Landtag von Baden-Württemberg **Drucksache 13 / 1500**
13. Wahlperiode **02. 12. 2002**

Mitteilung

des Landesbeauftragten für den Datenschutz

Dreiundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

Schreiben des Landesbeauftragten für den Datenschutz in Baden-Württemberg vom 2. Dezember 2002:

Anbei übersende ich Ihnen unseren 23. Tätigkeitsbericht, der nach § 31 Abs. 1 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 1. Dezember 2002 zu erstatten ist.

Zimmermann

Eingegangen: 02. 12. 2002 / Ausgegeben: 12. 12. 2002

Dreiundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

INHALTSVERZEICHNIS

1. Teil: Zur Situation

Am 31. Oktober 2002 endete die Amtszeit des zweiten Landesbeauftragten für den Datenschutz in Baden-Württemberg, Herrn Werner Schneider. Mit ihm ging ein Mann der ersten Stunde des Datenschutzes im Lande, denn er war mit Schaffung des Amtes im Jahr 1980 – zunächst als leitender Beamter der Dienststelle und in den letzten knapp sechs Jahren dann als Landesbeauftragter – hier tätig. Werner Schneider hat durch kontinuierliche und beharrliche Sacharbeit die Position des Datenschutzes im Lande weiter gefestigt.

Wie geht es weiter? Zunächst ist hervorzuheben, dass es diesmal gelungen ist, die Position des Landesbeauftragten ohne zeitliche Verzögerung neu zu besetzen. Dies ist für das Amt und ganz sicherlich für mich als Amtsnachfolger positiv, da die Übergabe ohne Bruch erfolgen konnte. Trotz Wechsels geblieben sind natürlich die Rahmenbedingungen. Diese sind für die öffentliche Verwaltung insgesamt nicht rosig. Auch der Landesbeauftragte für den Datenschutz darf realistischerweise kaum erwarten, dass sich wie aus einem Füllhorn zusätzliche Personalstellen über ihn ergießen werden. Dabei würde der Datenschutz eine stärkere Präsenz des Landesbeauftragten durchaus vertragen. Denn der Datenschutz ist zwar insgesamt – schon angesichts seines mittlerweile vorgerückten Alters von mehr als 30 Jahren – durchaus den Kinderschuhen entwachsen; die Anforderungen an ihn sind deshalb aber nicht geringer geworden. Leider wird er oft immer noch nicht als eine Daueraufgabe begriffen, die – will man dem Grundrecht auf Datenschutz gerecht werden – eine ständige Auseinandersetzung mit den rechtlichen und technischen Anforderungen des Datenschutzes erfordert. Wie sonst ist es zu erklären, dass gerade im vergangenen Berichtsjahr Probleme aufgetreten sind, die man nun wirklich nicht mehr für möglich gehalten hätte? So zeigte sich etwa wiederholt, dass in den Behörden zwar durchaus akzeptable Datenschutzkonzepte erarbeitet wurden. Nicht selten fehlten aber offenbar das Bewusstsein und der Wille, diese bestehenden Vorgaben sozusagen auch bis zum Ende in die Tat umzusetzen. Mehrfach mussten wir jedenfalls bei Kontrollbesuchen vor Ort feststellen, dass selbst höchst sensible persönliche Daten einfach in den Abfall gewandert sind und so einem breiteren Publikum ohne weiteres zugänglich gemacht worden waren. Dies ist ein Rückfall in die Steinzeit des Datenschutzes und zeigt, dass auch das kleine Einmaleins des Datenschutzes nicht verlernt werden darf, sondern immer wieder neu geübt und auch praktiziert werden muss. Vereinzelt geäußerter Kritik der betroffenen Stellen an den geschilderten Kontrollmaßnahmen nach dem Motto: „Haben die denn nichts Besseres zu tun als in Abfalltonnen herumzukramen?“ muss ich entgegenhalten, dass die Suche in Abfallbehältern zwar tatsächlich nicht die Hohe Schule der Datenschutzkontrolle ausmacht. Die betrüblichen Ergebnisse unterstreichen aber nachdrücklich, dass Datenschutz nicht nur vom grünen Tisch aus betrieben werden kann, sondern auch ganz pragmatische Vorgehensweisen erfordert.

Die sozusagen am Ende der Datenschutzkette festgestellten gravierenden Mängel sollen aber nicht den Blick auf die eigentlichen inhaltlichen Probleme des Datenschutzes verstellen. Diese ergeben sich vor allem aus der zunehmend komplizierter werdenden Kommunikationslandschaft, in der sich auch die öffentliche Verwaltung zurechtfinden und behaupten muss. Und hier kann festgestellt werden, dass die Bereitschaft, sich den rechtlichen und technischen Anforderungen des Datenschutzes zu stellen, bei den Behörden und den anderen öffentlichen Stellen durchaus vorhanden ist, wobei die erhöhte Sensibilität der Bürgerinnen und Bürger in Sachen Datenschutz sicherlich auch dazu beigetragen hat. Die ständige und dynamische Fortentwicklung der Informationstechnologie erfordert jedoch, dass der Datenschutz mithalten muss, wenn er dem Grundrecht auf informationelle Selbstbestimmung auf Dauer wirklich die erforderliche Beachtung sichern will. Gelingen wird dies allerdings nur, wenn die öffentliche Verwaltung ihre Kräfte sinnvoll bündelt. Für das Amt des Landesbeauftragten für den Datenschutz bedeutet dies, dass die Gewichte der einzelnen Aufgabenbereiche neu austariert werden sollten. Völlig unangetastet bleiben muss dabei allerdings die Funktion als Anlaufstelle für Beschwerden der Bürgerinnen und Bürger. Dies ist und bleibt eine wichtige Aufgabe. Es muss auch in Zukunft sichergestellt sein, dass ein Beschwerdeführer zu seinen Fragen in angemessener Zeit eine aussagekräftige Stellungnahme des Daten-

schutzbeauftragten erhält. Deutlich an Gewicht zunehmen müssen und werden allerdings die Beratungsaktivitäten des Landesbeauftragten für den Datenschutz. Dies bestätigen zahlreiche Anfragen, die auf eine solche Beratung oder auch auf Fortbildungsmaßnahmen in Sachen Datenschutz gerichtet sind. Nicht allen Anfragen kann indes wegen fehlender Personalkapazitäten in dem wünschenswerten Maß entsprochen werden. Es sei denn, man würde künftig auf die dritte Aufgabensäule, nämlich auf die Kontrollfunktion, deutlich weniger Wert legen. Dass dies kaum sinnvoll ist, liegt angesichts der Ergebnisse unserer Kontrollen gerade im vergangenen Jahr auf der Hand.

Für Beratung und Kontrolle muss das Motto vielmehr heißen: „Das eine – verstärkt – tun, das andere nicht lassen." Die in aller Regel aufwändige Beratung erfordert in jedem Fall hohe Personalkapazitäten. Da mit einer strammen Zuweisung neuer Personalstellen nicht gerechnet werden darf und um einen höheren Beratungseinsatz nicht auf Kosten der bislang ohnehin nur sehr lückenhaft möglichen Kontrollen gehen zu lassen, bleibt nur der Weg, durch andere Maßnahmen die vorhandenen Kräfte zu konzentrieren, um dadurch den nötigen Spielraum für ein verstärktes Beratungs-Engagement zu erhalten. Die Möglichkeit hierfür gibt es. Es ist zwar kein neuer Gedanke, aber angesichts der schmalen öffentlichen Kassen bietet es sich gerade in der gegenwärtigen Situation an, die Datenschutzaufsicht im öffentlichen Bereich, die beim Landesbeauftragten liegt, und diejenige im nicht-öffentlichen Bereich, die gegenwärtig vom Innenministerium wahrgenommen wird, zusammenzulegen. Technisch und rechtlich sind die Fragestellungen in beiden Aufgabenbereichen jedenfalls in weiten Teilen inhaltsgleich, so dass eine Aufsicht aus einer Hand und aus einem Guss eine deutlich effizientere Aufgabenerledigung ermöglichen würde.

Insgesamt wird in der näheren Zukunft kritisch zu beobachten sein, welcher Stellenwert dem Datenschutz gerade auch in schwereren Zeiten beigemessen werden wird. So haben etwa die Ereignisse des 11. September 2001 in ihren Nachwehen zunächst zu teilweise verständlichen Spontanreaktionen geführt, die eine stärkere Einschränkung des individuellen Rechts auf informationelle Selbstbestimmung ins Visier genommen haben; zum anderen betrifft das Diktat der leeren öffentlichen Kassen auch den Datenschutz, da bei erkennbar komplexeren und umfangreicheren Herausforderungen nicht mit einer entsprechenden materiellen Stärkung des Datenschutzes gerechnet werden darf. Die Gefahr jedenfalls ist groß, dass der Datenschutz zwischen den Fronten, wenn nicht zerrieben, vielleicht aber doch zu einer beliebigen Verhandlungsmasse abgewertet werden wird.

2. Teil: Öffentliche Sicherheit und Justiz

1. Öffentliche Sicherheit

Kaum jemals zuvor gab es in Deutschland so viel Konsens, auch durch den Einsatz rechtlicher Instrumentarien die Freiheit zu sichern wie nach den Terroranschlägen vom 11. September 2001 in den USA. Die Gesetzgebungsmaschinerie kam rasch auf Touren. Bundestag und Bundesrat verabschiedeten im Parforceritt das Terrorismusbekämpfungsgesetz. Bereits am 11. Januar 2002 stand es im Bundesgesetzblatt. Wenn auch nicht alles, was von Sicherheitspolitikern in die Debatte geworfen und gefordert worden war, Gesetz geworden ist und im Gesetzgebungsverfahren mancherlei Korrekturen an den Gesetzentwürfen vorgenommen worden sind, bleibt dennoch zu konstatieren, dass dieses Gesetz den Sicherheitsbehörden eine Vielzahl neuer Befugnisse an die Hand gegeben hat, die das Grundrecht auf Datenschutz erheblich strapazieren. Dieses Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wer wann was über ihn weiß. Von diesem Grundsatz bleibt nach dem Terrorismusbekämpfungsgesetz wieder ein Stück weniger übrig.

Sofort nach den Anschlägen startete weltweit die Suche nach den Drahtziehern der Attentate und den Helfershelfern der Terroristen. Wer die Medien verfolgt hat, kennt die Meldungen von den Fahndungserfolgen hier und dort. Er weiß aber auch, dass sich immer wieder die Frage stellte, was den Sicherheitsbehörden in den USA und anderswo bekannt war und ob es nicht möglich gewesen wäre, die Anschläge zu verhindern. Auffällig an den Ermittlungserfolgen ist jedoch, dass sie offensichtlich auf konventioneller kriminalistischer Arbeit beruhen. Kein einziger mutmaßlicher Terrorist oder Unterstützer wurde bislang durch die bundesweite Rasterfahndung aufgespürt, die noch im September 2001 in Gang gekommen war. Während in anderen Bundesländern Gerichte die Rasterfahndungsanordnungen ganz oder teilweise aufhoben, gab es hierzulande infolge der Tatsache, dass unser Polizeigesetz nun wirklich keine allzu hohen Hürden vor einer Rasterfahndung aufbaut, keine durchgreifenden Bedenken gegen die Rasterfahndungsanordnungen des Landeskriminalamts (vgl. 22. Tätigkeitsbericht, LT-Drs. 13/520, S. 13 f.). Die praktizierte Rasterfahndung schauten wir uns bei Kontrollbesuchen im Landeskriminalamt an.

1.1 Die Rasterfahndung – wie es weiterging

Mit der Rasterfahndung will die Polizei islamistischen Gewalttätern und so genannten Schläfern, mithin also Personen auf die Spur kommen, die hierzulande unauffällig leben, um irgendwann als Terrorist aktiv zu werden. Um sie per Datenabgleich ausfindig machen zu können, wandte sich das Landeskriminalamt mit Rasterfahndungsanordnungen an zahlreiche Stellen in Baden-Württemberg. Sie sollten ihm Daten über Personen herausgeben, auf die die in den jeweiligen Anordnungen genannten Kriterien zutrafen. Beispielsweise sollten die Einwohnermeldeämter Daten über Männer bestimmten Alters liefern, die aus bestimmten Staaten stammen. Bei Universitäten und Hochschulen waren Daten eines bestimmten Kreises von Studenten gefragt. Andere Stellen wiederum sollten für die Rasterfahndung Daten über Inhaber einer Fluglizenz oder eines Führerscheins für Gefahrguttransporte an das Landeskriminalamt weitergeben.

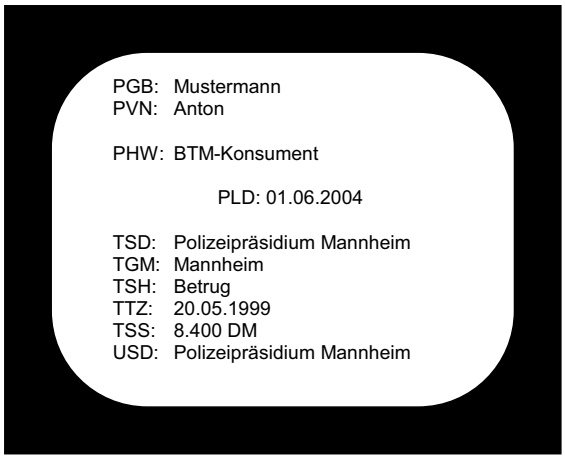
Die Stellen, an die das Landeskriminalamt seine Rasterfahndungsanordnungen gerichtet hatte, übermittelten ihm insgesamt Daten über Hunderttausende von Personen. Nach § 40 des Polizeigesetzes (PolG) durften diese Stellen andere als die in den Rasterfahndungsanordnungen bezeichneten Daten an das Landeskriminalamt nur weitergeben, wenn das Aussortieren der zu übermittelnden Daten einen unverhältnismäßigen Aufwand verursachte. Der Frage, ob diese Anforderungen hinreichend beachtet wurden, konnten wir bei unseren Kontrollen nicht im Einzelnen nachgehen. Fest steht jedoch, dass das Landeskriminalamt in mühsamer Kleinarbeit aus den angelieferten Datenbeständen die Datensätze heraussuchen musste, die den in seinen Rasterfahndungsanordnungen

vorgegebenen Merkmalen entsprachen. Das Ergebnis seiner Datenselektion war: Nur 40 % aller angelieferten Datensätze entsprachen den Kriterien, die das Landeskriminalamt seinen Rasterfahndungsanordnungen zugrunde gelegt hatte; die übrigen 60 % der angelieferten Datensätze lagen außerhalb dieser Merkmalskombinationen. Mit anderen Worten: Das Landeskriminalamt hat im Durchschnitt über mehr als doppelt so viel Personen Daten erhalten, als es für die Rasterfahndung haben wollte. Um den mit der Weitergabe der Daten dieser Personen an das Landeskriminalamt einhergehenden Eingriff in das Recht auf informationelle Selbstbestimmung so gering wie möglich zu halten, war für uns von Anfang an wichtig, dass das Landeskriminalamt diese „überschießenden" Daten unverzüglich löscht. Nach einiger Bedenkzeit ließ uns das Innenministerium wissen, dass das Landeskriminalamt die entsprechenden Originaldatenträger samt den davon erstellten Arbeitskopien inzwischen vernichtet hat.

Mancher wird sich fragen, wann eigentlich die Rasterfahndung abgeschlossen ist. Das ist der Fall, sobald der maschinelle Datenabgleich durchgeführt ist. Danach muss das Landeskriminalamt die ihm übermittelten und im Zusammenhang mit dem Abgleich zusätzlich angefallenen Daten löschen und die Unterlagen vernichten, soweit sie nicht zur Verfolgung von Straftaten erforderlich sind. Das Landeskriminalamt muss dann auch – darin geht das Innenministerium mit uns einig – für die Löschung der Daten sorgen, die es im Zuge der Rasterfahndung an das Bundeskriminalamt weitergegeben hat. Dass es jetzt Hals über Kopf zum Ende kommen muss, verlangt dabei niemand. Andererseits ist aber auch klar, dass sich die Rasterfahndung nicht zu einer Daueraufgabe des Landeskriminalamts auswachsen kann – und einige Zeit ist ja seit ihrem Start nun wirklich schon ins Land gegangen.

1.2 Speicherung personengebundener Hinweise BTMK und DROG in der PAD

Anfang 2002 waren in der Personenauskunftsdatei (PAD) 1320 Personen registriert, bei denen zwar ein personengebundener Hinweis „Betäubungsmittelkonsument" (BTMK) oder „Konsument harter Drogen" (DROG) eingespeichert, jedoch kein mutmaßlich oder tatsächlich begangenes Betäubungsmitteldelikt erfasst war. Das hatte eine PAD-Auswertung ergeben, die das Landeskriminalamt auf Bitten unseres Amtes durchgeführt hat. Am PAD-Bildschirm sah das beispielsweise so aus:



Zeichenerklärung:

PGB:	Geburtsname	TGM:	Tatortgemeinde
PVN:	Vorname	TSH:	Straftat
PHW:	Hinweis zur Person	TTZ:	Tatzeit
PLD:	Löschungstermin	TSS:	Schaden
TSD:	sachbearbeitende Polizeidienststelle	USD:	Kriminalakten führende Dienststelle

Jeder Polizeibeamte, der die PAD abfragt, weiß damit dreierlei: Zum einen sieht er auf den ersten Blick, dass das Polizeipräsidium Mannheim den Betroffenen wegen eines mutmaßlich oder tatsächlich im Jahr 1999 begangenen Betrugs für fünf Jahre bis 1. Juni 2004 in der PAD erfasst hat. Zum anderen bekommt er den Hinweis, der Betroffene sei Betäubungsmittelkonsument. Zum Dritten erfährt er, dass es beim Polizeipräsidium Mannheim eine Akte über die PAD-Speicherung gibt. Wer meint, ein BTMK-Hinweis oder DROG-Hinweis in der PAD sei belanglos, irrt. Jedem, der mit BTMK oder DROG in der PAD erfasst ist, haftet das Etikett „Rauschgiftsüchtiger“ an. Dieses bleibt ihm erhalten, solange Daten über ihn in der PAD gespeichert sind. Wie lange dies dauert, hängt wiederum von der Speicherfrist für die ihm zur Last gelegte und in der PAD erfasste Straftat ab, die in der Regel fünf Jahre und bei gravierenderen Tatvorwürfen zehn Jahre und im Falle der Zuspeicherung weiterer Tatvorwürfe im PAD-Datensatz des Betroffenen noch länger sein kann. Allein mit der Speicherung eines BTMK- oder DROG-Hinweises in der PAD hat es für den Betroffenen indes nicht sein Bewenden. Wer nämlich in der PAD mit BTMK oder DROG registriert ist, muss jedes Mal, wenn er in eine Polizeikontrolle gerät, nicht nur damit rechnen, dass er den kontrollierenden Polizeibeamten Rede und Antwort stehen muss, ob er Drogen dabei oder konsumiert hat, sondern auch damit, dass sein Auto oder er selbst nach Drogen durchsucht wird. Die Polizei fragt nämlich im Zuge solcher Kontrollen in der Regel u. a. die PAD nach Erkenntnissen über die kontrollierte Person ab und erfährt dabei immer auch, ob über sie ein personengebundener Hinweis BTMK oder DROG in der PAD gespeichert ist. Wie belastend dies sein kann, erfuhr ein Mann, der wiederholt in Polizeikontrollen geraten und dabei nach Drogen durchsucht worden war. Weil die Polizeibeamten jeweils zur Tat geschritten waren, nachdem sie die PAD über ihn abgefragt hatten, mutmaßte er, dort sei registriert, dass er mit Drogen zu tun habe. In der Tat waren – wie sich rasch zeigte – in seinem PAD-Datensatz ein BTMK- und ein DROG-Hinweis gespeichert. Beide Hinweise löschte die Polizei sofort, weil sie keine Belege für die Einstufung des Mannes als „Betäubungsmittelkonsument“ und „Konsument harter Drogen“ hatte und auch nicht sagen konnte, wie es zu der Erfassung der beiden personengebundenen Hinweise im PAD-Datensatz des Mannes gekommen war.

Wenngleich es gewiss nicht jedem, in dessen PAD-Datensatz ein BTMK- oder DROG-Hinweis gespeichert ist, so ergehen muss, ist es trotzdem unerlässlich, dass die Polizei die für die Speicherung solcher Hinweise geltenden Regeln strikt beachtet. Dies ist nicht immer der Fall, wie sich bei unseren Kontrollen bei der Landespolizeidirektion Stuttgart II und bei den Polizeipräsidien Karlsruhe und Mannheim zeigte, bei denen wir von den 1320 Fällen, bei denen zwar ein BTMK- oder DROG-Hinweis, jedoch kein Betäubungsmitteldelikt in der PAD erfasst war, 170 nach dem Zufallsprinzip ausgewählte PAD-Datensätze näher unter die Lupe nahmen.

1.2.1 Wie die Polizei verfuhr

Zu der Einspeicherung der personengebundenen Hinweise BTMK und DROG in die PAD war es im Zusammenhang mit Ermittlungsverfahren wegen anderer Straftaten als Betäubungsmitteldelikten gekommen, sei es, dass es um Ladendiebstahl, Betrug, Verstoß gegen das Ausländergesetz, Hehlerei oder Körperverletzung ging. In keinem dieser Ermittlungsverfahren gab es irgendwelche Anhaltspunkte dafür, dass der Betroffene Betäubungsmittel oder harte Drogen konsumiert. Dementsprechend hatten die ermittlungsführenden Polizeidienststellen auf dem Formular für die PAD-Erfassung weder das BTMK- noch das DROG-Datenfeld angekreuzt. Zu den BTMK- und DROG-Speicherungen in der PAD war es vielmehr so gekommen: Der Prüfdienst der drei Polizeidienststellen, der auf die Richtigkeit und Vollständigkeit der PAD-Speicherungen zu achten hat und der im Zuge einer PAD-Erfassung das auf dem Rechner des Bundeskriminalamts

laufende polizeiliche Informationssystem der Polizeien des Bundes und der Länder (INPOL) nach dem Betroffenen abfragt, sah sich auf Grund solcher INPOL-Abfragen aufgerufen, BTMK- und DROG-Hinweise in die PAD-Datensätze der Betroffenen einzuspeichern. Dabei verfuhr er so:

– Zeigte sich bei der INPOL-Abfrage, dass eine Polizeidienststelle außerhalb Baden-Württembergs den Betroffenen in INPOL mit einem BTMK- oder DROG-Hinweis erfasst hatte, speicherten die drei Polizeidienststellen in den PAD-Datensatz des Betroffenen einen entsprechenden personengebundenen Hinweis ein, ohne zu wissen, worauf die Speicherung des BTMK- oder DROG-Hinweises in INPOL eigentlich beruht, und ohne in ihren Akten zu dokumentieren, wie es zu dem BTMK- oder DROG-Hinweis in der PAD gekommen ist.

– Das Polizeipräsidium Mannheim ging noch weiter. Stieß es bei der INPOL-Abfrage zwar nicht auf einen BTMK- oder DROG-Hinweis, jedoch auf einen stichwortartigen Eintrag einer Polizeidienststelle außerhalb Baden-Württembergs wie beispielsweise die als Grund für eine erkennungsdienstliche Behandlung des Betroffenen vermerkte Angabe „Kreditkartenbetrug/Verstoß gegen das Betäubungsmittelgesetz“ nahm es dies zum Anlass, in den PAD-Datensatz des Betroffenen einen BTMK- oder DROG-Hinweis einzuspeichern.

1.2.2 Was dazu zu sagen war

Mit dem Kopieren von BTMK- und DROG-Hinweisen aus INPOL trugen die drei Polizeidienststellen §§ 37, 38 des Polizeigesetzes (PolG) nicht hinreichend Rechnung. Erst recht unzulässig war die Vorgehensweise des Polizeipräsidiums Mannheim, aus stichwortartigen INPOL-Einträgen BTMK- und DROG-Hinweise zu konstruieren und in die PAD einzuspeichern.

– Zum Kopieren von BTMK- und DROG-Hinweisen

Die Polizei darf in der PAD personengebundene Hinweise BTMK und DROG nur speichern, wenn sie zum einen hinreichende Anhaltspunkte dafür hat, dass jemand Betäubungsmittelkonsument bzw. Konsument harter Drogen ist, und zum anderen feststellbar ist, bei welcher Stelle die der Speicherung zugrunde liegenden Unterlagen geführt werden. Zudem muss die rechtzeitige Löschung solcher gespeicherten Hinweise gewährleistet sein. Daran fehlt es beim Kopieren von BTMK- und DROG-Hinweisen aus INPOL. Zum einen haben die Polizeidienststellen in keinem Einzelfall geprüft, ob hinreichende Anhaltspunkte dafür vorliegen, dass gerade diese Person Betäubungsmittelkonsument oder Konsument harter Drogen sei. Sie haben vielmehr einfach die von Polizeidienststellen außerhalb Baden-Württembergs in INPOL eingespeicherten BTMK- und DROG-Hinweise für bare Münze genommen und in den PAD-Datensatz der betreffenden Person kopiert. Zum anderen gibt es bei den drei Polizeidienststellen keine Unterlagen, aus denen ersichtlich gewesen wäre, worauf die kopierten BTMK- und DROG-Hinweise beruhen. Bei der Speicherung solcher personengebundener Hinweise in der PAD muss aber – wie bei jeder Datenspeicherung – die für die Datenspeicherung verantwortliche Stelle nicht nur feststellbar sein, sondern anhand von Akten und Unterlagen belegen können, worauf die Speicherung der BTMK- und DROG-Hinweise beruht. Gerade bei solchen Hinweisen, die das tatsächliche Geschehen nur verkürzt wiedergeben, besteht nämlich die Gefahr, dass mit der stichwortartigen Angabe Informationsverluste einhergehen und deshalb falsche Schlüsse zum Nachteil des Betroffenen gezogen werden. Schließlich ist auch die rechtzeitige Löschung solcher BTMK- und DROG-Hinweise in der PAD

nicht sichergestellt, weil die hiesige Polizei nichts davon erfährt, wenn die auswärtigen Polizeidienststellen ihre BTMK- und DROG-Hinweise in INPOL löschen, weil ihre weitere Speicherung zur Aufgabenerfüllung der Polizei nicht mehr erforderlich ist.

Ganz in Ordnung fand das Innenministerium das Kopieren der BTMK- und DROG-Hinweise aus INPOL auch nicht. Es ließ uns wissen, dass die Polizei künftig den entsprechenden INPOL-Ausdruck zu ihren Unterlagen nehmen wird; damit sei nachvollziehbar, wer aktenführende Dienststelle ist. Ein eigenes Bild, worauf ein von einer Polizeidienststelle außerhalb Baden-Württembergs in INPOL eingespeicherter BTMK- oder DROG-Hinweis beruht, müsse sich die hiesige Polizeidienststelle jedoch nicht machen; sie könne davon ausgehen, dass die Aufnahme eines derartigen Hinweises in INPOL durch die auswärtige Polizeidienststelle zu Recht erfolgt ist. Da traut das Innenministerium der Polizei anderer Bundesländer offenbar mehr zu als der eigenen. Zwei der drei kontrollierten Polizeidienststellen hatten nämlich schon auf die Ankündigung unserer Besuche von sich aus gleich mehrere BTMK- und DROG-Hinweise in der PAD gelöscht, weil sie nicht zu rechtfertigen waren.

– Konstruieren von BTMK- und DROG-Hinweisen unzulässig

Auch das Polizeipräsidium Mannheim musste auf unsere Beanstandung zur PAD-Löschtaste greifen und BTMK- und DROG-Hinweise in der PAD löschen. Das Innenministerium ging nämlich mit uns einig, dass die Praxis des Polizeipräsidiums nicht mit §§ 37, 38 PolG vereinbar ist; diese Praxis bestand darin, aus stichwortartigen INPOL-Speicherungen von Polizeidienststellen außerhalb Baden-Württembergs wie beispielsweise „Btm-Erwerb am 5. Januar 1998 (Haschisch)“ BTMK- oder DROG-Hinweise zu konstruieren, obgleich die auswärtige Polizeidienststelle in INPOL keinen solchen personengebundenen Hinweis vergeben hatte. Aus solch dürren Angaben lässt sich nämlich beim besten Willen nicht folgern, der Betroffene sei Betäubungsmittelkonsument oder Konsument harter Drogen. Deshalb hätte sich das Polizeipräsidium Mannheim besser gleich an die Beurteilung der sachnäheren auswärtigen Polizeidienststellen halten sollen, die sich in Kenntnis der den stichwortartigen INPOL-Speicherungen zugrunde liegenden Vorgänge nicht veranlasst gesehen haben, einen solchen personengebundenen Hinweis zu vergeben.

1.3 Initiativprogramm „Jugendliche Intensivtäter“

Im Jahr 1999 startete unter Federführung des Innenministeriums das Initiativprogramm „Jugendliche Intensivtäter“. Die Idee war, Kinder und Jugendliche, die durch viele oder gravierende Straftaten aufgefallen sind, ganz gezielt unter die Fittiche zu nehmen. Dazu sollen auf Landkreisebene Jugendämter, Polizei, Staatsanwaltschaften und – soweit es um ausländische Kinder und Jugendliche geht – die Ausländerbehörden in regelmäßigen Koordinierungsgesprächen ihre Präventions- und Interventionsmaßnahmen abstimmen, um die „jugendlichen Intensivtäter“ wieder auf den rechten Weg zurückzuführen. Weil uns klar war, dass die Koordinierungsgespräche wegen der heterogenen Zusammensetzung der Runde und der ganz unterschiedlichen Aufgaben und Informationsverarbeitungsbefugnisse der beteiligten Stellen für den Datenschutz ein Kraftakt sind, haben wir uns gleich am Anfang in das Vorhaben des Innenministeriums, eine gemeinsame Empfehlung für die Vorgehensweise bei den Koordinierungsgesprächen zu erarbeiten, eingeschaltet. Wichtig war uns, dass von vornherein die Weichen so gestellt werden: Jede Stelle, die personenbezogene Informationen in ein Koordinierungsgespräch einbringen will, muss prüfen, ob eine Rechtsvorschrift ihr die damit einhergehende Datenübermittlung an alle anderen

am Tisch sitzenden Stellen erlaubt. Die Jugendämter dürfen dabei Informationen über Kinder und Jugendliche nur insoweit in die Runde einbringen, als dies zum Erreichen ihres gesetzlichen Hilfeauftrags erforderlich ist und der Erfolg einer Jugendhilfeleistung dadurch nicht gefährdet wird. Soweit im konkreten Fall eine an der Koordinierungsrunde beteiligte Stelle nicht zuständig und damit eine Datenübermittlung an sie von vornherein nicht erforderlich ist, muss die Besprechung anonymisiert oder ohne ihr Beisein erfolgen. In der Regel trifft dies bei strafunmündigen Kindern auf die Staatsanwaltschaft zu. Gleiches gilt für die Ausländerbehörden bei „jugendlichen Intensivtätern“ mit deutscher Staatsangehörigkeit. All dies und was es aus der Sicht des Datenschutzes sonst noch bei den Koordinierungsgesprächen zu beachten gilt, steht in der gemeinsamen Empfehlung von Landkreis-, Städte- und Gemeindetag sowie Innen-, Justiz- und Sozialministerium zur intensivierten Zusammenarbeit von Jugendämtern, Staatsanwaltschaften, Ausländerbehörden und Polizei im Bereich jugendlicher Intensivtäter vom 28. Juli 1999 (im Folgenden: gemeinsame Empfehlung). Geregelt ist darin auch, dass über die Koordinierungsgespräche Protokoll zu führen ist. Als wir im Frühjahr 2002 anhand solcher Protokolle die Probe aufs Exempel machten, zeigte sich, dass die Regelungen in der gemeinsamen Empfehlung eine Sache, die Praxis mitunter jedoch eine andere ist.

– Was die Frage der Beteiligung der Staatsanwaltschaften an den Koordinierungsgesprächen angeht, waren sich die örtlichen Koordinierungsrunden der Vorgaben der gemeinsamen Empfehlung durchaus bewusst. Hin und wieder stand in dem Protokoll über die konstituierende Sitzung der Koordinierungsrunde zu lesen, für die anwesenden Vertreter von Jugendamt, Polizei, Staatsanwaltschaft und Ausländeramt sei klar, dass die Staatsanwaltschaft bei Strafunmündigen an den Fallbesprechungen nicht teilnimmt. Mancherorts geriet diese Marschroute freilich alsbald in Vergessenheit. Aus den meisten der von uns eingesehenen Protokolle ergab sich, dass Staatsanwaltschaften entgegen der Vorgaben der gemeinsamen Empfehlung auch dann am Tisch saßen, wenn es um strafunmündige Kinder ging. In einem Fall fand die Koordinierungsrunde nichts dabei, dass die Staatsanwaltschaft selbst dann als Protokollführerin fungierte, als in der Koordinierungsrunde vier Fälle strafunmündiger Kinder zur Sprache kamen.

– Nach der gemeinsamen Empfehlung muss die Besprechung anonymisiert oder ohne die betreffende Stelle stattfinden, die für den konkreten Fall nicht zuständig ist. Für Ausländerbehörden folgt daraus, dass sie an Koordinierungsgesprächen von vornherein nicht teilnehmen dürfen, wenn es um „jugendliche Intensivtäter“ mit deutscher Staatsangehörigkeit geht und deren Identität auf den Tisch gelegt wird. Damit ist es aber nicht getan. Selbstverständlich muss eine Ausländerbehörde auch dann den Raum verlassen, wenn der Fall eines ausländischen Kindes oder Jugendlichen zur Sprache kommt, der nicht in ihrem, sondern im Bereich des benachbarten Ausländeramtes spielt. Im Datenschutz gilt nämlich seit jeher der Grundsatz, dass Datenübermittlungen an nicht zuständige Stellen unnütz und deshalb schlechterdings nicht erforderlich sind. Dass es gleichwohl in der Praxis zu solchen Datenübermittlungen gekommen war, konnten wir in Protokollen nachlesen. Beispielsweise saßen bei einem Koordinierungsgespräch sowohl das Ausländeramt des Landratsamts als auch die Ausländerämter von zwei Großen Kreisstädten am Tisch, obwohl für die ausländischen Jugendlichen, deren Fälle zur Sprache kamen, jeweils nur eines der drei Ämter zuständig war.

