem ihr unter anderem mitgeteilt wurde, dass das mit der Stellenbesetzung betraute Team zwar ihre fachliche Qualifikation und Berufserfah-

rung anerkennt, sich aber gleichwohl mehrheitlich für eine andere Bewerberin entschieden hat.

- Mehrere sozialtherapeutische Dokumentationen, in denen unter anderem die einzelnen soziotherapeutischen Maßnahmen aufgezählt und dazu das Datum der Maßnahme, die Dauer, das jeweilige Ziel, der Inhalt und der Behandlungsverlauf dargestellt waren. In einer dieser Dokumentationen war beispielsweise ausgeführt: *„Terminabsprache schwierig“, „Keine Motivation, hat Ängste“, „Verfolgungswahn“, „Er hat 30 Tropfen Haloperlidol zu viel genommen“, „Suizidgedanken“*. Daneben war in einer weiteren Tabelle die Zusammenarbeit mit verordnendem Arzt und sonstigen Leistungserbringern dargestellt. Darin war neben dem jeweiligen Datum u. a. vermerkt: *„Arztgespräch, es geht mit den Medikamenten besser. Problem bleibt Alkohol“, „Arztbesuch: Kontrolle, dass er seine Spritze abholt“* oder *„Erstgespräch mit dem Betreuten Wohnen. Arbeitsbündnis konnte mit Herrn X und der Familie erzielt werden“*.
- Einverständniserklärung, mit der eine durch Namen und Anschrift bezeichnete Person ihr Einverständnis dazu erklären sollte, dass die Arbeit ihres Kindes am Tonfeld per Videokamera aufgezeichnet wird.
- Ein Schreiben an eine durch Namen und Anschrift bezeichnete Person, in dem ihr der Termin für ein Erstgespräch mitgeteilt wurde.

– Fotos aus der Kfz-Geschwindigkeitsüberwachung

Zugegriffen werden konnte auf etwa 100 000 Bilddateien mit Fotos und Fotoausschnitten, von denen jeweils fünf einen Geschwindigkeitsverstoß dokumentieren. Dabei zeigte ein Großbild das Fahrzeug mit Insassen. Ferner waren darin als Messdaten Tagesdatum und Uhrzeit sowie die gemessene Geschwindigkeit eingeblendet. Ein zweites Bild enthielt einen vergrößerten Bildausschnitt, der in der Regel die Fahrerin oder den Fahrer zeigte. Weitere Fotos gaben das Kfz-Kennzeichen wieder. Daneben konnte auf andere Dateien zugegriffen werden, die weitere im Zuge der Ahndung der Geschwindigkeitsverstöße verarbeitete Daten enthielten.

– Dokumente einer Außenstelle des Sozialamts

- Ein Aktenvermerk, in dem die Situation einer durch Namen, Geburtsdatum und Wohnanschrift bezeichneten Klientin beschrieben und dazu unter anderem ausgeführt wurde:

  „Die Situation von Frau X wurde im Arbeitskreis ‚Betreutes Wohnen‘ am ... besprochen und es wurde dort beschlossen, Frau X in das Betreute Wohnen aufzunehmen.

  ...

  Frau X stammt aus ... und betrachtet den Ort auch als ihre Heimat.

  ...

  Vom ... bis ... befand sich Frau X im Zentrum für Psychiatrie XY zur stationären Behandlung. Gem. dem dortigen Attest liegt eine schwere depressive Störung mit Suicidalität sowie zeitweise auftretenden Panikattacken bei abhängiger Persönlichkeitsstörung vor. Nach ihrer Entlassung wohnte sie zunächst bei ... in ..., wo es jedoch zu größeren Schwierigkeiten kam, so dass sie am ... wieder nach ... übersiedelte.

  Aufgrund ihrer psych. Erkrankung braucht Frau X umfassende Anleitung und Versorgung im Alltag, wenngleich sie nicht pflegebedürftig ist.“

- Ein „Freier Mitarbeiter-Vertrag“, dem neben Name und Anschrift des Mitarbeiters unter anderem Art und Inhalt der Aufgaben sowie die Honorarvereinbarung zu entnehmen waren.

- Ein an eine Hochschule adressiertes Schreiben, in dem es über eine ehemalige Praktikantin hieß:

  „In Ergänzung unseres Dienstzeugnisses vom ... teilen wir mit, dass Frau X im Rahmen der von uns beurteilbaren Leistungen für ihr Praktikum vom ... bis ... eine Gesamtnote von 10 Punkten erhält.“

- Zugegriffen werden konnte auf eine Datei, in der offenbar personenbezogene Buchungsdaten eines Fachverfahrens des Jugendamts gespeichert waren und die zumindest teilweise lesbar gemacht werden konnten, ohne dafür das entsprechende Fachverfahren aufrufen zu müssen. Vielmehr war es möglich, die Datei mit Hilfe eines einfachen Dateieditors zu öffnen. So ließen sich zahlreiche personenbezogene Angaben im Klartext lesen. Unter anderem fanden sich in den einzelnen Datensätzen Buchungszeichen, Datumsangaben sowie Betreffeinträge wie „Unterhaltsvorschuss“, „Erstattung UVG-Leist“, wobei jeweils auch Vor- und Nachnamen genannt waren.

Die Zugriffsberechtigungen waren dabei vielfach so gestaltet, dass alle Mitarbeiterinnen und Mitarbeiter des Landratsamts, die einen PC nutzen, die genannten Dokumente nicht nur öffnen und lesen konnten, sondern die Dokumente auch hätten ändern können. Zum Teil waren die Zugriffsberechtigungen auf die Bediensteten des Sozialamts beschränkt.

1.3 Mängel im Netz eines weiteren Landratsamts

Bei einer stichprobenweisen Überprüfung an einem Arbeitsplatz des Sozialamts war es möglich, beispielsweise auf folgende Dokumente des Gesundheitsamts zuzugreifen:

– Das Protokoll einer mündlichen Heilpraktiker-Prüfung, die von Vertretern des Gesundheitsamts durchgeführt wurde. Darin waren zunächst die jeweiligen Fragen und Antworten des Prüflings protokolliert. Anschließend erfolgte eine Bewertung der Antworten. Das Protokoll endet mit der Feststellung:

  „Nach ausführlicher Diskussion wird übereinstimmend festgestellt, dass die Überprüfung aufgrund erheblicher Kenntnislücken im Bereich des Basiswissens nicht bestanden ist.“

– Ein per Einschreiben zu versendender Brief an einen Heilpraktiker, dem zu entnehmen ist, wann ihm von wem die Erlaubnis zur Ausübung der Heilkunde erteilt wurde. Ferner heißt es:

  „Dem Landratsamt – Gesundheitsamt – wurden Tatsachen bekannt, nach denen es nicht länger möglich ist, dass Sie weiterhin als Heilpraktiker tätig sind.

  ...

  Uns liegt ein Urteil des Amtsgerichts ... vom ... Aktenzeichen ... vor, mit dem Sie rechtskräftig wegen Missbrauchs von Titeln, Berufsbezeichnungen und Abzeichen in ... Fällen und wegen Betruges verurteilt wurden.

  ...

  Sie haben sich in mindestens ... nachgewiesenen Fällen insbesondere im Rahmen Ihrer Tätigkeit als Heilpraktiker des Doktortitels bedient, obwohl Ihnen dieser – wie Sie sehr wohl wussten – nicht verliehen worden war. ... Das vorliegende Verhalten lässt den Schluss zu, dass Ihnen die nach § 2 Abs. 1 f 1 DV HprG notwendige sittliche bzw. berufliche Zuverlässigkeit fehlt.“

– Ein Vermerk über den Entzug der Heilpraktikererlaubnis eines Heilpraktikers. Ergänzend war diesem Vermerk zu entnehmen:

  „Gegen den Betreffenden wird seit Jahren ermittelt. Zunächst wegen des Betreibens der Arztpraxis, die von Herrn X nicht ordnungsgemäß

als Heilpraktikerpraxis ausgewiesen wurde. Des Weiteren hatte er bei einem Besuch der Gesundheitsbehörde verschreibungspflichtige und zudem abgelaufene Medikamente im Schrank. Anschließend wegen erheblicher Steuerschulden aus einer vorherigen selbstständigen Tätigkeit."

– Ein Schreiben an einen Heilpraktiker, in dem es heißt:

„Wie uns von der Staatsanwaltschaft ... mitgeteilt wurde, sind Sie bereits zum zweiten Mal wegen Diebstahl rechtskräftig verurteilt worden. ... Die vorliegenden Straftaten begründen eine Rücknahme der Erlaubnis [gemeint ist die Heilpraktikererlaubnis] noch nicht. Wir möchten Sie jedoch auf die Möglichkeit hinweisen, wenn zusätzliche Tatsachen eintreten, die eine berufliche Unzuverlässigkeit vermuten lassen."