– Andernorts informierte die Koordinierungsrunde via Protokoll alle Teilnehmer über alle Fälle, die bei dem Koordinierungsgespräch erörtert worden waren, und übersah dabei, dass keineswegs alle teilnehmenden Stellen mit jedem Fall zu tun hatten. Beispielsweise verschickte eine Koordinierungsrunde Protokolle über alle erörterten Fälle an alle Teilnehmer, ganz gleich, ob das Ausländeramt des Landratsamts oder das städtische Ausländeramt oder die Staatsan-

waltschaft X oder der Jugendrichter am Amtsgericht Y oder am Amtsgericht Z oder das Jugendamt des Landratsamts oder das städtische Jugendamt überhaupt mit den Kindern und Jugendlichen, deren Fälle Gegenstand des Koordinierungsgesprächs gewesen waren, zu tun gehabt hatte. Eine solche gegenseitige Unterrichtung steht aber mit der gemeinsamen Empfehlung nicht im Einklang, weil sie dazu führt, dass Stellen überflüssigerweise Näheres über die aktuellen Lebensumstände und Familienverhältnisse von Kindern und Jugendlichen erfahren.

Die Reaktion des beim Initiativprogramm „Jugendliche Intensivtäter“ federführenden Innenministeriums, an das wir diese Ungereimtheiten herangetragen haben, fiel zwiespältig aus. Einerseits habe es – wie das Innenministerium uns wissen ließ – auf der Grundlage der von den betroffenen Stellen eingeholten Äußerungen die Überzeugung gewonnen, dass diese sensibel mit den Daten der Betroffenen umgegangen sind. Insbesondere hätten die Staatsanwaltschaften in Koordinierungsgesprächen über strafunmündige Kinder nicht mehr erfahren, als sie bereits zuvor gewusst haben, was freilich kein Grund dafür ist, von der in der gemeinsamen Empfehlung verankerten Regel abzugehen, dass Koordinierungsgespräche bei strafunmündigen Kindern ohne Beisein der Staatsanwaltschaft erfolgen. Andererseits sah es sich durch unsere Hinweise veranlasst, die mit dem Programm „Jugendliche Intensivtäter“ befassten Stellen zu sensibilisieren, die in der gemeinsamen Empfehlung verankerten Grundsätze beim Umgang mit personenbezogenen Daten zu beachten.

1.4 Einzelfälle aus der Praxis

Beinahe tagtäglich wenden sich Bürger an unser Amt, weil sie befürchten oder wissen, dass die Polizei Daten über sie speichert, und weil sie geprüft haben möchten, ob die Datenspeicherungen mit dem geltenden Recht in Einklang stehen. Beispielsweise ging es um Folgendes:

1.4.1 Erkennungsdienstliche Behandlung aus Anlass einer Sitzdemonstration gegen einen Castor-Transport

Ein junger Mann, der im Zuge einer Sitzdemonstration gegen einen Castor-Transport von einer Polizeidienststelle vorübergehend in Gewahrsam genommen und erkennungsdienstlich behandelt worden war, wandte sich an unser Amt und bat zu prüfen, ob die Polizei inzwischen – wie sie ihm versprochen habe – die erkennungsdienstlichen Unterlagen vernichtet hat. Als wir die Polizeidienststelle danach fragten, ließ sie uns wissen, dass sich der Anfangsverdacht einer Straftat gegen den jungen Mann aus Anlass seiner Teilnahme an der Sitzdemonstration nicht bestätigt hat und dass das gegen ihn angestrengte Ordnungswidrigkeitenverfahren eingestellt worden ist; dieses Verfahren war wegen des Verdachts eingeleitet worden, der junge Mann habe gegen die Pflicht verstoßen, sich nach Auflösung der Versammlung unverzüglich zu entfernen. Die erkennungsdienstlichen Unterlagen habe sie inzwischen mit Ausnahme eines Polaroidfotos vernichtet, das sie zum Zweck der vorbeugenden Bekämpfung von Straftaten und bedeutenden Ordnungswidrigkeiten drei Jahre lang aufbewahren wolle.

Dafür gibt es jedoch keine Rechtsgrundlage. Insbesondere lässt sich die weitere Aufbewahrung des Polaroidfotos nicht auf § 81 b 2. Alternative der Strafprozessordnung (StPO) stützen. Nach dieser Vorschrift darf ein Beschuldigter erkennungsdienstlich behandelt werden, wenn dieser hinreichend verdächtig ist, eine Straftat begangen zu haben. Hinzu kommen muss, dass der festgestellte Sachverhalt Anhaltspunkte für die Annahme bietet, dass der Beschuldigte künftig mit guten Gründen als Verdächtiger in den Kreis potenzieller Beteiligter an einer noch aufzuklärenden strafbaren Handlung einbezogen werden könnte, und zwar angesichts aller Umstände des Einzelfalls – insbesondere im Hinblick

auf Art, Schwere und Begehungsweise der dem Beschuldigten im strafrechtlichen Anlassverfahren zur Last gelegten Straftat sowie auf seine Persönlichkeit und unter Berücksichtigung des Zeitraums, während dessen er strafrechtlich nicht (mehr) in Erscheinung getreten ist. An beiden Voraussetzungen haperte es im Falle des jungen Mannes. Beschuldigter war er nicht. Die von dem jungen Mann bei der Sitzdemonstration an den Tag gelegten Verhaltensweisen rechtfertigten nach der Feststellung der Polizeidienststelle den Anfangsverdacht einer Straftat gerade nicht. Demzufolge war gegen ihn auch kein Ermittlungsverfahren eingeleitet worden. Es fehlte aber auch an einer stichhaltigen Begründung der Polizeidienststelle dafür, der junge Mann werde künftig eine Straftat begehen. Insbesondere lässt sich aus der von der Polizeidienststelle angeführten Zielsetzung der Anti-KKW-Bewegung, durch Aktionen des zivilen Ungehorsams eine Abschaltung einzelner Kernkraftwerke und damit letztendlich den Ausstieg aus der Kernenergie zu erzwingen, eine solche Prognose nicht herleiten. Immerhin schützt Art. 8 des Grundgesetzes (GG) nach ständiger Rechtsprechung des Bundesverfassungsgerichts die Freiheit kollektiver Meinungskundgabe bis zur Grenze der Unfriedlichkeit, die nicht schon dann erreicht ist, wenn es bei einer Versammlung zu Behinderungen Dritter kommt. Zwar ist danach das den Grundrechtsträgern durch Art. 8 GG eingeräumte Selbstbestimmungsrecht über Ort, Zeitpunkt sowie Art und Inhalt der Veranstaltung durch den Schutz der Rechtsgüter Dritter und der Allgemeinheit begrenzt. Mit der Ausübung des Versammlungsrechts sind jedoch häufig unvermeidbar gewisse nötigende Wirkungen in Gestalt von Behinderungen Dritter verbunden. Derartige Behinderungen Dritter sind aber – wie das Bundesverfassungsgericht betont – durch Art. 8 GG gerechtfertigt, soweit sie als sozialadäquate Nebenfolgen mit rechtmäßigen Demonstrationen verbunden sind. Ebenso wenig lässt sich eine Prognose, der junge Mann werde künftig Straftaten begehen, darauf stützen, dass es im Zusammenhang mit Castor-Transporten zu Straftaten gekommen ist. Diese Tatsache rechtfertigt nämlich keineswegs den Schluss, dass alle anderen Personen, die sich an (Sitz-)Demonstrationen gegen Castor-Transporte beteiligen, Straftaten im Schilde führen. Eine solche Zielsetzung kann man Personen, die an solchen Demonstrationen gegen Castor-Transporte teilnehmen, nicht einfach pauschal unterstellen. Bei ihnen handelt es sich, wie jeder weiß, der die öffentlichen Auseinandersetzungen um Castor-Transporte aufmerksam verfolgt, keineswegs um eine homogene Gruppe mit einer einheitlichen, auf die Begehung von Straftaten ausgerichteten Motivation. Deshalb und weil es auch sonst keine Rechtsgrundlage dafür gab, das Polaroidfoto drei Jahre lang aufzubewahren, forderten wir die Polizeidienststelle auf, dieses Foto zu vernichten. Dies tat sie dann auch nach einiger Bedenkzeit, wohl eher der Not gehorchend als der inneren Überzeugung.

1.4.2 Wirklich keine Daten gespeichert?

Ein Lehrer bat uns um Hilfestellung. Was war passiert? Der Lehrer hatte an einer Fortbildungsveranstaltung teilgenommen. Während einer Tagungspause war der Lehrer von zwei Polizeibeamten überprüft und zunächst daran gehindert worden, am Fortgang der Tagung teilzunehmen. Später hatten zwei Kriminalbeamte den Lehrer aus dem Tagungssaal geholt und ihn vernommen und fotografiert. Man suche – so war die Begründung – nach einem Mann, der in der Gegend einen sexuellen Missbrauch begangen hat. Rasch hatte sich herausgestellt, dass der Lehrer mit dieser Sache nun wirklich nichts zu tun hatte. Weil er die Fotos und das Vernehmungsprotokoll vernichtet wissen wollte und auf seine entsprechende, an die Polizeidienststelle gerichtete schriftliche Bitte noch keine Antwort bekommen hatte, wandte sich der Lehrer an uns. Auf Anfrage bestätigte uns die der Polizeidienst-

stelle vorgesetzte Polizeidirektion, dass sich die Sache wie geschildert abgespielt hatte. Zugleich betonte die Polizeidirektion, die Polizei habe dem Lehrer inzwischen geantwortet und ihm dabei dargelegt, dass über ihn bei der Polizei keinerlei Daten gespeichert und die gefertigten Lichtbilder gelöscht sind. Hinter dieser Auskunft steht für den Kenner der Materie freilich ein ganz dickes Fragezeichen. Er weiß nämlich, dass in Vernehmungsprotokollen immer auch die Personalien der vernommenen Person stehen, dass die Polizei verpflichtet ist, Vernehmungsprotokolle zu der Ermittlungsakte zu nehmen und dass die Polizei nach Abschluss der Ermittlungen und Vorlage der Akten an die Staatsanwaltschaft üblicherweise ein Doppel der Ermittlungsakte für sich behält. So war die Polizeidienststelle – woran nichts auszusetzen war – auch im Falle des Lehrers verfahren, wie uns die Polizeidirektion auf Nachfrage etwas kleinlaut eingestand, wohl wissend, dass es deshalb mit der Antwort an den Lehrer, die Polizei speichere keinerlei Daten über ihn, nicht so weit her war.

1.4.3 In der PAD gelöscht

– Ein Autofahrer, der kurz hintereinander in zwei Verkehrskontrollen geraten war, wunderte sich nicht schlecht, dass – wie er uns schrieb – das Klima beide Male etwas frostiger geworden war, nachdem die kontrollierenden Polizeibeamten den Polizeicomputer abgefragt hatten. Womöglich, so mutmaßte er, stehe dort Negatives über ihn. Damit lag er richtig. Bei unseren Nachforschungen stellte sich rasch heraus, dass er in der Personenauskunftsdatei (PAD), das ist das landesweit automatisiert geführte Informationssystem der baden-württembergischen Polizei, das alle Polizeibeamten rund um die Uhr in Sekundenschnelle online abfragen können, aus viererlei Anlässen registriert war. Danach soll er im Frühjahr 1999 eine Nötigung im Straßenverkehr begangen und auf einem Parkplatz eines Supermarkts einen anderen Autofahrer beleidigt haben. Das Ermittlungsverfahren wegen des Verdachts einer Nötigung im Straßenverkehr stellte das Amtsgericht wegen Geringfügigkeit ein; der Anzeige wegen Beleidigung gab die Staatsanwaltschaft keine Folge und verwies den Anzeigeerstatter auf den Privatklageweg. Dass der Autofahrer mit diesen beiden Tatvorwürfen für drei Jahre in der PAD registriert war, mag noch angehen. Dass daneben in der PAD noch ein sage und schreibe 20 Jahre alter Vorwurf der Nötigung im Straßenverkehr und ein 12 Jahre zurückliegender Vorwurf eines Vergehens eines gefährlichen Eingriffs in den Straßenverkehr registriert waren, verstehe wer will. Verkehrskontrollen kann der Autofahrer jetzt jedenfalls gelassener entgegensehen; seine PAD-Einträge sind gelöscht.

– Ein Mann hatte bei der Polizei Auskunft darüber beantragt, welche Daten sie über ihn speichert, und die Auskunft auch erhalten. Weil die Polizei dem Auskunftsbescheid zufolge in ihrer PAD 20 Jahre alte und noch ältere Tatvorwürfe und Daten über ihn sogar aus Anlass solcher Ermittlungsverfahren speicherte, die vor Gericht mit seinem Freispruch geendet hatten, und weil die Polizei sein Löschungsbegehren in Bausch und Bogen abgelehnt hatte, legte der Mann dagegen Widerspruch ein und bat uns um Hilfe. Am Ende unserer langwierigen Bemühungen waren 12 der 17 PAD-Einträge gelöscht; in den anderen 5 Fällen war die PAD-Speicherung nicht zu beanstanden.

2. Die Justiz

Auch in diesem Jahr beschäftigte uns eine Vielzahl unterschiedlichster Fälle aus dem Bereich der Justiz. Und auch in diesem Jahr mussten wir einigen Bürgern, die sich an unsere Dienststelle gewandt hatten, weil sie der Meinung waren, ein Richter habe sie im Rahmen eines Gerichtsverfahrens in ihrem Recht auf informationelle Selbstbestimmung verletzt, mitteilen, dass wir in ihrer Angelegenheit nicht tätig werden können. Dies aber nicht etwa

deshalb – wie uns teilweise von den Betroffenen vorgeworfen wird –, weil wir uns um die Arbeit „drücken“ wollen, sondern weil unsere Kontrollbefugnis bei Gerichten, auf Grund der im Grundgesetz garantierten richterlichen Unabhängigkeit, eingeschränkt ist. Die Tätigkeit von Gerichten können wir daher nur überprüfen, sowie diese in Verwaltungsangelegenheiten tätig werden. Da es jedoch in den meisten der an uns gerichteten Eingaben, die sich auf die Tätigkeit von Gerichten beziehen, nicht um Verwaltungsangelegenheiten geht, sondern beispielsweise um die Art und Weise der Prozessführung und die Beweiswürdigung durch den Richter, können wir oftmals nichts anderes tun, als die Betroffenen auf unsere Unzuständigkeit hinzuweisen. Dass wir trotz dieser Einschränkungen auch im Bereich der Justiz vielfältige Aufgaben wahrnehmen, zeigen die folgenden Beispiele:

2.1 Datenschutzkontrolle bei den Gerichten

Dem regelmäßigen Leser unseres Tätigkeitsberichts wird das Thema „Datenschutzkontrolle bei den Gerichten“ bekannt vorkommen. Seit 1999 findet sich hierzu in jedem unserer Tätigkeitsberichte ein Beitrag (LT-Drs. 12/4600, S. 68 f., LT-Drs. 12/5740, S. 53 f. und LT-Drs. 13/520, S. 30). Ausgangspunkt war, dass wir im Jahre 1999 prüfen wollten, ob die Amtsgerichte bei ihren Computern die technischen und organisatorischen Maßnahmen getroffen haben, die für einen datenschutzgerechten Einsatz der EDV-Technik unerlässlich sind. Dies hat das Justizministerium verhindert. Auch im folgenden Jahr verweigerte das Justizministerium gesetzwidrig eine beabsichtigte Kontrolle der beim Verwaltungsgericht Stuttgart eingesetzten EDV. Nach § 2 Abs. 3 (LDSG) darf unsere Dienststelle die Gerichte tatsächlich nur kontrollieren, soweit diese in Verwaltungsangelegenheiten tätig werden. Eine Beschränkung, die unser Amt stets respektiert hat. Genau aus diesem Grund haben wir jeweils eindeutig zum Ausdruck gebracht, dass wir lediglich prüfen wollen, ob die Justizverwaltung die nach § 9 LDSG gebotenen technischen und organisatorischen Maßnahmen getroffen hat. Eine Kontrolle der richterlichen Datenverarbeitung oder der richterlichen Arbeitsweise am Fall war niemals beabsichtigt. Es bestand somit kein Anlass, unserer Dienststelle die geplanten Kontrollen zu verweigern.

Das Justizministerium beurteilte dies jedoch völlig anders. Jahrelang vertrat es die Ansicht, die Rechtspflege sei umfassend vom Kontrollbereich unseres Amtes ausgenommen und damit auch der Einsatz der EDV-Technik.

Diese Auffassung ist mit dem geltenden Recht nicht in Einklang zu bringen. Denn nach § 2 Abs. 3 LDSG ist nur die nicht auf Verwaltungsangelegenheiten bezogene, also die Recht sprechende Tätigkeit der Gerichte – wegen der im Grundgesetz garantierten Unabhängigkeit der Richter – von der Datenschutzkontrolle unseres Amtes ausgenommen. Zur Recht sprechenden Tätigkeit gehören etwa die eigentliche Spruchtätigkeit und alle damit im Zusammenhang stehenden Tätigkeiten, unabhängig davon, ob sie der Vorbereitung der Entscheidung dienen, ob sie während der Verhandlung ausgeübt werden oder ob sie nach der richterlichen Entscheidung erfolgen.

Die EDV-Ausstattung von Gerichten, also die Beschaffung und der Einsatz sächlicher Mittel für die Tätigkeit der Gerichte, ist mit diesen Angelegenheiten jedoch nicht zu vergleichen. Dass die EDV-Ausstattung nicht zur Recht sprechenden Tätigkeit gehört und der Grundsatz der richterlichen Unabhängigkeit hierfür nicht bemüht werden kann, zeigt sich bereits daran, dass das Justizministerium bestimmt, welche Hard- und Softwarekomponenten bei den Gerichten eingesetzt werden. Wenn die EDV-Ausstattung einerseits vom Justizministerium vorgegeben werden kann, ohne in die richterliche Unabhängigkeit einzugreifen, kann sie nicht andererseits, wegen der richterlichen Unabhängigkeit, der Kontrolle unserer Dienststelle entzogen sein. Unsere immer wieder vorgetragenen Argumente haben das Justizministerium jedoch zunächst in keiner Weise beeindruckt. Erst nachdem dieses Thema zum wiederholten Male im Tätigkeitsbericht für das Jahr 2000 behandelt worden

war, signalisierte Herr Justizminister Dr. Goll, dass sein Haus bereit sei, in dieser Angelegenheit nach einer Linie zu suchen, die der unserem Amt im Landesdatenschutzgesetz eingeräumten Kontrollbefugnis Rechnung trägt. Zur Unterstützung dieser Bemühungen stellten wir für das Justizministerium eine Liste zusammen, die typische Fragen des technischen und organisatorischen Datenschutzes enthielt, um so exemplarisch zu verdeutlichen, dass sich derartige Maßnahmen sehr wohl prüfen lassen, ohne dabei die richterliche Datenverarbeitung zu tangieren. Diese Liste enthielt unter anderem folgende Punkte:

Welche Anforderungen stellt das Gericht an die Gestaltung von Passwörtern (z. B. Mindestlänge, Änderungshäufigkeit)? Inwieweit wird die Einhaltung dieser Anforderungen technisch, also z. B. vom Betriebssystem eines Windows-Domänen-Servers, gewährleistet? Gibt es eine automatische Bildschirmsperre, die nach einigen Minuten ohne Eingaben dafür sorgt, dass der Bildschirm automatisch abgedunkelt wird, und kann diese Sperre nur durch Eingabe des Passworts wieder aufgehoben werden? Was unternimmt das Gericht, um Schäden durch Computerviren zu vermeiden? Sofern die vom Gericht eingesetzte Hard- oder Software von einer anderen Dienststelle oder einem Privatunternehmen online gewartet wird, stellt sich die Frage, ob das Gericht ausreichende Schutzmaßnahmen ergriffen hat, um zu verhindern, dass die Auftragnehmer unberechtigt auf personenbezogene Daten zugreifen können, die auf Computern des Gerichts gespeichert sind. Falls das Computernetz des Gerichts an das Internet oder andere Computernetzwerke angeschlossen ist oder mit diesen zumindest zeitweise (z. B. über ISDN-Wählverbindungen) Verbindung aufnehmen kann, muss sichergestellt sein, dass diese Verbindungen und Verbindungsmöglichkeiten nicht zu unberechtigten Zugriffen auf personenbezogene Daten genutzt werden können, die im lokalen Netzwerk des Gerichts gespeichert sind. In diesem Zusammenhang stellt sich auch die Frage, ob das Gericht ein Firewall-System nutzt, wie dieses aufgebaut und konfiguriert ist, wie es Angriffsversuche aus dem Internet erkennt oder was im Einzelnen geschieht, wenn ein solcher Angriffsversuch festgestellt wird. Tauscht das Gericht über Internet personenbezogene Daten mit anderen Internet-Teilnehmern aus, stellt sich die Frage, wie die übertragenen Daten vor unberechtigter Kenntnisnahme und Veränderung geschützt sind.

Die Antwort des Justizministeriums ließ zwar rund neun Monate auf sich warten. Schließlich bestätigte es im Frühjahr 2002 unsere Auffassung, dass es sich bei den von uns aufgeführten Punkten um technisch-organisatorische Fragestellungen handelt, auf die sich die Kontrollkompetenz unseres Amtes erstreckt. Allerdings vertrat das Justizministerium die Ansicht, dass sich die Datenschutzkontrolle auf die von uns nur exemplarisch aufgeführten Punkte beschränke, die Liste mit Beispielen also als abschließende Aufzählung betrachtet werde. Eine Auffassung, der wir uns nicht anschließen können. Denn da die EDV-Technik und damit auch die nach § 9 LDSG zu treffenden technischen und organisatorischen Maßnahmen einem ständigen Wandel unterliegen, lässt sich die Reichweite unserer Kontrollbefugnis bei Gerichten nicht durch eine starre Auflistung von Einzelfragen festlegen, sondern muss an die jeweiligen technischen Gegebenheiten angepasst werden.

Angesichts der – nun endlich bestehenden – weitgehenden Übereinstimmung zur Frage der Reichweite der Kontrollkompetenz unseres Amtes bei Gerichten gehen wir jedoch davon aus, dass auch für künftig auftretende Fragestellungen einvernehmliche Lösungen gefunden werden können, die sowohl dem Grundsatz der richterlichen Unabhängigkeit als auch den gesetzlichen Kontrollbefugnissen unserer Dienststelle Rechnung tragen.

2.2 Auf dem Weg zum gläsernen Internet-Nutzer?

Die modernen Telekommunikationsdienste und Teledienste, wie beispielsweise das Internet, bieten allen Bürgern in ständig steigendem Maße vielfältige Möglichkeiten, sich umfassend zu informieren, im Netz mitzudiskutieren und in elektronischer Form am Wirtschaftsleben

teilzunehmen. Zumindest ebenso bedeutsam ist die freie, sichere und uneingeschränkte Nutzung der neuen Kommunikations- und Informationsdienste für die Wirtschaftsunternehmen und für die Bereiche Bildung, Wissenschaft und Arbeit. Auch der Staat macht sich für seinen Kontakt mit den Bürgern immer mehr die modernen Telekommunikations- und Teledienste zunutze; die Bürger sollen künftig nicht nur ihre Behördengänge online erledigen, sondern via Internet möglicherweise sogar wählen können. Kurzum: Der Nutzung der modernen Informations- und Kommunikationsdienste kommt inzwischen in nahezu allen Lebensbereichen eine immer größere Bedeutung zu. Jeder, der sich dieser Informations- und Kommunikationstechniken bedient, hinterlässt jedoch infolge der technischen Ausgestaltung dieser Dienste nolens volens eine Fülle von Datenspuren. Wegen der daraus resultierenden Risiken für das Grundrecht auf Datenschutz ist bislang allen Bürgern bei der Inanspruchnahme von Telekommunikations- und Telediensten gesetzlich verbrieft, dass nur die für die Abwicklung und Abrechnung erforderlichen Daten für eine gewisse Zeit gespeichert werden dürfen. Das von diesem Grundsatz und vom Gebot der Datenvermeidung und der Datensparsamkeit sowie der Möglichkeit der anonymen Nutzung des Internets geprägte Teledienstedatenschutzrecht will eine Mehrheit im Bundesrat auf den Kopf stellen. Nach dem mit der Stimme Baden-Württembergs beschlossenen Gesetzentwurf sollen die bei der Nutzung von Telekommunikationsdienstleistungen und von Telediensten anfallenden Bestands-, Nutzungs- und Abrechnungsdaten auf Vorrat gespeichert werden und für die Erfüllung sämtlicher Aufgaben von Polizei, Verfassungsschutz, Bundesnachrichtendienst, Militärischem Abschirmdienst und Zollkriminalamt genutzt werden können. Wie lange die Provider die Daten speichern müssen und unter welchen Voraussetzungen die Sicherheitsbehörden auf diesen gigantischen Datenbestand zugreifen dürfen, soll nach dem Gesetzentwurf des Bundesrats nicht der Gesetzgeber, sondern die Exekutive per Rechtsverordnung festlegen.

Das Internet ist jedoch nicht von vornherein ein Hort des Verbrechens. Die modernen Informations- und Kommunikationstechniken sind nicht bereits als solche ein Instrumentarium, das stärker als andere Medien die Kriminalität begünstigt. Sie werden freilich – wie andere Medien und Einrichtungen auch – mitunter für die Begehung von Straftaten missbraucht, denen wirksam begegnet werden muss. Die bestehenden Befugnisse der Strafverfolgungsbehörden gewährleisten jedoch schon jetzt eine effektive Strafverfolgung etwa im Internet, wo es beispielsweise Providern ohne weiteres technisch möglich ist, IP-Adressen ab dem Zeitpunkt des Vorliegens eines entsprechenden gerichtlichen Beschlusses oder – bei Gefahr im Verzug – einer staatsanwaltschaftlichen Anordnung vorzuhalten. Die allermeisten Menschen, die diese neuen Medien nutzen, halten sich dabei jedoch an die gesetzlichen Vorgaben. Es besteht deshalb kein Anlass, Personen, die sich die Möglichkeiten der virtuellen Welt zunutze machen und ihre Angelegenheiten über das Internet erledigen, stärkeren Eingriffen in ihr Grundrecht auf Datenschutz zu unterziehen als Personen, die sich in der realen Welt bewegen. Gerade darauf läuft aber der Gesetzentwurf des Bundesrats hinaus. Niemand wird in der realen Welt beispielsweise beim Betreten eines Kaufhauses registriert, und es wird auch nicht notiert, was man sich dort angesehen, wie lange man ein Buch oder welche Ware man sonst in der Hand gehalten hat, welche Zeitschrift oder was sonst man sich gekauft hat und in welchen Laden man dann gegangen ist und für welche Produkte man sich dort interessiert hat. Gerade dies würde aber die Protokollierung aller Internet-Aktivitäten, die der Bundesrat mit seinem Gesetzentwurf herbeiführen will, bedeuten. Solche Maßnahmen der Datenerhebung und Datensammlung auf Vorrat über alle Internet-Nutzer und alle Nutzer sonstiger Informations- und Kommunikationsdienste würden einen unverhältnismäßigen Eingriff in das Grundrecht auf Datenschutz darstellen. Die Tatsache, dass es bei diesen modernen Diensten auf Grund der bei ihrer Nutzung ohnehin anfallenden Datenspuren technisch möglich ist, umfangreiche Informationen über die Nutzer zu erheben und zu speichern, darf nicht zur Folge haben, dass für Eingriffe in die Datenschutzrechte vieler völlig unbescholtener Bürger die eherne

Schwelle des Anfangsverdachts außer Kraft gesetzt wird und Daten über sie ins Blaue hinein auf Vorrat gesammelt werden. Solche Vorhaben, wie sie der Gesetzentwurf des Bundesrats verfolgt, beeinträchtigen das Grundrecht auf informationelle Selbstbestimmung nachhaltig und bauen den Datenschutz bei der Inanspruchnahme von Telekommunikationsdienstleistungen und von Telediensten in unvertretbarer Weise ab; die Datenschutzbeauftragten des Bundes und der Länder sind ihnen deshalb entschieden entgegengetreten (s. Anhang 1 und 3). Statt den Gesetzentwurf des Bundesrats, der in Richtung gläserner Internet-Nutzer führt, weiter zu verfolgen, sollte man sich hierzulande besser an die Enquete-Kommission „Entwicklung, Chancen und Auswirkungen neuer Informations- und Kommunikationstechnologien in Baden-Württemberg“ des Landtags von Baden-Württemberg (Multimedia-Enquete) aus dem Jahr 1995 erinnern und deren berechtigter Forderung zum Durchbruch verhelfen, dass bei der Inanspruchnahme der neuen Informations- und Kommunikationsmedien so wenig wie möglich personenbezogene Daten anfallen.

2.3 Beschlagnahmeschutz und Reichweite des Sozialgeheimnisses

Das öffentliche Interesse an der Strafverfolgung einerseits und das Individualinteresse an der Beachtung der Privatsphäre andererseits widersprechen sich regelmäßig. Meist hat der Gesetzgeber dem Strafverfolgungsinteresse den Vorrang eingeräumt. Allerdings gibt es auch Bereiche, in denen der besonderen Sensibilität der Daten Tribut gezollt wird. So etwa bei medizinischen und bei Sozialdaten. Darauf zu achten, dass die dort vorhandenen Beschränkungen bei der Ermittlungstätigkeit beachtet werden, ist ein besonderes Anliegen des Datenschutzes. Eine nicht immer einfache Sache, wie folgende Fälle zeigen:

2.3.1 Der Patient als Zeuge

Nicht selten kommt es vor, dass Polizei oder Staatsanwaltschaft im Rahmen strafrechtlicher Ermittlungsverfahren bei Ärzten oder Krankenhäusern anklopfen und Einsicht in Patientenunterlagen fordern. Wird dies unter Hinweis auf die ärztliche Schweigepflicht verweigert, folgt die Beschlagnahmeverfügung meist auf dem Fuß. Bei den Betroffenen herrscht dann Unklarheit darüber, wie sie sich verhalten sollen. Anlässlich eines konkreten Falles hatten wir versucht, mit der Staatsanwaltschaft Stuttgart in dieser Frage zu einem Einvernehmen zu kommen. Dies ist letztlich leider nicht ganz gelungen.

Unstreitig sind Ärzte berechtigt, gegenüber den Ermittlungsbehörden das Zeugnis darüber zu verweigern, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist (§ 53 Abs. 1 Satz 1 Nr. 3 der Strafprozessordnung [StPO]). Mit diesem Zeugnisverweigerungsrecht geht ein Verbot der Beschlagnahme ärztlicher Aufzeichnungen einher, welche Informationen enthalten, die der Arzt nicht preisgeben muss. Allerdings, und hier setzen die Probleme ein, spricht der Wortlaut des § 97 Abs. 1 Nr. 2 StPO von Mitteilungen, die der „Beschuldigte“ dem Arzt gemacht hat. Die Staatsanwaltschaft schließt daraus, dass Mitteilungen, die ein Patient, der nicht Beschuldigter, sondern (nur) Zeuge in einem Strafverfahren ist, seinem Arzt gemacht hat, grundsätzlich keinem Beschlagnahmeverbot unterliegen würden. Dies sehen wir anders.

Es gibt mehrere Gerichtsentscheidungen, welche die von der Staatsanwaltschaft zunächst vertretene pauschale Ablehnung eines Beschlagnahmeschutzes von Zeugenunterlagen als nicht haltbar erscheinen lassen. So vertritt der Bundesgerichtshof die Auffassung, ein Beschlagnahmeverbot könne sich auch unmittelbar aus dem Grundgesetz ergeben, wenn in grundrechtlich geschützte Bereiche unter Verstoß gegen den Grundsatz der Verhältnismäßigkeit eingegriffen werde. Hier sei eine Interessensabwägung erforderlich. Bei dieser sei die Schwere der Tat zu

berücksichtigen, so dass jedenfalls in Fällen schwerer Kriminalität die Beschlagnahme von Krankenakten Dritter zulässig sein könne. In einer anderen Entscheidung hat er klargestellt, dass die erzwungene Beiziehung von Krankenunterlagen, und zwar auch wenn sie Zeugen eines Strafverfahrens betreffen, unverhältnismäßig in einen besonders sensiblen Bereich der Privatsphäre eingreifen. Dies sei jedenfalls dann unzulässig, wenn diese Beiziehung ohne konkrete Beweisbehauptung und Tatsachengrundlage erfolge und deshalb nur der Ausforschung diene. Auch dürfe sich der Antrag nicht undifferenziert auf die gesamten Krankenunterlagen erstrecken, sondern müsse sich vielmehr immer auf konkrete einzelne Urkunden beziehen.

Dies zeigt, dass sich ein routinemäßiges Vorgehen verbietet. Vielmehr müssen in jedem Einzelfall die betroffenen Interessen unter Berücksichtigung aller Umstände gegeneinander abgewogen werden. Dabei kommt dem allgemeinen Interesse an einer funktionstüchtigen Strafrechtspflege nicht grundsätzlich der Vorrang vor dem Interesse des Patienten an der Respektierung seiner Privatsphäre zu. Dies hat das Bundesverfassungsgericht jüngst in einer Entscheidung nochmals ausdrücklich bestätigt, in der es um die Frage der Verwertbarkeit von Zeugenaussagen ging, die auf dem rechtswidrigen Mithören von Telefongesprächen Dritter beruhten. Der Staatsanwaltschaft hatten wir dies in mehreren Schreiben erläutert. Ihr letztes Antwortschreiben lässt darauf schließen, dass sie von ihrer ursprünglichen strikten Auffassung abgerückt ist.

2.3.2 Die Berufsgenossenschaft und der Staatsanwalt

Wir leben in einem Sozialstaat. Die wesentlichen Lebensrisiken werden durch Sozial(versicherungs)leistungen abgedeckt. Sollen diese in Anspruch genommen werden, muss der Betreffende die für die Bearbeitung seines Anspruchs erforderliche Datengrundlage zur Verfügung stellen. Damit erhalten die Leistungsträger regelmäßig tiefen Einblick in die privaten, oft auch intimen Lebensumstände der Leistungsempfänger. Als Ausgleich hierfür hat der Gesetzgeber die Daten, die als „Sozialdaten“ bezeichnet werden, dem Sozialgeheimnis unterworfen. Dieses bewirkt einen stärkeren Schutz, als ihn das allgemeine Datenschutzrecht bietet. Hierauf mussten wir die Staatsanwaltschaft Stuttgart hinweisen.

Zugrunde lag dem die Eingabe einer Berufsgenossenschaft. Diese war von der Staatsanwaltschaft im Rahmen eines Ermittlungsverfahrens wegen fahrlässiger Körperverletzung aufgefordert worden, medizinische Unterlagen über die geschädigte Person vorzulegen, welche die Berufsgenossenschaft zuvor von den behandelnden Ärzten erhalten hatte. Nachdem sich die Berufsgenossenschaft geweigert hatte, diesem Ersuchen nachzukommen, erwirkte die Staatsanwaltschaft einen richterlichen Beschluss und veranlasste die Beschlagnahme. Dies hätte sie nicht gedurft.

Grundsätzlich ist ein Sozialversicherungsträger allenfalls dann verpflichtet, der Staatsanwaltschaft Auskunft zu geben oder ihr Schriftstücke auszuhändigen, wenn das Gesetz im Einzelfall eine Datenübermittlung zulässt (§ 35 Abs. 3 des Sozialgesetzbuches (SGB) Erstes Buch (I) – Allgemeiner Teil –). Mit dieser Regelung hat der Gesetzgeber dem Sozialgeheimnis ausdrücklich den Vorrang auch gegenüber dem Strafverfolgungsinteresse eingeräumt. § 35 Abs. 3 SGB I begründet insoweit ein Beschlagnahmeverbot zugunsten der Sozialbehörde. Bei der entscheidenden Frage, ob die Berufsgenossenschaft der Staatsanwaltschaft hier die Sozialdaten übermitteln durfte, war besonders zu berücksichtigen, dass es um medizinische Daten ging, welche die Berufsgenossenschaft selbst wiederum von einem Arzt erhalten hatte. Für solche Fälle der Zweitübermittlung schränkt das Sozialgesetzbuch die Übermittlungsbefugnis der Sozialleistungsträger gene-

rell ein. Die medizinischen Daten dürfen nämlich nur dann (weiter) übermittelt werden, wenn der Arzt selbst hierzu berechtigt wäre (§ 76 Abs. 1 des Sozialgesetzbuches (SGB) Zehntes Buch (X) – Verwaltungsverfahren –). Hier wäre demnach eine schriftliche Erklärung des Patienten über die Entbindung von der ärztlichen Schweigepflicht erforderlich gewesen. Eine solche lag allerdings nicht vor.

Bedauerlicherweise hatte im konkreten Fall auch das Amtsgericht, das die Beschlagnahme angeordnet hatte, diese Rechtslage nicht berücksichtigt. Der Staatsanwaltschaft gegenüber haben wir bedauert, dass sie diesen fehlerhaften Beschluss zur Grundlage einer zwangsweisen Beschaffung der Arztunterlagen gemacht hatte und darum gebeten, bei allem Verständnis für die Belange der Strafverfolgung dem Datenschutz der Betroffenen in diesem besonders sensiblen Bereich künftig stärkere Bedeutung beizumessen. In einer ersten Reaktion teilte uns die Staatsanwaltschaft mit, man habe den Fall zum Anlass genommen, die Mitarbeiter auf die Problematik hinzuweisen und sie aufzufordern, den Datenschutzregelungen künftig Beachtung zu schenken. Es wird sich zeigen, ob hier tatsächlich ein Umdenken stattfindet.

2.3.3 Das Ermittlungsverfahren gegen den Jugendamtsmitarbeiter

Um das Spannungsverhältnis zwischen Strafverfolgungsmaßnahmen der Staatsanwaltschaft einerseits und dem Schutz von Sozialdaten andererseits ging es auch in einem Fall, in dem ein Jugendamt uns um Rat ersuchte. Was war geschehen?

Gegen eine Sozialarbeiterin des Jugendamts war Strafanzeige erhoben worden. Das Besondere daran war, dass die Vorwürfe u. a. der Nötigung und der Vorteilsannahme aus dem Kreis der von ihr zu betreuenden Klienten stammten. Die Staatsanwaltschaft bat die Sozialarbeiterin um eine Stellungnahme zu den Vorwürfen. Die Strafverfolgungsbehörde vertrat die Ansicht, dass es sich hierbei ausschließlich um eine Beschuldigtenvernehmung handele. Sozialdaten würden in diesem Rahmen von Seiten der Mitarbeiterin des Jugendamts nicht übermittelt, vielmehr nehme sie nur zu den Vorwürfen des Anzeigeerstatters Stellung. Hier irrte die Strafverfolgungsbehörde.

Entschließt sich nämlich ein Beschuldigter, sich zu Vorwürfen zu äußern, was ihm nach der Strafprozessordnung freisteht, so hat er bei seiner Aussage sehr wohl das Sozialgeheimnis und damit die speziellen Übermittlungsbefugnisse des Sozialgesetzbuchs zu beachten. Das Sozialgeheimnis verpflichtet ausdrücklich auch die Bediensteten einer Organisation. Nach § 35 Abs. 3 SGB I sind deshalb Auskünfte durch Mitarbeiter des Jugendamts nur dann zulässig, wenn auch das Jugendamt selbst die erfragten Angaben rechtmäßig weitergeben dürfte.

Das wirft hier die spannende Frage auf, ob sich die Sozialarbeiterin etwa nicht zu möglicherweise unberechtigten Vorwürfen äußern darf, wenn dies gleichzeitig und zwangsläufig dazu führt, dass sie Informationen aus einem Leistungsfall des Jugendamts weitergibt.

Insoweit konnten wir das Landratsamt und seine Mitarbeiterin beruhigen. Das Sozialgesetzbuch erlaubt nämlich die Weitergabe von Sozialdaten insbesondere auch dann, wenn die Übermittlung zur Durchführung eines Strafverfahrens erforderlich ist und dieses mit einer Jugendhilfemaßnahme in sachlichem Zusammenhang steht (§ 69 Abs. 1 Nr. 2 SGB X). Richtet sich das Strafverfahren gegen eine Mitarbeiterin des Jugendamts und werden Sozialdaten einer Klientin zur Sachverhaltsermittlung benötigt, kommt diese gesetzliche Übermittlungserlaubnis damit in Betracht. Der sachliche Zusammenhang bestand darin, dass der Mitarbeiterin vorgeworfen wurde, sich gerade bei dieser Maßnahme der Jugendhilfe strafwürdig verhalten zu haben.

Was aber gilt nun für die Sozialarbeiterin, wenn sie zusätzlich als Angehörige ihrer Berufsgruppe einer besonderen Schweigepflicht unterliegt?

Nach dem Strafgesetzbuch (StGB) ist es einer staatlich anerkannten Sozialarbeiterin unter Strafandrohung verboten, unbefugt Dinge zu offenbaren, die ihr im Vertrauen auf die Verschwiegenheit mitgeteilt oder die ihr im Zusammenhang mit ihrer Aufgabe sonst bekannt wurden (§ 203 Abs. 1 Nr. 5 StGB). Aber auch aus diesem Dilemma konnten wir einen Weg weisen. Die Verletzung der beruflichen Schweigepflicht ist u. a. dann gerechtfertigt, wenn die Wahrung der Interessen des Schweigeverpflichteten dies ausnahmsweise erfordert. Das ist z. B. der Fall, wenn der Bruch der Schweigepflicht zur Abwendung der Gefahr einer unbegründeten strafrechtlichen Verfolgung notwendig ist oder auch wenn das berufliche Ansehen des Schweigepflichtigen durch unwahre Behauptungen leiden könnte. Beides hielten wir für gegeben.

2.4 Die Privilegierung des Finanzamts

Seit Inkrafttreten des Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes (StVollzG) am 1. Dezember 1998 ist die Verarbeitung personenbezogener Daten im Strafvollzug und damit auch die Frage, an wen und unter welchen Voraussetzungen die Justizvollzugsanstalten personenbezogene Daten von Gefangenen übermitteln dürfen, gesetzlich geregelt. Seit dem 1. Dezember 1998 konnten die Strafvollzugsbehörden Gläubigern eines Gefangenen nach § 180 Abs. 5 Satz 1 StVollzG unter den dort beschriebenen Voraussetzungen nur Auskunft darüber erteilen, ob sich eine bestimmte Person in Haft befindet sowie ob und wann deren Entlassung voraussichtlich innerhalb eines Jahres bevorsteht. Darüber hinausgehende Informationen, wie z. B. ob einem Gefangenen pfändbare Geldmittel zur Verfügung stehen, durften lediglich an Opfer einer Straftat weitergegeben werden, wenn dies zur Durchsetzung von Rechtsansprüchen gegen den Gefangenen erforderlich war. Andere Gläubiger erhielten dagegen keine Auskünfte über die Vermögensverhältnisse von Gefangenen, und zwar unabhängig davon, ob es sich um private oder öffentliche Gläubiger, wie z. B. die Finanzverwaltung, handelte. Insoweit war der öffentliche Gläubiger eines Strafgefangenen wie jeder andere Gläubiger auf die allgemeinen Möglichkeiten der Zwangsvollstreckung zu verweisen.

Die Bundesregierung hielt es wegen des öffentlichen Interesses an der Durchführung einer gleichmäßigen Besteuerung jedoch für sachlich nicht gerechtfertigt, dass selbst Finanzämter keine weitergehenden Informationen erhalten konnten. Sie legte deshalb im Frühjahr 2002 einen Gesetzentwurf vor, der vorsah, in § 180 StVollzG eine Ermächtigungsgrundlage einzufügen, die die Übermittlung personenbezogener Daten von Gefangenen für Zwecke der Besteuerung zulässt.

Dem Bundesrat ging dieser Gesetzentwurf nicht weit genug: Er empfahl, Datenübermittlungen zur Geltendmachung von allen Forderungen juristischer Personen des öffentlichen Rechts – also nicht nur für Forderungen, die aus der Besteuerung resultieren – zuzulassen. Dies wurde von den Datenschutzbeauftragten des Bundes und der Länder in einer gemeinsamen Stellungnahme entschieden abgelehnt. Denn mit einer solchen Regelung würde nicht nur das in § 180 Abs. 5 Satz 1 StVollzG verankerte Prinzip der Gleichbehandlung von öffentlichen und privaten Gläubigern aufgegeben. Sie würde die öffentliche Hand sogar gegenüber solchen privaten Gläubigern privilegieren, deren Rechtsanspruch auf einer Straftat des Gefangenen beruht. Schließlich würde eine solche Regelung zu erheblichen Eingriffen in das Grundrecht auf Datenschutz der Strafgefangenen führen, deren Erforderlichkeit nur bejaht werden könnte, wenn die bisherige Rechtslage zu Unzuträglichkeiten bei der Geltendmachung von Forderungen juristischer Personen des öffentlichen Rechts gegen Strafgefangene geführt hätte. Derartige Umstände wurden jedoch nicht dargetan.

Obwohl bereits die Empfehlung des Bundesrats aus datenschutzrechtlicher Sicht nicht akzeptabel war, war das Justizministerium Baden-Württemberg der Ansicht, dass § 180 StVollzG um eine noch weiter gehende Regelung ergänzt werden sollte: Die Übermittlung von personenbezogenen Daten Gefangener sollte nicht nur zur Geltendmachung von Forderungen öffentlicher Stellen zulässig werden, sondern pauschal für die Aufgabenerledigung öffentlicher Stellen. Eine Regelung, die das informationelle Selbstbestimmungsrecht der Gefangenen im Verhältnis zu öffentlichen Stellen in unverhältnismäßigem Umfang einschränken würde.

Zur Erleichterung aller Datenschutzbeauftragten hat sich der Vorschlag aus Baden-Württemberg nicht durchgesetzt. Auch die Empfehlung des Bundesrats, Datenübermittlungen zur Geltendmachung von Forderungen juristischer Personen des öffentlichen Rechts generell zuzulassen, ist nicht umgesetzt worden. Der Bundestag hat mit Zustimmung des Bundesrats – entsprechend dem Gesetzentwurf der Bundesregierung vom Frühjahr 2002 – vielmehr beschlossen, die Übermittlungsbefugnis der Strafvollzugsbehörden ausschließlich zugunsten der Finanzämter um den Zweck „zur Durchführung der Besteuerung“ zu erweitern.

Aus datenschutzrechtlicher Sicht wäre es zwar wünschenswert gewesen, wenn die Übermittlungsbefugnisse in § 180 StVollzG überhaupt nicht erweitert worden wären. Angesichts der während des Gesetzgebungsverfahrens diskutierten Alternativen ist das Ergebnis jedoch durchaus zufrieden stellend.

2.5 Die Dolmetscherliste im Internet

Schon lange kommt kein Gericht mehr ohne Verhandlungsdolmetscher und Urkundenübersetzer aus. Wird nämlich unter Beteiligung von Personen verhandelt, die der deutschen Sprache nicht mächtig sind, ist ein Dolmetscher zuzuziehen. Das Recht auf Zuziehung eines Dolmetschers ist unverzichtbar. Ist das Gericht überzeugt, dass der Beteiligte der deutschen Sprache nicht oder nur ungenügend mächtig ist, muss es ohne Rücksicht auf seinen Willen einen Dolmetscher zuziehen. Damit dies reibungslos geschehen kann, führen die Landgerichte Verzeichnisse über die in ihrem Sprengel ansässigen amtlich beeidigten Verhandlungsdolmetscher und Urkundenübersetzer. Aus den einzelnen Verzeichnissen erstellt das Oberlandesgericht Stuttgart jährlich einmal ein Gesamtverzeichnis der in Baden-Württemberg amtlich beeidigten Verhandlungsdolmetscher und Urkundenübersetzer, das im Amtsblatt des Justizministeriums „Die Justiz“ veröffentlicht wird. Dieses altbewährte Verfahren will das Justizministerium modernisieren und das Gesamtverzeichnis im Internet veröffentlichen.

Als es uns dazu um Rat gefragt hat, haben wir das Justizministerium darauf hingewiesen, dass das in § 14 Abs. 6 und § 15 Abs. 5 des Gesetzes zur Ausführung des Gerichtsverfassungsgesetzes und von Verfahrensgesetzen der ordentlichen Gerichtsbarkeit (AGGVG) geregelte Recht auf Einsicht in die bei den Landgerichten zu führenden Dolmetscher- und Urkundenübersetzerverzeichnisse deren Veröffentlichung im Internet nicht rechtfertigen kann. Die weltweiten millionenfachen Zugriffs- und Auswertungsmöglichkeiten, die bei einer Einstellung dieses Verzeichnisses in das Internet bestehen, können nicht mit dem jedermann zustehenden Einsichtsrecht auf regionaler Ebene auf eine Stufe gestellt werden. Auch zwischen der Veröffentlichung im Amtsblatt „Die Justiz“ und der Internet-Veröffentlichung besteht ein qualitativer Unterschied allein schon deshalb, weil sich der Personenkreis, der als Leser des Amtsblatts in Betracht kommt, doch ganz erheblich von den Millionen von Internet-Nutzern unterscheidet. Andererseits ist nicht zu verkennen, dass die weit überwiegende Zahl der beeidigten Dolmetscher und Urkundenübersetzer keine Einwände gegen die Internet-Veröffentlichung haben wird. Nicht völlig auszuschließen ist freilich, dass der eine oder andere, z. B. weil er Repressalien seines (früheren) Heimatstaats befürchtet, zwar durchaus nichts dagegen hat, dass hierzulande seine Dolmetscher- und Urkundenübersetzertätigkeit für Gerichte

bekannt wird, wohl aber eine Veröffentlichung im Internet ablehnt. Aus diesen Gründen haben wir dem Justizministerium empfohlen, den beeidigten Dolmetschern und Urkundenübersetzern nach vorangegangener Unterrichtung über die Absicht, das Dolmetscher- und Urkundenübersetzerverzeichnis im Internet zu veröffentlichen, wenigstens die Möglichkeit zu geben, der Veröffentlichung zu widersprechen und einen entsprechenden Widerspruch dann auch zu respektieren. Widerhall haben wir damit beim Justizministerium nicht gefunden. Mittlerweile hat die Landesregierung einen Gesetzentwurf zur Änderung des Landesgesetzes über die freiwillige Gerichtsbarkeit, des Gesetzes zur Ausführung des Gerichtsverfassungsgesetzes und von Verfahrensgesetzen der ordentlichen Gerichtsbarkeit und des Landesjustizkostengesetzes in den Landtag eingebracht (LT-Drs. 13/1373), in dem das Justizministerium eine Rechtsgrundlage für die Veröffentlichung des Dolmetscher- und Urkundenübersetzerverzeichnisses im Internet schaffen will, ohne dass ein Dolmetscher oder Urkundenübersetzer dieser Veröffentlichung widersprechen könnte. Im Interesse des Datenschutzrechts der beeidigten Dolmetscher und Urkundenübersetzer bleibt zu hoffen, dass unser Vorschlag im Laufe der parlamentarischen Beratung des Gesetzentwurfs aufgegriffen wird.

2.6 Einzelfälle im Strafvollzug

Wie bereits unter 2.4 angesprochen, ist die Verarbeitung personenbezogener Daten im Strafvollzug seit Inkrafttreten des Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes am 1. Dezember 1998 gesetzlich geregelt. Obwohl diese Vorschriften hinter dem zurückbleiben, was aus datenschutzrechtlicher Sicht wünschenswert ist, hatten wir erwartet, dass diese Regelungen zu mehr Sensibilität und Rechtssicherheit im Umgang mit Gefangenendaten führen werden und die Rechte des Gefangenen auf Datenschutz hierdurch zum Tragen kommen. Tatsächlich hat sich in den letzten Jahren in den Justizvollzugsanstalten einiges verändert. Dennoch hat man immer wieder den Eindruck, dass der Datenschutz die Gefängnismauern noch nicht überwunden hat. So kommt es vor, dass Vollzugsbehörden die Einführung datenschutzgerechter Vorgehensweisen unter Hinweis auf einen damit verbundenen Mehraufwand, die bestehende Arbeitsbelastung oder etwa deshalb ablehnen, weil sie irrtümlicherweise annehmen, Maßnahmen zum anstaltsinternen Datenschutz könne man sich sparen. Doch die Grundrechte von Strafgefangenen – und damit auch das informationelle Selbstbestimmungsrecht – sind nur insoweit eingeschränkt, als bereichsspezifische Vorschriften dies vorsehen. Die Datenschutzvorschriften des Strafvollzugsgesetzes, die abschließend regeln, in welchem Umfang und unter welchen Voraussetzungen personenbezogene Daten verarbeitet und genutzt werden dürfen, stehen daher nicht zur Disposition.

Auch der gesetzlich verankerten Pflicht, unsere Dienststelle bei der Erfüllung ihrer Aufgaben zu unterstützen, kommen die Justizvollzugsanstalten teils nur sehr zögerlich nach. Dies hat zur Folge, dass wir Eingaben von Strafgefangenen, die sich an uns wenden, weil sie der Ansicht sind, die Vollzugsanstalt habe sie in ihrem Recht auf informationelle Selbstbestimmung verletzt, oft erst nach Monaten abschließend bearbeiten können, weil die betreffende Vollzugsanstalt die von uns erbetene Stellungnahme zum Vorbringen des Gefangenen erst so spät abgibt. Dies führt letztlich dazu, dass wir unserer Verpflichtung, Eingaben von Bürgern nach § 27 LDSG nachzugehen und sie in angemessener Zeit zu bescheiden, nicht wirksam nachkommen können. Zum anderen ist dieses Verhalten mit § 29 LDSG nicht zu vereinbaren. Nach dieser Vorschrift sind alle öffentlichen Stellen des Landes und damit auch die Justizvollzugsanstalten verpflichtet, unser Amt bei der Erfüllung seiner Aufgaben zu unterstützen und ihm im Rahmen seiner Kontrollbefugnisse Auskunft zu Fragen zu geben, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Dass Stellungnahmen von den Justizvollzugsanstalten erst nach Monaten abgegeben werden, ist daher nicht hinnehmbar. Aus diesem Grund haben wir das Verhalten der Justizvollzugsanstalt Mannheim in drei besonders krassen Fällen

wegen Verstoßes gegen die Unterstützungspflicht förmlich beanstandet. In diesen Fällen äußerte sich die Vollzugsanstalt, trotz mehrmaliger schriftlicher und telefonischer Erinnerungen, letztendlich erst nach über sechs Monaten.

2.6.1 Zu weitgehende Zugriffsmöglichkeiten

Ein im Berichtsjahr bei einer Justizvollzugsanstalt durchgeführter Kontrollbesuch hat im Bereich der anstaltsinternen Informationsverarbeitung erhebliche Mängel offenbart. Hier einige Beispiele:

– Der anstaltsinterne Postlauf

In der für alle Beschäftigten der Justizvollzugsanstalt zugänglichen Poststelle befinden sich offene Postfächer, in die sowohl die von außen eingehende Post als auch anstaltsinterne Vorgänge eingelegt werden. Die Fächer werden von den jeweiligen „Inhabern", z. B. den Vollzugsleitern, den Stockwerksbeamten, Mitarbeitern der Sonderdienste usw., selbst geleert. Hausinterne Vorgänge, die für die Gefangenen bestimmt sind, wie z. B. Genehmigungen, Ablehnungen und sonstige Mitteilungen, werden im Regelfall unkuvertiert in das Postfach des für den jeweiligen Gefangenen zuständigen Stockwerksbeamten gelegt. Dieser händigt die verschiedenen Schreiben schließlich an die Strafgefangenen aus. Auch die für den bargeldlosen Einkauf in der Anstalt verwendeten sog. Einkaufsscheine, die personenbezogene Daten der Gefangenen enthalten, oder etwa Kontoauszüge über das Eigengeld der Gefangenen – das ist der Teil der Bezüge der Strafgefangenen, über den sie in der Regel frei verfügen können – werden ihnen offen ausgehändigt. Dies hat nicht nur zur Folge, dass der Stockwerksbeamte über alle Angelegenheiten, die die in seiner Abteilung untergebrachten Gefangenen betreffen, umfassend informiert wird, sondern auch dass die offen im Postfach liegenden Schreiben im Grunde von allen Beschäftigten, die in die Poststelle kommen, eingesehen werden können.

Datenschutzrechtlich ist hierzu Folgendes zu sagen:

Nach § 183 Abs. 1 Satz 1 des Strafvollzugsgesetzes (StVollzG) darf sich der einzelne Vollzugsbedienstete von personenbezogenen Daten nur Kenntnis verschaffen, soweit dies zur Erfüllung der ihm obliegenden Aufgaben oder für die Zusammenarbeit in der Justizvollzugsanstalt erforderlich ist. Nach § 183 Abs. 2 Satz 1 und 3 StVollzG i. V. mit § 9 des Bundesdatenschutzgesetzes (BDSG) sind Akten und Dateien mit personenbezogenen Daten durch die erforderlichen technischen und organisatorischen Maßnahmen gegen unbefugten Zugang und unbefugten Gebrauch zu schützen, soweit der Aufwand dieser Maßnahmen in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Personenbezogene Daten dürfen daher auch anstaltsintern nur den zuständigen Vollzugsbediensteten und nur in dem zur Aufgabenerfüllung erforderlichen Maß weitergegeben werden. Die Möglichkeit, darüber hinaus von personenbezogenen Daten Kenntnis zu nehmen, muss die Justizvollzugsanstalt durch geeignete Maßnahmen verhindern. Dem entspricht die derzeitige Verfahrensweise der Vollzugsanstalt nicht. Denn obwohl alle Bediensteten eine Mitwirkungspflicht beim Strafvollzug haben, sind ihre Funktionen und Aufgaben und damit auch ihr berechtigtes Informationsinteresse unterschiedlich. Der Stockwerksbeamte, der täglich und unmittelbar mit den Gefangenen in Berührung kommt, hat sicher in nicht unerheblichem Umfang ein dienstlich veranlasstes Informationsinteresse. Dass er sämtliche Verfügungen und Aufstellungen über finanzielle Verhältnisse der in seinem Zuständigkeitsbereich untergebrachten Gefangenen kennen muss, ist jedoch nicht nachvollziehbar. Wir haben die Justizvollzugsanstalt

daher aufgefordert, den anstaltsinternen Postlauf so zu organisieren, dass die Gefahr unbefugter Kenntnisnahme so weit als möglich beseitigt wird, was z. B. durch die Verwendung verschlossener Umschläge erreicht werden kann.

– Die Gefangenenpersonalakten

  Die Gefangenenpersonalakte ist das Kernstück der Datenverarbeitung in der Justizvollzugsanstalt. Sie enthält unzählige, teils hochsensible Daten über den Gefangenen, z. B. über das religiöse Bekenntnis, Familienstand, Kinderzahl, Gutachten des psychologischen Dienstes, den während der Haft anfallenden Schriftverkehr, aber auch Daten über Dritte, wie z. B. Angehörige des Gefangenen. In der Vollzugsanstalt, die wir kontrolliert haben, kann praktisch jeder Bedienstete auf die gesamten Gefangenenpersonalakten zugreifen. Beschäftigte, die Einblick in eine Gefangenenpersonalakte wünschen, müssen lediglich einen Anforderungszettel ausfüllen. Die Geschäftsstelle, bei der die Gefangenenpersonalakten aufbewahrt werden, legt die angeforderte Akte, und zwar grundsätzlich die gesamte Akte, in das Postfach desjenigen Bediensteten, der diese angefordert hat.

Wie bereits ausgeführt, enthält § 183 StVollzG spezielle Regelungen für die anstaltsinterne Datenweitergabe bzw. Kenntnisnahme von personenbezogenen Daten und die Verpflichtung der Justizvollzugsanstalt sicherzustellen, dass Nutzung und Gebrauch dieser Daten nicht über das erforderliche Maß hinausgehen. Der Kreis der Zugriffsberechtigten und der Umfang ihrer Einsichts- und Nutzungsbefugnisse ist dabei für sämtliche personenbezogenen Daten, die in Akten oder Dateien enthalten sind, auf das für die Erledigung der Vollzugsaufgaben notwendige Maß beschränkt. Es ist daher datenschutzrechtlich unzulässig, wenn jeder Bedienstete jeweils die gesamte Gefangenenpersonalakte einsehen kann. So ist nicht einzusehen, dass sich etwa die Arbeitsverwaltung der Vollzugsanstalt über die nächsten Angehörigen oder das religiöse Bekenntnis eines Gefangenen informieren kann. Es dürfen daher nur die Aktenteile herausgegeben werden, auf die sich das berechtigte Informationsinteresse des jeweiligen Bediensteten bezieht. Wir forderten die Justizvollzugsanstalt daher auf zu prüfen, wie sichergestellt werden kann, dass bei Einsichtnahmen in die Akten nur der tatsächlich notwendige Teil zur Verfügung gestellt wird. Da auch die anstaltsinterne Zuleitung der Gefangenenpersonalakten über die offenen Postfächer erfolgt – wodurch sich auch unbefugte Personen vom Inhalt dieser Akten Kenntnis verschaffen können – haben wir die Justizvollzugsanstalt darüber hinaus aufgefordert, die Gefangenenpersonalakten oder Teile hieraus künftig in Verschlussmappen zu transportieren oder direkt auszuhändigen.

Die Reaktion der Justizvollzugsanstalt:

Die Justizvollzugsanstalt sah keinen Bedarf, auch nur einen Teil unserer Forderungen umzusetzen. Sie begründete dies beispielsweise mit der großen Zahl von Briefumschlägen, die sie sonst benötigen würde, mit Sicherheitsgründen – wobei die hierzu genannten Beispiele alles andere als überzeugend waren – und damit, dass die von uns geforderten Verfahrensweisen mit einem unverhältnismäßigen Mehraufwand verbunden wären. Eine ernst zu nehmende Auseinandersetzung mit § 183 StVollzG fand dagegen nicht statt. Dies zeigt sich z. B. daran, dass die Vollzugsanstalt erklärte, sie werde einem Beschluss der Strafvollstreckungskammer des Landgerichts Karlsruhe vom 18. Februar 2002, der zwar gegen eine andere Justizvollzugsanstalt ergangen war, in dem es jedoch genau um die hier angesprochene Problematik geht, nicht folgen. In dieser rechtskräftigen Entscheidung hatte die Strafvollstreckungskammer eine Justizvollzugsanstalt ver-

pflichtet, einem Gefangenen die von der Zahlstelle der Justizvollzugsanstalt erstellten Kontoauszüge und Einzahlungsbelege in einem von der Zahlstelle zu verschließenden Umschlag aushändigen zu lassen. Das Gericht begründete die Entscheidung folgendermaßen: Die Aushändigung in verschlossenen Umschlägen stelle für die Vollzugsanstalt zwar einen organisatorischen Mehraufwand dar. Angesichts des hohen Stellenwerts des Schutzes personenbezogener Daten rechtfertige dies jedoch nicht, die bisherige Vollzugspraxis, die Kontoauszüge und Einzahlungsbelege offen zu übergeben, beizubehalten. Der Auffassung der Vollzugsanstalt, der durch die Einkuvertierung entstehende Mehraufwand stünde in keinem angemessenen Verhältnis zum angestrebten Schutzzweck der gesetzlichen Regelung, könne es sich nicht anschließen.

Im Übrigen ging es auch in dem der Entscheidung zugrunde liegenden Fall um die Aushändigung von Unterlagen durch die Stockwerksbeamten. Die Strafvollstreckungskammer des Landgerichts Karlsruhe scheint daher ebenso wie unsere Dienststelle der Ansicht zu sein, dass das Informationsinteresse der Stockwerksbeamten nicht allumfassend ist.

Diese Entscheidung hat auch für den von der Justizvollzugsanstalt praktizierten Umgang mit Gefangenenpersonalakten rechtliche Bedeutung. Da die Justizvollzugsanstalt bereits bei der Zuleitung von Kontoauszügen an Gefangene – trotz des damit verbundenen Mehraufwands – sicherstellen muss, dass Bedienstete hiervon keine Kenntnis erhalten, muss Entsprechendes erst recht für die Einsichtsmöglichkeiten und den Transport von Gefangenenpersonalakten gelten, die ungleich mehr personenbezogene Daten enthalten als ein Kontoauszug oder eine einzelne Verfügung. Auch organisatorische Maßnahmen zum Schutz der in Gefangenenpersonalakten enthaltenen Daten können daher nicht einfach mit dem Hinweis auf einen damit verbundenen – im Übrigen nicht näher bezeichneten – Mehraufwand abgelehnt werden.

Wegen der bislang unbefriedigenden Reaktion der Vollzugsanstalt werden wir die Angelegenheit selbstverständlich weiter im Auge behalten.

2.6.2 Der verräterische Überweisungsträger

Immer wieder teilen uns Strafgefangene mit, dass Justizvollzugsanstalten Dritte über die Inhaftierung informieren, obwohl diese Information für die unterrichtete Stelle vollkommen unerheblich ist. Von einem Gefangenen, der sich zu Weiterbildungszwecken unter anderem regelmäßig auf eigene Kosten Bücher bestellt, haben wir z. B. Folgendes erfahren:

Die Bezahlung der von ihm bestellten Buchsendungen erfolge so, dass von seinem von der Justizvollzugsanstalt verwalteten Einkommen die Rechnungssumme an den jeweiligen Verlag überwiesen werde. Zur Durchführung dieser Überweisungen verwende die Vollzugsanstalt einen vorgedruckten Überweisungsträger, der als Kontoinhaber die Justizvollzugsanstalt nenne. Der Name des Gefangenen erscheine im Feld Verwendungszweck des Überweisungsträgers.

Dies hat zur Folge, dass neben dem Geldinstitut, bei dem die Justizvollzugsanstalt ihr Konto hat, auch die Firma, bei der der Gefangene etwas bestellt hat, und deren Bank erfahren, dass sich der Kunde, der lediglich eine Rechnung bezahlen will, in Haft befindet. Und dies, obwohl dieser Umstand für die Abwicklung des zwischen dem Gefangenen und der Firma bestehenden Vertrags keinerlei Rolle spielt. Auch das Strafvollzugsgesetz – welches regelt, unter welchen Voraussetzungen die Tatsache der Inhaftierung nichtöffentlichen Stellen mitgeteilt werden darf: nämlich auf Antrag und wenn diese Stelle ein berechtigtes Interesse hierfür

darlegt – sieht für diesen Fall keine Auskunftserteilung vor. Hierauf angesprochen, teilte die betreffende Justizvollzugsanstalt mit, dass es bei der Überweisung von Geldern der Gefangenen an Dritte unumgänglich sei, auf dem Überweisungsträger die Vollzugsanstalt als Kontoinhaber zu nennen.

Zwischenzeitlich hatten wir jedoch erfahren, dass es Justizvollzugsanstalten gibt, die diese Angabe auf dem Überweisungsträger verhindern, indem – in Absprache mit ihrer Bank – anstelle der Justizvollzugsanstalt lediglich das Postfach bzw. Straße und Hausnummer der Vollzugsanstalt im Feld Kontoinhaber angegeben werden. Da durch diese Vorgehensweise zumindest vermieden wird, dass der Überweisungsempfänger und seine Bank von der Inhaftierung Kenntnis erhalten, forderten wir die Justizvollzugsanstalt auf, die Angelegenheit zu prüfen und mitzuteilen, wie sie künftig verfahren werde, um zu verhindern, dass Dritte unnötigerweise von der Inhaftierung erfahren.

Angesichts der Möglichkeiten der EDV-Technik gingen wir davon aus, dass es kein größeres Problem darstellen dürfte, mit dem kontoführenden Institut eine datenschutzgerechte Verfahrensweise abzustimmen. Wider Erwarten teilte uns die Justizvollzugsanstalt jedoch mit, dass auch die wiederholte Prüfung der Fragestellung ergeben habe, dass gebührenfreie Überweisungen für Gefangene ohne Angabe der Justizvollzugsanstalt nicht durchgeführt werden könnten. Aus diesem Grund habe sie den Vorgang zur grundsätzlichen Klärung an das Justizministerium Baden-Württemberg weitergeleitet.

Eine Antwort hierzu liegt uns bislang noch nicht vor. Wir hoffen, dass sich das Justizministerium unserer Auffassung anschließt und so verhindert, dass Dritte auch weiterhin vollkommen überflüssigerweise von der Inhaftierung Kenntnis erlangen.

3. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheit

1. Die gesetzliche Krankenversicherung

Eine im Jahre 2001 durchgeführte umfassende Studie zum Thema Datenschutz hat ergeben, dass 90 % der Bevölkerung bei den Krankenkassen die umfangreichsten Datenspeicher vermuten. Richtig ist, dass die Krankenkassen eine große Menge an Informationen, auch medizinischer Art, über ihre Versicherten besitzen und auf Grund ihrer Aufgabenstellung auch besitzen müssen. Andererseits ist kein Sozialversicherungsträger strenger im Umgang mit diesen Daten reglementiert als gerade die Krankenkassen. Auch muss man sehen, dass das Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung – den Krankenkassen besonders sensible medizinische Informationen, wie etwa ärztliche Befunde, vorenthält. In aller Regel erhalten sie allein die Diagnoseangaben. Abrechnungen aus Arztpraxen erreichen sie grundsätzlich ohne Bezug zum konkreten Versicherten. Allerdings scheint sich hier neuerdings eine Entwicklung anzubahnen, die zu einem deutlichen Rückschritt führt. So wurden etwa im Zuge der Fortentwicklung des Risikostrukturausgleichs sog. „Disease Management Programme“ (DMP) eingeführt, in deren Verlauf die Krankenkassen erstmals auch aus dem Bereich der ambulanten ärztlichen Versorgung versichertenbezogene Krankheitsdaten erhalten. Die Erfahrung zeigt, dass Argumente des Datenschutzes bei solchen Entwicklungen nur sehr bedingt auf Gehör stoßen. Umso mehr muss es Aufgabe der Datenschutzkontrolle sein, darauf zu achten, dass in der täglichen Praxis den gesetzlichen Vorgaben entsprechend verfahren wird. Mit diesem Ziel haben wir mehrere Krankenkassen besucht. Hierzu und zu einigen ausgewählten Einzelfällen Folgendes:

1.1 Aus der Kontrollpraxis

Im Berichtszeitraum wurden zwei Bezirksdirektionen der AOK Baden-Württemberg und eine Regionaldirektion der IKK Baden-Württemberg besucht. Dabei haben sich vor allem folgende Problempunkte herauskristallisiert:

1.1.1 Zugriff auf Versichertendaten

Sowohl das von der AOK wie auch das von der IKK verwendete EDV-Verfahren wird jeweils am Hauptsitz der Versicherung zentral verwaltet. Die AOK setzt dabei das Verfahren IDVS II, die IKK das Verfahren ISKV ein. In diesen Verfahren werden alle Grund- und Leistungsdaten der Versicherten erfasst. Dabei ist es so, dass dem Grunde nach jeder Mitarbeiter und jede Mitarbeiterin einer Bezirks- oder einer Regionaldirektion auf alle im System gespeicherten Versichertendaten zugreifen kann – und zwar landesweit. Die innerhalb der Einheit vorhandene Möglichkeit, alle Versichertendaten der eigenen Einheit abrufen zu können, wird zum einen damit begründet, dass grundsätzlich alle Mitarbeiter in die Lage versetzt werden müssten, grundsätzlich jeden Kunden zu beraten. Technisch wird sie damit gerechtfertigt, dass das System eine auf den konkreten Arbeitsplatz zugeschnittene Differenzierung der Zugriffsrechte durch die jeweilige operative Einheit nicht zulasse. So kommt es also, dass beispielsweise ein Mitarbeiter oder eine Mitarbeiterin, der oder die ausschließlich für Zahnersatz zuständig ist, sich jederzeit auch alle Leistungsdaten aus anderen Bereichen (etwa Arbeitsunfähigkeit oder Krankenhausaufenthalt, immer auch mit Diagnoseangabe, oder auch die Daten aus dem Bereich der Pflegeversicherung) anzeigen lassen kann. Mit dem Datenschutzrecht ist diese Praxis nicht zu vereinbaren.

Sozialdaten unterliegen dem Sozialgeheimnis, das grundsätzlich auch innerhalb des Leistungsträgers zu beachten und sicherzu-

stellen ist (§ 35 Abs. 1 Satz 2 des Sozialgesetzbuches (SGB) Erstes Buch (I) – Allgemeiner Teil –). Dies bedeutet konkret, dass nicht nur die Krankenkasse als solche Sozialdaten nur im Rahmen der Erforderlichkeit verarbeiten darf (§ 284 SGB V). Es bedeutet vielmehr auch, dass intern jedem Mitarbeiter und jeder Mitarbeiterin nur die Daten zur Verfügung stehen dürfen, die er oder sie für die Erledigung der jeweils zugewiesenen Aufgaben benötigt. Der Zugriff auf Daten, deren Kenntnis für die Aufgabenerledigung nicht erforderlich ist, darf nicht eröffnet werden. Dem wird die Praxis der Krankenkassen mit ihren nahezu undifferenzierten Zugangsmöglichkeiten für alle Beschäftigten zu den Versichertendaten nicht gerecht. Erste zaghafte Ansätze zu einer Verbesserung des Datenschutzes in diesem wichtigen Punkt sind indes sichtbar. So hat die AOK in Aussicht gestellt, zumindest der Frage einer stärkeren Differenzierbarkeit bei den Abfrageberechtigungen nachzugehen. Es bleibt zu hoffen, dass es nicht dabei bleibt und damit auch innerhalb der Krankenkasse der „gläserne“ Versicherte verhindert wird.

Eine Steigerung erfährt das dargestellte Problem noch dadurch, dass der Zugriff auf die Daten nicht nur innerhalb der Bezirks- oder Regionaldirektion auf die Daten der „eigenen“ Versicherten, sondern sogar landesweit möglich ist. Es kann also ein Mitarbeiter, gleichgültig wo er beschäftigt ist, an seinem Arbeitsplatz auf die Daten aller Versicherten der jeweiligen Krankenkasse im ganzen Land zugreifen. Begründet wird dies damit, es sei Ausdruck besonderer Kundenfreundlichkeit, wenn ein Versicherter, ganz gleich wo er sich aufhält, die Möglichkeit habe, zum örtlichen Kundenberater zu gehen und dort bedient zu werden. Das ist an sich richtig und dagegen ist auch nichts zu sagen. Allerdings ist dabei zu bedenken, dass der weitaus überwiegende Teil der Versicherten diesen Service voraussichtlich kaum in Anspruch nehmen wird. Gleichwohl können alle im System gespeicherten Daten aller Versicherten während der gesamten Dauer des Versicherungsverhältnisses landesweit eingesehen werden. Sonderlich kundenfreundlich erscheint uns dies nicht. Zudem ist diese Praxis nicht mit dem Datenschutzrecht zu vereinbaren. Denn was für die zuvor dargestellte Frage der internen Zugänglichkeit der Datenbestände gilt, gilt für die externe Zugänglichkeit umso mehr. Dass etwa eine Krankenkasse in Friedrichshafen am Bodensee ihre Aufgaben nicht erfüllen kann, ohne Zugriff auf die Daten der Mitglieder der Krankenkasse in Heidelberg zu haben, dürfte schwerlich zu begründen sein. Eine Datenverarbeitung ist aber nur im Rahmen der Erforderlichkeit zulässig, wobei der Erforderlichkeitsgrundsatz aus dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz hergeleitet wird. Unverhältnismäßig wäre es aber, eine bestimmte Form der Datenverarbeitung generell zuzulassen, wenn diese konkret nur in vergleichsweise wenigen Einzelfällen zum Tragen kommt.

Wir hatten vorgeschlagen, jedem Versicherten die Wahl zu lassen, ob er den landesweiten Zugriff wünscht oder nicht. Nur wer wirklich beabsichtigt, die Dienste einer anderen als „seiner“ Bezirks- oder Regionaldirektion in Anspruch zu nehmen, wird dann der landesweiten Freischaltung seiner Daten zustimmen. Alle anderen könnten dann sicher sein, dass der Kreis der „Wissenden“ begrenzt bleibt, allerdings um den Preis des Verzichts auf eine auswärtige Betreuung. Die Krankenkassen wollten sich diesem, aus unserer Sicht praktikablen, Vorschlag leider nicht anschließen.

1.1.2 Das Archiv

Nicht nur die Verfügbarkeit der Daten im EDV-System bereitete Kummer. Auch soweit es um schriftliche Unterlagen geht, gab es aus unserer Sicht Anlass zu Kritik. So war es bei zwei der besuchten Krankenkassen Praxis, die Unterlagen, die nicht mehr

aktuell am jeweiligen Arbeitsplatz vorgehalten werden mussten, in der Altregistratur aufzubewahren. Das Problem dabei ist, dass zum einen mangels fester Registraturmitarbeiter grundsätzlich jede bei der Direktion beschäftigte Person Zutritt zum Archiv hat. Die Archivräume sind zwar abgeschlossen. Die Beschaffung des Schlüssels bereitet jedoch keine Schwierigkeiten, da hinsichtlich der sachlichen Berechtigung, auf die Altakten zuzugreifen, keine wirklichen Kontrollen stattfinden. Zum anderen sind in den Registraturen alle Unterlagen frei zugänglich. Wer sich demnach im Archiv befindet, kann sich nach Belieben bedienen. Es existiert auch keine interne Anweisung, die Entnahme von Unterlagen zu dokumentieren. Damit kann nachträglich nicht mehr festgestellt werden, wer wann welche Akte entnommen hat.

Datenschutzrechtlich gilt auch hier, dass die Möglichkeit, auf Sozialdaten versicherter Personen zugreifen zu können, so organisiert sein muss, dass Unbefugte von einer Kenntnisnahme ausgeschlossen sind. Nur dies entspricht dem Grundsatz der Erforderlichkeit, der für jede Form der Datenverarbeitung gilt und der mit technischen und organisatorischen Maßnahmen abgesichert werden muss (§ 78 a des Sozialgesetzbuches (SGB) Zehntes Buch (X) – Verwaltungsverfahren –). Es müssen also Maßnahmen getroffen werden, die einen selektiven Zugang zu den Akten je nach konkreter Funktion des Mitarbeiters oder der Mitarbeiterin und zu erfüllender Aufgabe zulassen. Dies kann vor allem dadurch erreicht werden, dass die Unterlagen, nach bestimmten Ordnungsmerkmalen (z. B. Pflegeversicherung, Zahnersatz usw.) getrennt, in jeweils verschließbaren und auch tatsächlich verschlossenen Aktenschränken aufbewahrt werden. Ergänzt werden muss dies um ein geeignetes und angemessenes Schlüsselmanagement und um interne Vorgaben über den Entnahme- und Rückgabevorgang mit entsprechender Überwachung.

Bei einer der besuchten AOK-Bezirksdirektionen war das Archiv in einem im obigen Sinne vorbildlichen Zustand. Die beiden anderen Direktionen haben wir aufgefordert, entsprechende Maßnahmen zu ergreifen. Dies wurde uns zugesagt.

1.1.3 Mitglieder- und Leistungskarten

Bei allen Krankenkassen wurden umfangreiche Bestände von Mitglieder- und Leistungskarten (Karteikartensammlung) vorgefunden. Diese enthalten neben den Versichertenstammdaten auch den Leistungsverlauf, zum Teil bis in die 40er bis 50er Jahre des letzten Jahrhunderts zurück. Als Grund für das Vorhalten dieser Altbestände wurde immer wieder angegeben, die Daten würden zur Blockfristenbildung für den Krankengeldbezug benötigt. Auch erfolge die Speicherung im Interesse der Versicherten. Diese hätten damit die Möglichkeit, gegenüber dem Rentenversicherungsträger ihre Versicherungszeiten nachzuweisen.

Zum ersten Argument ist zu sagen, dass das Grundrecht auf Datenschutz auch den Anspruch des Einzelnen auf Löschung der zu seiner Person gespeicherten Informationen beinhaltet. Eine zeitlich unbegrenzte Speicherung seiner Daten, die zur Bildung eines Persönlichkeitsprofils (hier: Krankheitsprofils) verwendet werden könnte, muss niemand hinnehmen. Für die Krankenkasse gilt es dabei, § 304 SGB V zu beachten. Diese Vorschrift bestimmt für bestimmte Daten konkrete Löschungsfristen und verweist im Übrigen auf die allgemeine Löschungsregelung des § 84 Abs. 2 SGB X. Bezogen auf die Mitglieder- und Leistungskarten gilt demnach Folgendes:

Nach § 48 SGB V wird im Falle krankheitsbedingter Arbeitsunfähigkeit Krankengeld gezahlt. Dieser Anspruch ist auf insgesamt 78 Wochen innerhalb von jeweils drei Jahren begrenzt. Ein neuer Anspruch auf Krankengeld wegen derselben Krankheit entsteht erst mit Beginn eines neuen Dreijahreszeitraums (Blockfrist).

Diese Blockfrist ist starr. Der erstmalige Eintritt der Arbeitsunfähigkeit wegen einer bestimmten Krankheit setzt insoweit eine Kette aufeinander folgender Blockfristen in Gang. Um also berechnen zu können, wann eine neue Blockfrist und damit gegebenenfalls ein neuer Krankengeldanspruch beginnt, benötigt die Krankenkasse bestimmte Daten, vor allem die Krankheitsdiagnosen. § 292 SGB V erlaubt deren Speicherung. § 304 Abs. 1 Satz 1 Nr. 1 SGB V begrenzt nun die Dauer dieser Speicherung auf höchstens zehn Jahre. Angesichts dieser klaren gesetzlichen Regelung kann es eigentlich keinen Zweifel daran geben, dass die zum Teil wesentlich längere Aufbewahrung der Leistungsdaten jedenfalls nicht mit der Blockfristenbildung begründet werden kann.

Was die Nutzung der Daten durch Versicherte für Zwecke der Rentenversicherung angeht, ist die Sache komplizierter. Die Krankenkassen berichten über eine rege Nachfrage nach diesen Daten durch die Versicherten. Offenbar gibt es bei den Rentenversicherungsträgern nach wie vor Unklarheiten im Versicherungsverlauf, die nur durch Rückgriff auf die bei den Krankenkassen vorhandenen „alten“ Daten beseitigt werden können (Versicherungs-, Ausfall-, Anrechnungszeiten). Nach § 84 Abs. 2 SGB X muss die Krankenkasse Sozialdaten dann nicht löschen, wenn Grund zur Annahme besteht, dass dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Dies ist der Fall, wenn Anhaltspunkte vorliegen, die eine Interessenbeeinträchtigung vermuten lassen.

Die von den Krankenkassen dargestellte Praxis belegt durchaus das erhebliche Interesse vieler Versicherter daran, dass die bei der Krankenkasse gespeicherten Daten nicht verloren gehen. Im Verhältnis zur Gesamtzahl der Versicherten handelt es sich dabei jedoch lediglich um eine Minderheit. Für die Mehrheit ist davon auszugehen, dass sie mit einer zeitlich unbegrenzten Aufbewahrung ihrer persönlichen Daten nicht einverstanden ist. Es muss deshalb eine Lösung gefunden werden, die den Belangen aller Betroffenen gerecht wird. Dabei ist zu berücksichtigen, dass nach § 17 der Datenerfassungs-Verordnung (DEVO) vom 24. November 1972 (BGBl. I S. 2159) der für die Führung des Versicherungskontos zuständige Rentenversicherungsträger verpflichtet war, dem Versicherten bis spätestens 31. Dezember 1977 erstmals einen Versicherungsverlauf zu übersenden (und dies seitdem in regelmäßigen Zeitabständen wiederholen muss; § 7 der Versicherungsnummern-, Kontoführungs- und Versicherungsverlaufsverordnung). Damit hatte seit dem damaligen Zeitpunkt jeder Versicherte inzwischen mehrmals die Möglichkeit (und nach der Verordnung sogar die Pflicht), diesen Versicherungsverlauf auf Richtigkeit und Vollständigkeit hin zu überprüfen und Mängel geltend zu machen. Wer diese Möglichkeit bisher nicht genutzt und sich bei seiner Krankenkasse rückversichert hat, ob die beim Rentenversicherungsträger vermerkten Versicherungszeiten korrekt sind, dem kann mittlerweile auch kein schutzwürdiges Interesse an der weiteren Speicherung mehr zugesprochen werden. Da die Mitglieder- und Leistungskartei auf Grund der Einführung der EDV bei den Krankenkassen nur bis etwa Mitte der 80er Jahre fortgeführt wurde, kann nach nunmehr fast 20 Jahren deren Vernichtung veranlasst werden. Mit den Krankenkassen werden wir wegen dieser Angelegenheit noch Gespräche führen müssen.

1.1.4 Fehlender Diskretionsbereich

Die Beratung der Versicherten bei den besuchten Direktionen findet in Großraumbüros statt. Dabei fiel auf, dass in einigen Fällen die Arbeitsplätze der Kundenberater so dicht beieinander liegen, dass bei gleichzeitiger Beratung mehrerer Versicherter jeweils gegenseitig mitgehört werden kann, was gesagt wird – je-

denfalls dann, wenn man sich nicht gerade im Flüsterton unterhält. Dies ist keine datenschutzgerechte Organisation. Denn das Sozialgeheimnis gebietet es auch, dass es dem Versicherten ermöglicht wird, Angaben, die er der Krankenkasse gegenüber machen will, so zu machen, dass keine Unbefugten mithören können. Der von einer Krankenkasse gemachte Vorschlag, dem Versicherten werde bei Gesprächen mit „sensiblem“ Inhalt angeboten, in ein separates Zimmer auszuweichen, reicht nicht aus. Dabei wird verkannt, dass dem Sozialgeheimnis nicht nur „sensible“ Daten unterfallen, sondern alle Daten, welche die Krankenkasse vom Versicherten erhält. Zur Lösung des Problems hatten wir gebeten, an den Arbeitsplätzen Schallschutzeinrichtungen anzubringen, die eine ungestörte Kommunikation zwischen Kunden und Kundenberater zulassen. Während dies im einen Fall zugesichert wurde, werden wir im anderen Fall wohl noch etwas Überzeugungsarbeit leisten müssen.

1.2 Datenübermittlung an private Gutachter

Immer wieder werden wir mit Fragen konfrontiert, die sich daraus ergeben, dass eine Krankenkasse durch private Gutachter klären lässt, ob und inwieweit sie bestimmte Leistungen zu tragen hat. Mit dem Gutachtenauftrag werden nämlich oft auch personenbezogene Daten an den Gutachter übermittelt.

Im Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung – ist vorgesehen, dass sich eine Krankenkasse an den Medizinischen Dienst der Krankenversicherung (MDK) wendet, wenn sie ihre Leistungspflicht im Einzelfall nicht einschätzen kann. Die Fachleute des MDK nehmen dann aus ärztlicher Sicht zu dem Fall Stellung. Es kann allerdings auch um so spezielle Fragen gehen, dass sie selbst der MDK nicht beantworten kann. Mit einer solchen Situation hatten wir uns zu befassen.

Begehrt ein Versicherter eine Sehhilfe und sind hierfür keine Festbeträge bestimmt worden, muss er einen Kostenvoranschlag einreichen. Die Krankenkasse prüft diesen dann auf Begründetheit und Angemessenheit. Da sich gezeigt hatte, dass die Krankenkassenmitarbeiter nicht immer über hinreichende Fach- und Marktkenntnisse verfügen, um die Prüfung dieser Kostenvoranschläge selbst durchzuführen, und sich auch der MDK hierzu nicht in der Lage sah (jedenfalls was die konkrete Preisangabe betraf), beauftragten einzelne Krankenkassen in Baden-Württemberg eine privatrechtliche Gesellschaft, die auf diesem Gebiet besondere Fachkenntnisse vorweisen kann, mit der Begutachtung. Gleichzeitig reichten sie die Unterlagen versicherten- und leistungserbringerbezogen weiter.

Wir sind der Auffassung, dass diese namensbezogene Datenweitergabe nicht erforderlich und deshalb datenschutzrechtlich unzulässig ist. Denn die Klärung, ob ein Kostenvoranschlag inhaltlich zutrifft, kann allein anhand der objektiven Daten erfolgen. Weder der Name des Patienten noch der des verordnenden oder des den Voranschlag erstellenden Arztes oder Augenoptikers spielen dabei eine Rolle. Die Krankenkassen haben wir deshalb aufgefordert, die Unterlagen nur noch ohne Name und Adresse der Beteiligten weiterzugeben. Eine Krankenkasse wollte dies zunächst nicht akzeptieren. Sie meinte, der Gutachter brauche die Namen, um sich bei Unklarheiten unmittelbar an die Betroffenen wenden zu können. Dieses Argument konnten wir allerdings nicht akzeptieren. Denn treten solche Unklarheiten auf, ist jedenfalls die Krankenkasse als Auftraggeber in der Lage, eine Klärung herbeizuführen. Hierzu muss sich der Gutachter im Einzelfall an die Krankenkasse wenden mit der Bitte, die nötigen Nachforschungen anzustellen. Es fehlt also an der Erforderlichkeit der namensbezogenen Datenübermittlung. Das Interesse der betroffenen Patienten am Schutz ihrer Sozialdaten ist letztlich wichtiger als die bürokratische Erleichterung, die darin liegt, dass sich der Gutachter ohne Zwischenschaltung seines Auftraggebers (der Krankenkasse) unmittelbar an den Arzt oder Augenoptiker wenden kann.

Bei diesen Überlegungen spielt auch eine Rolle, dass nicht in jedem Fall eine solche Rückfrage erfolgen wird. Die generelle Übermittlung der Identifizierungsdaten wäre deshalb oftmals, möglicherweise sogar in den meisten Fällen, völlig überflüssig.

Auf unser Betreiben sind die Krankenkassen dazu übergegangen, dem Gutachter nur noch pseudonymisierte Daten zur Verfügung zu stellen. Rückfragen werden erforderlichenfalls über den zuständigen Sachbearbeiter der Krankenkasse erledigt, der das Pseudonym wieder dem konkreten Versicherten zuordnen kann.

1.3 Die Bewerberdaten

Mitunter ist es eine Fügung glücklicher (oder unglücklicher?) Umstände, die auf die Spur nicht datenschutzgerechter Praktiken führen. So berichtete uns eine Bürgerin, sie habe sich auf eine Anzeige hin um eine Anstellung bei einer Krankenkasse beworben. Der Zufall wollte es, dass sie gerade bei dieser Krankenkasse auch Mitglied war. Nachdem die Wahl offenbar auf einen Mitbewerber oder eine Mitbewerberin gefallen war, erhielt die Betroffene eine Absage. Weniger dies schockierte sie als der Umstand, dass dem Ablehnungsschreiben die Kopie eines Ausdrucks aus ihrer Leistungsdatei beilag. Dieser war mit dem Vermerk „Ausdruck für Bewerbung“ versehen und enthielt haarklein die der Kasse gemeldeten Krankheiten der letzten Jahre. Dass diese Kenntnis letztlich die Entscheidung über die Bewerbung beeinflusst haben dürfte, ist anzunehmen.

Um Rat gefragt, erläuterten wir der Bürgerin die Rechtslage und ihre Datenschutzrechte. Sie gab an, zunächst mit dem Leiter der Direktion sprechen und die Angelegenheit klären zu wollen. Später teilte sie uns mit, man habe sich bei ihr entschuldigt und eingeräumt, dass etwas schief gelaufen sei. Das meinten wir in der Tat auch und nahmen den Fall zum Anlass, die Problematik allgemein mit der Krankenkasse zu besprechen.

Rechtlich sieht es so aus, dass die Krankenkasse bei der Verarbeitung der Sozialdaten ihrer Mitglieder nicht frei ist. Vielmehr setzt ihr das Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung – enge Grenzen. Erlaubt sind nur solche Verarbeitungen, die einem der im Gesetz genau definierten Zwecke dienen (§ 284 SGB V). Die Nutzung von Sozialdaten für Zwecke einer Stellenbewerbung ist dort nicht vorgesehen. Es ist sogar so, dass nach § 35 Abs. 1 SGB I Sozialdaten ausdrücklich vor dem Zugriff durch Personen, die Personalentscheidungen treffen, geheim gehalten werden müssen. Zwar ist dort ausdrücklich nur von Sozialdaten der Beschäftigten des Sozialleistungsträgers die Rede. Nach Sinn und Zweck muss dies aber auch für Personen gelten, die sich um eine Beschäftigung erst bewerben. Dies sah die Krankenkasse ebenso.

Wie es letztlich dazu kommen konnte, dass der für die Personalangelegenheit zuständige Sachbearbeiter an die Ausdrucke kam, ließ sich nachträglich (angeblich) nicht mehr aufklären. Jedenfalls reagierte man schnell und ergriff Maßnahmen, um solche Vorkommnisse zukünftig auszuschließen. So wurden die Mitarbeiter auf die Rechtslage aufmerksam gemacht und auf arbeitsrechtliche Konsequenzen bei Missachtung hingewiesen. Zum anderen wurde angeordnet, dass unmittelbar nach Eingang einer Bewerbung zunächst festzustellen ist, ob eine Mitgliedschaft besteht. Ist dies der Fall, muss ein so genanntes „Mitarbeiterkennzeichen“ gesetzt werden. Das bedeutet, dass die im System gespeicherten Daten mit einem Merkmal versehen werden, welches es nur noch einzelnen ausgewählten Mitarbeitern erlaubt, auf die Daten zuzugreifen. Es sind dies Mitarbeiter, die ansonsten die Leistungsangelegenheiten der bei der Krankenkasse versicherten eigenen Mitarbeiter bearbeiten. Diese Sperre wird erst dann wieder aufgehoben, wenn das Bewerbungsverfahren abgeschlossen ist.

Wir halten dies für ein akzeptables Verfahren. Erfreulich war, wie schnell und wie konsequent die Krankenkasse in diesem Fall reagiert

und die erforderlichen Maßnahmen getroffen hat. Der Betroffenen, die die Absage auf ihre Bewerbung diesem Fehlverhalten möglicherweise zu verdanken hatte, half dies allerdings nicht mehr. Gleichwohl hatte sie erklärt, mit der Krankenkasse insgesamt zufrieden zu sein und ihr die Treue zu halten.

1.4 Die Information des zukünftigen Arbeitgebers

Welche Auswirkungen es haben kann, wenn aus Unachtsamkeit Daten „in die falsche Schublade“ gelangen, zeigte sich in folgendem Fall:

Eine junge Frau wollte zum 1. August eine Lehre beginnen. Sie war bisher über ihre Mutter bei einer Krankenkasse familienversichert und wollte mit Beginn ihrer Ausbildung bei derselben Kasse ein eigenständiges Versicherungsverhältnis begründen. Dies hatte sie bereits vor Beginn der Ausbildung der Krankenkasse gegenüber erklärt.

Im Juli wandte sie sich an uns und schilderte, sie sei kurz zuvor in einem Krankenhaus stationär behandelt worden. Unmittelbar nach ihrer Entlassung habe sie einen Telefonanruf ihres späteren Arbeitgebers erhalten. Dieser sei von der Krankenkasse über den Krankenhausaufenthalt informiert worden und habe nun wissen wollen, woran sie erkrankt gewesen sei.

Nachdem wir die Krankenkasse gefragt hatten, wie sie dazu komme, künftigen Arbeitgebern ihrer Versicherten Sozialdaten zu übermitteln, klärte sie uns über die Hintergründe auf. Danach sei es üblich, künftige Mitglieder mit einer sog. Interimsanmeldung in das EDV-System aufzunehmen. Dies ermögliche beispielsweise eine frühzeitige Ausstellung der Krankenversichertenkarte. Im konkreten Fall sei es nun so gewesen, dass sowohl die für die Krankenhausaufnahmeanzeige als auch die im Kundencenter zuständigen Mitarbeiter die Vorläufigkeit der Anmeldung übersehen und die Angelegenheit so behandelt hätten, als ob ein versicherungspflichtiges Beschäftigungsverhältnis bereits bestehe. Deshalb sei die Krankenhausaufnahme in eine falsche Datei eingegeben worden, was wiederum dazu geführt habe, dass dem vermeintlichen Arbeitgeber die Aufnahme ins Krankenhaus mitgeteilt worden sei.

Es ist schon mehr als ärgerlich, dass der Umstand des Krankenhausaufenthalts hier in die falsche Datei „gerutscht“ war und dies niemand bemerkt hatte. Inakzeptabel ist aber, dass die Krankenkasse offensichtlich Krankenhausaufenthalte generell an den Arbeitgeber meldet. Hierfür bedürfte es einer eindeutigen Rechtsgrundlage. Eine solche gibt es indes nicht. Der Hinweis seitens der Krankenkasse auf § 69 Abs. 4 SGB V geht fehl. Die dort geregelte Übermittlungsbefugnis gilt angesichts des Gesetzeswortlauts jedenfalls nicht für erstmalige Erkrankungen. Sinn der Vorschrift ist es vielmehr, dem Arbeitgeber die Möglichkeit zu geben festzustellen, ob ein Anspruch des Arbeitnehmers auf Entgeltfortzahlung im Krankheitsfall ausnahmsweise entfällt. Dabei kommt es vor allem auf die Arbeitsunfähigkeitszeiten im Verhältnis zu früheren, für die Entgeltfortzahlung noch relevanten Arbeitsunfähigkeitszeiten an, die auf einer Fortsetzungserkrankung beruhen. Diese Informationen besitzen auf Grund der Diagnoseangaben in den Arbeitsunfähigkeitsbescheinigungen nur die Krankenkassen. Geht es dagegen nicht um eine Fortsetzungs-, sondern um eine Ersterkrankung, scheidet § 69 Abs. 4 SGB V als Übermittlungstatbestand aus. Vielmehr ist nach dem Entgeltfortzahlungsgesetz allein der Arbeitnehmer verpflichtet, dem Arbeitgeber die Arbeitsunfähigkeit und deren voraussichtliche Dauer unverzüglich mitzuteilen. Die Krankenkassen müssen deshalb solche Meldungen künftig unterlassen.

1.5 Auskunftsersuchen über Familienangehörige

Verschiedentlich hatten Krankenkassen bei uns nachgefragt, wie sie damit umgehen sollen, wenn Väter Auskünfte über familienversicherte Angehörige fordern. Meist geht es bei solchen Ersuchen darum, dass die Eltern getrennt leben und der Vater die Adresse der Kinder nicht kennt. Wir vertreten dazu folgende Auffassung:

Bei der Familienversicherung wird davon ausgegangen, dass Ehegatten und Kinder, deren Lebensunterhalt vom Erwerbseinkommen eines in der gesetzlichen Krankenversicherung Versicherten bestritten wird und für die der Versicherte im Krankheitsfall einstehen müsste, ebenfalls den Schutz der gesetzlichen Krankenversicherung erhalten sollen. Die Familienversicherung begründet dabei für die Angehörigen ein jeweils eigenständiges Versicherungsverhältnis.

Für die Behandlung von Fällen, in denen eine Person um Auskunft über Daten anderer ersucht, ist es wichtig zu wissen, dass die Datenschutzgesetze dem Betroffenen einen Auskunftsanspruch nur über die „zu seiner Person“ gespeicherten Daten einräumen. Allerdings wird davon ausgegangen, dass zu den zur Person gespeicherten Daten nicht nur die ausschließlich die Person selbst betreffenden Angaben, sondern auch die Angaben darüber gehören, dass eine Beziehung einer bestimmten Art zu einer anderen Person besteht (z. B. familiäre Beziehung), sowie die Angaben, die zur Identifizierung der Beziehungsperson notwendig sind, wie Name und Anschrift. Deshalb hat der Betroffene grundsätzlich einen Anspruch auf Auskunft auch über diese Daten. Verweigert werden kann die Auskunft dann, wenn die Daten wegen überwiegender berechtigter Interessen der dritten Person(en) geheim gehalten werden müssen. Dies muss jeweils im Einzelfall auf der Grundlage einer umfassenden Interessenabwägung entschieden werden.

Bei der Familienversicherung ist es so, dass einerseits die Mitgliedschaft der Familienangehörigen in der Krankenversicherung des Stammversicherten unmittelbar mit dessen Mitgliedschaft zusammenhängt. Erlischt dessen Versicherungsverhältnis, scheiden auch die Familienmitglieder aus der Versicherung aus. Andererseits besteht, solange der Stammversicherte Mitglied einer Krankenkasse ist, für die familienversicherten Personen jeweils ein eigenständiges, von dem des Stammversicherten unabhängiges Versicherungsverhältnis. Deshalb werden die auf die jeweiligen (familien-)versicherten Personen bezogenen Daten von der Krankenkasse auch jeweils getrennt gespeichert und allenfalls für bestimmte Verwaltungszwecke wieder zusammengeführt. Im Ergebnis meinen wir deshalb, dass es vertretbar und im Interesse eines effektiven Sozialdatenschutzes der familienversicherten Personen auch geboten ist, die über die Angehörigen des Hauptversicherten gespeicherten Daten, auch die Adressdaten, nicht den (auch) zur Person des Hauptversicherten gespeicherten Sozialdaten zuzurechnen. Damit entfällt ein Anspruch des Stammversicherten auf Auskunft über diese Daten.

Den Krankenkassen haben wir unsere hier dargestellte Rechtsauffassung mitgeteilt.

2. Die Gesundheitsverwaltung

Im Bereich der Gesundheitsverwaltung gehört es zu unseren Aufgaben, die verschiedensten Einrichtungen zu beraten und zu kontrollieren. Das Spektrum reicht von den kommunalen Krankenhäusern über die Gesundheitsämter bis zu den Kassenärztlichen Vereinigungen und den Ärztekammern. Meist geht es in diesem Bereich um medizinische Daten, die der ärztlichen Schweigepflicht unterliegen. Entsprechend heikel sind die Fälle und entsprechend sensibel reagieren die Betroffenen auf die Verletzung ihrer Rechte.

2.1 Einschaltung eines Fachgutachters

Zu tun hatten wir mit der Beschwerde eines Beamten, der sich vom Amtsarzt auf seine Dienstfähigkeit untersuchen lassen sollte. Der Amtsarzt seinerseits hielt eine fachärztliche Begutachtung für erforderlich. Nachdem er sich für einen bestimmten Fachgutachter entschieden hatte, legte er ihm die Unterlagen über den Betroffenen vor, ohne diesen allerdings zuvor ausdrücklich um seine Zustimmung hierfür zu bitten. Obwohl der Betroffene der Verwendung des Fachgutachtens widersprach, legte es der Amtsarzt seinem ärztlichen Zeugnis zugrunde.

Indem der Amtsarzt Informationen über seinen Patienten an den Fachgutachter weitergegeben hat, hat er seine ärztliche Schweigepflicht

durchbrochen. Dies wäre nur zulässig gewesen, wenn ihn ein spezielles Gesetz oder eine Einwilligung des Patienten hierzu berechtigt hätte (§ 16 Abs. 1 des Gesundheitsdienstgesetzes [ÖGDG]). Da es ein solches spezielles Gesetz aber nicht gibt, hätte der Amtsarzt eine entsprechende Erklärung des Patienten über die Entbindung von der Schweigepflicht einholen müssen, und zwar schriftlich. In einer einschlägigen Verwaltungsvorschrift des Sozialministeriums ist ausdrücklich auf das Schriftformerfordernis der Schweigepflichtentbindung hingewiesen. Das Sozialministerium hat eigens hierfür einen Vordruck entwickelt und dessen Verwendung vorgeschrieben.

Im konkreten Fall hatte der Amtsarzt diese Vorgaben nicht beachtet. Nachträglich versuchte er anhand von Indizien darzulegen, dass der Patient trotzdem mit der Begutachtung einverstanden gewesen sei. Überzeugen konnte er nicht. Da das Schriftformerfordernis der datenschutzrechtlichen Einwilligung gerade auch den Sinn hat, von vornherein für klare Verhältnisse zu sorgen, hätte sich der Amtsarzt die nachträglichen Auseinandersetzungen um die Rechtmäßigkeit seines Handelns ersparen können. So musste festgestellt werden, dass das Fachgutachten unter Verstoß gegen die Geheimhaltungspflichten erhoben worden war. Dies hatte die Unzulässigkeit der Speicherung des Gutachtens und damit dessen Sperrung zur Folge (§ 24 Abs. 2 Satz 1 LDSG). Ohne Einwilligung des Betroffenen durfte es nicht weiter genutzt werden.