1.4 Mängel im Netz eines Staatlichen Schulamts

Das Kultusministerium hat bereits vor Jahren ein privates Unternehmen mit dem Betrieb der PC und lokalen Netzwerke des Kultusministeriums, der Oberschulämter, der staatlichen Schulämter und weiterer, der Kultusverwaltung angehörender Einrichtungen beauftragt. Dabei wurde auch festgelegt, dass für jede Dienststelle eine sog. allgemeine Ablage einzurichten ist. Daneben sollten, je nach Bedarf der einzelnen Dienststellen, weitere Ablagen eingerichtet werden, auf die nicht die gesamte Dienststelle, sondern nur ein Teil der Bediensteten zugreifen können soll. Die Einrichtung und Nutzung derartiger Ablagen ist datenschutzrechtlich immer dann erforderlich, wenn personenbezogene Daten verarbeitet werden und nicht alle Bediensteten, die auf die allgemeine Ablage zugreifen können, Kenntnis von diesen Daten erhalten dürfen. Demgegenüber speicherte das von uns kontrollierte Staatliche Schulamt grundsätzlich sämtliche Daten im Verzeichnis „Allgemeines". Dazu gehören unter anderem auch Daten über die Durchführung der sonderpädagogischen Untersuchung einzelner Schülerinnen und Schüler, bei denen darüber zu entscheiden ist, ob sie einen besonderen Förderungsbedarf haben und, wenn ja, ob die notwendige besondere Förderung an der bisherigen Schule oder an einer anderen Schule erbracht werden kann. Es liegt in der Natur der Sache, dass dabei zum Teil medizinische und andere sensible personenbezogene Daten verarbeitet werden. Bei stichprobenweisen weiteren Kontrollen ergab sich, dass in der allgemeinen Ablage auch Daten über Bewerber und andere im Zusammenhang mit einer Stellenbesetzung erfasste Daten sowie beispielsweise auch Arbeitszeitblätter einzelner Mitarbeiter abgelegt waren.

1.5 Woran haperte es?

Die bei mehreren Kontrollen festgestellten gravierenden Datenschutzmängel im Umgang mit lokalen und überregionalen Computernetzwerken machen deutlich, dass offenbar nicht nur in Einzelfällen erheblicher Nachholbedarf in Sachen Netzwerksicherheit besteht. Um durchgreifende Verbesserungen erzielen zu können, galt es zunächst, die Ursachen dieser Datenschutzmängel zu ermitteln. Dabei stellte sich heraus, dass die festgestellten Mängel insbesondere auf folgende Fehler zurückzuführen waren:

1.5.1 Nachlässiger Umgang mit Dateifreigaben

Schließt man mehrere Computer zu einem Netzwerk zusammen, so können über die Funktion der so genannten Dateifreigabe die auf einem Computer gespeicherten Daten für einen Zugriff durch andere am Netz angeschlossene Computer bereitgestellt werden. Die bei den Justizvollzugsanstalten sowie einem Landratsamt festgestellten Mängel gingen jeweils darauf zurück, dass solche Dateifreigaben für Verzeichnisse eingerichtet waren, für die sie nicht hätten eingerichtet werden dürfen. Diese höchst kritische Eigenschaft von Verzeichnissen erfordert, dass Freigaben nur nach gründlicher Planung und kritischer Prüfung der dadurch gewährten Zugriffsmöglichkeiten eingerichtet werden dürfen.

1.5.2 Nachlässige Konfiguration der Arbeitsplatz-PC

Aufgrund ihrer datenschutzkritischen Rolle dürfen Freigaben nur von autorisierten Personen, in der Regel somit von Netzwerkadministratoren, eingerichtet werden. Das bedeutet zugleich, dass die Bildschirmarbeitsplätze so eingerichtet werden müssen, dass die dort tätigen Sachbearbeiter keine solchen Dateifreigaben einrichten können. Leider waren in den betroffenen Dienststellen die Computer häufig so eingerichtet, dass jeder Nutzer Freigaben einrichten konnte.

1.5.3 Installation von Fachverfahren unzulänglich

Die Mängel bei den Freigaben lenkten den Blick auch auf folgendes Problem: Mitunter waren Fachverfahren so installiert, dass man mit ganz einfachen Mitteln, wie einem in jedem Windows-System verfügbaren Texteditor (z. B. Notepad), unter Umgehung der von den Fachverfahren selbst realisierten Zugriffsbeschränkungen quasi geradewegs und ungefiltert auf die von diesen Verfahren bearbeiteten Daten zugreifen konnte. Alle innerhalb des Verfahrens gebotenen Maßnahmen zur Zugriffsverwaltung und -beschränkung laufen dann ins Leere, wenn ein solcher unmittelbarer Zugriff nicht verhindert wird.

1.5.4 Unzulänglichkeiten beim Betrieb und bei der Nutzung von Terminalservern

Um sich die Bereitstellung und Pflege einheitlich ausgestatteter Bildschirmarbeitsplätze zu erleichtern, setzen einige Dienststellen sog. Terminalserver ein. Dabei werden alle diejenigen Anwendungen und Daten, die ansonsten lokal auf jedem einzelnen Arbeitsplatz-PC installiert und gespeichert werden, nur noch auf einem oder einigen wenigen Terminalservern installiert. Der lokale PC dient dann nur noch dazu, die Tastatureingaben des Benutzers an den Terminalserver zu leiten und den vom Terminalserver erzeugten Bildschirminhalt am Monitor des Arbeitsplatz-PC anzuzeigen. In einem der oben genannten Fälle wurden die unberechtigten Zugriffsmöglichkeiten dadurch eröffnet, dass ein Nutzer die schutzbedürftigen Daten auf der lokalen Festplatte des Terminalservers gespeichert hatte. Da die dafür eingerichteten Zugriffsberechtigungen einen Vollzugriff durch alle Nutzer des Terminalservers vorsahen, hätten auch sämtliche anderen Nutzer dieses Terminalservers ohne weiteres auf diese lokal gespeicherten Daten zugreifen können, auch wenn sie dies zur Erfüllung ihrer dienstlichen Aufgaben gar nicht benötigten.

1.5.5 Unzureichende Sicherheitsmaßnahmen bei der Netzkoppelung

Zumindest die im Netz der Justizvollzugsanstalten sowie die im Netz eines Landratsamts festgestellten standort- und dienststellenübergreifenden Netzzugriffe sind nur dann möglich, wenn die zur Verknüpfung der verschiedenen lokalen Netze dienenden Netzknotencomputer (die sog. Router) die dazu benötigten Kommunikationswege bereitstellen. Welche Kommunikationsmöglichkeiten ein Router unterstützt und welche nicht, lässt sich vom Betreiber des Netzwerks in sog. Routing- und Filtertabellen festlegen. Die festgestellten Mängel machen deutlich, dass die Netzbetreiber nur unzureichend von dieser Möglichkeit Gebrauch gemacht haben, denn die Netzknotencomputer ermöglichten netzübergreifende Zugriffe im Rahmen der Dateifreigabe, die dienstlich nicht erforderlich sind. Hätten die Dienststellen die Möglichkeit genutzt, die Netzknotencomputer so zu konfigurieren, dass diese nur die erforderlichen Datenströme über die Grenzen des eigenen lokalen Netzes hinaus an andere Computer und Netzwerke weiterleiten, so hätten die unter Nummern 1.5.1 bis 1.5.3 beschriebenen Fehler zumindest nur die jeweiligen lokalen Netze berührt.

1.5.6 Unsachgemäße Nutzung vorhandener Ablagestrukturen

Die beim Staatlichen Schulamt festgestellten Mängel rührten daher, dass dort – offenbar aufgrund fehlenden Problembewusstseins – ein auf einem Server eingerichtetes Dateiverzeichnis, auf das alle Bediensteten Zugriff hatten, genutzt wurde, um schutzbedürftige personenbezogene Daten zu speichern, auf die nur einige wenige Bedienstete zur Erfüllung ihrer dienstlichen Aufgaben zugreifen können müssen.