Dieser Fall war kein Einzelfall. Mehrfach hatten wir mit Beschwerden darüber zu tun, dass Amtsärzte Fachgutachter beauftragt hatten, ohne hierfür eine schriftliche Einwilligung einzuholen. Dies veranlasst uns, nochmals nachdrücklich auf die Verpflichtung der Amtsärzte hinzuweisen, Fachgutachten nur zu vergeben, wenn der Patient vorher sein schriftliches Einverständnis in die Weitergabe seiner Daten an den Facharzt erteilt hat.

2.2 Der Chefarzt als Gutachter

Die oben unter Nummer 2.1 dargestellte Problematik wies einen weiteren Aspekt auf, dem wir nachzugehen hatten. Wird nämlich ein Fachgutachter tätig, so verarbeitet auch dieser in Erledigung seines Auftrags personenbezogene Daten. Treten hier datenschutzrechtliche Fragen auf, muss klar sein, nach welchen Regeln diese zu beantworten sind und wer die Datenschutzkontrolle ausübt. Unklarheiten bestehen insoweit dann, wenn – wie geschehen – der begutachtende Arzt nicht deutlich macht, in welcher Funktion er tätig wird. Konkret ging es darum, dass ein Gesundheitsamt den Chefarzt eines städtischen Klinikums mit einer Begutachtung beauftragt hatte. Der Arzt erstattete sein Gutachten nun aber unter Verwendung des offiziellen Briefpapiers des Klinikums und mit dem Hinweis auf seine Stellung als Chefarzt. Damit konnte der Eindruck entstehen, hier werde er nicht persönlich, sondern als Bediensteter des Klinikums und damit für dieses tätig. Als wir uns mit einer Frage zur Sache an ihn wandten, meinte er, wir seien nicht zuständig, da er als Privatperson gehandelt habe. Im Übrigen sei ihm von seinem Arbeitgeber die Nutzung des offiziellen Briefpapiers des Klinikums gestattet worden.

Richtig ist, dass Krankenhausärzte, wenn sie ein fachärztliches Gutachten erstellen, insoweit einer Nebentätigkeit nachgehen. Sie werden also neben ihren ansonsten im Rahmen eines Beschäftigungsverhältnisses für den Arbeitgeber zu erbringenden Leistungen als Privatperson tätig. Dafür werden sie dann auch vom Auftraggeber unmittelbar bezahlt. Richtig ist auch, dass der Landesbeauftragte für den Datenschutz auf Grund der bestehenden Zuständigkeitsregelungen keinerlei Aufsichtsbefugnisse gegenüber Privatpersonen hat. Diese im Gesetz klar bestimmten Zuständigkeiten können allerdings nur dann beachtet werden, wenn im konkreten Fall deutlich wird, wer in welcher Eigenschaft handelt oder gehandelt hat. Genau dies war hier nicht der Fall und führte zu unnötigem Verwaltungsaufwand. Denn die Verwendung des offiziellen Briefpapiers des städtischen Klinikums ließ zunächst darauf schließen, es seien hier personenbezogene Daten durch eine öffentliche Stelle ver-

arbeitet worden, für die unsere Dienststelle zuständig war. Als sich herausgestellt hatte, dass diese Annahme falsch war, konnten wir nichts weiter unternehmen. Allerdings wandten wir uns an die Stadt mit der Bitte, dem Chefarzt die Verwendung des städtischen Briefpapiers zu untersagen. Die Stadt erklärte in ihrer Antwort, sie teile unsere Auffassung in vollem Umfang. Auch sie halte die Verwendung des Briefpapiers für eine ambulante Gutachtertätigkeit für unzulässig. Sie habe dafür gesorgt, dass die leitenden Ärztinnen und Ärzte hierauf nochmals ausdrücklich hingewiesen werden. Damit dürfte der Zuständigkeitswirrwarr insoweit hoffentlich der Vergangenheit angehören.

2.3 ... und keiner will's gewesen sein

Wer kennt dies nicht von seinen Kindern: Irgendetwas ist schief gelaufen, man weiß, einer muss es gewesen sein, aber keiner will's gewesen sein. An diese Situation fühlten wir uns erinnert, als sich ein Arzt an uns wandte und Folgendes schilderte:

Einem Kollegen habe er eine bestimmte Bescheinigung ausgestellt, die dieser der Bezirksärztekammer Südbaden vorgelegt habe. Kurze Zeit darauf habe sich die Kassenärztliche Vereinigung Südbaden an ihn gewandt und unter Bezugnahme auf diese Bescheinigung eine Stellungnahme erbeten. Da der Arzt vermutete, die Kassenärztliche Vereinigung habe die Bescheinigung von der Bezirksärztekammer erhalten, bat er um datenschutzrechtliche Prüfung der Angelegenheit.

Zunächst wandten wir uns an die Bezirksärztekammer mit der Bitte um eine Erklärung, weshalb sie die ausschließlich für ihre eigenen Aufgaben erhaltene Bescheinigung an die Kassenärztliche Vereinigung weitergegeben habe und wie sie dies datenschutzrechtlich begründe. Zu unserer Verblüffung erhielten wir zur Antwort, alle Mitarbeiter seien befragt worden und alle hätten versichert, die Kassenärztliche Vereinigung nicht informiert zu haben. Dies konnten wir kaum glauben. Wir wandten uns deshalb an die Kassenärztliche Vereinigung und baten um Auskunft, von wem sie die Bescheinigung erhalten habe. Dabei gingen wir davon aus, dass zumindest der Mitarbeiter oder die Mitarbeiterin, der oder die für die Bearbeitung der Angelegenheit zuständig sei, wissen müsse, woher die Information stammte. Weit gefehlt! Bei der Kassenärztlichen Vereinigung konnte sich niemand daran erinnern, wie man zu dem Schreiben gekommen sei. Es sei mehr oder weniger aus dem Nichts aufgetaucht und in den Geschäftsgang gelangt. Dabei muss man allerdings wissen, dass Bezirksärztekammer und Kassenärztliche Vereinigung im gleichen Gebäude untergebracht sind. Auch eine nochmalige Nachfrage bei der Bezirksärztekammer brachte keine neuen Erkenntnisse. Vehement wies man zurück, etwas mit der Sache zu tun zu haben.

Letztlich mussten wir dem Arzt mitteilen, irgendwer habe wohl seine Daten unbefugt übermittelt, es sei aber nicht festzustellen, wer dies konkret zu verantworten habe. Deshalb könnten wir auch nichts Weiteres unternehmen. Dass solche „Spielchen“ auf dem Rücken des Bürgers ausgetragen werden, halten wir für bedauerlich.

2. Abschnitt: Soziales

1. Der Antragsvordruck für die Sozialhilfe – ein Dauerthema

Ein Thema begleitet unsere Dienststelle nun nahezu von Beginn an: der Vordruck für Anträge auf soziale Leistungen, insbesondere der Antragsvordruck in der Sozialhilfe. Mittlerweile hat sich dieser Bereich zum Selbstläufer in unseren Tätigkeitsberichten gemausert. Offensichtlich führen wir hier einen Kampf gegen Windmühlenflügel, da die Sozialleistungsträger eben nicht bereit sind, ihre Verantwortung für eine rechtmäßige Datenerhebung zu erkennen und diese wahrzunehmen.

Genau genommen bedarf es für die Gewährung von Sozialhilfe keines Antrags. Der Gesetzgeber hat nämlich ausdrücklich auf ein solches Erfordernis verzichtet und das Einsetzen der Sozialhilfe vielmehr an den Zeitpunkt der

Kenntnis des Leistungsträgers von der Notlage geknüpft (§ 5 Bundessozialhilfegesetz [BSHG]); und diese Kenntnis kann er auch ohne einen formalen Antrag erlangen. Dem steht aber nicht entgegen, dass die Sozialämter vor der Gewährung insbesondere finanzieller Hilfeleistungen vom Hilfesuchenden das Ausfüllen auch umfangreicher Formulare verlangen. Eine solche Praxis muss möglich sein, um den Sozialämtern die Arbeit zu erleichtern und eine rasche Hilfeleistung sicherzustellen; schließlich gilt für diese Behörden der Grundsatz der Soforthilfe. Dies darf aber nicht dazu führen, dass die Sozialämter auf diesem Wege mehr persönliche Daten erheben, als sie für die Entscheidung über die Bewilligung einer Hilfeleistung in Art, Form und Umfang benötigen. Das Sozialgesetzbuch hat daher einer etwaigen Datensammelwut Grenzen gesetzt. Danach ist das Erheben von Sozialdaten nur insoweit zulässig, als die Sozialbehörde die Daten für ihre Aufgaben auch tatsächlich benötigt (§ 67 a des Sozialgesetzbuchs (SGB) Zehntes Buch (X) – Verwaltungsverfahren –). Dies versuchten wir zuletzt in unserem 21. Tätigkeitsbericht (LT-Drs. 12/5740) deutlich zu machen. Aber noch immer tauchen Vordrucke auf, mit denen die Behörden irrelevante Angaben erheben, mangelhafte Einwilligungserklärungen abverlangen sowie verwirrende und deplatzierte Hinweise geben.

Ein Beispiel aus unserer aktuellen Prüftätigkeit mag dies veranschaulichen:

Im Rahmen eines Kontrollbesuchs bei einem Landratsamt fiel uns das dortige Formular „Antrag auf Gewährung von Sozialhilfe“ in die Hände, das wir auszugsweise abgedruckt haben.

III. Unterhaltspflichtige Angehörige außerhalb des Haushalts:

	1	2	3	4	5
Familienname - ggf. Geburtsname -					
Vorname(n)					
Geburtsdatum					
Geburtsort					
Staatsangehörigkeit					
Familienstand					
Verwandtschaftsverhältnis z. Antragsteller					
Wohnanschrift PLZ, Ort, Straße, Nr.					
Beruf (ausgeübte Tätigkeit)					
Arbeitgeber Name, Anschrift					
(wenn Rentenempfänger) Art der Rente					

Danach sind zunächst „Unterhaltspflichtige Angehörige außerhalb des Haushalts“ aufzuführen und Angaben zu deren Beruf, Arbeitgeber und Art der Rente (wenn Rentenempfänger) zu machen.

Das ist so nicht richtig! Diese Rubrik dient zwar dem Zweck der Feststellung derjenigen Angehörigen, die dem Hilfesuchenden nach bürgerlichem Recht unterhaltspflichtig sind. Diese Personen sollen nämlich ihrer Pflicht nicht durch Leistungen der Sozialhilfe enthoben werden, so dass ein etwaiger Unterhaltsanspruch auf die Behörde übergeht. Das Sozialamt übersieht dabei aber, dass ein solcher Übergang gesetzlich ausgeschlossen ist, wenn es sich z. B. um Großeltern oder Enkel des Hilfeempfängers handelt. Anders ausgedrückt: Der Sozialhilfeträger kann nur Unterhaltsansprüche gegen Eltern und Kinder des Hilfeempfängers geltend machen (§ 91 BSHG). Von dieser Rechtslage hat der Hilfeempfänger aber regelmäßig keine Kenntnis. Er wird stattdessen alle Personen aufführen und diese zudem noch mit den genannten Angaben versehen. Wir schlugen daher vor, die Rubrik durch

eine Aufzählung der relevanten unterhaltspflichtigen Angehörigen zu ergänzen.

X. Vermögenswerte:

a) des Hilfesuchenden	b) des Ehegatten/Lebenspartner - falls minderjährig beider Eltern -
Spar-, Bank- und Postsparguthaben ☐ nein ☐ ja, bei: Kreditinstitut, BLZ, Konto-Nr. Betrag	Spar-, Bank- und Postsparguthaben ☐ nein ☐ ja, bei: Kreditinstitut, BLZ, Konto-Nr. Betrag
Kreditinstitut, BLZ, Konto-Nr. Betrag	Kreditinstitut, BLZ, Konto-Nr. Betrag
Die Bankinstitute ermächtige ich hiermit zur Auskunftserteilung.	Die Bankinstitute ermächtige ich hiermit zur Auskunftserteilung.

Mit dieser Rubrik „X. Vermögenswerte“ sollen verschiedene Kreditinstitute zur Auskunftserteilung an den Sozialhilfeträger ermächtigt werden. Dieses Einverständnis in die Einholung einer Bankauskunft genügt aber nicht den gesetzlichen Anforderungen an eine Einwilligungserklärung des Hilfesuchenden; die Erklärung ist deshalb schlichtweg unbeachtlich. Der Gesetzgeber verlangt nämlich für das Vorliegen einer wirksamen Einwilligungserklärung u. a., dass der Betroffene auf die Folgen der Verweigerung einer solchen Erklärung hingewiesen wird. Zudem muss dem Bürger auch klar sein, dass er mit seiner Unterschrift auf dem Formular eine solche weit reichende Einwilligungserklärung überhaupt abgibt. Zu diesem Zweck ist der Erklärungstext in seinem äußeren Erscheinungsbild hervorzuheben. Beides ist nicht beachtet.

Damit aber nicht genug. Nachforschungen des Sozialamts bei einem Kreditinstitut zur Ermittlung der Vermögensverhältnisse des Hilfesuchenden müssen zurückstehen, solange der Betroffene bereit und in der Lage ist, diese Verhältnisse selbst darzulegen. Dann darf aber auch eine dahin gehende Einwilligungserklärung erst eingeholt werden, wenn die Auskunft der Bank für die Entscheidung des Sozialamts unbedingt benötigt wird. Dass das Landratsamt nun verlautbarte, es verwende die im Vordruck enthaltene und damit „auf Vorrat“ besorgte Einwilligungserklärung nicht, macht die Vorgehensweise der Behörde deshalb nicht besser.

Nach dem leichten Aufgalopp greift das Sozialamt dann aber unter der Rubrik „Erklärung des Hilfesuchenden ...“ in die Vollen:

Erklärung des Hilfesuchenden und seines Ehegatten/Lebenspartners:

Ich versichere, dass die vorstehenden Angaben wahr sind und dass ich nichts verschwiegen habe.
Mir ist bekannt, dass ich wegen wissentlich falscher oder unvollständiger Angaben strafrechtlich verfolgt werden kann und zu Unrecht erhaltene Hilfe zurückzahlen muss.
Mir ist bekannt, dass meine Ansprüche gegen Drittverpflichtete (z. B. auf Unterhalt) auf den Träger der Hilfe übergeleitet und Erstattungsansprüche gegen andere Leistungsträger (z. B. auf Wohngeld, Arbeitslosengeld/-hilfe, Krankengeld, Rente) geltend gemacht werden können.
Ich bestätige ausdrücklich, davon unterrichtet worden zu sein, dass ich jede Änderung der Familien-, Einkommens- und Vermögensverhältnisse, vorübergehende Abwesenheit vom Wohnort, unverzüglich und unaufgefordert dem Träger der Hilfe mitzuteilen habe.
Die Aufnahme jeder Arbeit, auch Gelegenheitsarbeit usw. werde ich vor Aufnahme der Arbeit ebenfalls sofort anzeigen.
Den Träger der Hilfe ermächtige ich hiermit - soweit für die Hilfegewährung erforderlich - Akten anderer Sozialleistungsträger einzusehen, von denen ich Leistungen erhalten habe oder erhalte.
Jeder Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis - § 35 SGB I). Die Übermittlung von Sozialdaten ist nur unter den Voraussetzungen zulässig, unter denen diese Person selbst übermittlungsbefugt wäre (§ 76 Abs. 1 SGB X). Dies gilt nicht im Rahmen des § 69 Abs. 1 Nr. 1 SGB X für Sozialdaten, die im Zusammenhang mit einer Begutachtung wegen der Erbringung von Sozialleistungen oder wegen der Ausstellung einer Bescheinigung übermittelt worden sind, es sei denn, dass der/die Betroffene der Übermittlung widerspricht (§ 76 Abs. 2 SGB X). Von meinem Widerspruchsrecht habe ich Kenntnis genommen.
Diese Ermächtigung gilt zugleich als datenschutzrechtliche Einwilligung. Gemäß § 117 des Bundessozialhilfegesetzes ist es den Trägern der Sozialhilfe ermöglicht, einen automatisierten Datenabgleich durchzuführen. Der automatische Datenabgleich nach § 117 BSHG verstößt nicht gegen das Sozialgeheimnis.
Sind die Voraussetzungen für Kriegsopferfürsorge erfüllt, wird diese Hilfe hiermit beantragt und die Zustimmung nach § 54 Abs. 2 der Verordnung zur Kriegsopferfürsorge (zur Leistung von Amts wegen) erteilt.

Ort, Datum	Unterschrift des Hilfesuchenden oder seines gesetzl. Vertreters	Unterschrift des Ehegatten/Lebenspartners

Der Antrag wurde auf Wunsch im Amt aufgenommen, die Richtigkeit wird hiermit bestätigt.

Unterschrift des Antragstellers	Unterschrift des Aufnehmenden

Stellungnahme Wohnsitzgemeinde: (nur ausfüllen, wenn eine Prüfungszuständigkeit auf Grund von gesetzlichen oder anderen Regelungen besteht)

Vorstehende Angaben entsprechen ☐ der Wahrheit ☐ nicht der Wahrheit

Die Notlage wird ☐ anerkannt ☐ nicht anerkannt. (Bei Verneinung der Notlage, nähere Bemerkungen bitte auf Beiblatt)

Die Notlage ist hier seit Datum bekannt geworden.

Die Gemeinde hat im Jahre ☐ für folgende im Antrag aufgeführten Personen eine Lohnsteuerkarte ausgestellt.

Bei ledigen minderjährigen Hilfesuchenden

☐ Antragsteller(in) ☐ Ehegatte ☐ Vater ☐ Mutter

Nr.	Nr.	Nr.	Nr.	Nr.

Mit ☐ Anlagen an die Stadt / das Landratsamt / den Landkreis

Ort, Datum	
Unterschrift	

In fast stakkatomäßiger Abfolge hageln nun Hinweise und Erklärungen auf den oder die Antragsteller nieder. Aus datenschutzrechtlicher Sicht herausragend ist dabei zunächst die Bestätigung des Hilfesuchenden, darüber unterrichtet worden zu sein, dass jede vorübergehende Abwesenheit vom Wohnort unverzüglich und unaufgefordert dem Träger der Sozialhilfe mitzuteilen ist, sowie die Befugnis der Behörde, die Akten anderer Sozialleistungsträger einzusehen.

Es besteht für den Leistungsempfänger zwar die gesetzliche Pflicht, Änderungen in seinen Verhältnissen mitzuteilen, soweit sie für die Leistung erheblich sind. Es ist aber nicht nachvollziehbar, wie jede auch nur vorübergehende Abwesenheit derartige Folgen für das Leistungsverhältnis zeitigen kann. Das Landratsamt trug nun vor, dass es hierbei „vor allem“ um Aufenthalte in Krankenhäusern oder sonstigen Einrichtungen gehe. Dies werde im anschließenden Leistungsbescheid durch einen entsprechenden Hinweis auch klargestellt.

Wir empfehlen deshalb nach wie vor, die genannte Passage in dem Vordruck entweder zu präzisieren oder zu streichen und es so bei einem klaren Hinweis im Bescheid zu belassen.

Für die Erklärung des Hilfesuchenden, er gestatte dem Sozialleistungsträger Einsicht in Akten anderer Leistungsträger, besteht neben formalen Mängeln bereits kein Bedürfnis. Die „anderen Leistungsträger“ können die benötigten Sozialdaten nämlich auch ohne Einwilligung übermitteln, soweit diese nicht vom Hilfesuchenden zu erlangen sind.

Anschließend klärt das Landratsamt den Antragsteller dann mit großer Hingabe über die weiteren behördlichen Möglichkeiten auf. Da ist einmal der Hinweis auf die Vorschrift des § 76 SGB X mit der Erläuterung, dass die Übermittlung von Sozialdaten nur unter den Voraussetzungen zulässig ist, unter denen diese Person selbst übermittlungsbefugt wäre. Die gesetzlichen Einschränkungen dieser Übermittlungssperre folgen auf dem Fuße, einschließlich der Erklärung, dass der Hilfesuchende von seinem Widerspruchsrecht Kenntnis genommen habe.

Des Weiteren ergeht der Hinweis, dass „diese Ermächtigung“ zugleich als „datenschutzrechtliche Einwilligung“ gilt. Das Bild rundet die Information ab, dass der Träger der Sozialhilfe automatisierte Datenabgleiche durchführen kann.

Hierbei handelt es sich um das Paradebeispiel einer Überinformation. Die Vorschrift des § 76 SGB X will die Übermittlungen besonders schutzwür-

diger Sozialdaten, wie z. B. Gesundheitsdaten, einschränken. Sie ist aber nur unvollständig wiedergegeben und an dieser Stelle nicht angebracht. Das in dieser Norm verankerte Widerspruchsrecht des Betroffenen wird daher auch nicht deutlich. Von einer Kenntnisnahme dieses Rechts kann somit in keinem Fall ausgegangen werden. Gleiches gilt für die äußerst nebulöse „datenschutzrechtliche Einwilligung". Es bleibt nämlich auch bei wiederholter Lektüre völlig unklar, in welchen Datenverarbeitungsvorgang eingewilligt wird.

Wir teilten dem Landratsamt daher mit, dass eine spätere Datenverarbeitung jedenfalls auf solche für den normalen Bürger völlig unverständliche Hinweise nicht gestützt werden kann.

Auch die Zusammenfassung der gesetzlichen Befugnis zum automatisierten Datenabgleich ist insgesamt kein großer Wurf. Dieser Hinweis ist, wenn er schon gegeben wird, unbedingt um die Bezeichnung der Stellen zu ergänzen, mit denen ein solcher Datenabgleich vorgenommen wird.

Den Abschluss bildet die „Stellungnahme der Wohnsitzgemeinde". Diese erhält damit die Möglichkeit, die Notlage anzuerkennen oder nicht anzuerkennen. Dass dies keineswegs zu den Aufgaben der Wohnortgemeinde gehört, bedarf keiner weiteren Erwähnung. Hierauf haben wir bereits ausführlich in unserem 19. Tätigkeitsbericht (LT-Drs. 12/3480, S. 14 f.) hingewiesen.

Das Landratsamt hat den Verlag inzwischen gebeten, den Vordruck zu überarbeiten und ihn den gesetzlichen Bestimmungen anzupassen.

2. Zu viel verlangt

Die Sozialämter sind, wie die anderen Sozialleistungsträger auch, verpflichtet, Sozialdaten in erster Linie bei den Betroffenen selbst zu erheben. Hintergrund dieses gesetzlichen Grundsatzes des Vorrangs der Datenerhebung beim Betroffenen (§ 67 a Abs. 2 Satz 1 SGB X) ist, dass der Hilfesuchende als Träger des Grundrechts auf informationelle Selbstbestimmung auch dementsprechend Herr über seine Daten bleiben soll. Ihm selbst kommt vorrangig die Entscheidung zu, welche persönlichen Daten an den Sozialleistungsträger gelangen; unter Umständen muss der Antragsteller aber für eine solche Entscheidung auch Rechtsverluste in Kauf nehmen. Andererseits ist aber nicht zu verkennen, dass der Leistungsträger aus verschiedenen Gründen ein Interesse daran haben kann, Auskünfte zu den Verhältnissen des Antragstellers auch bei dritten Personen oder Stellen einzuholen. Dies kann z. B. aus dem Interesse entstehen, die Angaben bei Dritten auf ihre Schlüssigkeit nachzuprüfen oder einfach daraus, dass manche Informationen ihrer Art nach sinnvollerweise eben nur von verständigen dritten Personen gegeben werden können. Um dem Sozialleistungsträger hier die entsprechenden Instrumente an die Hand zu geben, sieht der Gesetzgeber eine Mitwirkungspflicht des Hilfesuchenden im Verwaltungsverfahren vor. Deshalb besteht für einen Antragsteller die Obliegenheit, der Auskunftserteilung durch Dritte an die Behörde zuzustimmen (§ 60 Abs. 1 Nr. 1 SGB I).

Bei einer solchen Vorgehensweise ist aber vor allem eines zu beachten: Gradmesser jedweder Datenerhebung ist das Prinzip der Verhältnismäßigkeit. Von besonderer Bedeutung ist dieser Grundsatz im Rahmen einer Datenerhebung bei anderen Personen oder Stellen. Das gilt in gleichem Maße, wenn die Behörde von dem Antragsteller eine Zustimmung zur Auskunftserteilung durch Dritte verlangt. In jedem Fall geht nämlich eine solche Art der Datenerhebung mit der Bekanntgabe von Sozialdaten an diesen Dritten einher.

– Ein selbstständig Tätiger, der Sozialhilfe in Anspruch nehmen musste, konnte als Nachweis über seine Einkünfte lediglich einen Steuerbescheid für das Jahr 1998 beim Sozialamt vorlegen. Die Sozialbehörde verlangte daraufhin von dem Antragsteller die Erteilung einer Auskunftsermächtigung für eine Steuerberatungsgesellschaft, die der Hilfesuchende beauftragt hatte. Dieser erteilte seine Einwilligung, die Bitte um Auskunft zur aktuellen Situation brachte das Sozialamt im Ergebnis aber nicht weiter.

Des Weiteren verlangte das Sozialamt die Ermächtigung zur Einholung von Auskünften bei einem bestimmten Kreditinstitut. Diese erteilte der Hilfesuchende nicht; ein Herantreten an die Bank erwies sich später auch gar nicht mehr als notwendig.

In dem geschilderten Fall hat die zuständige Sozialbehörde den Grundsatz der Verhältnismäßigkeit gleich zweimal außer Acht gelassen. Warum? Die Erklärung ist einfach: Wie bereits gesagt, hat derjenige, der Sozialleistungen begehrt, u. a. auch der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen. Ob diese Einwilligung dann tatsächlich verlangt wird, steht aber nicht im freien Belieben des Sozialamts. Es hat nämlich hierüber nach seinem pflichtgemäßen Ermessen zu befinden; dabei hat die Behörde vor allem den Grundsatz der Verhältnismäßigkeit zu beachten. Falls es somit für den Hilfesuchenden mehrere Möglichkeiten gibt, die notwendigen Angaben nachzuweisen, bedeutet dies, dass das Sozialamt nur den Nachweis verlangen kann, dessen Beschaffung für den Antragsteller mit den geringsten Belastungen verbunden ist.

Im geschilderten Fall heißt das: Vor der Einholung von Auskünften beim Steuerberater und auch schon vor dem Verlangen einer dahin gehenden Zustimmungserklärung des Hilfesuchenden hätte das Sozialamt diesem die Möglichkeit geben müssen, Auskünfte des Steuerberaters selbst zu beschaffen. Gerade dies wäre nämlich die schonendere Vorgehensweise gewesen und hätte verhindert, dass der Steuerberater ohne Not Kenntnis von dem Kontakt seines Auftraggebers mit dem Sozialamt erlangt. Überflüssig, weil verfrüht, war auch das Verlangen der Ermächtigung zur Einholung einer Bankauskunft, wie sich im späteren Verlauf der Angelegenheit zeigte.

Wir riefen die Behörde zur künftigen Beachtung auf.

– Ähnlich ist die Problematik bei einer Klientenvollmacht gelagert, auf die wir anlässlich eines Besuchs bei der Schuldnerberatungsstelle eines Sozialamts stießen.

  Mit einer vorgedruckten Erklärung erteilt der Klient bis auf Widerruf Vollmacht zur Wahrnehmung seiner Sozial- und Vermögensangelegenheiten im Rahmen der persönlichen Hilfe nach dem Bundessozialhilfegesetz. Hierzu muss man wissen, dass diese persönliche Hilfe außer der Beratung in Fragen der Sozialhilfe auch eine Beratung in sonstigen sozialen Angelegenheiten umfasst, wie es viel sagend im Bundessozialhilfegesetz lautet. Besagte Vollmacht erstreckt sich deshalb auch darauf, für den Klienten „im Rahmen sozialer und finanzieller Rehabilitierungsbemühungen Verhandlungen zu führen oder Erklärungen abzugeben oder wegen bestehender Forderungen Vereinbarungen zu treffen im Hinblick auf Anerkennung oder Ablehnung, auf Stundung, Erlass, Ratenzahlung oder Vergleiche“. Zu diesem Zweck entbindet der Klient mit seiner Unterschrift zudem Banken, Sparkassen und andere Kreditinstitute vom Bankgeheimnis bzw. von der Einschränkung durch das Datenschutzgesetz. Entsprechendes gilt auch für den oder die Arbeitgeber, öffentliche Stellen (Finanzamt, Kindergeldstelle) und für Auskunftsbüros, einschließlich der Schufa.

  Klar ist, dass bei dieser umfassenden und pauschalen vorgedruckten Einwilligungserklärung vom Grundsatz des Vorrangs der Datenerhebung beim Betroffenen kaum noch etwas übrig bleibt. Schon aus diesem Grund sahen wir Anlass, diese „Generalvollmacht“ zur Einholung von Auskünften bei Dritten zu bemängeln.

  Gerade an diesem Beispiel wird außerdem deutlich, warum der Gesetzgeber ausdrücklich festgeschrieben hat, dass eine Einwilligung nur wirksam ist, wenn sie auf der freien Entscheidung des Betroffenen beruht (§ 67 b Abs. 2 SGB X). Es kann hier nicht davon ausgegangen werden, dass der Einwilligende die Tragweite seiner Erklärung erfassen kann. Teilweise wird in dem Vordruck der Text von § 8 Abs. 2 BSHG aufgegriffen, der von „sonstigen sozialen Angelegenheiten“ spricht. Was damit gemeint ist, wird jedoch nicht deutlich. Der Rat Suchende wird aber vernünftigerweise nicht darin einwilligen wollen, dass die

Schuldnerberatungsstelle des Landratsamts in allen Angelegenheiten für ihn handelt. Konturenlos ist die Vollmacht auch, wenn sie dem Behördenmitarbeiter erlaubt, im Rahmen sozialer und finanzieller Rehabilitierungsbemühungen des Klienten tätig zu werden. Für den Hilfebedürftigen ist dabei nicht zu erkennen, auf was er sich einlässt, zumal auch der Zusammenhang mit den Aufgaben der Schuldnerberatungsstelle hier nicht mehr ohne weiteres deutlich wird.

Insgesamt ist diese Vollmacht keine wirksame Grundlage einer Datenverarbeitung durch die Schuldnerberatungsstelle. Die Behörde teilte unsere Kritik jedoch nicht in vollem Umfang.

3. Die Mietkaution

Bei Notlagen, in denen der Mieter außer Stande ist, eine etwaige Mietkaution aus eigenen Mitteln aufzubringen, aber der Vermieter den Abschluss des Mietverhältnisses von der Zahlung einer Kautionssumme abhängig macht, sieht das Bundessozialhilfegesetz (BSHG) die Hilfe des zuständigen Sozialamts vor (§ 15 a BSHG). Es steht dann im pflichtgemäßen Ermessen des Sozialleistungsträgers, ob er die beantragte Übernahme der Kaution z. B. als Darlehen erbringt. Die Hilfeleistung soll erbracht werden, wenn der Antragsteller ansonsten ohne Wohnung dasteht. Die Geldleistung darf aber nur dann direkt an den Vermieter ausgezahlt werden, wenn die Gefahr besteht, dass der Hilfesuchende die Leistung anderweitig verwenden würde. In gleicher Weise ist bei der Zahlung der Miete durch das Sozialamt zu verfahren. Aber gerade hier kann ein Problem liegen, wie folgender Fall zeigt:

Darin war ein Sozialamt zwar nicht abgeneigt, eine Kautionssumme zu übernehmen, die Zahlung sollte aber grundsätzlich nur an den Vermieter erfolgen. Zur Untermauerung seiner Haltung verwies das Sozialamt auf eine angebliche „einheitliche Praxis, mindestens im süddeutschen Raum“. Nun, diesem Hinweis vermochten wir nicht nachzugehen, jedoch ist offensichtlich, dass eine derartige Verwaltungsübung nicht dem Sinn des Gesetzes entspricht. Spröde wies die Behörde zudem darauf hin, dass es sich hierbei nicht um eine Frage des Datenschutzes handele. Sie ignorierte dabei aber die Tatsache, dass die Auszahlung des Darlehens an den Vermieter diesem den Kontakt seines Mieters zum Sozialamt offenbart.

Auch im weiteren Verlauf der Angelegenheit blieb die Sozialbehörde widerborstig; trotz eindeutiger Rechtslage erfolgte nämlich bislang noch kein Signal, die dortige Praxis zu ändern. Den Antragstellern wurde stattdessen vorab mitgeteilt, dass das Landratsamt bei der Durchführung der Sozialhilfe nicht an Weisungen anderer Behörden gebunden sei; im Übrigen werde der Ausgang eines anhängigen Gerichtsverfahrens abgewartet.

Wir aber fragen uns: Was macht es aus der Sicht des Sozialdatenschutzes für einen Sinn, den Mietzins in Einzelfällen an den Hilfeempfänger zu leisten, die Mietkaution grundsätzlich aber nur an den Vermieter?

4. Sozialpädagogen im Mehrpersonenzimmer?

Platz ist in der kleinsten Hütte, scheint sich ein Landratsamt gesagt zu haben. Wegen „bestehender Raumknappheit“ in der Verwaltungsbehörde, so die Begründung, war bei einem Jugendamt die „Zusammenlegung von jeweils zwei Sozialpädagogen/innen in einen Büroraum“ vorgesehen. Betroffen von dieser Maßnahme waren rund 20 Fachkräfte des Jugendhilfeträgers, die im Gegenzug drei zusätzliche Besprechungszimmer erhalten sollten.

Nun unterliegen Angehörige bestimmter Berufsgruppen, wozu auch staatlich anerkannte Sozialarbeiter und Sozialpädagogen gehören, einer besonderen gesetzlichen Verpflichtung zur Geheimhaltung. Diese verbietet ihnen bei Strafandrohung, all das, was ihnen bei der Ausübung ihrer Tätigkeit anvertraut oder sonst bekannt wird (fremde Geheimnisse), unbefugt zu offenbaren (§ 203 Strafgesetzbuch [StGB]). Diese Geheimhaltungspflicht gilt sowohl behördenintern als auch im Verhältnis der schweigepflichtigen Personen zueinander.

Untersagt diese Rechtslage vertrauliche Gespräche oder sogar telefonische Unterredungen in Anwesenheit des Zimmergenossen? Diese Frage trug das betroffene Amt an uns heran.

Zu Recht war es sensibel für diese Problematik, wie nicht zuletzt ein Urteil des Bundesarbeitsgerichts aus dem Jahr 1987 zeigt. In der sog. Telefondatenerfassungsentscheidung hatte das Bundesarbeitsgericht damals im Falle eines für einen Landkreis tätigen Psychologen geurteilt: „Eine fachgerechte psychologische Beratung und Behandlung, die Aussicht auf Erfolg haben soll, setzt ein Vertrauensverhältnis zwischen der zu betreuenden Person und dem Psychologen voraus, dessen Entstehen wesentlich dadurch bedingt ist, dass die Beratung und Behandlung vertraulich bleibt, d. h. anderen Personen nicht bekannt wird. Davon, dass die psychologische Beratung und Behandlung von Personen eine solche Vertraulichkeit erfordert und dass die behandelte Person gegen den Psychologen einen Anspruch auf Wahrung dieser Vertraulichkeit hat, geht § 203 Abs. 1 Nr. 2 und 4 StGB aus. ... Schon die Tatsache, dass jemand die Beratung oder Behandlung des Klägers in seiner Eigenschaft als Berufspsychologe in Anspruch nimmt, ist ein solches Geheimnis im Sinne des § 203 StGB und nicht erst das Problem oder die Krankheit, die Anlass für die Inanspruchnahme des Berufspsychologen ist.“

Diese Ausführungen des Bundesarbeitsgerichts beanspruchen in gleichem Maße Geltung für die hier betroffenen Sozialpädagogen und Sozialarbeiter; das ist einleuchtend, hält man sich einmal vor Augen, dass gerade diesen Fachkräften in der Regel die sog. Kernaufgaben des Trägers der öffentlichen Jugendhilfe obliegen. Diese reichen von der Mitwirkung bei den Hilfen zur Erziehung und den „anderen Aufgaben der Jugendhilfe“, wie der Inobhutnahme von Kindern, bis hin zu Beratungstätigkeiten z. B. in Fragen der Partnerschaft, Trennung und Scheidung.

Die Beispiele zeigen, dass die Vertraulichkeit des gesprochenen Wortes eine wesentliche Voraussetzung für die Akzeptanz der Arbeit der Jugendämter ist. Zudem macht die genannte Entscheidung deutlich, dass auch telefonische Kontakte der Mitarbeiter mit (möglichen) Klienten dem gesetzlichen Geheimnisschutz unterfallen. Schließlich forderte das Bundesarbeitsgericht noch, dass der Arbeitgeber kraft seiner Fürsorgepflicht gegenüber seinem schweigeverpflichteten Mitarbeiter gehalten ist, „alles zu unterlassen, was diesen in einen Konflikt mit seiner Geheimhaltungspflicht bringen kann“.

Eingedenk dieser Ausführungen meinten wir, dass sich die Pläne des Landratsamts, jedenfalls im Bereich des Jugendamts, grundsätzlich nicht mit den dargelegten Positionen vertragen. Sollte allerdings die organisatorische Maßnahme unumgänglich sein, gaben wir der Behörde u. a. folgende Hinweise:

– es sollten sich ausschließlich die Mitarbeiter ein Büro teilen, die wechselseitig vertretungsberechtigt sind;

– die Mitarbeiter müssen stets die Möglichkeit zu einem vertraulichen Gespräch in einem Besprechungszimmer oder einer anderen Räumlichkeit unter Ausschluss nicht an der Beratung beteiligter Mitarbeiter haben. Da als Befugnis für eine Offenbarung im Sinne des § 203 StGB regelmäßig nur eine Einwilligung des Betroffenen in Betracht kommt, ist ansonsten eine solche Erklärung einzuholen. Keinesfalls sollten zwei Klienten gleichzeitig in ein und demselben Büro beraten werden, selbst wenn sie in diesen Vorgang ausdrücklich eingewilligt haben.

4. Teil: Kommunales und anderes

1. Abschnitt: Kommunales

Wie in jedem Jahr war im kommunalen Bereich auch dieses Mal manches zu kritisieren. Nun wäre es unfair, den Kommunen generell vorzuwerfen, der Datenschutz habe dort einen geringeren Stellenwert als anderswo. Gerade die Aufgabenvielfalt und die Vielzahl der Verwaltungsvorgänge können dazu führen, dass hier Fehler unterlaufen. Dies ändert aber nichts daran, dass auch im kommunalen Bereich weiter daran gearbeitet werden muss, dem Datenschutz die notwendige Beachtung zu verschaffen. Erfolg oder Misserfolg hängen dabei entscheidend davon ab, welche Bedeutung die Führungsebene diesem Thema beimisst. Wenn dort das Interesse an einem wirkungsvollen Datenschutz vorhanden ist, wird sich dies auch auf den einzelnen Arbeitsplatz positiv auswirken – umgekehrt gilt natürlich das Gegenteil.

1. Der behördliche Datenschutzbeauftragte

Im 22. Tätigkeitsbericht (LT-Drs. 13/520) hatten wir noch einmal Sinn und Zweck eines örtlichen Datenschutzbeauftragten erläutert und gehofft, vor allem die größeren Städte im Lande, allen voran die Landeshauptstadt, davon überzeugen zu können, hier mit gutem Beispiel voranzugehen. Diese Hoffnung wurde leider bisher enttäuscht. So hatte die Landeshauptstadt Stuttgart, nicht zuletzt veranlasst durch einzelne Missstände, deren Aufdeckung breiten Widerhall in der Öffentlichkeit fanden, nach außen zwar ihre ablehnende Haltung aufgegeben und die Bestellung eines eigenen Datenschutzbeauftragten angekündigt. Mehr ist bisher aber auch nicht geschehen. Offenbar tut man sich äußerst schwer damit, das „ungeliebte Kind“ aus der Taufe zu heben. Wenn man aber tatsächlich nicht will, dann sollte man das auch klipp und klar sagen, anstatt die Bestellung einfach im bürokratischen Alltag versickern zu lassen. Offenbar spielen auch andere Städte in dieser Frage auf Zeit. In Mannheim und in Baden-Baden ist man nunmehr schon seit Jahren am Prüfen und am Verhandeln – Ausgang ungewiss. Fast schon sympathisch ist da die Offenheit der Oberbürgermeister von Ulm und Karlsruhe, die unmissverständlich klar gemacht haben, dass man einen eigenen Datenschutzbeauftragten für überflüssig halte. Erstaunlich dabei allerdings die Begründung aus Karlsruhe, wonach man die Bestellung eines solchen sogar für „kontraproduktiv“ halte, auch weil die Gefahr bestehe, ein solcher Datenschutzbeauftragter könne „der Kontrolle durch die Verwaltung entgleiten“ (!). Bei einem solchen Verständnis der Rolle eines Datenschutzbeauftragten wäre in der Tat nicht viel gewonnen. Bedauerlich nur für die Bürger, um deren Datenschutzrechte es geht. Denn dass es eminent wichtig ist, vor Ort einen Verantwortlichen zu haben, der die Mitarbeiter der städtischen Ämter berät und rechtzeitig einschreitet, bevor Schlimmeres passiert, zeigen die nachfolgenden Sachverhalte.

2. Der ganz alltägliche Schlendrian

Bisweilen läuft man als Datenschützer Gefahr, sich zu sehr in die abstrakte Diskussion anspruchsvoller datenschutzrechtlicher Themen zu versteigen und dabei das kleine Einmaleins des Datenschutzes aus den Augen zu verlieren. Dabei ist es doch gerade der alltägliche Umgang der Behörden mit den persönlichen Daten, der die Bürger besonders betrifft und anhand dessen man am ehesten deutlich machen kann, dass Datenschutz tatsächlich jeden angeht. Wir haben es uns deshalb zur Aufgabe gemacht, gemäß dem Wahlspruch „Zurück zu den Wurzeln“ verstärkt darauf zu schauen, ob die Grundregeln des Datenschutzes in der behördlichen Praxis eingehalten werden. Begonnen haben wir mit dem Ende der Datenverarbeitungskette, nämlich der Entsorgung nicht mehr benötigter Daten. Dazu muss man wissen, dass die Datenschutzgesetze dazu verpflichten, personenbezogene Daten zu löschen, wenn sie für die Erfüllung der Aufgaben, für die sie erhoben wurden, nicht mehr erforderlich sind. Wie die Behörden dieser Pflicht nachkommen, ist im Einzelnen nicht vorgeschrieben. Vorgeschrieben ist allerdings, dass die Löschung oder Vernichtung in einer Weise erfolgt, die dem Bedürfnis der Betroffenen an der Wahrung der Vertraulichkeit ihrer Daten

gerecht wird. Hierzu muss die verpflichtete Stelle technische und organisatorische Maßnahmen treffen, die sie zu dokumentieren hat. Und sie muss, um die Einhaltung der getroffenen Maßnahmen zu gewährleisten, für geeignete Kontrollmechanismen sorgen. Hier liegt, wie leider festzustellen war, offensichtlich manches im Argen.

Die Idee war, dass sich Mitarbeiter des Amtes auf den Weg machen und einmal die öffentlich zugänglichen Altpapiertonnen bei den Gebäuden unter die Lupe nehmen, in denen Ämter der Landeshauptstadt Stuttgart untergebracht sind, die Sozialdaten verarbeiten. Dabei war es Vorgabe, dass es um Mülltonnen gehen sollte, die jedermann öffentlich zugänglich sind, und dass nur untersucht werden sollte, was dort obenauf liegt. Das Ergebnis war verblüffend: Schon die erste Tonne war ein Volltreffer! Gleich mit Aktendeckel konnten stapelweise Anschreiben an Sozialhilfeempfänger mit deren Name und Adresse herausgefischt werden. Und so ging es weiter. Ob ein notdürftig zerrissenes Schreiben einer Schwangerschaftskonfliktberatungsstelle – mit allen Angaben über die persönlichen Verhältnisse der betroffenen Frau und deren Familie – oder ob seitenweise Ausdrucke über Sozialdatenabgleiche, in nahezu jedem Altpapiercontainer wurden Unterlagen mit sensiblen Inhalten gefunden. Nebenbei wurde noch festgestellt, dass viele Briefkästen der Ämter so beschaffen sind, dass man eingelegte Post ohne Mühe wieder herausnehmen kann. In einem Fall beobachteten unsere Mitarbeiter, wie der Kunde eines Sozialamts zunächst den Briefkasten leerte, um dann seinen Brief als ersten wieder einzuwerfen. Hier kann nur jedem geraten werden, Briefe mit sensiblen Inhalten persönlich abzugeben, wenn solche Zustände festgestellt werden!

Angesichts dieser Erfahrungen wollten wir wissen, ob Stuttgart hier ein unrühmlicher Ausnahmefall sei. Die Aktion wurde deshalb auf Karlsruhe und Mannheim ausgedehnt. Auch dort zeigte sich jedoch das gleiche Bild: Immer dann, wenn in Behördengebäuden die Abfalltonnen öffentlich zugänglich waren, wurden Unterlagen mit persönlichen Daten von Bürgern gefunden. Den Vogel schoss dabei ein Bürgerdienst der Stadt Mannheim ab. Eine am Bürgersteig abgestellte unverschlossene Baumulde war randvoll mit Aktenvermerken, behördlichen Bescheiden, Auszügen aus Geburtenbüchern, Mitteilungen an andere Behörden und Ähnlichem. Ungehindert konnten wir uns bedienen.

Als Fazit bleibt festzuhalten, dass unabhängig von Zeit und Ort der Überprüfung immer dann, wenn eine Altpapiertonne öffentlich zugänglich aufgestellt war, Papiere mit persönlichen Daten von Bürgern entdeckt wurden. Dieses Ergebnis spricht eindeutig dagegen, hier von Einzelfällen zu reden. Vielmehr liegt der Schluss nahe, dass sich, zumindest was die Entsorgung schriftlicher Unterlagen anbelangt, bei den Mitarbeitern der öffentlichen Verwaltung eine gewisse Sorglosigkeit breit gemacht hat. Und dabei geht es nicht nur um kommunale Dienststellen, wie weitere Kontrollbesuche bei zwei staatlichen Behörden zeigten. Obwohl die Ergebnisse der Müllaktion bei den Städten landesweit in der Presse publiziert und obwohl die Kontrollen vorher angekündigt worden waren, wurden nach wie vor umfangreiche personenbezogene Unterlagen im Papierabfall entdeckt. Dies ist aus Sicht der Betroffenen unerträglich und kann so nicht akzeptiert werden. Nachdem in den meisten Fällen entsprechende innerbehördliche Verfahrensanweisungen bestehen, muss es aus unserer Sicht in erster Linie darum gehen, regelmäßig zu kontrollieren, ob die bestehenden Regeln auch tatsächlich eingehalten werden. Wäre in den betroffenen Städten ein Datenschutzbeauftragter bestellt worden, wäre dies seine Aufgabe gewesen. Davon abgesehen hängt beim Umgang der Behördenmitarbeiter mit den Bürgerdaten viel davon ab, welchen Stellenwert ihre Vorgesetzten dem Datenschutz einräumen. Damit schien es uns jedenfalls bei der Stadt Mannheim nicht weit her zu sein. Denn als wir den Leiter des besagten Bürgerdienstes unmittelbar vor Ort auf die Missstände aufmerksam machten, ernteten wir wenig mehr als ein Schulterzucken. Auch die Reaktion des Oberbürgermeisters auf den Mängelbericht fiel zunächst ausgesprochen spärlich aus – mehr als den üblichen „Kanzleitrost“ gab es nicht! Erst nach mehr als vier Monaten und zweimaliger Erinnerung sah man sich in der Lage, zur Sache Stellung zu nehmen. Allerdings meinen wir, dass die von der Stadt nunmehr veranlasste Aufstellung der Altpapierbehälter in Bereichen, die ausschließlich für Mit-

arbeiter zugänglich sind, das Problem nur teilweise beseitigt. Vielmehr muss es darum gehen, den Mitarbeitern klar zu machen, dass personenbezogene Daten nicht in den Papierkorb gehören. Dafür müssen die Ämter mit Spezialcontainern und/oder elektrischen Aktenvernichtern ausgestattet werden. Und, insoweit müssen wir uns wiederholen, es muss auch wirksam kontrolliert werden, ob diese tatsächlich genutzt werden, um etwaigen Nachlässigkeiten von vornherein entgegenzuwirken. Dass die Stadt Mannheim, aber auch die anderen betroffenen Stellen, die Vorkommnisse hierzu zum Anlass nehmen werden, ist zu hoffen. Wir werden dies sicher gelegentlich nachprüfen.

3. Das automatisierte Personalausweis-/Passregister und der Lichtbildabgleich

Mehr Publicity als ihr lieb war hatte die Stadt Stuttgart. „Stadt sucht Rotlichtsünder Online im Passregister“ oder „Big Brother in der Stadt?“ prangten ihr eines Morgens die Schlagzeilen aus der Zeitung entgegen. Die Bußgeldstelle der Stadt Stuttgart hatte einer Frau einen Anhörungsbogen ins Haus geschickt, in dem der Frau zur Last gelegt worden war, trotz Rotlichts an einer Ampel weitergefahren zu sein. Weil der Verkehrsverstoß mit dem Auto ihres Mannes begangen worden war, wunderte sich die Frau, wie die Bußgeldstelle auf sie gekommen war. Das Rätsel war rasch gelöst. Die Bußgeldstelle hatte – wie sie gegenüber der Zeitung einräumte – mit Hilfe ihres Online-Anschlusses an die Personalausweis-/Passdatei der Stadt in den Ausweisbildern nachgeschaut, wer in der Familie des Fahrzeughalters zu der „geblitzten“ Person passt. Damit kam der Stein ins Rollen. Bei unserer Kontrolle vor Ort zeigte sich rasch, dass der Online-Anschluss der Bußgeldstelle a priori unzulässig und darüber hinaus auch noch mit weiteren Mängeln behaftet war. Damit nicht genug: Auch die automatisierte Personalausweis-/Passdatei der Stadt lief nicht datenschutzkonform. Doch jetzt die Fehler der Reihe nach:

3.1 Das Grundsatzproblem: Online-Anschluss unzulässig

Fährt jemand in Stuttgart zu schnell und wird er deswegen oder weil er trotz Rotlicht an einer Ampel weitergefahren ist geblitzt, bekommt er es mit der Bußgeldstelle der Stadt Stuttgart zu tun. Sie stellt anhand des amtlichen Kennzeichens des geblitzten Fahrzeugs fest, wer dessen Halter ist. Dem Fahrzeughalter schickt sie einen Anhörungsbogen, mit dem er sich binnen einer Woche zu dem Geschwindigkeits- bzw. Rotlichtverstoß äußern kann und in dem er zugleich darauf hingewiesen wird, dass die Bußgeldstelle das Beweisfoto mit seinem in der Personalausweis-/Passdatei hinterlegten Ausweisfoto abgleichen kann, wenn er sich zur Sache nicht äußern will oder in Abrede stellt, der geblitzte Autofahrer zu sein. Räumt der Fahrzeughalter den Verkehrsverstoß ein, ergeht ein entsprechender Bußgeldbescheid; die allermeisten Fälle erledigen sich so. In den anderen Fällen schreitet die Bußgeldstelle zu dem im Anhörungsbogen angekündigten Fotovergleich. Bei auswärtigen Autofahrern wendet sie sich dazu schriftlich an deren Wohnsitzgemeinde und bittet um die Übersendung einer Kopie des entsprechenden Ausweisfotos. Wohnt der Fahrzeughalter in Stuttgart und hält die Bußgeldstelle ihn oder auf Grund einer durchgeführten Melderegisterabfrage ein Mitglied seiner Familie für den verantwortlichen Autofahrer, so wurde wie folgt verfahren: Die Bußgeldstelle suchte beim Personalausweis-/Passamt der Stadt entweder schriftlich im Einzelfall um die Übersendung einer Kopie des Ausweisfotos der betreffenden Person nach, die im Verdacht stand, der geblitzte Autofahrer zu sein, oder ließ ein paar Fälle zusammenkommen, mit denen dann einer ihrer Mitarbeiter im benachbarten Personalausweis-/Passamt wegen der Ausweisfotos vorsprach. Weil die Bußgeldstelle dieses eingespielten Verfahrens überdrüssig geworden war, ließ sie sich im März 2000 einen Online-Anschluss an die Personalausweis-/Passdatei der Stadt schalten. Damit konnten praktisch alle Mitarbeiter der Bußgeldstelle von ihren Arbeitsplatz-Computern aus per Mausklick auf die ca. 800 000 Ausweisbilder und weitere Informationen über die Stuttgarter Ausweisbesitzer zugreifen.

Keine Frage: Rotlichtverstöße und Geschwindigkeitsüberschreitungen im Straßenverkehr sind keine Lappalien. Deshalb sind die in der Personalausweis-/Passdatei gespeicherten Ausweisfotos für die Bußgeldstelle nicht von vornherein tabu, wenn es um die Ahndung solcher Verkehrsverstöße geht. Nach § 2 b des Personalausweisgesetzes darf nämlich die Personalausweisbehörde aus ihrer Personalausweisdatei personenbezogene Daten, zu denen auch die Ausweisfotos gehören, bei Vorliegen der weiteren Voraussetzungen dieser Vorschrift auf Ersuchen an die Bußgeldstelle übermitteln. Dasselbe gilt nach § 22 des Passgesetzes für die Passdatei. Ein Ersuchen nach diesen Vorschriften setzt jedoch eine förmliche Anforderung der Bußgeldstelle an das Personalausweis-/Passamt voraus, ihr bestimmte Daten zu einer bestimmten Person aus der Personalausweis-/Passdatei zu übermitteln. Ein solches Ersuchen, das schriftlich zu stellen oder zu dokumentieren ist, ist keineswegs bloß eine reine Formalie. Mit dieser Voraussetzung wollte der Gesetzgeber vielmehr gesichert wissen, dass Daten aus dieser Datei nur in eng begrenztem Umfang übermittelt werden und sie nicht zu einem Auskunftsregister mutiert. Das Personalausweis-/Passamt hat sich deshalb bei jedem Ersuchen um eine Weitergabe von Daten aus seiner Personalausweis-/Passdatei zu vergewissern, dass das Ersuchen im Rahmen der Aufgaben der ersuchenden Behörde liegt und ob das Übermittlungsersuchen danach plausibel ist. Über diese Rechtslage setzte sich die Stadt Stuttgart mit der Einrichtung des Online-Anschlusses hinweg. Dies ist keineswegs nur eine Petitesse. Denn ein Online-Anschluss birgt besondere Risiken in sich. Wer einen Online-Anschluss besitzt, braucht weder jemanden um Erlaubnis fragen noch sein Auskunftsersuchen schriftlich oder mündlich zu begründen. Er kann zudem beliebig oft und beliebig viel abfragen, ohne sich dafür rechtfertigen zu müssen. Wer einen Online-Anschluss hat, kann es sich auch leisten, prinzipiell die Richtigkeit dessen zu bezweifeln, was der Bürger sagt und ihm erst zu glauben, wenn die Computer-Abfrage nichts Gegenteiliges ergibt. Je mehr Online-Anschlüsse die herkömmliche Art und Weise ablösen, Informationen im Einzelfall bei der anderen Stelle mündlich, telefonisch oder schriftlich zu erheben, desto weniger durchsichtig und nachvollziehbar wird die Informationsverarbeitung für den Bürger. Er kann dann nur noch schwer abschätzen, wer was wann über ihn erfahren kann. Deswegen muss der Gesetzgeber klar sagen, wer wann und auf welche Weise und in welchem Umfang Daten über Bürger online abfragen darf. Eine solche Regelung gibt es jedoch weder im Personalausweisgesetz noch im Passgesetz. Weil es nach alledem für den Online-Anschluss der Bußgeldstelle an die Personalausweis-/Passdatei keine Rechtsgrundlage gab, haben wir diesen Online-Anschluss gegenüber dem Oberbürgermeister der Stadt beanstandet. Die Stadt hat daraufhin den Online-Anschluss gekappt.

3.2 Weitere Mängel des Online-Anschlusses

Über dieses grundsätzliche Manko hinaus zeigte sich aber auch sonst, dass der Datenschutz bei der Einrichtung des Online-Anschlusses nicht gerade Pate gestanden hatte.

3.2.1 Zugriff auf zu viele Daten

Statt den Online-Zugriff wenigstens auf die aktuellen Ausweisfotos und die zur Feststellung der Identität der Ausweisinhaber erforderlichen Angaben und damit auf die Datenarten zu beschränken, die für eine Übermittlung an die Bußgeldstelle auf ein entsprechendes Ersuchen allenfalls in Frage gekommen wären, konnte die Bußgeldstelle sich über ihren Online-Anschluss mir nichts, dir nichts praktisch alle Daten an ihrem Bildschirm anzeigen lassen, die in der Personalausweis-/Passdatei der Stadt über Stuttgarter Ausweisbesitzer gespeichert sind. So konnte sie beispielsweise nicht nur auf die Fotos schon längst abgelaufener Personalausweise und Pässe online zugreifen, sondern auch nachschauen, wann der Betroffene seinen Personalausweis oder Pass beantragt und ob er oder sein Vater oder seine Mutter oder sein

Vormund den ausgestellten Personalausweis oder Pass abgeholt hat. Damit nicht genug: Die Bußgeldstelle konnte sich über den Online-Anschluss auf ihrem Bildschirm auch anzeigen lassen, ob der Betroffene durch Geburt, Legitimation oder Einbürgerung Deutscher ist, ob zur Feststellung seiner Identität ein Personenfeststellungsverfahren notwendig war, ob Passversagungsgründe vorlagen oder ob das Personalausweis-/Passamt angeordnet hatte, dass der Personalausweis nicht zum Verlassen des Bundesgebiets berechtigt. Weil all diese Angaben über Personen, die einen Personalausweis oder Pass beantragt haben, für die Ahndung von Geschwindigkeitsverstößen und Rotlichtverstößen schlechterdings nicht erforderlich sind, haben wir beanstandet, dass die Bußgeldstelle gleichwohl über ihren Online-Anschluss auf diese Daten in der Personalausweis-/Passdatei zugreifen konnte.

3.2.2 Zu weitgehende Suchmöglichkeiten

Auf ein Ersuchen i. S. von § 2 b des Personalausweisgesetzes bzw. § 22 des Passgesetzes darf das Personalausweis-/Passamt der Bußgeldstelle jeweils nur das Ausweisfoto der in dem Ersuchen genannten Person übermitteln. Eine Weitergabe von Lichtbildern anderer Personen, etwa solcher aus dem verwandtschaftlichen Umfeld, wäre im Rahmen eines solchen Ersuchens nicht zulässig. Auch über diese Rechtslage setzte sich die Stadt Stuttgart hinweg, weil der Online-Anschluss ihrer Bußgeldstelle an die Personalausweis-/Passdatei so programmiert war, dass die Bußgeldstelle mit Hilfe eingebauter Suchmöglichkeiten auf die Daten namensgleicher Personen zugreifen und sich deshalb nicht nur das Ausweisfoto des Fahrzeughalters, sondern zugleich auch die Ausweisfotos seiner Familienangehörigen am Bildschirm anzeigen lassen konnte. Diese viel zu weitgehenden Suchmöglichkeiten der Bußgeldstelle in der Personalausweis-/Passdatei haben wir ebenfalls beanstandet.

3.2.3 Technische Datenschutzmaßnahmen unzureichend

Die Stadt hatte bei dem Online-Anschluss auch die gebotenen technischen Datenschutzmaßnahmen nicht recht bedacht, wie schon folgende Beispiele zeigen:

- Werden personenbezogene Daten elektronisch gespeichert, sind diese gegen unberechtigte Nutzung zu schützen. Dazu gehört u. a., dass Bildschirmschoner eingerichtet werden, die den Bildschirm automatisch nach einer gewissen Zeit ohne Eingaben abdunkeln und mit einer Sperre versehen, die nur durch ein Passwort aufgehoben werden kann. Dieser Standardmaßnahme des technischen Datenschutzes war bei dem Online-Anschluss der Bußgeldstelle an die Personalausweis-/Passdatei nicht Rechnung getragen, weil das Zeitintervall für die automatische Aktivierung des Bildschirmschoners zu lang war und der Bildschirmschoner durch Drücken einer beliebigen Taste deaktiviert werden konnte.
- Dass bei der Verarbeitung personenbezogener Daten eine Protokollierung der Zugriffe auf die Daten notwendig ist, gehört inzwischen zum kleinen Einmaleins des technischen Datenschutzes. Ohne eine solche Protokollierung können Schwachstellen der Systemsicherheit nicht aufgedeckt und unbefugte Zugriffe nicht ans Licht gebracht werden. Gleichwohl betrieb die Stadt Stuttgart den Online-Anschluss ihrer Bußgeldstelle an die Personalausweis-/Passdatei ohne eine entsprechende Protokollierung. Deshalb konnte bei der Stadt niemand sagen, wer wann weshalb welche Ausweisfotos online abgerufen hatte.

3.3 Fehler in der Personalausweis-/Passdatei

Die aufgezeigten Mängel des Online-Zugriffs der Bußgeldstelle hatten noch dadurch an Brisanz gewonnen, weil auch die Personalausweis-/Passdatei der Stadt Stuttgart nicht datenschutzkonform lief.

3.3.1 Daten zu lange gespeichert

Die Stadt Stuttgart speichert in ihrer Personalausweis-/Passdatei außer den Personalien, dem Wohnort, dem Geburtstag und Geburtsort sowie den Ausweisfotos von ca. 800 000 Stuttgarter Ausweisinhabern die Seriennummer der Personalausweise und Pässe sowie weitere Angaben über die Ausweisinhaber. Diese Daten darf die Stadt Stuttgart nicht bis zum Sankt-Nimmerleins-Tag speichern. Nach § 2 a Abs. 3 des Personalausweisgesetzes ist sie vielmehr verpflichtet, die in ihrer Personalausweisdatei gespeicherten Daten spätestens fünf Jahre nach Ablauf der Gültigkeit des Personalausweises, auf den sie sich beziehen, zu löschen. Entsprechendes gilt nach § 21 Abs. 4 des Passgesetzes für die Löschung personenbezogener Daten in der Passdatei.

Diesen Vorgaben an die Datenlöschung in ihrer Personalausweis-/Passdatei war die Stadt Stuttgart nicht nachgekommen. Dabei mag es noch angehen, dass die Stadt nach der Ausstellung eines neuen Ausweises nicht Zug um Zug die Daten über den alten Ausweis löscht, sondern weiter speichert. Nicht mehr akzeptabel weil gesetzwidrig war, dass die Stadt – wie sich bei einer nach dem Zufallsprinzip gezogenen Stichprobe bei unseren Kontrollen gezeigt hatte – auch dann nicht zur Datenlöschung schritt, wenn der Personalausweis oder Pass schon seit fünf Jahren oder noch länger abgelaufen war. Eine Datenlöschung stante pede konnte die Stadt Stuttgart nicht bewerkstelligen, weil in der Personalausweis-/Passdatei ein Datenwirrwarr entstanden war, von dem jetzt gleich die Rede ist.

3.3.2 Unrichtige Daten gespeichert

Will man sicherstellen, dass in einer Datei des Ausmaßes der Personalausweis-/Passdatei der Stadt Stuttgart Daten nach Ablauf der gesetzlich vorgeschriebenen Speicherfrist termingerecht gelöscht werden, kann man dies angesichts der in die Hunderttausende gehenden Datensätze nur mit Hilfe eines EDV-Programms bewerkstelligen. Dazu muss das Programm das Ende der Speicherfrist berechnen. Hierzu wiederum muss es das Datum kennen, an dem der Ausweis seine Gültigkeit verliert. Ab da dürfen Daten des Ausweisinhabers nämlich höchstens noch fünf Jahre lang gespeichert werden. Das Gültigkeitsdatum ließ die Stadt Stuttgart jeweils anhand des Geburtsdatums des Ausweisinhabers, der Ausweisart und des Antragsdatums von einem Fristenprogramm berechnen. Dieses Fristenprogramm arbeitete nicht immer fehlerfrei. Wo genau der Fehler lag, ließ sich im Nachhinein nicht mehr sicher klären. Fest steht jedoch, dass das Fristenprogramm das Antragsdatum, das Geburtsdatum und das Gültigkeitsdatum vertauschte und so in der Personalausweis-/Passdatei der Stadt unrichtige Datensätze en masse produzierte.

Diese unrichtigen Datenspeicherungen und die unterbliebenen Datenlöschungen in der Personalausweis-/Passdatei der Stadt haben wir gegenüber dem Oberbürgermeister der Stadt Stuttgart beanstandet. Dabei haben wir der Stadt geraten, bei der Neuausstellung eines Personalausweises oder Passes Zug um Zug die Daten über den abgelaufenen Personalausweis oder Pass in ihrer Personalausweis-/Passdatei zu löschen. Damit hätte sich die Stadt nicht nur leichter beim Führen ihrer Datei getan, sondern zugleich auch den in § 9 LDSG verankerten Grundsatz der Datenvermeidung und der Datensparsamkeit Rechnung getragen, nach dem die öffentlichen Stellen des Landes gehalten sind, so wenig Daten wie möglich über Bürger zu verarbeiten. Auf Gegenliebe bei der Stadt Stuttgart stieß dieser Rat nicht. Stattdessen hat sie ein EDV-Ver-

fahren eingeführt, bei dem die Datenspeicherungen über abgelaufene Personalausweise und Pässe erst gelöscht werden, wenn die fünfjährige Maximalspeicherfrist verstrichen ist. Die unrichtigen Datensätze hat die Stadt inzwischen korrigiert.

4. Die Kommune im Internet

Jede Gemeinde, die etwas auf sich hält, präsentiert sich heutzutage mit einer eigenen Homepage im Internet. Solange die Gemeinden sich darauf beschränken, die Internet-Nutzer auf ihre Einwohnerzahl, auf ihre Lage, auf ihre Sehenswürdigkeiten oder auf ihre Geschichte aufmerksam zu machen, ist gegen diese moderne Serviceleistung aus der Sicht des Datenschutzes natürlich nichts einzuwenden. Gleiches gilt, wenn eine Gemeinde z. B. auf die Zuständigkeiten, Öffnungszeiten und Erreichbarkeit ihrer Ämter oder öffentlichen Einrichtungen hinweist.

Datenschutzrechtlich anders zu beurteilen ist die Einstellung von Namen, Anschriften, Telefon- und Telefax-Nummern, E-Mail-Adressen oder Lichtbildern von Gemeinderatsmitgliedern, Vereinsvorsitzenden, Gewerbetreibenden usw. in das Internet. Desgleichen z. B. die Wiedergabe der Interviews von Feriengästen oder Altenheimbewohnern mit Namen, Anschrift und/oder Lichtbild. Ebenso die Verbreitung von Fotos, auf denen Benutzer kommunaler Bibliotheken, Kindergartenkinder oder andere Personen erkennbar sind. Zu dieser Kategorie von Veröffentlichungen können auch sog. Webcam-Aufnahmen gehören, die z. B. Fußgängerzonen oder Bürgerbüros zeigen, wenn abgebildete Personen identifiziert oder Sachen wie Kraftfahrzeuge einer bestimmten Person zugeordnet werden können; dann ist nämlich jederzeit feststellbar, wer sich wann an welchem Ort aufgehalten hat. In allen genannten Fällen übermittelt die Gemeinde weltweit personenbezogene Daten. Schon § 18 LDSG, der für Datenübermittlungen innerhalb des Bundesgebiets und gemäß § 20 Abs. 1 LDSG auch für Übermittlungen in andere EU-Mitgliedstaaten gilt, stünde einer Verbreitung der genannten Daten über das Internet entgegen: Zum einen fehlt es angesichts des auf das Gemeindegebiet beschränkten Aufgaben- und Wirkungskreises der Gemeinden an der Erforderlichkeit zur Aufgabenerfüllung. Zum anderen kann schlechterdings nicht unterstellt werden, dass der weltweite Kreis der Internet-Nutzer ein berechtigtes Interesse an der Kenntnis der Daten hat. Schließlich kann ein schutzwürdiges Interesse der Betroffenen am Ausschluss der Datenübermittlung nicht von vornherein verneint werden. Erst recht lassen die für Datenübermittlungen außerhalb der Europäischen Union geltenden strengeren Vorschriften des § 20 Abs. 2 bis 5 LDSG derartige Präsentationen im Internet nicht zu. Wir geben in diesem Zusammenhang zu bedenken, dass das weltweit nutzbare Medium Internet datenschutzrechtlich eine ganz andere Qualität hat als Veröffentlichungen herkömmlicher Art. Das Internet ermöglicht nämlich vielfältige Verknüpfungs- und Auswertungsmöglichkeiten, die besondere Gefahren für die schutzwürdigen Interessen der Betroffenen mit sich bringen.