1.5.7 Unzulänglichkeiten im Sicherheitskonzept

Um ein möglicherweise sogar über mehrere Standorte verteiltes Computernetzwerk datenschutzgerecht zu betreiben, ist eine Vielzahl technischer und organisatorischer Aspekte zu berücksichtigen. Schon weil diese auf der einen Seite netzwerkweit abgestimmt sein müssen, auf der anderen Seite aber oft von mehreren, zum Teil nur örtlich tätigen Systembetreuern umgesetzt werden müssen, ist es notwendig, die insgesamt notwendigen Datenschutzmaßnahmen in einem IT-Sicherheitskonzept für den Betrieb dieses Netzwerks zusammenzufassen. Die vorgefundenen Mängel machen deutlich, dass diese Konzepte, soweit überhaupt vorhanden, unzulänglich waren. Zwar hätte allein das Vorhandensein eines solchen Konzepts noch nicht ausschließen können, dass einmal eine darin vorgesehene Maßnahme nicht korrekt umgesetzt wird. Angesichts der Tatsache, dass die beschriebenen Mängel teilweise mehrere der oben genannten einzelnen Fehler voraussetzen, muss aber davon ausgegangen werden, dass die Erarbeitung und konsequente Umsetzung eines solchen Konzepts dazu beigetragen hätte, das Auftreten solch folgenschwerer Fehler zu vermeiden.

1.6 Datenschutzrechtliche Beurteilung

Die gewährten, aber nicht erforderlichen Möglichkeiten zum Zugriff auf die genannten, vielfach besonders sensiblen Justiz-, Personal- und Gesundheitsdaten habe ich gegenüber dem Justizministerium sowie gegenüber den betroffenen Landratsämtern beanstandet. Im Hinblick auf die Beanstandung des oben erstgenannten Landratsamts spielte für mich dabei auch eine Rolle, dass Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung nämlich nach § 203 Abs. 1 des Strafgesetzbuchs all das, was ihnen bei der Ausübung ihrer Tätigkeit anvertraut oder sonst bekannt wird, nicht unbefugt offenbaren dürfen. Diese strafbewehrte berufliche Schweigeverpflichtung gilt in gleichem Maße für staatlich anerkannte Sozialarbeiter und staatlich anerkannte Sozialpädagogen. Unter anderem war bei etlichen der unzureichend geschützten Dokumente der hier angesprochenen Psychologischen Beratungsstelle von solchermaßen anvertrauten Informationen auszugehen. Ferner war zu berücksichtigen, dass die unzureichend geschützten Dokumente teilweise auch Personalaktendaten enthielten, die dem Personalaktendatengeheimnis unterliegen.

Mein Kontrollbericht hinsichtlich der Mängel bei dem kontrollierten Staatlichen Schulamt wird dieser Tage versandt. Um die Mängel auszuräumen, forderte ich die Landratsämter, das Justizministerium und die Justizvollzugsanstalten auf, ihre Konzeptionen für netzinterne und netzübergreifende Zugriffsmöglichkeiten zu überprüfen und sicherzustellen, dass nichtzulässige Zugriffe technisch auch nicht durchgeführt werden können. Daneben sind für Fachverfahren Ablagekonzepte zu erarbeiten und umzusetzen, die es künftig verhindern, dass Nutzer unmittelbar auf die von den Fachverfahren benutzten Dateien zugreifen und dadurch Daten in Erfahrung bringen können, die nicht für sie bestimmt sind.

Ferner sind Sicherheitskonzepte für die im standortübergreifenden Verbund betriebenen lokalen Netzwerke zu erarbeiten, die verhindern, dass Daten für einen Zugriff über Netz freigegeben werden, ohne dass dies zuvor unter Berücksichtigung der Konsequenzen ausdrücklich so fest-

gelegt wurde. Vorgaben hinsichtlich der Konfiguration der einzelnen Arbeitsplatz-PC sind dazu ebenso erforderlich wie Richtlinien darüber, wer unter welchen Voraussetzungen Freigaben einrichten darf. Generell sollten diese Konzeptionen so gestaltet sein, dass auch Mitarbeiter, die zur Wahrnehmung ausschließlich lokaler Systemverwaltertätigkeit über Administrationsberechtigungen verfügen, damit nicht auf personenbezogene oder andere schutzbedürftige Daten zugreifen können, die in anderen lokalen Netzen gespeichert sind.

Beim Einsatz von Terminalservern ist darauf zu achten, dass durch entsprechende Zugriffsberechtigungen die Speichermöglichkeiten auf der lokalen Festplatte möglichst weitgehend unterbunden werden und die Nutzer zudem für die Problematik sensibilisiert werden.

Im Hinblick auf die Nutzung zentraler Dateiablagestrukturen muss sichergestellt sein, dass diese – insbesondere im Hinblick auf die damit verbundenen Zugriffsberechtigungen – auf die dienstlichen Bedürfnisse der nutzenden Dienststelle abgestimmt sind und dass die Bediensteten dafür sensibilisiert werden, personenbezogene oder andere schutzbedürftige Daten nur in solchen Ablagen zu speichern, auf die jeweils nur diejenigen anderen Nutzer zugreifen können, die dies zur Erfüllung ihrer Aufgaben benötigen.

Zu begrüßen ist, dass alle betroffenen Stellen rasch reagiert und Abhilfe zugesichert haben.

2. Gravierende Mängel in Computernetzen

2.1 Auf Gemeindeebene

Bei der Kontrolle einer Gemeinde stießen wir erneut auf Unzulänglichkeiten, wobei wir eigentlich gehofft hatten, diese nicht mehr vorfinden zu müssen. Konkret ging es um die Einstellungen hinsichtlich der Kennwörter, die beim Start eines Rechners bei der Anmeldung einzugeben sind, und um die Anforderungen an die Durchführung von Anmeldungen. Diese Festlegungen sind deshalb wichtig, weil mit der Anmeldung und dem Kennwort der im Landesdatenschutzgesetz geforderten Benutzerkontrolle Genüge getan werden soll. Die Risiken bei unachtsamer Wahl des Kennworts und ungenügender Anmeldeprozedur bestehen darin, dass Kennwörter leichter abgehört oder erraten werden können und dann unberechtigterweise auf personenbezogene Daten zugegriffen werden kann. Die Brisanz der ungenügenden Maßnahmen wird dadurch verschärft, dass bei dem von der Gemeinde verwendeten Betriebssystem sehr häufig, ohne dass die Benutzer es merken, automatisch Anmeldungen in ihrem Namen an anderen Systemen durchgeführt werden, sobald beispielsweise auf so genannte Netzlaufwerke, Netzdrucker oder Postfächer zugegriffen wird. Im Einzelnen wurde Folgendes festgestellt:

– Fehlende minimale Kennwortlänge

  Moderne Betriebssysteme erlauben es normalerweise, dass eingestellt werden kann, wie lange ein Kennwort für eine Anmeldung mindestens sein muss. Die Einstellung der minimalen Länge der Kennworte war bei der Gemeinde nicht vorgenommen worden. Das hat dann meist zur Folge, dass Benutzer, um sich nicht ein Kennwort merken zu müssen, das aus acht oder mehr Zeichen besteht, und um sich Tipparbeit bei der Eingabe zu sparen, ein Kennwort wählen, das aus einem oder – wohl um das Sicherheitsniveau um rechnerisch ja richtige 100 Prozent zu „steigern“ – zwei Zeichen besteht. Dabei wird einfallsreich häufig auf die Initialen des eigenen Vor- und Nachnamens zurückgegriffen. Den Benutzern ist häufig nicht bekannt, dass Unbefugte unter ihrem Namen über andere Rechner auf die von ihnen verarbeiteten personenbezogenen Daten zugreifen können – wenn vor diesem Hintergrund Benutzer auf ein Benutzerkennwort sogar gänzlich verzichten, ist dies besonders bedenklich. Dem muss die Gemeinde dadurch präventiv entgegenwirken, dass sie die Mindestlänge eines Benutzerkennworts auf acht Zeichen festlegt.

– Vermeidung der Kennwortalterung

Moderne Betriebssysteme erlauben es normalerweise, dass eingestellt werden kann, wie lange ein Kennwort gültig ist. Wenn die Gültigkeit des Kennworts erloschen ist, wird der Benutzer aufgefordert, ein neues Kennwort einzugeben. Seit langem empfehlen technische Datenschützer, zur Erhöhung der Systemsicherheit einen Mechanismus zur Vermeidung der Kennwortalterung zu nutzen, da ein Kennwort immer wieder einmal, etwa durch versehentliches lautes Buchstabieren bei der Eingabe oder dadurch, dass Dritte bei der Eingabe auf die Tastatur blicken, offenbart werden kann. Anscheinend war der Gemeinde dies nicht bekannt, denn dieser Empfehlung hatte sie sich nicht angeschlossen und darauf verzichtet, den entsprechenden Systemschutz einzuschalten. Das muss sie jetzt nachholen.