Die Gemeinden dürfen die oben beispielhaft genannten Daten wie Namen, Anschriften, Telefonnummern oder Lichtbilder deshalb nur dann über das Internet verbreiten, wenn sie vorher die Einwilligung der betroffenen Personen eingeholt haben. Die Einwilligung muss sich ausdrücklich auf das Internet beziehen. Es reicht deshalb nicht aus, wenn sich z. B. Gemeinderäte, Vereinsvorsitzende oder Gewerbetreibende gegenüber der Gemeinde damit einverstanden erklärt haben, dass diese ihre Daten im gemeindlichen Mitteilungsblatt oder in einer Broschüre abdruckt. Dass eine Gemeinde die Einwilligung der von Webcam-Aufnahmen Betroffenen einholt, erscheint allerdings nicht praktikabel, weil die Aufnahmen automatisch erfolgen und in regelmäßigen Abständen im Internet aktualisiert werden. Webcam-Bilder dürfen daher nur im Internet gezeigt werden, wenn die Gemeinde in technischer Hinsicht Vorsorge trifft, dass jeder Personenbezug vermieden wird.

Rechtlich nicht ganz so einfach einzuordnen war die von einer Großen Kreisstadt im Internet angebotene „virtuelle Stadtrundfahrt“, auf die uns ein Bürger aufmerksam gemacht hat. Unsere Recherchen ergaben folgenden Sachverhalt: Die Stadt hatte von einem Unternehmen aus Niedersachsen eine digitale Datenbank erworben, in der sämtliche Gebäude im Stadtgebiet

im Bild festgehalten sind. Das Unternehmen hatte die Aufnahmen von einem durch die Straßen fahrenden Kraftfahrzeug aus gefertigt. Die Stadt stellte diese Gebäudebilddatenbank in das Internet ein. Zwar waren die einzelnen Gebäudebilder nicht automatisch mit der zugehörigen Adresse verknüpft. Doch war es weltweit jedem Internet-Nutzer möglich, durch Eingabe eines Straßennamens und einer Hausnummer sich z. B. an ein bestimmtes Wohnhaus „heranzutasten". Zu erkennen waren dann nicht nur die Größe und der äußere Zustand des Gebäudes, sondern u. a. auch, ob der Hausgarten gepflegt ist und ob sich der Eigentümer einen Swimmingpool leisten kann. Auch Typ und Kennzeichen von auf dem Grundstück abgestellten Fahrzeugen waren erkennbar.

Entscheidend für die Zulässigkeit des Anbietens der „virtuellen Stadtrundfahrt" im Internet war für uns, ob es sich bei den abgebildeten Gebäuden und Grundstücken um personenbezogene Daten im Sinne des Landesdatenschutzgesetzes handelt. Wir haben diese Frage bejaht, da die Gebäude mit Hilfe von jedermann zur Verfügung stehenden Hilfsmitteln wie Adress- oder Telefonbüchern, d. h. ohne größeren Aufwand, bestimmten Personen zugeordnet werden konnten. Dies galt jedenfalls dann, wenn im Internet die Hausnummer eines Gebäudes erkennbar war. Bei einer entsprechenden Beschriftung des Hauses stand der Personenbezug ohnehin nicht in Frage. Wir gelangten deshalb zu dem Ergebnis, dass die Große Kreisstadt weltweit personenbezogene Daten ohne Einwilligung der Betroffenen und damit unzulässigerweise übermittelt. Den Datenschutzverstoß haben wir beanstandet. Erfreulicherweise hat die Stadt unverzüglich reagiert und die „virtuelle Stadtrundfahrt" aus dem Internet entfernt, obwohl sie unsere datenschutzrechtliche Einschätzung nicht teilt.

5. Standortverzeichnisse von Mobilfunkanlagen

Im Laufe des Berichtsjahres hatten verschiedene Stellen, vor allem aber Städte und Gemeinden, bei uns angefragt, ob es unter datenschutzrechtlichen Gesichtspunkten zulässig sei, für ihr Stadt- oder Gemeindegebiet ein Verzeichnis über die Standorte von Mobilfunkanlagen zu veröffentlichen, wobei teilweise auch beabsichtigt war, diese Informationen im Internet zur Verfügung zu stellen.

Obwohl der Wunsch der Kommunen, ein solches Standortverzeichnis zur Information der Bürger zu veröffentlichen, durchaus nachvollziehbar ist, mussten wir die anfragenden Stellen auf Folgendes hinweisen:

Soweit diese Datenbanken Standortdaten von Mobilfunkantennen enthalten, die eigentumsrechtlich einer natürlichen Person zuzurechnen sind, z. B. wenn Straßennamen mit Hausnummern angegeben werden sollen, handelt es sich um personenbezogene Daten i. S. von § 3 Abs. 1 LDSG. Nach § 4 Abs. 1 LDSG ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Landes Baden-Württemberg jedoch nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder soweit der Betroffene eingewilligt hat. Den Kommunen wird jedoch weder im Immissionsschutzrecht oder in der Landesbauordnung noch in telekommunikationsrechtlichen Vorschriften eine derartige Aufgabe zugewiesen. Auch auf die Gemeindeordnung oder das Landesdatenschutzgesetz lässt sich die Veröffentlichung eines flächendeckenden Katasters nicht stützen. In Baden-Württemberg bedarf die Veröffentlichung eines Standortkatasters mit personenbezogenen Daten mangels einschlägiger Rechtsgrundlage somit der Einwilligung der Betroffenen.

Nur wenn solche Standortverzeichnisse keine personenbezogenen Daten enthalten, z. B. wenn lediglich Straßenzüge ohne Hausnummern oder Stadtviertel genannt werden, wäre aus datenschutzrechtlicher Sicht nichts gegen eine Veröffentlichung der bei der Kommunalverwaltung vorgehaltenen Daten auch ohne Einwilligung der Betroffenen einzuwenden. Denn das informationelle Selbstbestimmungsrecht wäre durch die insoweit anonyme Weitergabe der Informationen an die Öffentlichkeit nicht berührt.

Da diese Thematik bundesweit von Bedeutung ist, halten es die Datenschutzbeauftragten des Bundes und der Länder für erforderlich, dass eine einheitliche Vorschrift geschaffen wird, in der geregelt ist, wie derartige

Kataster erstellt werden sollen, aber auch, ob und unter welchen Voraussetzungen eine Veröffentlichung solcher Verzeichnisse im Internet und vergleichbaren Medien zulässig ist. Die Datenschutzbeauftragten des Bundes und der Länder haben den Bundesgesetzgeber daher aufgefordert, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden (s. Anhang 6).

6. Die Sitzungsunterlagen

Die Gemeindeordnung schreibt vor, dass der Bürgermeister den Gemeinderat schriftlich mit angemessener Frist einberuft und den Gemeinderatsmitgliedern rechtzeitig die einzelnen Verhandlungsgegenstände mitteilt; dabei sind die für die Verhandlung erforderlichen Unterlagen beizufügen, soweit nicht das öffentliche Wohl oder berechtigte Interessen Einzelner entgegenstehen. Die Gemeinderäte sollen sich mit Hilfe der Unterlagen mit den Beratungsgegenständen vertraut machen und auf die Sitzung vorbereiten können. Wir empfehlen den Gemeinden regelmäßig, bei der Abfassung der Sitzungsunterlagen jeglichen Personenbezug zu vermeiden. Allerdings haben wir die Erfahrung gemacht, dass einzelne Gemeinden nicht immer in dieser Weise verfahren.

Die Gemeinden gehen zunehmend dazu über, die Unterlagen für öffentliche Sitzungen nicht nur – wie es die Gemeindeordnung fordert – den Gemeinderatsmitgliedern zu übersenden, sondern auch für die Zuhörer und für die Presse im Sitzungsraum auszulegen oder sie gar in das Internet einzustellen. Diesen auf den ersten Blick bürgerfreundlichen Service beurteilen wir, soweit es um Unterlagen mit Personenbezug geht, datenschutzrechtlich wie folgt:

– Indem solche Sitzungsunterlagen für die Zuhörer und für die Presse im Sitzungsraum ausgelegt werden, werden – datenschutzrechtlich gesehen – personenbezogene Daten verarbeitet. Das ist nach § 4 LDSG nur zulässig, wenn dieses Gesetz selbst oder eine andere Rechtsvorschrift es erlaubt oder soweit die Betroffenen eingewilligt haben. Weder die Gemeindeordnung noch eine andere Rechtsnorm außerhalb des Landesdatenschutzgesetzes lassen es zu, dass eine Gemeindeverwaltung personenbezogene Sitzungsunterlagen „öffentlich“ auslegt. Auch die für die Übermittlung von personenbezogenen Daten an Stellen außerhalb des öffentlichen Bereichs, zu denen auch Privatpersonen und die Presse gehören, einschlägige Vorschrift des Landesdatenschutzgesetzes (§ 18) erlaubt das Auslegen solcher Sitzungsunterlagen nicht. Die mancherorts geübte Verfahrensweise, die Sitzungsvorlagen unverändert auszulegen, wäre deshalb nur mit ausdrücklicher Einwilligung der Betroffenen zulässig, was aber im Regelfall nicht praktikabel sein wird.

  Wie bereits einleitend dargelegt, empfehlen wir den Gemeinden, schon in den für die Gemeinderatsmitglieder bestimmten Sitzungsunterlagen möglichst jeden Personenbezug zu vermeiden. Diese Vorgehensweise bietet den Vorteil, dass Mehrfertigungen solcher Vorlagen ohne weiteres, d. h. ohne größeren Aufwand wie Schwärzen bestimmter Textstellen oder Straffen des Textes, im Sitzungsraum für die Zuhörer und für die Presse bereitgehalten werden können.

– Wie schon angedeutet, gehen manche Kommunen über die oben geschilderte Verfahrensweise noch hinaus. Als Teil der Präsentation der Gemeinde im Internet nehmen sie z. B. auch Beschlussvorlagen für den Gemeinderat in ihr Internet-Angebot auf.

  Diesen Service nahm die Bürgerin einer Stadt dankbar an. Sie las eine Sitzungsunterlage im Internet nach und stieß dabei zu ihrer Überraschung auf jenen Brief, mit dem sie selbst zuvor Kritik an einem Bebauungsplanentwurf gegenüber der Stadtverwaltung geübt hatte. Hierzu muss man wissen, dass die Gemeinden nach dem Baugesetzbuch (BauGB) die ausgearbeiteten Entwürfe ihrer Bauleitpläne einschließlich Erläuterungsbericht oder Begründung öffentlich, also zu jedermanns Einsicht, auszulegen haben. Damit sollen vor allem die Bürger Gelegenheit erhalten, zu den Entwürfen von Bauleitplänen Anregungen vorzubringen. Über diese Anregungen, Vorbehalte oder Ablehnungen ent-

scheidet in der Regel der Gemeinderat. Damit er das Vorbringen prüfen und darüber ordnungsgemäß und sachgerecht beraten und beschließen kann, muss ihm zumindest der Inhalt des Bürgervotums durch die Verwaltung zur Kenntnis gebracht werden.

Tatsächlich hatte die betreffende Kommune u. a. die Vorlage für eine kurz zuvor abgehaltene Sitzung des Gemeindeparlaments in ihr Internet-Angebot aufgenommen; die Vorlage bot in ihrem Anhang die Möglichkeit, mehrere Anlagen anzuklicken und aufzurufen. Bei fünf dieser Links handelte es sich um Schreiben an die Stadtverwaltung, mit denen Bedenken und Anregungen zum Bebauungsplanentwurf vorgebracht wurden. Der Text der Vorlage verwies ausdrücklich auf diese „Originalbriefe im Anhang“. Die Stadt reagierte umgehend. Nachdem wir die Kommune darauf hingewiesen hatten, nahm sie die Schreiben aus ihrer Homepage, die versehentlich mit diesen Briefen bestückt worden sei.

Dieser Vorgang brachte uns auf die Idee einer umfassenden Recherche, bei der wir uns dem Internet-Angebot von über 20 Kommunen im Land zuwandten. Konkreter Gegenstand der Überprüfung waren dabei ausschließlich Sitzungs- und Beratungsunterlagen in Bauleitplanverfahren. Ziel der Überprüfung war es zu ermitteln, ob die Gemeinden in diesem Zusammenhang personenbezogene Daten unbegrenzt öffentlich machen.

Um es kurz zu machen: Eine Stadt nahm auch Namen von Personen, die sich mit den ausgelegten Entwürfen auseinander gesetzt hatten, in verschiedene Beschlussvorlagen für den Gemeinderat auf und verbreitete diese Sitzungsunterlagen über das Internet. Zum Teil konnte dabei einzelnen Personen auch der Inhalt ihres Vorbringens direkt zugeordnet werden. Eine Sitzungsunterlage enthielt den Entwurf eines städtebaulichen Vertrags, wobei die vertragschließenden Parteien bezeichnet waren.

Etwas dezenter ging eine andere Stadt vor. Sie benannte die Personen, die Anregungen und Bedenken gegen die Planung vorbrachten, nicht namentlich, sondern bezeichnete sie u. a. als Eigentümer bzw. Miteigentümer bestimmter Flurstücke und fügte die entsprechenden Flurstücksnummern hinzu. Dafür wurden dann aber auch Anregungen teilweise zitiert und somit stellenweise wortwörtlich wiedergegeben. Wer sich die Mühe machte, die entsprechende Beschlussvorlage im Internet aufmerksam zu lesen, konnte deshalb von einem nach wie vor aktuellen Kaufinteresse eines Bürgers für ein bestimmtes Grundstück wie auch vom Hinweis eines Grundstückseigentümers auf angeblich baurechtlich nicht genehmigte Stellplätze auf einer bezeichneten Parzelle erfahren.

Klar ist, dass die Personen, die die Stadtverwaltung hinter Flurstücksnummern verbarg, für den einen oder anderen Interessierten durchaus identifizierbar waren.

Im Ergebnis waren die beiden Gemeinden nicht berechtigt, Daten mit Personenbezug oder doch zumindest Informationen über Personen, die identifizierbar sind, mit Hilfe des Internets zu verbreiten. Hierfür ist nämlich weder eine Rechtsgrundlage noch ein Bedürfnis der Kommunen ersichtlich. Insbesondere kann dafür nicht die Regelung der Gemeindeordnung über die Öffentlichkeit der Sitzungen des Gemeindeparlaments ins Felde geführt werden (§ 35 Gemeindeordnung [GemO]). Zwar dürfen danach Ortsfremde nicht von öffentlichen Sitzungen des Gemeinderats ausgeschlossen werden; aber die Vorschrift zielt auf eine Zugänglichkeit der Sitzungen und eben nicht auf den unbeschränkten Zugriff auf die Sitzungsunterlagen. Auch die einschlägige Bestimmung des § 18 LDSG erlaubt eine derartige Weitergabe personenbezogener Angaben nicht. Weder hat der weltweite Personenkreis der Internet-Nutzer ein berechtigtes Interesse an der Kenntnis dieser Informationen noch können die Gemeinden ohne weiteres davon ausgehen, dass die betroffenen Personen kein schutzwürdiges Interesse an der Verhinderung der weltweiten Verbreitung ihrer Angaben haben. Schließlich und endlich gehört es auch nicht zu den Aufgaben der Städte, die genannten Details einem weltweiten Benutzerkreis zur Verfügung zu stellen.

Auf all dies wiesen wir diese beiden Kommunen kürzlich hin. Eine Stadt teilte nun mit, dass die von uns genannten Beschlussvorlagen aus dem Internet-Auftritt entfernt wurden und dass künftig die im Internet erscheinenden Gemeinderatsdrucksachen nicht mehr die Namen von Beteiligten in Bauleitplanverfahren enthalten werden. Die andere Kommune konnte in der Kürze der Zeit hierzu noch nicht Stellung nehmen.

7. Dienstliche Unterlagen für private Zwecke?

Ein empörter Bürger hat sich Hilfe suchend an uns gewandt und dabei folgenden Sachverhalt geschildert: Ein früherer Mieter seiner Eigentumswohnung, der Bürgermeister einer Kleinstadt, habe seine dienstlich erlangten Kenntnisse über die Einzelheiten eines Grundstückskaufvertrags privat verwertet. Der Bürgermeister, mit dem er vor Gericht einen Mietstreit führe, habe den Erwerber der inzwischen verkauften Eigentumswohnung unter einem Vorwand aufs Rathaus bestellt. Dort habe der Bürgermeister aus dem Grundstückskaufvertrag vorgelesen und mit strafrechtlichen Schritten gedroht, um für sich Vorteile in der Mietsache zu erreichen. Der Bürger hielt die Handlungsweise des Bürgermeisters für unvereinbar mit dem Datenschutz.

Wir gaben dem Bürgermeister Gelegenheit, sich zu den Vorwürfen zu äußern. Dieser klärte uns darüber auf, der Notar habe eine Mehrfertigung des von ihm beurkundeten Kaufvertrags, wie es das Baugesetzbuch vorschreibt, dem städtischen Gutachterausschuss zugeleitet. Wie die gesamte an die Stadt gerichtete Post sei auch der besagte Kaufvertrag über seinen Schreibtisch gegangen. Auf diese Weise habe er von dem Vertragsinhalt Kenntnis erhalten. Im Übrigen habe er bei dem Gespräch mit dem Wohnungskäufer nicht aus dem Vertrag vorgelesen, sondern Teile davon aus dem Gedächtnis wiedergegeben. Darin sah der Bürgermeister keinerlei datenschutzrechtliche Relevanz, weil es sich bei seinem Gesprächspartner um eine der Vertragsparteien und damit um einen Betroffenen gehandelt habe und die personenbezogenen Daten somit nicht einem Dritten offenbart worden seien.

Um das Ergebnis unserer datenschutzrechtlichen Prüfung vorwegzunehmen: Nicht der Bürgermeister lag mit seiner rechtlichen Einschätzung des Sachverhalts richtig, sondern der Bürger. Und zwar aus folgenden Gründen: Der Notar hat dem städtischen Gutachterausschuss den Grundstückskaufvertrag zur Führung der Kaufpreissammlung nach dem Baugesetzbuch übersandt. Der Bürgermeister hat weder den Vorsitz in dem genannten Gremium inne noch leitet er dessen Geschäftsstelle. Selbst wenn man die Frage nicht vertieft, ob der Bürgermeister unter diesen Umständen den Vertrag überhaupt hätte zu Gesicht bekommen dürfen, war jedenfalls dessen weiteres Vorgehen datenschutzrechtlich nicht in Ordnung. Er hätte die über den Inhalt des Kaufvertrags erlangten Kenntnisse allenfalls für dienstliche Zwecke nutzen dürfen. Und das auch nur, wenn eine der Voraussetzungen des § 15 LDSG vorgelegen hätte. Es kann dahingestellt bleiben, ob Letzteres der Fall war, nachdem der Bürgermeister die personenbezogenen Daten zweifelsfrei nicht in dienstlicher Eigenschaft, sondern als Privatmann genutzt hat. Eine Rechtsvorschrift, welche die Nutzung von Behördendaten für private Zwecke erlauben würde, gibt es nicht.

Wir haben deshalb gegenüber der Stadt den Datenschutzverstoß des Bürgermeisters beanstandet und sie gebeten, die datenschutzrechtlichen Vorschriften künftig zu beachten.

8. Bürgermeister oder Vereinsvorsitzender?

Eine Behörde gab die Kopie eines Strafurteils über einen ihrer Beschäftigten weiter. Das Strafurteil enthielt naturgemäß personenbezogene Daten des Beschäftigten, etwa die Angaben zu seiner Person sowie zur Straftat. Der Beschäftigte war außerdem ehrenamtlich tätig: als Ortschaftsrat in einer Gemeinde und zudem in einem privatrechtlichen Verein. Das war er allerdings nicht mehr lange, denn er musste nach der Weitergabe der Kopie des Strafurteils, wie er uns mitteilte, beide ehrenamtlichen Tätigkeiten einstellen. Der Empfänger der Kopie des Strafurteils übte ebenfalls mehrere Funktionen aus: Er war sowohl Bürgermeister derselben Gemeinde als auch Vorsit-

zender des genannten Vereins. In welcher Funktion er die Kopie angefordert und erhalten hatte, ob als Bürgermeister (also für die Gemeinde) oder als Vereinsvorsitzender (also für den Verein), konnten wir im Rahmen unserer Nachforschungen nicht aufklären: Während die Gemeinde behauptete, der Empfänger habe den Vorgang nicht als Bürgermeister, sondern als Vereinsvorsitzender vorgelegt bekommen, machte die Beschäftigungsbehörde geltend, der Empfänger habe bei ihr als Bürgermeister angerufen und mit Blick auf die ehrenamtliche Tätigkeit des Betroffenen als Ortschaftsrat gebeten, ihm eine Kopie des Strafurteils zu senden.

Unabhängig davon, welche der Sachverhaltsvarianten nun tatsächlich zutraf, hatte die Beschäftigungsbehörde in jedem Fall das Personalaktengeheimnis verletzt und damit gegen den Datenschutz verstoßen, denn sie durfte die Kopie des Strafurteils weder an die Gemeinde noch an den Verein herausgeben (§113 d Abs. 2 Satz 1 des Landesbeamtengesetzes).

Bei der Gemeinde verhielt es sich dagegen wie folgt:

Hätte der Empfänger die Kopie des Strafurteils ausschließlich als Vereinsvorsitzender erhalten und verwendet, so würde dies bedeuten, dass die Gemeinde die Kopie nicht erhalten und deswegen von vornherein datenschutzrechtlich aus dem Schneider gewesen wäre.

Wenn der Empfänger jedoch die Kopie des Strafurteils als Bürgermeister angefordert hätte, so hätte die Gemeinde damit bei der Beschäftigungsbehörde personenbezogene Daten über den Betroffenen erhoben. Dies wäre jedoch rechtswidrig gewesen, weil die Gemeinde diese Daten nicht zur Aufgabenerfüllung benötigte – auch wenn der Betroffene Ortschaftsrat war (§ 13 Abs. 1 LDSG). Wenn der Empfänger diese Kopie als Bürgermeister erhalten und sie daraufhin jedoch (auch) als Vereinsvorsitzender verwendet hätte, so läge damit eine Datenübermittlung der Gemeinde an den Verein vor. Dass dabei nur eine Person, der Empfänger, beteiligt war, ändert hieran nichts, denn sobald dieser die Kopie oder auch nur Kenntnisse, die er daraus als Bürgermeister erlangt, als Vereinsvorsitzender verwendet, liegt eine Datenverarbeitung des Vereins vor; dies setzt notwendigerweise voraus, dass die Daten dem Verein übermittelt wurden, hier von der Gemeinde. Darauf, ob die Datenübermittlung (zunächst) von außen nicht wahrnehmbar war, weil sie lediglich im Kopf stattfand, kommt es dabei nicht an; aus Sicht des Datenschutzes müssen Personen mit mehreren Funktionen, wenn es um personenbezogene Daten geht, die „Schere im Kopf“ einsetzen. Hätte also die Gemeinde die Kopie des Strafurteils dem Verein übermittelt, so wäre dies, soweit von hier aus beurteilbar, ebenfalls rechtswidrig gewesen: Anhaltspunkte dafür, dass der Verein ein berechtigtes Interesse an der Kenntnis des Strafurteils hatte, waren nicht ersichtlich; zudem hatte der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung (§ 18 Abs. 1 LDSG).

Dass die Zuständigkeit für die Datenschutzaufsicht über private Stellen beim Innenministerium Baden-Württemberg liegt und nicht beim Landesdatenschutzbeauftragten, wirkte sich hier gleich zweifach aus: Einerseits durften wir den privatrechtlichen Verein zu der Angelegenheit nicht anhören, um in Anbetracht der einander widersprechenden Darstellungen der Beschäftigungsbehörde und der Gemeinde den Sachverhalt weiter aufzuklären. Andererseits waren wir auch nicht befugt, das Verhalten des Vereins (durch den Empfänger der Kopie als Vereinsvorsitzender) datenschutzrechtlich zu kontrollieren und zu beurteilen. Ein Beleg mehr dafür, dass es geboten wäre, die Datenschutzkontrolle in eine Hand zu geben – weder ist es für die internen Arbeitsabläufe förderlich, wegen eines einheitlichen Lebenssachverhaltes unterschiedliche Datenschutzkontrolleure tätig sein zu lassen, noch kann diese gespaltene Zuständigkeit glaubhaft nach außen vermittelt werden.

9. Mitteilungen der Gewerbebehörde an das Finanzamt

Der 1. Vorsitzende eines Vereins wandte sich mit folgendem Anliegen an unser Amt: Im Jahr 2001 habe sein Verein auf einem Maimarkt Speisen und Getränke verkauft. Die hierfür erforderliche gaststättenrechtliche Gestattung habe er im April 2001 bei der Gewerbebehörde beantragt. Ein Jahr später habe er zu seiner Überraschung vom Finanzamt anstatt des von ihm erwarteten Steuerbescheids die Aufforderung erhalten, noch fehlende Angaben zu machen bzw. Belege vorzulegen, nachdem er auf dem Maimarkt 2001 Speisen und Getränke verkauft habe; hierfür sei eine entsprechende Gewinnermittlung einzureichen. Der Bürger war empört darüber, dass die Gewerbebehörde offenbar Daten, die seine ehrenamtliche Tätigkeit als Vereinsvorsitzender betrafen, ohne sein Wissen und auch noch teilweise unrichtig an das Finanzamt weitergegeben hatte. Das Finanzamt habe ihm auf seine Nachfrage hin erklärt, dass es von der Gewerbebehörde über die erteilte gaststättenrechtliche Genehmigung informiert worden war. Aus dieser Mitteilung sei jedoch nicht ersichtlich gewesen, dass die Gestattung für den Verein – und nicht für ihn als Privatperson – beantragt worden war. Das Finanzamt sei daher gezwungen gewesen, auf die Mitteilung entsprechend zu reagieren. Der Bürger sah in der Handlungsweise der Gewerbebehörde eine Verletzung des Datenschutzes – zu Recht, wie unsere Nachforschungen ergeben haben.

Wie sich herausstellte, hatte die Gewerbebehörde die gaststättenrechtliche Gestattung irrtümlich dem Bürger als Privatperson anstatt dem Verein erteilt und das Finanzamt hierüber unterrichtet. Dazu muss man wissen, dass die Gewerbebehörde nach § 6 Nr. 2 der Verordnung über Mitteilungen an die Finanzbehörden durch andere Behörden und öffentlich-rechtliche Rundfunkanstalten (Mitteilungsverordnung [MV]) verpflichtet ist, dem Finanzamt ohne Ersuchen die Erteilung einer gaststättenrechtlichen Genehmigung mitzuteilen. Die (den Bürger als Privatperson betreffende) Mitteilung an das Finanzamt war hier jedoch unzulässig, da die gaststättenrechtliche Gestattung fälschlicherweise dem Bürger anstatt seinem Verein erteilt worden war. Außerdem stellte sich heraus, dass die Gewerbebehörde es unterlassen hatte, den Bürger über die Mitteilung an das Finanzamt zu unterrichten. Hierzu wäre sie jedoch verpflichtet gewesen, wie sich aus § 11 MV ergibt. Nun war die Gewerbebehörde überrascht: Sie hatte ihre Mitteilungspflicht in der Vergangenheit völlig übersehen. Die Gewerbebehörde hat in das von ihr verwendete Formular „Gaststättenrechtliche Erlaubnisse“ inzwischen einen Hinweis zur Mitteilungspflicht an das Finanzamt mit aufgenommen und damit der Rechtslage – die seit September 1993 gilt – Rechnung getragen.

10. Die Weitergabe von Meldedaten

Die Meldebehörden haben nach dem Meldegesetz (MG) zum einen die Aufgabe, die in ihrem Zuständigkeitsbereich wohnenden Personen (Einwohner) zu registrieren, um deren Identität und Wohnungen feststellen und nachweisen zu können; zum anderen übermitteln sie aus dem Melderegister Daten an Empfänger aus dem öffentlichen und privaten Bereich. Für bestimmte Datenempfänger sieht das Meldegesetz eine besondere Form der (Gruppen-)Auskunft vor, die jeweils auf die Bedürfnisse dieser Datenempfänger abgestimmt ist. In diesem Zusammenhang sind die Herausgabe von Einwohnerdaten an Parteien für Wahlwerbungszwecke, die Veröffentlichung von Jubiläumsdaten, die Herausgabe von Adressbüchern und die Übermittlung von Einwohnerdaten an den Südwestrundfunk (SWR) zu nennen. Viele Bürger ärgern sich bzw. äußern ihr Unverständnis darüber, dass die Meldebehörden ihre Daten, ohne sie zuvor fragen oder auch nur unterrichten zu müssen, für die genannten Zwecke herausgeben dürfen. Das belegen die Bürgereingaben, die regelmäßig bei uns eingehen. Doch es sind nicht nur Bürger, die sich wegen der Weitergabe von Meldedaten an unser Amt wenden; wir erhalten auch immer wieder Anfragen von Gemeinden, die von uns wissen wollen, ob die Erteilung von bestimmten Melderegisterauskünften mit dem Datenschutz in Einklang steht.

– Gruppenauskünfte an Parteien

Die Meldebehörde (Gemeinde) darf u. a. im Zusammenhang mit allgemeinen Wahlen zu parlamentarischen und kommunalen Vertretungskörperschaften in den sechs Monaten vor der Wahl den Parteien und anderen Trägern von Wahlvorschlägen, die sich an der Wahl beteiligen, auf Antrag die Vor- und Familiennamen, Doktorgrade und Anschriften von wahlberechtigten Personen bestimmter Altersgruppen mitteilen; die Geburtstage dürfen nicht mitgeteilt werden. Rechtsgrundlage hierfür ist § 34 Abs. 1 MG. Die Daten sollen es den Parteien ermöglichen, mit potentiellen Wählern persönlichen Kontakt aufzunehmen, indem sie diesen persönlich adressierte Schreiben zukommen lassen. Die Datenempfänger dürfen die Adressen der Wahlberechtigten nur für Zwecke der Werbung für die Wahl verwenden, für die sie die Adressen erhalten haben. Sie sind verpflichtet, die Daten spätestens einen Monat nach der Wahl zu löschen.

Im Vorfeld der Bundestagswahl im September 2002 wandten sich mehrere Gemeinden an unser Amt, da sie sich nicht sicher waren, inwieweit sie Parteien die Daten von Wahlberechtigten für Zwecke der Wahlwerbung zur Verfügung stellen dürfen. So hatte der Bundesgeschäftsführer einer Partei eine Gemeinde darum gebeten, ihm die Adressdaten sämtlicher Wahlberechtigter zu übermitteln; in einem anderen Fall hatte der Kreisverband einer Partei von der Gemeinde die Herausgabe der Adressdaten aller Wahlberechtigter der Altersstufen „18-30“, „30-45“ und „58-68“ verlangt. Die betreffenden Gemeinden baten uns um Rat, ob die Erteilung von Melderegisterauskünften in den geschilderten Fällen mit § 34 Abs. 1 MG zu vereinbaren ist.

Wir konnten den Gemeinden dazu Folgendes sagen:

Eindeutig zulässig wäre es beispielsweise, an eine Partei die Adressen von Jung- oder Erstwählern oder von Senioren herauszugeben. Auch eine Auskunft über die Angehörigen beider genannten Gruppen würde sich noch im Rahmen des § 34 Abs. 1 MG halten, wenn die Partei dartut, dass sie die beiden Gruppen mit jeweils unterschiedlichen altersspezifischen Themen ansprechen möchte. Nachdem der Gesetzgeber die Auskunftserteilung aber bewusst auf „Gruppen von Wahlberechtigten“ beschränkt hat, darf sich eine Gruppenauskunft nach § 34 Abs. 1 MG nicht auf alle Wahlberechtigten erstrecken. Soweit alle Wahlberechtigten angesprochen werden sollen, ist auf anderweitige Möglichkeiten wie z. B. Postwurfsendungen zu verweisen.

Der Gemeinde, die um Übermittlung der Adressdaten der Wahlberechtigten von insgesamt 40 Jahrgängen ersucht worden war, haben wir mitgeteilt, dass dieses Auskunftsersuchen als Umgehung der o. g. Vorschrift angesehen und damit abgelehnt werden könnte. Allerdings konnten wir der Gemeinde die Entscheidung, ob sie die Adressdaten herausgibt oder nicht, nicht abnehmen, da sie diese im Rahmen des ihr vom Gesetzgeber eingeräumten pflichtgemäßen Ermessens letztlich selbst treffen musste. Wir haben die Gemeinde aber darauf hingewiesen, dass eine positive Entscheidung zumindest voraussetze, dass die Partei die verschiedenen Gruppen jeweils altersspezifisch anschreiben möchte.

– Veröffentlichung von Jubiläumsdaten

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

Ja, es ist tatsächlich so, dass eine Meldebehörde dies tun darf. Rechtsgrundlage hierfür ist § 34 Abs. 2 MG. Danach dürfen Namen, Doktorgrad und Anschriften von Altersjubilaren (ab 70. Geburtstag) und Ehejubilaren (ab goldener Hochzeit) sowie Tag und Art des Jubiläums veröffentlicht und an Presse und Rundfunk zum Zwecke der Veröffentlichung herausgegeben werden. Ob die Meldebehörde so verfährt oder nicht, steht in ihrem Ermessen; weder Bürger noch Presse oder Rundfunkanstalten haben einen Anspruch darauf, dass Jubiläumsdaten herausgegeben werden. Viele Städte und Gemeinden verfahren jedoch bekanntlich so.

Die Einstellung von Jubiläumsdaten in das Internet bedarf der ausdrücklichen Einwilligung der Betroffenen.

– Übermittlung von Einwohnerdaten zum Zwecke der Veröffentlichung eines „Adressbuches“ im Internet

Eine Gemeinde bat uns um Auskunft, ob sie Einwohnerdaten zum Zwecke der Veröffentlichung im Internet an einen Adressbuchverlag herausgeben darf. Die Rechtslage ist wie folgt:

Die Meldebehörde darf Vor- und Familiennamen, Doktorgrad und Anschriften der volljährigen Einwohner in Einwohnerbüchern und ähnlichen Nachschlagewerken veröffentlichen und an andere zum Zwecke der Herausgabe solcher Werke übermitteln (§ 34 Abs. 3 MG). Schon nach dem Wortlaut dieser melderechtlichen Vorschrift, aber auch nach deren Sinn und Zweck, ist die Weitergabe von Einwohnerdaten auf ein Werk in Buchform beschränkt. An eine Verbreitung über Medien wie Internet oder CD-ROM hatte der Gesetzgeber seinerzeit mit Sicherheit nicht gedacht. Vor allem aber hat das Einstellen von Daten in das Internet eine völlig andere Qualität als die Veröffentlichung in Papierform, weil die Daten weltweit abgerufen werden können. Die Veröffentlichung im Internet erreicht damit einen viel größeren Personenkreis als jede auflagenbegrenzte Veröffentlichung in Buchform. Außerdem eröffnet die Veröffentlichung im Internet vielfältige Auswertungs- und Verknüpfungsmöglichkeiten, durch die schutzwürdige Interessen der Betroffenen berührt sein können. Die Veröffentlichung von Adressdaten im Internet ist deshalb nicht vergleichbar mit der Herausgabe eines Adressbuches in Papierform und kann daher nicht auf § 34 Abs. 3 MG gestützt werden. Sie darf deshalb nur vorgenommen werden, wenn die Einwohner dazu ihr ausdrückliches Einverständnis gegeben haben. Dabei genügt es den datenschutzrechtlichen Anforderungen nicht, den Betroffenen lediglich das Recht einzuräumen, der beabsichtigten Datenweitergabe zu widersprechen, wie es Artikel 1 Nr. 8 der Verordnung des Innenministeriums zur Änderung der Meldeverordnung vom 11. Januar 2002 für die Aufnahme der Adressen auf CD-ROM als Hinweis auf der Rückseite des Meldescheins vorsieht.