– Fehlende Kennworthistorie

Hat man den Mechanismus zur Vermeidung der Kennwortalterung eingeschaltet, versuchen Benutzer diesen häufig dadurch zu umgehen, dass sie das Kennwort nach erzwungenem Kennwortwechsel sofort auf das alte Kennwort zurücksetzen. Moderne Betriebssysteme erlauben es daher nicht nur, die Dauer, für die ein Kennwort mindestens gültig sein muss, einzustellen, sondern sie führen für jeden Benutzer eine Liste der Kennwörter, die der Benutzer schon verwendet hat. Das Führen einer solchen Kennworthistorie wird dringend empfohlen. Sie sollte ausreichend umfangreich sein, so dass sichergestellt ist, dass die Benutzer bei jedem erzwungenen Kennwortwechsel ein neues Kennwort wählen müssen.

Um der Neigung vorzubeugen, dass Benutzer Begriffe aus einem Lexikon als Kennwörter verwenden, ist noch anzumerken, dass die Zusammensetzung von Kennwörtern bei modernen Betriebssystemen auch vorgegeben werden kann. Schwer zu erratende Kennwörter sollten aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen wie Punkt, Komma oder Ausrufungszeichen bestehen.

– Fehlende Anmeldesperre

Moderne Betriebssysteme erlauben es, missbräuchliche Anmeldeversuche dadurch zu blockieren, dass die Benutzerkennung nach einer bestimmten Anzahl von Anmeldeversuchen deaktiviert wird und Anmeldungen mit dieser Benutzerkennung ohne Freischaltung der Benutzerkennung durch einen Systemadministrator nicht mehr möglich sind. Diese Vorkehrung ist notwendig, weil innerhalb eines Netzwerks Anmeldungen von jedem Rechner durchgeführt werden können. Die dafür notwendigen Benutzernamen können auf vielfältige Weise in Erfahrung gebracht werden. Es kann dann unter Nutzung des Benutzernamens auf die in einem System gespeicherten Daten zugegriffen werden, indem Anmeldungen vorgenommen werden, wobei versucht wird, das Kennwort, das der Benutzerkennung zugeordnet ist, zu erraten. Die Rateversuche werden automatisch von einem anderen Rechner über ein Netzwerk durchgeführt und als Kennwörter beispielsweise Begriffe aus einem Lexikon oder einem Wörterbuch benutzt. Wenn das Kennwort, wie bei den Einstellungen dieser Gemeinde möglich, einfach aufgebaut ist, dann führen die Rateversuche, die auch bei langsameren Systemen mindestens fünfmal pro Sekunde durchgeführt werden können, früher oder später zum Erfolg. Deshalb ist es erforderlich, eine Maßnahme zu ergreifen, die dies verhindert, indem weitere Versuche, eine Anmeldung mit der Benutzerkennung durchzuführen, nach einer festen Anzahl fehlgeschlagener Anmeldeversuche unterbunden werden. Aber genau diese Einstellung hatte die Gemeinde nicht getroffen. Bei den angetroffenen Einstellungen war es möglich, beliebig viele Anmeldeversuche mit einer Benutzerkennung zu unternehmen. Verschlimmert wird das Ganze noch dadurch, dass dies häufig von den Benutzern gar nicht bemerkt wird. Erst wenn eine Anmeldesperre greift, würde erkennbar, dass fehlgeschlagene Anmeldungen mit einer Benutzerkennung durchgeführt wurden.

Neben diesen Mängeln stießen meine Mitarbeiter bei der Überprüfung des Aktenmanagementsystems auf einen weiteren datenschutzrechtlichen Fehltritt: Die Gemeinde verwaltet ihre Akten rechnergestützt mit einem Aktenmanagementsystem. Damit bildet sie den Landesaktenplan ab. Eine Akte besteht hierbei aus Informationen zur Akte und aus Dokumenten. Die Informationen, die der Suche und Auswertung dienen, werden in einem Datenbanksystem hinterlegt. Die Dokumente, die zu einer Akte gehören, werden im Dateisystem eines Servers gespeichert. Das Aktenmanagementsystem erlaubt sehr spezialisierte Einstellungen dahin gehend, wer worauf Zugriff hat. Diese Zugriffsmechanismen wurden von der Gemeinde auch genutzt, indem sie die Mitarbeiter der Gemeindeverwaltung entsprechend den einzelnen Ämtern so in Gruppen eingeteilt hatte, wie die Tätigkeiten der Mitarbeiter den Zugriff auf die einzelnen Akten erfordern. Sowohl auf der Ebene des Datenbanksystems als auch auf der des Dateisystems wurden die Akten und Dokumente durch Gruppenattribute geschützt. Nur Mitgliedern der entsprechenden Gruppen wurde der Zugriff auf die Dokumente gewährt. Insofern gab es nichts zu bemängeln. Dennoch hatte die Gemeinde einen datenschutzrechtlich schweren Fehler begangen. Sie hatte nämlich eine Akte „Alles“ angelegt und geführt, auf die jeder Mitarbeiter der Gemeindeverwaltung lesenden und schreibenden Zugriff hatte. In dieser Akte wurden beispielsweise die Ratsvorlagen für Gemeinderatssitzungen gesammelt. Darunter befanden sich Vorgänge zu Anträgen auf Stundungen von Bestattungsgebühren, zu unbefristeten Niederschlagungen von Zahlungsrückständen und zur Vergabe von Bauplätzen. Hierbei wurden nicht nur die Namen der Antragsteller und die Höhe der Geldforderungen, sondern auch Einzelheiten aus dem familiären Umfeld der Betroffenen in den Dokumenten offenbart. Die Gemeinde wurde auf die datenschutzrechtlich nicht zulässige Verarbeitung personenbezogener Daten hingewiesen; sie hat die Fehler eingeräumt und zugesagt, dass die Akte gelöscht und zukünftig bei der Vorbereitung von Gemeinderatssitzungen ein datenschutzrechtlich korrektes Verfahren angewandt wird.

2.2 Das neue Lebensmittelüberwachungs- und Veterinärinformationssystem LÜVIS

Was wir tagtäglich an Nahrung zu uns nehmen, soll höchsten Qualitätsansprüchen genügen. Ungenießbares oder sogar Gesundheitsgefährdendes gehört weder in die Verkaufsregale noch auf den Teller. Deshalb werden Lebensmittelerzeugung und Lebensmittelvertrieb gründlich überwacht. Dienststellen bei Gemeinden, Kreisen, Regierungspräsidien und Ministerien des Landes nehmen hierbei unterschiedlichste Aufgaben wahr. Um die Aufgaben, die zukünftig an die Lebensmittelüberwachung gestellt werden, bewältigen zu können, mussten die bisher verwendeten Systeme – Lebensmittelbetriebsdatei (LmBD) und Veterinärinformationssystem (VIS) – durch ein neues Informationssystem abgelöst werden. Mit dem neuen Verfahren LÜVIS wird ein Informationssystem zum Einsatz kommen, das den Behörden einen umfassenden Überblick im Lebensmittel- und Veterinärbereich geben soll. Jeder Betrieb, der im Land mit der Herstellung und dem Import von Lebensmitteln sowie mit dem Lebensmittelhandel zu tun hat, wird in diesem System gespeichert. Ebenso erstreckt sich die Kontrolle auf die Aufzucht von Tieren und die daran beteiligten Personen wie etwa Landwirte oder Tierärzte. Aber auch personenbezogene Angaben von Bürgern, die sich über ein Produkt eines Betriebes beschwert haben, werden in dem System erfasst.

Das bedeutet, dass in dem Informationssystem Daten einer Vielzahl von Personen gespeichert werden. Das System muss daher den Anforderungen gerecht werden, die das Datenschutzrecht an die Verarbeitung personenbezogener Daten stellt. Besonders zu beachten ist dabei, dass die Daten von unterschiedlichen Stellen erhoben und gespeichert werden, dass aber alle mit der Lebensmittelüberwachung beauftragten Stellen auf die Informationen ihres Verwaltungsbereichs zugreifen können müssen. Dass das Verfahren im Rahmen einer Datenverarbeitung im

Auftrag von einer Dienststelle des Ministeriums für Ernährung und Ländlichen Raum für die nutzenden Kommunal- und Landesbehörden betrieben wird, macht die Sache nicht einfacher. Das hat das Ministerium, das den Entwicklungsauftrag für die Anwendung gegeben hat, erkannt und uns um beratende Mitwirkung gebeten.

Im Einzelnen haben wir uns zu folgenden Problemen geäußert:

– Automatisiertes Abrufverfahren

  In dem System werden von unterschiedlichen Stellen personenbezogene Daten eingegeben und abgerufen. Es müssen dann die nach dem Landesdatenschutzgesetz für einen Abruf erforderlichen Maßnahmen getroffen werden. Insbesondere muss mindestens im Rahmen eines Stichprobenverfahrens die Zulässigkeit einer Übermittlung festgestellt und überprüft werden können. Hierfür sind entsprechende Protokollierungsmechanismen bereitzustellen.

– Speicherung von Bürgern als Beschwerdeführer

  Die grundsätzliche Erforderlichkeit der Speicherung von personenbezogenen Daten von Bürgern, die an eine Behörde mit der Bitte um Prüfung herangetreten sind, ist nicht von der Hand zu weisen. Schließlich hat der Bürger ein Recht darauf, dass seine Eingabe beschieden wird, und dazu muss ihm mitgeteilt werden können, ob seine Beschwerde begründet war und welche Maßnahmen zur Wiederherstellung der Lebensmittelsicherheit ergriffen wurden. Hieraus ergibt sich auch, dass die Daten des Bürgers in einen Zusammenhang mit Ermittlungen, die beispielsweise in Probeentnahmen bestehen können, gebracht werden müssen. Wichtig ist jedoch, dass sich die Speicherfrist für die Daten des Bürgers von der Speicherfrist der im Zusammenhang mit der Beschwerde erhobenen Daten unterscheidet. Während Probedaten mehrere Jahre gespeichert werden dürfen, können die Daten von Bürgern häufig viel früher gelöscht werden. Wir haben darauf hingewiesen, dass die Systemarchitektur dem Grundsatz der Datenvermeidung Rechnung tragen muss.

– Speicherung von Betriebsangehörigen

  Bei diversen Maßnahmen ist es aus Gründen der Beweissicherung notwendig, dass neben dem Geschäftsführer, dessen Identitätsdaten im Allgemeinen gespeichert sind, die Identität von anwesendem Betriebspersonal gespeichert wird, da diese Mitarbeiter möglicherweise als Zeuge auftreten müssen. Die gespeicherten Daten von Betriebsangehörigen sollten unverzüglich gelöscht werden, wenn absehbar ist, dass es zu keiner verwaltungsgerichtlichen Überprüfung der Maßnahme kommt. Gibt es ein verwaltungsgerichtliches Verfahren, so sollten die personenbezogenen Daten der Betriebsangehörigen nach Abschluss des Verfahrens gelöscht werden – die Daten einer Probeentnahme bleiben regelmäßig über den Zeitpunkt eines verwaltungsgerichtlichen Verfahrens hinaus gespeichert. Auch hier ist darauf hinzuwirken, dass unterschiedliche Speicherfristen systemtechnisch eingehalten werden können.

– Freitextfelder

  Es ist nachzuvollziehen, dass nicht alle Daten eines Informationssystems, in dem Daten eines so breit gefächerten Anwendungsbereichs gespeichert werden, aus standardisierten Einzelangaben, wie beispielsweise Namen, Messwerten und Katalogbegriffen, bestehen können. Daher werden an einer Vielzahl von Stellen innerhalb der Anwendung sog. Freitextfelder verwendet. Allerdings bergen Freitextfelder, sofern die gespeicherten Daten einen Personenbezug haben, folgende Risiken:

  • Die in Freitextfeldern gespeicherten Daten könnten einer unterschiedlichen Speicherfrist unterliegen. Eine automatische Löschung scheidet aufgrund der Unstrukturiertheit der Daten aus.

Das heißt, dass eine datenschutzrechtlich zulässige Löschung nur dadurch bewerkstelligt werden kann, dass jeder Datensatz eines Freitextfelds manuell von einem Sachbearbeiter überprüft und gegebenenfalls Teile davon gelöscht werden. Dass diese Verfahrensweise ab einer bestimmten Anzahl von Datensätzen an seine Realisierungsgrenzen stößt, bedarf keiner weiteren Erklärung.

- Die in den Freitextfeldern gespeicherten Daten könnten nicht der Zweckbindung unterliegen, wobei wir regelmäßig davon ausgehen, dass die Lösung vom Zweckbindungsgebot nicht absichtlich erfolgt. Wenn man wie bei dieser Anwendung die Möglichkeit hat, in nahezu unbegrenztem Umfang Freitext einzugeben, besteht die Gefahr, dass man persönliche oder sachliche Verhältnisse des Betroffenen festhält, obwohl deren Speicherung nicht erforderlich ist und nach dem Datenvermeidungsgrundsatz unterbleiben sollte.

Es ist daher immer zu prüfen, ob die Daten, die in einem Freitextfeld gespeichert werden sollen, nicht ganz oder teilweise in Einzeldatenfeldern gespeichert werden können.

– Revisionsfähigkeit

Das Landesdatenschutzgesetz fordert von einer Anwendung, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in ein Datenverarbeitungssystem eingegeben worden sind.

Dieser Anforderung wird durch LÜVIS in vollem Umfang Rechnung getragen. Jeder Datensatz besteht neben den Anwendungsdaten aus weiteren Datenfeldern, in denen abgespeichert wird, wann und von wem der Datensatz angelegt und zuletzt geändert wurde.

– Löschung

Daten, die für das weitere Verwaltungshandeln nicht mehr erforderlich sind, müssen gelöscht werden. Dies ist ein eherner Grundsatz des Datenschutzrechts. Ihm muss man auch nachkommen, wenn die Datenbestände, die eine Person betreffen, aus unterschiedlichen Quellen herrühren können. Die Löschung darf sich dabei nicht wie in dem Verfahren darauf beschränken, zu löschende Datensätze als „gelöscht“ zu markieren und bei einer Abfrage nicht mehr anzuzeigen. Dann handelt es sich nämlich nicht um eine Löschung, sondern lediglich um eine Sperrung. Voraussetzung für eine Sperrung ist aber, dass die Richtigkeit der Daten entweder vom Betroffenen bestritten wird, Grund zur Annahme besteht, dass schutzwürdige Interessen des Betroffenen beeinträchtigt werden oder dass die Löschung nur mit unverhältnismäßig hohem Aufwand möglich ist. Liegen diese Voraussetzungen nicht vor, muss die dann gebotene Löschung in Form einer physikalischen Löschung, die zur Unkenntlichkeit der Daten führt, durchgeführt werden.

– Datenexport in Excel-Tabellen

An mehreren Stellen des Verfahrens besteht die Möglichkeit, die Daten aus der Anwendung zu exportieren und in einem anderen Programm weiter zu verarbeiten. Hinsichtlich des technischen Datenschutzes ist dann zu befürchten, dass auf den lokalen Festplatten einer Vielzahl von PC personenbezogene Daten gespeichert werden. Diese Vorgehensweise birgt unkontrollierbare Risiken, denn es kann dann nicht kontrolliert werden, ob

- diese Daten entsprechend der Zweckbindung verarbeitet werden,
- der Zugriff auf die Daten nur durch Befugte möglich ist und
- die Daten entsprechend des Erforderlichkeitsgrundsatzes gelöscht werden.

Aus diesem Grund halten wir folgende Maßnahmen für erforderlich, wenn ein sog. Download aus einer Anwendung unterstützt werden soll:

- Durch einen Berechtigungsmechanismus muss sichergestellt sein, dass nur für den Download Berechtigte diesen durchführen können. Der Kreis der Berechtigten ist minimal zu halten.
- Die Speicherung von personenbezogenen Daten im Rahmen eines Downloads sollte nur auf Festplatten von Servern geschehen. Es ist sicherzustellen, dass die Speicherung in Speicherbereichen erfolgt, die Zugriffsregelungen unterliegen, so dass nur Berechtigte auf die Daten zugreifen können.

Häufig wird unsere Frage, warum ein Download notwendig sei und warum die nach dem Download beabsichtigte Verarbeitung nicht im Verfahren selbst durchgeführt werde, damit beantwortet, dass man die konkrete Verarbeitung noch nicht im Detail festlegen könne. Wenn aber der Umfang der Verarbeitung noch nicht feststeht, kann es mit der Einhaltung des Zweckbindungsgrundsatzes wohl nicht so weit her sein. Für eine Verarbeitung außerhalb des eigentlichen Verfahrens spricht nämlich nur, dass die Anwendung, mit der die Daten weiterverarbeitet werden, schon besteht und durch Verwendung dieser bereits bestehenden Anwendung ein Einspareffekt hinsichtlich der Programmierung erzielt werden kann.

– Ein nicht unwesentlicher Zweck der Anwendung besteht darin, den gesetzlichen Berichtspflichten nachzukommen. Hierfür soll der Datenbestand statistisch ausgewertet werden. Dabei war das Problem zu erörtern, dass bei statistischen Auswertungen die Treffermenge bisweilen aus einem Exemplar der Grundgesamtheit bestehen kann. Wenn sich dies so verhält, kann nicht mehr generell davon gesprochen werden, dass eine Statistik nur aus anonymisierten Daten besteht. Wir sind in der Sache so verblieben, dass versucht wird, die Grundgesamtheit für die Auswertungen so groß wie möglich zu wählen. Dadurch erhöht sich die Wahrscheinlichkeit, dass Treffermengen aus mehreren Exemplaren der Grundgesamtheit bestehen.

Die Entwicklung von LÜVIS, das schon produktiv eingesetzt wird, ist noch nicht beendet. Es ist beabsichtigt, weitere Anwendungsfelder in das System zu integrieren. Hierbei wird darauf zu achten sein, dass auch hinsichtlich der Erweiterungen die datenschutzrechtlichen Anforderungen angemessen berücksichtigt werden.

3. Virenschutz im LVN

Mittlerweile hat wahrscheinlich schon jeder von Computer-Viren und deren unheilvoller Wirkung gehört oder gelesen. Dazu kommen noch die Unannehmlichkeiten, wenn der am Arbeitsplatz oder zu Hause genutzte PC von einem Computer-Virus befallen ist. Eine unwillkommene Unterbrechung eigener Tätigkeiten ist noch das Harmloseste, wenn sich der Computer-Virus – im besten Fall – durch allerlei Schabernack zu erkennen gibt. Um den Computer-Virus zu entfernen, sollte man sich aus dem Internet Antikörper in Form von Virensignaturen besorgen, mit denen die Dateien auf Virenbefall geprüft und die Computer-Viren auf Wunsch entfernt werden, und mit einem Virenprüfprogramm den Rechner säubern. Die Wirkung von Computer-Viren beschränkt sich aber nicht nur darauf, die Benutzer von produktiver Arbeit abzuhalten, sondern es gibt beispielsweise auch Computer-Viren, die klammheimlich Dateien des Rechners, auf dem sie sich eingenistet haben, an beliebige, auf dem Rechner vorgefundene E-Mail-Adressen verschicken. Andere ermöglichen es Dritten, den Rechner aus der Ferne zu steuern und beispielsweise abzuhören, welche Tasten betätigt wurden, oder Dateien zu übertragen. Da in den so versendeten Dateien personenbezogene Daten gespeichert sein könnten, greift für Rechner von Behörden das Landesdatenschutzgesetz. Danach sind dem technischen Stand entsprechende Maßnahmen gegen die unbefugte Kenntnisnahme und Nutzung personenbezogener Daten zu ergreifen. Das machen die Behörden anscheinend auch,

denn im abgelaufenen Berichtsjahr haben wir bei den durchgeführten Kontrollen keine Rechner vorgefunden, auf denen nicht ein Virenschutzprogramm installiert gewesen wäre. Aber welchen Erfolg haben die Behörden bei der Virenbekämpfung? Zur Erörterung dieser Frage muss man zunächst die Bedrohungslage erläutern. Alle Behörden des Landes sind an das Landesverwaltungsnetz (LVN) angeschlossen. Das LVN selbst ist – etwas anderes wäre heutzutage undenkbar – mit dem Internet gekoppelt. Innerhalb dieses Netzverbunds können die Mitarbeiter Nachrichten durch elektronische Post austauschen, die sie nach Landesstandard mit dem Programm Outlook empfangen, lesen und gegebenenfalls weiterverarbeiten. Wenn man nun weiß, dass Computer-Viren bevorzugt mit Anhängen dieser Nachrichten verbreitet werden, weil mit Outlook eine Infizierung schon durch einen unbedachten Mausklick eines Benutzers bewirkt werden kann, ist klar, dass die Bedrohung durch einen Computer-Virus nicht zu unterschätzen ist.

Die Netzwerkstruktur des LVNs erlaubt es, an einer zentralen Stelle, an der die Koppelung der Netze der einzelnen Ressorts und des LVNs mit dem Internet realisiert wird, einen Viren-Scanner zu installieren, der eine detaillierte Statistik über sein Tun führt. Dieser Statistik ist Folgendes zu entnehmen:

– Im Jahr 2003 hat der zentrale Viren-Scanner in E-Mails, die zwischen den Ressorts ausgetauscht wurden – also nur im Intranet der Landesverwaltung – über 2 100 Nachrichten entdeckt, die virenverseucht waren. Vom 1. Januar 2004 bis Mitte November 2004 wurden in den E-Mails über 90 000 verseuchte Nachrichten entdeckt. Dies entspricht einer Steigerung von mehr als 4 200 % gegenüber dem Vorjahr.

– Im Jahr 2003 wurden in E-Mails aus dem Internet über 370 000 Computer-Viren entdeckt. Vom 1. Januar 2004 bis zum 18. November 2004 waren es über 7 300 000 verseuchte Nachrichten. Dies entspricht einer Steigerung von mehr als 1 900 % gegenüber dem Vorjahr.

– Der März 2004 mit ca. 38 000 und der April 2004 mit ungefähr 21 500 Nachrichten waren die Monate mit dem größten Aufkommen an verseuchten E-Mails. Im Durchschnitt belief sich das monatliche Aufkommen im Jahr 2004 auf ungefähr 9 000 Nachrichten, mit einer Schwankungsbreite zwischen 1 700 und besagten 38 000 Nachrichten.

– Während 2003 bei den internen Computer-Viren der Computer-Virus namens Sobig-F nur knapp vor Brod-A und Dumaru-A lag, die in der Summe nicht auf über 1 000 verseuchte E-Mails kamen, ist im Jahr 2004 Netsky-D mit mehr als 60 000 verseuchten Nachrichten einsamer Spitzenreiter. Den Grundstein hierfür legte er im März 2004 mit über 37 000 und im April 2004 mit mehr als 17 500 Nachrichten, in denen er sich einnisten konnte. Abgeschlagener Zweiter im Jahr 2004 ist MyDoom-A mit ca. 7 800 Nachrichten. Noch nicht entschieden ist das Rennen um Platz drei zwischen Netsky-B mit ca. 3 600 und MyDoom-O mit ungefähr 4 600 Nachrichten pro Jahr.

– Obwohl er im LVN wohl der am meisten verbreitete Computer-Virus ist, ist Netsky-D interessanterweise weder im März noch im April 2004 und auch nicht im laufenden Jahr der in E-Mails aus dem Internet am häufigsten enthaltene Computer-Virus. Auf Monatsbasis können Roca-A im März mit 436 000 und Netsky-P im April mit 310 000 Nachrichten punkten. Im laufenden Jahr führt bei E-Mails aus dem Internet Netsky-P mit ca. 1 900 000 verseuchten Nachrichten.

Dass nach wie vor eine erhebliche Zahl von Computer-Viren in E-Mails verbreitet wird, was gleichzeitig bedeutet, dass auch eine nicht unerhebliche Anzahl von PC, von denen die E-Mails abgeschickt wurden, infiziert sind, liegt an mehreren Faktoren:

– Die Hersteller von Virenprüfprogrammen können nur auf neue Computer-Viren reagieren. Wegen der hohen Verbreitungsgeschwindigkeit kommt es zu einer Vielzahl von Infektionen, bevor ein wirksames Gegenmittel entwickelt wurde. Das hat zur Folge, dass die Vorlaufzeit, die die Systemadministratoren haben, um die Virensignaturen auf den Rechnern des LVN zu installieren, sehr kurz ist. Deshalb gelingt es den Com-

puter-Viren vermehrt, in das LVN einzudringen, bevor der zentrale Viren-Scanner mit aktuellen Virensignaturen ausgestattet werden kann.

– Die Verbreitung von Computer-Viren ist – zumindest bei den Computer-Viren, die sich über Anhänge in E-Mails verbreiten – abhängig von der Mitwirkung der Benutzer.

– Es ist möglich, dass durch den Einsatz von Notebooks eine Infektion eingeschleppt wird, wenn beispielsweise auf Postfächer von externen Mail-Providern zugegriffen wird.

– In seltenen Fällen werden von den Virenherstellern Virensignaturen verbreitet, die einen neuen Computer-Virus nicht effektiv bekämpfen, oder die Installation der Virensignaturen funktioniert nicht reibungslos.

Eine Analyse des derzeitigen Zustandes kann sich nicht darauf beschränken, die Defizite aufzuzeigen. Für eine verbesserte Bekämpfung von Computer-Viren gibt es folgende Ansatzpunkte:

– Bei den Computer-Viren, die sich nicht über eine E-Mail verbreiten, sondern das System direkt zu infizieren versuchen, sind die Hersteller gefordert. Die Sicherheit der Software muss erhöht werden. Eine Infektion, die dadurch herbeigeführt wird, dass ein Bild in einem Internet-Browser angezeigt wird, oder dass man, während man im Internet surft, mit der Maus eine bestimmte Aktion durchführt, kann nur durch entsprechend sichere Software verhindert werden. Gegebenenfalls sollte der Einsatz alternativer Produkte erwogen werden.

– Die Bekämpfung von Computer-Viren, die sich über E-Mail weiterverbreiten, kann durch Schulung der Benutzer verbessert werden. Noch immer klicken Benutzer unbesehen auf E-Mail-Anhänge von Nachrichten, deren Absender sie nicht kennen und die die Neugier der Empfänger zu wecken verstehen.

Die Antwort auf die eingangs gestellte Frage, wie erfolgreich die Behörden des Landes im Kampf gegen die Flut von Computer-Viren sind, kann angesichts der geschilderten Feststellungen nicht durchweg positiv ausfallen. Dass Sicherheit etwas Relatives sei, erklären uns die Experten bei jeder Infektionswelle, die von einem neuen Computer-Virus ausgelöst wird. Das gilt anscheinend auch im LVN. Der Glaube, die Rechner im LVN seien hinsichtlich der Infektion mit Computer-Viren sicher, muss angesichts der Zahlen zu Grabe getragen werden. Wenn man die Steigerungsraten betrachtet, schneidet das LVN sogar schlechter ab als das Internet, da die prozentuale Steigerungsrate der virenverseuchten internen E-Mails doppelt so hoch ist wie bei E-Mails aus dem Internet. Täglich – außer an Feiertagen – werden im Intranet der Landesverwaltung im Durchschnitt ca. 250 infizierte E-Mails verschickt. Dabei kann es sich nicht immer nur um die gleichen PC handeln. An einem Tag, an dem über 4 500 virenverseuchte E-Mails von Rechnern des LVNs verschickt werden, muss davon ausgegangen werden, dass zu diesem Zeitpunkt ca. 40 PC verseucht sind. Andererseits bedeutet dies auch, dass permanent die Gefahr besteht, personenbezogene Daten gegenüber Unbefugten zu offenbaren. Und das sind nur die bekannten Zahlen. Daneben gibt es natürlich noch eine Dunkelziffer von nicht erkennbaren Vorgängen.

4. Datensicherheit in Funknetzwerken

Die zunehmende Verbreitung funkgestützter Computernetzwerke (WLAN) haben wir bereits in unserem vergangenen Tätigkeitsbericht zum Anlass genommen, auf die damit verbundenen Datenschutzrisiken und entsprechende Lösungsmöglichkeiten hinzuweisen. Auch in diesem Jahr beschäftigte uns das Thema.

4.1 Ungesichertes WLAN eines Staatlichen Seminars für Lehrerbildung

Unzureichend gesicherte WLANs stellen in verschiedener Hinsicht ein Risiko für den Betreiber dar. Zum einen können dessen Daten Unberechtigten bekannt werden, zum anderen kann dem Betreiber eines solchen Netzwerks auch ein handfester finanzieller Schaden entstehen, etwa wenn Fremde über die Funkverbindung eine kostenpflichtige In-

ternet-Verbindung des Betreibers in Anspruch nehmen. Vor diesem Hintergrund führten Computer-Fachzeitschriften und Verbraucher-Magazine des Fernsehens stichprobenweise Tests durch, in denen sie untersuchten, wie leicht es gelingt, in fremde WLANs einzudringen. Die dabei zu Tage tretenden Erkenntnisse sind alarmierend: Trotz aller Versuche, die Sicherheitsprobleme und auch die finanziellen Risiken eines schlecht konfigurierten WLANs zu vermitteln, macht eine Mehrzahl der Betreiber nicht einmal von den einfachsten Sicherheitstechniken Gebrauch. Darüber, dass es derartige Sicherheitslücken auch bei einem Staatlichen Seminar für Lehrerbildung nachweisen konnte, unterrichtete uns ein Fernseh-Team. Es hatte herausgefunden, dass man auch noch auf der Straße und auf dem Fußweg vor dem Bürogebäude des Seminars ohne weiteres Zugang zu dessen WLAN erhalten konnte. Unsere daraufhin durchgeführte Kontrolle bestätigte, dass das Seminar bei der Einrichtung des WLANs offenbar nicht an die Möglichkeit einer unberechtigten Nutzung gedacht und entsprechend keinerlei Schutzmaßnahmen ergriffen hatte. Das Computernetz, das auf diese Weise zugänglich war, dient Ausbildungszwecken, und es ist davon auszugehen, dass darin in der Regel keine personenbezogenen Daten verarbeitet werden. Gleichwohl ist auch der Betrieb eines solchen Netzwerks datenschutzrechtlich nicht ohne Risiko. Sind etwa auf einem Notebook, das gerade drahtlos mit diesem Schulungs-WLAN verbunden ist, Dateien, Verzeichnisse oder ganze lokale Laufwerke zum Zugriff über Netz freigegeben (vgl. die in Nr. 1.5.1 dargestellte Problematik), so könnten Personen, die sich ihrerseits drahtlosen Zugang zu dem Netz verschafft haben, unberechtigt auf diese Daten zugreifen. Das Seminar hat mittlerweile Maßnahmen zum Schutz seines WLANs ergriffen.

4.2 Weiterentwicklung der Sicherheitstechniken

Die in unserem letzten Tätigkeitsbericht enthaltene Übersicht über die standardmäßig in den WLAN-Produkten verfügbaren Sicherheitstechniken machte deutlich, dass diese insgesamt nicht ausreichen, um etwa auch die Verarbeitung sensibler personenbezogener Daten zu schützen. Die bis dahin verabschiedeten Sicherheitsstandards haben sich vielmehr als in vielfältiger Weise unzulänglich erwiesen. Es ist deshalb sehr zu begrüßen, dass der lange in Aussicht gestellte neue Sicherheitsstandard (der sog. IEEE 802.i-Standard) im Juni dieses Jahres verabschiedet wurde. Da dessen Umsetzung eine erhöhte Sicherheit gewährleistet, sollten alle Dienststellen, die ein WLAN betreiben oder dies beabsichtigen, auf Komponenten zurückgreifen, die diesen Standard unterstützen. Zu einem leichtfertigen Einsatz eines WLANs darf aber auch dieser neue Sicherheitsstandard nicht verleiten. Denn zum einen bleibt abzuwarten, ob sich die neuen Produkte auch in der Praxis als so verlässlich erweisen, wie dies die Theorie verheißt. Und zum anderen erfordert auch eine Technik, die zahlreiche Sicherheitsfunktionen bietet, dass die Nutzer verantwortungsvoll damit umgehen und diese Sicherheitsfunktionen nicht ungenutzt lassen oder gar absichtlich deaktivieren.

5. Überraschungen beim Kauf eines Softwarepakets

Wir erhielten einen Hinweis darauf, dass zwei baden-württembergische Universitäten ein Softwareentwicklungspaket erworben haben sollen, das neben den von den Universitäten benötigten Entwicklungswerkzeugen auch eine Datenbank umfasste, die personenbezogene Daten ehemaliger Beschäftigter und Kunden des Softwareunternehmens enthalten habe. Auf unsere Nachfragen bestätigten die Universitäten, dass in der zum Softwarepaket gehörenden Datenbank personenbezogene Daten gespeichert waren, die die Universitäten weder benötigten noch haben erwerben wollen. Datenschutzrechtlich ist diese Speicherung personenbezogener Daten durch die Universitäten aus zwei Gründen problematisch:

Zum einen speicherten die Universitäten, wenn auch möglicherweise zunächst, ohne dass ihnen das überhaupt bewusst war, personenbezogene Daten, die sie nicht benötigen.

Zum anderen waren die in der Software enthaltenen personenbezogenen Daten zum Teil in Form von persönlichen Benutzerberechtigungen und den zur Nutzung einzugebenden Passwörtern gespeichert, die möglicherweise nach Installation der Software durch die Universitäten von Dritten hätten genutzt werden können. Diese könnten dann missbräuchlich auf die Software und die damit verarbeiteten Daten zugreifen.

Wir forderten die Universitäten daher auf, die im Softwareentwicklungspaket gespeicherten und von den Universitäten nicht benötigten personenbezogenen Daten umgehend zu löschen. Dem kamen beide Universitäten nach.

Inhaltsverzeichnis des Anhangs

Anhang 1

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. März 2004

Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004
zum Großen Lauschangriff und zur präventiven
Telekommunikationsüberwachung

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechts- und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 3. März 2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten.

Anhang 2

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 28./29. Oktober 2004

Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum „Großen Lauschangriff“ in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens“ offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und andern engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

Anhang 3

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. März 2004

Automatische Kfz-Kennzeichenerfassung durch die Polizei

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können.

Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz-Kennzeichen-Erfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. Schon der mit der Feststellung gesuchter Fahrzeuge verbundene Abgleich würde zu einem neuen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen führen, die weit überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.

Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.

Die Datenschutzbeauftragten weisen darauf hin, dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen.

Anhang 4

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 28./29. Oktober 2004

Gravierende Datenschutzmängel bei Hartz IV

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20. September 2004 sog. „Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II“ zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

Anhang 5

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schließt sich voll inhaltlich der folgenden Entschließung an*:

Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

Entschließung zu Radio-Frequency Identification
vom 20. November 2003
(Übersetzung)

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kreditkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

a) sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen, zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;

b) wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;

c) dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur so lange aufbewahrt werden, wie es zu Erreichung dieses Zwecks erforderlich ist und

d) soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

* Beschluss vom 25./26. März 2004

Anhang 6

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. März 2004

Einführung eines Forschungsgeheimnisses für medizinische Daten

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnen und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden – anders als insbesondere den behandelnden Ärztinnen und Ärzten – nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,
- in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,
- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

Anhang 7

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 13. Februar 2004

Übermittlung von Flugpassagierdaten an die US-Behörden

Die Datenschutzbeauftragten des Bundes und der Länder bestärken die Bundesregierung darin, sich für Verbesserungen des Datenschutzes bei der Übermittlung von Flugpassagierdaten an die Zoll- und Sicherheitsbehörden der USA einzusetzen.

Durch einseitigen Rechtsakt haben die USA die Fluggesellschaften, die ihr Land anfliegen, unter Androhung teilweise empfindlicher Strafen verpflichtet, den US-Zoll- und Sicherheitsbehörden den Zugang zu ihren Reservierungsdatenbanken zu eröffnen, um anhand der darin enthaltenen Informationen über die Fluggäste mögliche terroristische oder kriminelle Aktivitäten frühzeitig zu erkennen. In den Reservierungsdatenbanken halten die an der Reisedurchführung beteiligten Stellen alle Informationen fest, die sie benötigen, um die Flugreise abzuwickeln. Es werden z. B. Name, Reiseverlauf, Buchungsstelle, Art der Bezahlung, bei Zahlung mit Kreditkarte deren Nummer, Sitzplatz, Essenswünsche, notwendige Reisevorkehrung wegen einer Erkrankung eines Fluggastes, Hotel- und Mietwagenreservierungen im Buchungssystem gespeichert. Teilweise sind die gespeicherten Daten sensitiv, weil sie Rückschlüsse auf die Gesundheit einzelner Fluggäste oder religiöse oder politische Anschauungen ermöglichen.

Die US-Zollbehörden wollen alle Reservierungsdaten mindestens 3,5 Jahre speichern ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorlag oder nicht. Passagierdaten, die im Einzelfall überprüft wurden, sollen zudem weitere 8 Jahre gespeichert werden.

Die Datenschutzbeauftragten verkennen nicht, dass nach den Ereignissen des 11. Septembers 2001 ein erhöhtes Bedürfnis nach Sicherheit im Flugverkehr offensichtlich ist. Sie verschließen sich deshalb keineswegs Forderungen, die auf eine sichere Identifikation der Fluggäste zielen. Dennoch muss festgestellt werden, dass die Forderungen der USA weit über das hinausgehen, was erforderlich ist. Da die Reservierungsdatenbanken nicht für Sicherheitszwecke, sondern zur Durchführung der Flugreisen angelegt werden, enthalten sie auch eine Vielzahl von Daten der Reisenden, die für eine Sicherheitsüberprüfung der Passagiere irrelevant sind.

Mit dem Zugriff ist wegen der teilweise hohen Sensibilität der Daten ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen verbunden. Besonders hervorzuheben ist in diesem Zusammenhang, dass die US-Behörden hier aufgrund US-amerikanischen Rechts auf Datenbanken außerhalb ihres Hoheitsbereichs zugreifen. Die betroffenen Personen werden gegenüber dem Zugriff auf ihre Daten durch eine ausländische Stelle in ihren Datenschutzrechten weitgehend schutzlos gelassen. Ein vergleichbares Ansinnen deutscher Sicherheitsbehörden wäre schwerlich mit unserer Verfassung vereinbar.

Die Problematik kann sich weiter verschärfen, wenn die USA die Passagierdaten zukünftig auch im sog. CAPPS II-System einsetzen wollen. Dieses System ermöglicht sowohl einen automatisierten Abgleich mit Fahndungslisten als auch mit Informationen aus dem privaten Sektor. Insbesondere sollen Kreditkarten- und Adressdaten mit Informationen aus der Kreditwirtschaft abgeglichen werden.

Die Europäische Kommission bemüht sich seit über einem Jahr in Verhandlungen darum, den Datenzugang der US-Behörden auf ein angemessenes Maß zu beschränken. Leider führten die Verhandlungen nur in Teilbereichen zum Erfolg. Die erzielten Ergebnisse in ihrer Gesamtheit gewähren den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte. Dies hat die Gruppe nach Artikel 29 der Europäischen Datenschutzrichtlinie (EG-DSRL) in ihrer Stellungnahme vom 29. Januar 2004 deutlich herausgearbeitet:

Die darin vertretenen Positionen werden von den Datenschutzbeauftragten ausdrücklich unterstützt. Dennoch beabsichtigt die Europäische Kommission das Ergebnis ihrer Verhandlungen als einen angemessenen Datenschutzstandard förm-

lich anzuerkennen. Die Datenschutzbeauftragten appellieren an die Bundesregierung, sich gegen diese Entscheidung der Kommission zu wenden. Wenn die Kommission diesen unbefriedigenden Verhandlungsergebnissen ein angemessenes Datenschutzniveau attestiert, setzt sie damit Maßstäbe sowohl für die Auslegung der EU-Datenschutzrichtlinie als auch für Verhandlungen mit anderen Staaten über die Anerkennung des dortigen Datenschutzniveaus. Die Bundesregierung sollte sich demgegenüber für eine Lösung einsetzen, die Sicherheitsaspekte und den Schutz der Persönlichkeitsrechte in ein angemessenes Verhältnis setzt. Insbesondere sind die Informationen ausdrücklich zu benennen, die für die Passagieridentifikation benötigt werden. Diese Daten können zu einem angemessenen Zeitpunkt vor dem Abflug bereitgestellt werden. Ein unmittelbarer pauschaler Zugriff auf europäische Datenbanken, wie er zurzeit praktiziert wird, muss ausgeschlossen werden.

Anhang 8

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. März 2004

Personennummern

Das Bundesverfassungsgericht hat schon in seinem „Volkszählungsurteil“ aus dem Jahre 1983 besonders betont, dass ein Personenkennzeichen nicht verfassungsgemäß ist. Deshalb gibt die Einführung von einheitlichen Personennummern z. B. im Steuerbereich oder auch im Arbeits-, Gesundheits- und Sozialbereich Anlass zu grundsätzlicher Kritik. Der Staat darf seine Bürgerinnen und Bürger nicht zur Nummer abstempeln. Durch die technische Entwicklung sind vorhandene Dateien leicht miteinander zu verknüpfen und könnten zu einer vom Bundesverfassungsgericht strikt abgelehnten allgemeinen Personennummer führen.

Die Konferenz appelliert an die Gesetzgeber, solche Personennummern zu vermeiden. Soweit jedoch im Einzelfall derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

Anhang 9

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 28./29. Oktober 2004

Datensparsamkeit bei der Verwaltungsmodernisierung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

Anhang 10

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 26. November 2004

Staatliche Kontenkontrolle muss auf den Prüfstand!

Das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23. Dezember 2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93 b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24 c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z. B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.

Nunmehr sollen neben Finanzbehörden auch andere Behörden, z. B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen“ verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch „Wohnung“, „Kindergeld“, „Arbeitnehmer“), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z. B. anlässlich Steuererklärung, BAföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen.

Die Auskunft erstreckt sich zwar nicht auf die Kontostände; aufgrund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).