Um die Beachtung dieser Rechtslage sicherzustellen, haben wir der Gemeinde geraten, den Adressbuchverlag bei der Übermittlung von Einwohnerdaten ausdrücklich dazu zu verpflichten, die Veröffentlichung des Adressbuches nur in Papierform vorzunehmen. Die Gemeinde teilte uns daraufhin – was wir sehr begrüßt haben – mit, dass sie sich dazu entschlossen habe, das neue Adressbuch wie bisher nur in Papierform herauszugeben.

Nachdem diese Angelegenheit von allgemeiner Bedeutung ist, haben wir den Gemeinde-, den Städte- und den Landkreistag Baden-Württemberg sowie das Innenministerium hierüber unterrichtet. Das Innenministerium teilt unsere Rechtsauffassung und hat die Kommunen sogleich in einem Erlass darauf hingewiesen, dass die Einstellung von Einwohnerdaten in das Internet mit § 34 Abs. 3 MG nicht vereinbar ist und dies sowohl für Veröffentlichungen durch die Meldebehörde selbst als auch durch Dritte wie z. B. Adressbuchverlage gilt.

– Übermittlung von Einwohnerdaten an den SWR

Die Frage, ob und ggf. unter welchen Voraussetzungen die Meldebehörde berechtigt ist, Daten an den SWR bzw. an die Gebühreneinzugszentrale (GEZ) zu übermitteln, ist ein regelrechter „Dauerbrenner“, wie aus der Vielzahl der uns zugehenden Eingaben deutlich wird. In der Tat ist die Meldebehörde auf Grund verschiedener Rechtsvorschriften befugt oder sogar verpflichtet, bestimmte Einwohnerdaten an den SWR weiterzugeben:

Nach § 35 Abs. 1 MG ist die Meldebehörde berechtigt, den SWR oder die von ihm mit dem Einzug der Rundfunkgebühr beauftragte GEZ über den Zuzug, den Wegzug und den Tod von volljährigen Einwohnern zu unterrichten. Dabei darf sie Familiennamen, Vornamen, frühere Namen,

Geburtstag, Anschriften, Tag des Ein- und Auszugs, Familienstand und Sterbetag übermitteln. Diese Regelung wurde, obwohl wir uns nachdrücklich gegen sie gewandt hatten, im Jahre 1995 in das Meldegesetz eingefügt. Wir hatten dabei die Auffassung vertreten, dass diese Art von Meldedienst über das hinausgeht, was zur Ermittlung von „Schwarzsehern und -hörern" verhältnismäßig wäre.

Obwohl nahezu alle Gemeinden und Städte im Land dem SWR nach § 35 MG regelmäßig Veränderungen mitteilen, begnügt sich der SWR damit nicht immer. Zur Erleichterung der Arbeit der eingesetzten Gebührenbeauftragten bei der Ermittlung von „Schwarzsehern und -hörern" versucht der SWR darüber hinaus offenbar des Öfteren, von Bürgermeisterämtern komplette Listen mit den Adressdaten aller volljährigen Einwohner zu erhalten. Immer wieder wenden sich von einem solchen Auskunftsersuchen betroffene Gemeinden an uns mit der Frage, ob sie dem SWR die erbetenen Listen übermitteln dürfen.

Wir haben die Herausgabe solcher Listen stets als unzulässig angesehen, weil ein solcher Rundumschlag unverhältnismäßig ist. An dieser Rechtsauffassung halten wir fest, obwohl der Verwaltungsgerichtshof Baden-Württemberg in seinem Urteil vom 15. November 1994 (Az. 1 S 310/94) die Auffassung vertritt, eine solche Datenübermittlung an die Rundfunkanstalt sei auf Grund von § 29 MG möglich. Die Rundfunkanstalt hat jedoch nach der Auffassung des Verwaltungsgerichtshofs keinen absoluten Übermittlungsanspruch; vielmehr hat das Bürgermeisteramt eine Ermessensentscheidung zu treffen und dabei zu prüfen, ob die Rundfunkanstalt besondere Gesichtspunkte geltend macht, die über das grundsätzlich bestehende öffentliche Interesse an der Aufgabenwahrnehmung der Rundfunkanstalten hinausgehen. Ein solcher von der Rundfunkanstalt geltend zu machender Gesichtspunkt könnte nach Ansicht des Verwaltungsgerichtshofs sein, dass eine bestimmte Gemeinde oder ein Stadtteil im Verhältnis zu vergleichbaren Gemeinden oder Stadtteilen und entgegen der statistisch belegten Aussage, dass nahezu alle Haushalte der Bundesrepublik über Rundfunkgeräte verfügen, nach dem der Rundfunkanstalt vorliegenden Bestandsverzeichnis zu wenig Anmeldungen von Rundfunkteilnehmern aufweist.

Unabhängig von den beiden vorgenannten Rechtsgrundlagen für die Weitergabe von Meldedaten an den SWR darf dieser nach § 4 Abs. 6 des Rundfunkgebührenstaatsvertrags bei den Meldebehörden unter bestimmten Voraussetzungen im Einzelfall Auskünfte über Personen einholen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie ein Rundfunkempfangsgerät zum Empfang bereithalten und dies nicht oder nicht umfassend angezeigt haben.

Ein für die Bürger wichtiger Aspekt im Zusammenhang mit der Weitergabe von Einwohnerdaten ist, ob und ggf. wie der Einzelne die Weitergabe seiner Daten durch die Meldebehörde verhindern kann. Was die Weitergabe von Einwohnerdaten an den SWR betrifft, bleibt uns nur, den Betroffenen zu sagen, dass es hier keine Möglichkeit gibt, die Datenweitergabe zu verhindern. Anders hingegen verhält es sich, was die Herausgabe von Einwohnerdaten für Wahlwerbungszwecke, die Veröffentlichung von Jubiläumsdaten und die Herausgabe von Adressbüchern angeht. Hier haben die Betroffenen das Recht, der Weitergabe ihrer Daten zu widersprechen; die Meldebehörde ist verpflichtet, die Bürger auf ihr Widerspruchsrecht hinzuweisen (§ 34 MG). Wir halten diese Regelung für einen gerade noch vertretbaren Kompromiss zwischen dem Informationsinteresse der Parteien bzw. der Allgemeinheit und dem Geheimhaltungsinteresse der einzelnen Bürger, weil sie letzteren wenigstens die Möglichkeit gibt, die Herausgabe ihrer Daten zu verhindern. Weil aber trotz der den Gemeinden obliegenden Hinweispflichten erfahrungsgemäß viele Einwohner über ihr Widerspruchsrecht nicht Bescheid wissen, würden wir es begrüßen, wenn der Gesetzgeber die geltende Widerspruchslösung durch eine Einwilligungslösung ersetzen würde.

2. Abschnitt: Anderes

1. Personalwesen

Von den vielfältigen Fragen, die wir im Berichtszeitraum aus dem Bereich des Personaldatenschutzrechts zu beurteilen hatten, nehmen diejenigen zur elektronischen Datenverarbeitung einen breiten Raum ein. Auch durch diesen Bereich zieht sich wie ein roter Faden der Grundsatz der Erforderlichkeit: Sei es bei der Kosten- und Leistungsrechnung im Rahmen des Projekts Neue Steuerungsinstrumente, sei es bei einer Kontrolle von (Internet-)Rechnern der Beschäftigten oder beim Veröffentlichen von Personaldaten, stets ist zu fragen: Ist es notwendig, dass der Dienstherr oder Arbeitgeber dabei personenbezogene Daten der Beschäftigten verwendet und sie, wenn er sie ins Internet einstellt, weltweit veröffentlicht? Insbesondere beim Einheitlichen Personalverwaltungssystem ist auch zu fragen: Benötigt der Dienstherr oder Arbeitgeber alle personenbezogenen Daten, auf die er zugreift oder die er speichert? Doch nun zu den einzelnen Themen:

1.1 Projekt Neue Steuerungsinstrumente (NSI)

Die Einführung der Neuen Steuerungsinstrumente in Baden-Württemberg – sie umfassen im Wesentlichen das landesweite automatisierte Haushaltsmanagementsystem, die Kosten- und Leistungsrechnung sowie ein Berichtswesen als Führungsinformationssystem – ist auch unter dem Blickwinkel des Personaldatenschutzes von erheblicher Bedeutung. In Einklang mit dem allgemeinen Projektfortschritt wurden uns im Berichtszeitraum mehrere, die datenschutzrechtliche Seite des Projekts behandelnde Konzeptionen zur Begutachtung vorgelegt. Im Einzelnen waren das:

- Die Strukturkonzeption, die beschreibt, welche Konzepte erstellt werden. Von den acht spezifisch für das Projekt zu erstellenden Teilkonzepten sind uns bisher drei vorgelegt worden. Auf großes Interesse wird das „Sicherheitskonzept Anwendungsdaten“ stoßen, denn in diesem Konzept wird hoffentlich erstmals dargelegt werden, welche Daten von wem erhoben, gespeichert und zu welchen Ergebnissen verarbeitet werden.
- Die Konzeption und die Rahmenbedingungen zu Datenschutz und Datensicherheit, die die gesetzlichen Grundlagen und den technisch-organisatorischen Rahmen, innerhalb dessen die Konzepte erarbeitet werden, beschreiben. Hierzu war aus unserer Sicht klarzustellen, dass eine Übertragung der datenschutzrechtlichen Verantwortlichkeit nicht möglich ist. Verantwortlich ist jeweils die Stelle, die Daten entsprechend der Zweckbindung erhebt, speichert und verarbeitet. Eine Übertragung dieser Verantwortlichkeit beispielsweise auf das Finanzministerium, wie sie in der Konzeption anklang, ist nicht möglich. Ebenso konnte die Einschränkung, dass dem Landesbeauftragten für den Datenschutz kein Einblick in die firmenspezifischen Datenschutzkonzeptionen gewährt werden solle, nicht akzeptiert werden; es wurde klargestellt, dass wir auf diese Einsicht gar nicht verzichten dürfen. Es bleibt also dabei, dass uns auch bei diesem Projekt auf Wunsch alle den Datenschutz und die Datensicherheit betreffenden Konzeptionen auch des Auftragnehmers auszuhändigen sind. Anders lautende vertragliche Abmachungen sind datenschutzrechtlich a priori ungültig.

Neben diesen Dokumenten, die keine Datenschutzkonzepte im strengen Sinn sind, da es sich nur um die Nennung von Rahmenbedingungen und eine Aufzählung noch zu erstellender Datenschutzkonzepte handelt, wurden folgende Konzepte zur Begutachtung vorgelegt:

- Das Konzept „Netzanbindung Rechenzentrum Göppingen – Datenschutz- und Datensicherheitskonzept“ beschreibt die technische Anbindung des Landesverwaltungsnetzes an das Rechenzentrum des Auftragnehmers.
- Das „Rahmenberechtigungskonzept“ beschreibt, wie einzelnen Benutzern oder Benutzergruppen die Berechtigung zum Zugriff auf welche

Daten eingeräumt wird. Das System verfügt über ein vielseitiges und komplexes Berechtigungssystem, das über Profile erlaubt festzulegen, wer welche Aktivität innerhalb eines Buchungskreises oder einer Kostenstelle durchführen darf. Hierzu ist zu sagen, dass die Festlegung, wer welche Aktivität durchführen darf, durch die Behörde erfolgen muss. Diese meldet die Berechtigungsanforderungen an das Rechenzentrum weiter, wo durch das so genannte Kompetenzzentrum NSI Competence Center (NSI CC) entsprechend der Anforderung eine Berechtigung generiert und in das System eingegeben wird. Daneben müssen noch Benutzer mitgeteilt werden, denen die Berechtigung verliehen werden soll. Der Vorgang selbst läuft vom Fachvorgesetzten über einen so genannten User-Help-Desk an die Benutzerverwalter, Berechtigungsverwalter und Modulverantwortlichen im NSI CC. Der Ablauf wird in dem Konzept formal beschrieben; es weist keine Lücken auf. Im Alltag besteht aber bei dieser mehrstufigen Vorgehensweise, bei der zudem die Zuweisung von Berechtigungen an Benutzer durch ein Vier-Augen-Prinzip realisiert wird, die Gefahr, dass letztendlich dem Bediensteten fälschlicherweise im System Berechtigungen eröffnet werden, die er nicht haben soll. Der Fachvorgesetzte müsste – um die korrekte Zuordnung zu gewährleisten – entsprechende Berechtigungstests vornehmen; ob hierfür genügend Zeit zur Verfügung steht, ist mehr als fraglich. Daneben ist die Vertreterregelung anzusprechen. Sie wird so gehandhabt, dass für einen Vertreter keine neue Benutzerkennung angelegt, sondern seiner Benutzerkennung die Berechtigungen des Vertretenen zugewiesen werden. Nach Ablauf der Vertretung müssen die Berechtigungen der Benutzerkennnung des Vertreters wieder entzogen werden. Wenn nicht bei Beginn der Vertretung deren zeitliches Ende an das NSI CC mitgeteilt wird und die Berechtigungen automatisch zurückgesetzt werden, dann ist es erforderlich, dass über den oben beschriebenen Ablauf jeweils ein Änderungswunsch an das NSI CC mitgeteilt wird; dies müsste in geeigneter Weise sichergestellt werden.

Daneben wurde im Oktober 2002 ein Dokument mit dem Titel „Sicherheitskonzept Schnittstellen Fachvorverfahren und Landesoberkasse“ vorgelegt. Hierzu ist die Begutachtung noch nicht abgeschlossen.

Auch zum Bilden von Kostenstellen erhielten wir Anfragen von Behörden und Beschäftigten. Kostenstellen sind der erste Schritt zur Einführung der Kosten- und Leistungsrechnung. Sie sollen in Anlehnung an die bestehende Organisationsstruktur gebildet werden. Der Kostenstelle werden u. a. die Personalkosten der dort Beschäftigten zugeordnet. Indem die auf einer Kostenstelle gebuchten (Personal-)Kosten einem Produkt (d. h. einer Leistung, welche die Verwaltung erstellt hat, etwa eine Dienstleistung für den Bürger) zugeordnet werden, sollen dann die Kosten des Produkts ermittelt werden.

Rechtsgrundlage für die Verarbeitung personenbezogener Daten von Beschäftigten im Rahmen des Projektes NSI ist grundsätzlich § 36 Abs. 1 LDSG. Danach dürfen diese Daten nur verarbeitet werden, soweit dies u. a. zur Durchführung innerdienstlicher planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienst- oder Betriebsvereinbarung dies vorsieht. Personenbezogene Daten, d. h. Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 LDSG), dürfen also im Rahmen des Projektes NSI verarbeitet werden, sofern dies zur Haushalts- oder Kostenrechnung erforderlich ist.

Die verarbeiteten Daten dürfen somit möglichst von vornherein keinen Personenbezug aufweisen, d. h. sie dürfen keiner bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Soweit ein Personenbezug (zunächst) unumgänglich ist, muss dieser möglichst frühzeitig aufgehoben oder zumindest verringert werden, etwa indem die Daten mehrerer Beschäftigter zusammengefasst werden. Damit diesen Anforderungen Rechnung getragen werden kann, muss u. a. festgehalten sein, wer wozu welche Daten wie verarbeiten können soll.

Demgemäß müssen Kostenstellen möglichst so viele Beschäftigte umfassen, dass ein Rückschluss auf einzelne Personen ausgeschlossen ist. Generell sind also aus Gründen des Datenschutzes „größere“ Kostenstellen „kleineren“ vorzuziehen. In diese Richtung zielt auch der „Leitfaden zur Kostenstellenbildung“, in dem u. a. vorgegeben wird, „Kleinst“-Kostenstellen zu vermeiden. Entsprechendes gilt für die Produktbildung, wobei zu berücksichtigen ist, dass die Aussagen zu Produktkosten Rückschlüsse auf die Arbeitsmenge eines bestimmbaren Beschäftigten zulassen können (etwa wenn dieser ausschließlich und als einziger bestimmte Produkte erstellt) und daher besonders zu schützen sind.

In Anbetracht der Schwierigkeiten, die Erforderlichkeit von „Kleinst“-Kostenstellen zu begründen, empfahlen wir, zunächst Kostenstellen so „groß“ zu bilden, dass kein Personenbezug besteht. Sollte sich dann zeigen, dass für die Kosten- und Leistungsrechnung einzelne Kostenstellen „kleiner“ zu fassen sind, so dürfte dies dann einfacher und anhand konkreter Beispiele schlüssiger zu begründen sein. Ein solches Vorgehen wäre datenschutzfreundlicher und zudem für die betroffenen Behörden wohl effizienter.

1.2 Projekt EPVS/DIPSY

Zum Einheitlichen Personalverwaltungssystem (EPVS), das aus dem Dialogisierten Integrierten Personalverwaltungssystem (DIPSY) weiterentwickelt wird, nahmen wir auch in diesem Jahr gegenüber dem Innenministerium Stellung. Dieses Personalverwaltungssystem dient nicht nur der zentralen elektronischen Speicherung der Personaldaten der Beschäftigten des Landes, sondern soll unter anderem den Personal verwaltenden Stellen die Auswertung ihrer Personaldatenbestände ermöglichen.

Wir äußerten uns u. a. zu der Frage, inwieweit lokale Kopien (Download) von Personaldaten zulässig sein sollen. Dabei geht es darum, ob und gegebenenfalls welche Dienststellen welche Daten ausdrucken oder bei sich in Form einer Tabelle abspeichern können, um beispielsweise eigene Auswertungen durchzuführen. Aus der Sicht des Datenschutzes ist es – auch mit Blick auf den Grundsatz der Datensparsamkeit – vorzuziehen, wenn die Daten auf möglichst wenigen Rechnern verarbeitet werden. Soweit personenbezogene Daten für eine Statistik oder das Erstellen von Schreiben benötigt werden, ist technisch sicherzustellen, dass diese nur auf einem zentralen Rechner der jeweiligen Dienststelle elektronisch gespeichert werden können und nicht – auch nicht zeitweise – auf Arbeitsplatzrechnern oder mobilen Datenträgern. Soweit es unumgänglich sein sollte, lokale Kopien zu erstellen, so muss in einem Datenschutz- und Datensicherheitskonzept festgelegt sein, wer welche Daten wozu wie kopieren und sonst verarbeiten darf. Außerdem ist die Herstellung lokaler Kopien zu protokollieren, damit eine datenschutzrechtliche Überprüfung möglich ist.

Ein weiteres Problem sind aus unserer Sicht Freitextfelder, also Felder, deren Inhalt nicht durch einen Katalog vorgegeben ist. Soweit sie nicht zu vermeiden sind, sollte ihr Inhalt nur befristet gespeichert werden, besteht doch die Gefahr, dass in diesen Feldern Daten abgelegt werden, die im Rahmen der Zweckbindung für die Personalverwaltung nicht erforderlich sind.

Auch im Bereich der Personalverwaltung wird der Einsatz eines so genannten Data Warehouse geplant. Der Einsatz von derartigen Informationssystemen ist deshalb kritisch zu sehen, weil eine Zweckbindung der gespeicherten Daten von Anfang an nicht gewünscht ist. Das Ziel der Verarbeitung liegt nicht fest, sondern soll sich „evolutorisch“ ergeben. Dadurch ist für denjenigen, dessen Daten in einem Data Warehouse gespeichert und verarbeitet werden, keine Transparenz mehr gegeben. Er kann nicht mehr wissen, wie und mit welchem Ergebnis seine Daten verarbeitet werden. Noch werden mit DIPSY und dem Personalabrechnungssystem DAISY in der Personaldatenverarbeitung zwei Systeme betrieben, die voneinander getrennt sind. Auch im Berichtszeitraum haben wir wiederholt zum Ausdruck gebracht, dass dies so bleiben muss.

1.3 Kontrolle von (Internet-)Rechnern der Beschäftigten?

Ein Beschäftigter bei einer Behörde wandte sich in folgender Angelegenheit an uns: Ihm stehe an seinem Arbeitsplatz ein dienstlicher Rechner zur Verfügung, über den er auch ein Textverarbeitungsprogramm nutzen sowie E-Mails senden und empfangen könne. Als Speicherplatz stehe ihm u. a. ein Laufwerk „O:“ zur Verfügung, das die Bezeichnung „Persönlicher Ordner“ trage. Er habe auf dem Laufwerk „O:“ private Dokumente gespeichert gehabt, darunter zwei private E-Mails. Sein Vorgesetzter habe diese Dokumente ohne sein Wissen eingesehen.

Unsere Nachfrage bei der Behörde bestätigte diese Schilderung. Die Behörde verwies auf eine Dienstanweisung, wonach Daten per E-Mail nur zur Wahrnehmung dienstlicher Aufgaben übermittelt werden durften. Der Vorgesetzte des Betroffenen habe die Dokumente und E-Mails überprüft, weil er den Verdacht gehabt habe, dass dieser während der Dienstzeit privaten Tätigkeiten nachgegangen sei und dazu dienstliche Datenverarbeitungseinrichtungen genutzt habe.

Ob, unter welchen Voraussetzungen und wozu der Dienstherr oder Arbeitgeber protokollieren und kontrollieren darf, wie die Beschäftigten dienstliche Datenverarbeitungseinrichtungen nutzen, ist anhand des § 36 Abs. 1 LDSG zu beurteilen. Danach dürfen personenbezogene Daten von Beschäftigten nur verarbeitet werden, soweit dies u. a. zur Durchführung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienst- oder Betriebsvereinbarung dies vorsieht. Die Frage, wie weit eine Kontrolle der Beschäftigten reichen darf, ist im Rahmen einer Abwägung der maßgeblichen Interessen der Beschäftigten und des Dienstherrn oder Arbeitgebers zu beantworten. Dieser hat ein berechtigtes Interesse daran festzustellen, inwieweit die Beschäftigten die von ihnen geschuldete Arbeitsleistung tatsächlich erbringen, um gegebenenfalls personalrechtliche oder organisatorische Maßnahmen zu treffen; dies gilt auch für die Feststellung, ob der Beschäftigte dienstliche Einrichtungen (unerlaubt) privat nutzt. Die Beschäftigten ihrerseits haben ein berechtigtes Interesse daran, dass Kontrollen nicht zu Persönlichkeitsprofilen oder zu einem unangemessenen Überwachungsdruck führen.

In dem geschilderten Fall hatte die Behörde deswegen gegen datenschutzrechtliche Bestimmungen verstoßen, weil die Kontrolle nicht heimlich hätte erfolgen dürfen; es kam hier also nicht darauf an, ob hinreichende Verdachtsmomente vorlagen, die eine Kontrolle mit Kenntnis des Beschäftigten gerechtfertigt hätten. Von einer Beanstandung sah unser Amt ab, nachdem die Behörde den Verstoß eingeräumt hatte.

Dass die datenschutzrechtlichen Anforderungen an eine Kontrolle der Nutzung der dienstlichen Datenverarbeitungseinrichtungen durch Beschäftigte von allgemeinem Interesse sind, ist auch daran abzulesen, dass sowohl Beschäftigte wie auch Dienstherren oder Arbeitgeber uns dazu häufig um Rat fragten. Die – teilweise nur für die jeweilige Fallgestaltung bedeutsamen – Detailfragen sollen hier nicht dargestellt werden. Vielmehr verweisen wir wegen der Anforderungen an eine datenschutzgerechte Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz auf die Orientierungshilfe des Arbeitskreises Medien sowie die Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu diesem Thema (s. Anhang 8).

1.4 Die Veröffentlichung von Personaldaten – im Internet und in anderer Form

Die Frage, welche personenbezogenen Daten von Beschäftigten bekannt gegeben werden dürfen, etwa im Internet, in einer Bürgerbroschüre oder auf Tür- oder Namensschildern, wurde uns oft gestellt. Soweit es sich nicht um Personalaktendaten handelt, also die Daten nicht in einem unmittelbaren inneren Zusammenhang mit dem Beschäftigungsverhältnis stehen, richtet sich die Frage einer Veröffentlichung

ohne Einwilligung der Beschäftigten nach § 36 Abs. 1 LDSG, wenn nicht eine spezielle Vorschrift anwendbar ist. Eine Veröffentlichung personenbezogener Daten von Beschäftigten ist danach nur zulässig, soweit diese zur Abwicklung des Dienstbetriebs und Geschäftsverkehrs erforderlich ist. Bei der Beurteilung dieser Frage sind die Interessen des Dienstherrn oder Arbeitgebers mit denjenigen des Beschäftigten abzuwägen.

Dabei ist zunächst zu fragen, inwieweit es zur Abwicklung des Dienstbetriebs und Geschäftsverkehrs notwendig ist, dass andere unmittelbar mit dem jeweiligen Beschäftigten Kontakt aufnehmen können. Dies wird bei Mitarbeitern, die nicht unmittelbar nach außen wirkende Aufgaben wahrnehmen, nicht notwendig sein; anders kann sich die Situation darstellen, wenn diese eine leitende oder in besonderem Maße eigenverantwortliche Tätigkeit ausüben. Ist danach die Veröffentlichung der Daten bestimmter Beschäftigter erforderlich, so ist weiter zu prüfen, welche Daten für die Kontaktaufnahme nötig sind und ob dies voraussetzt, dass die Daten gerade in der beabsichtigten Form (etwa in einer gedruckten Broschüre oder im Internet und damit weltweit) bekannt gegeben werden.

Eine Veröffentlichung von Personaldaten im Internet ist grundsätzlich nur mit Einwilligung der Beschäftigten zulässig, denn dort eingestellte Daten können anders als in einer (auflagenbegrenzten) schriftlichen Veröffentlichung von einem ungleich größeren Personenkreis ohne weiteres weltweit abgerufen sowie auf vielfältige Art ausgewertet und verknüpft werden. Dies erhöht das Risiko erheblich, dass schutzwürdige Interessen der Betroffenen verletzt werden. Ausnahmen sind nur hinsichtlich der Namen, dienstlichen Funktion und dienstlichen Erreichbarkeit von leitenden Mitarbeitern sowie Mitarbeitern mit regelmäßigen Außenkontakten vertretbar, wobei auf die Umstände des jeweiligen Einzelfalles abzustellen ist.

Die – auch vor dem Hintergrund der Fürsorgepflicht des Dienstherrn oder Arbeitgebers – zu berücksichtigenden Interessen des Beschäftigten können ferner dazu führen, dass (bestimmte) personenbezogene Daten eines Beschäftigten nicht in Verzeichnissen veröffentlicht werden dürfen, etwa wenn bei seiner Tätigkeit das Risiko überdurchschnittlich hoch ist, dass er im privaten Bereich belästigt wird. Der Betroffene hat zudem nach § 4 Abs. 6 LDSG das Recht, gegenüber der Verarbeitung seiner Daten, auch wenn sie ansonsten rechtmäßig ist, ein schutzwürdiges, in seiner persönlichen Situation begründetes Interesse einzuwenden. Macht ein Betroffener von diesem Einwendungsrecht Gebrauch, so ist die Datenverarbeitung nur zulässig, wenn eine Abwägung ergeben hat, dass sein Interesse hinter dem öffentlichen Interesse an der Verarbeitung (hier: der Veröffentlichung) zurückzustehen hat. Aus Sicht des Datenschutzes sind die Beschäftigten vorab darauf hinzuweisen, dass sie ihre gegen eine Bekanntgabe ihrer Daten sprechenden Interessen geltend machen können.

Ist die Bekanntgabe von Daten eines Beschäftigten nur mit dessen Einwilligung zulässig, so darf sie nur erfolgen, wenn er – nach Aufklärung u. a. über die beabsichtigte Datenverarbeitung und deren Zweck gemäß § 4 Abs. 2 LDSG – schriftlich eingewilligt hat. Sollen Daten ins Internet eingestellt werden, so hat die Aufklärung aus Sicht des Datenschutzes auch die damit verbundenen Risiken zu umfassen. Doch nun zu den einzelnen Fallgestaltungen:

1.4.1 Der Vertretungsplan für Lehrer im Internet

Dieser darf nach den dargestellten Grundsätzen nur mit Einwilligung der betroffenen Lehrer ins Internet eingestellt werden, denn es ist nichts dafür ersichtlich, dass die Daten von Lehrern in Vertretungsplänen weltweit abrufbar sein müssen, etwa um den Unterricht in Vertretungsfällen sicherzustellen. Dies gilt auch, wenn ein Vertretungsplan lediglich Namenskürzel enthalten soll, die den Lehrern zuzuordnen sind.

1.4.2 Der Geschäftsverteilungsplan einer Universität im Internet

§ 125a Abs. 5 des Universitätsgesetzes (UG) stellt eine besondere Rechtsgrundlage für die Veröffentlichung von Daten der Beschäftigten der Universitäten dar. Diese umfasst, wie der Gesetzesbegründung zu entnehmen ist, auch die Veröffentlichung im Internet (vgl. LT-Drs. 12/4404, S. 262). Bei der Veröffentlichung von Beschäftigtendaten ist danach für die Universitäten zu differenzieren. Geht es um Professoren, Hochschul- und Privatdozenten, Mitarbeiter des wissenschaftlichen Dienstes, Lehrbeauftragte, Lehrkräfte für besondere Aufgaben sowie sonstige Mitarbeiter, die herausgehobene Funktionen in der Universität wahrnehmen, so sind Veröffentlichungen bei Angaben über die dienstliche Erreichbarkeit zulässig; ohne Einwilligung jedoch nur Name, Amts-, Dienst- und Funktionsbezeichnung, Telefon- und Telefaxnummern sowie E-Mail- und Internet-Adressen. Diese Beschäftigten können der Veröffentlichung widersprechen, wenn ihr schutzwürdiges Interesse wegen ihrer besonderen persönlichen Situation das Interesse der Universität an der Veröffentlichung überwiegt; dies setzt nach der Gesetzesbegründung (vgl. LT-Drs. 12/4404, S. 262) voraus, dass die Universität die betroffenen Beschäftigten vor der Veröffentlichung informiert. Andere Angaben zu den oben aufgeführten Beschäftigten und alle Angaben zu den übrigen Beschäftigten dürfen nur mit deren Einwilligung veröffentlicht werden.

Gleichwohl hatte eine Universität ihr Personalverzeichnis ins Internet eingestellt, das auch Daten von Beschäftigten enthielt, die nicht zu dem in § 125 a Abs. 5 Satz 1 UG genannten Personenkreis gehörten, wie etwa Beschäftigte in Sekretariaten, in der Registratur, im Archiv, im Schreibdienst und im Reinigungsdienst; die dafür erforderlichen schriftlichen Einwilligungen dieser Beschäftigten hatte die Universität nicht eingeholt. Wir beanstandeten diesen datenschutzrechtlichen Verstoß und forderten die Universität auf, die Rechtslage künftig zu beachten.

1.4.3 Namen der Leiter der Fachbereiche und Sachgebiete einer Stadtverwaltung in einer Bürgerinformationsbroschüre

Eine Stadt wollte wissen, ob sie die Leiter von Fachbereichen und Sachgebieten der Stadtverwaltung auch ohne deren Einwilligung namentlich in ihrer gedruckten städtischen Bürgerinformationsbroschüre nennen darf.

Wir haben der Stadt geantwortet, dass sie dies dürfe, um eine unmittelbare Kontaktaufnahme mit diesen leitenden Beschäftigten zu ermöglichen, soweit dem nicht im Einzelfall deren Interessen entgegenstünden.

1.4.4 Der Vorname des Beschäftigten – besonders geschützt?

Von Interesse für Behörden wie Beschäftigte war die Frage, ob für eine Bekanntgabe (auch) des Vornamens strengere Voraussetzungen gelten als für die Bekanntgabe (nur) des Nachnamens, sei es auf Namens- und Türschildern oder in einer städtischen Bürgerinformationsbroschüre.

Diese Frage ist generell zu verneinen: Wenn der Dienstherr oder Arbeitgeber ohne Einwilligung des Beschäftigten dessen Namen bekannt geben darf, so umfasst dies dessen Vor- und Nachname, denn diese gehören zur vollständigen Bezeichnung einer Person. Jedoch kann im Einzelfall das Interesse des Beschäftigten der Bekanntgabe seines Vornamens entgegenstehen.

1.5 Der ausländische Stellenbewerber und die Ausländerakte

Darf das Personalamt auf den Inhalt der Ausländerakte über einen ausländischen Stellenbewerber zugreifen, um festzustellen, ob er strafrechtlich in Erscheinung getreten ist?

Die Antwort auf diese Frage einer Stadtverwaltung hängt davon ab, inwieweit das Personalamt Daten aus der Ausländerakte überhaupt zur Aufgabenerfüllung benötigt und ob es sich wegen der Angaben oder Unterlagen nicht unmittelbar an den Bewerber wenden muss.

Zur Aufgabenerfüllung benötigt das Personalamt diejenigen Daten, die es kennen muss, um über die Besetzung der Stelle entscheiden zu können. Strafrechtlich bedeutsame Vorgänge muss das Personalamt dazu lediglich kennen, soweit sie nach einem objektiven Maßstab für die in Rede stehende Tätigkeit von Bedeutung sind. Nicht zur Aufgabenerfüllung erforderlich ist zudem die Kenntnis solcher Straftaten eines Bewerbers, die er nach § 53 des Bundeszentralregistergesetzes nicht zu offenbaren braucht, weil andernfalls diese Vorschrift umgangen würde. Weiter können bei ausländischen Bewerbern Angaben zu Pass oder Passersatz, Aufenthaltsgenehmigung und Arbeitserlaubnis erforderlich sein.

Dass das Personalamt bestimmte Daten aus der Ausländerakte zur Aufgabenerfüllung benötigt, bedeutet jedoch noch nicht, dass es diese bei der Ausländerbehörde anfordern darf. Vielmehr muss das Personalamt den Grundsatz der Datenerhebung beim Betroffenen und dessen Recht auf informationelle Selbstbestimmung beachten; das Personalamt muss die erforderlichen Daten daher in erster Linie beim Bewerber selbst erheben. An die Ausländerbehörde darf es sich grundsätzlich nur wenden, wenn es Angaben des Bewerbers überprüfen muss, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit vorliegen. Ansonsten muss das Personalamt, etwa wegen noch fehlender Unterlagen, auf den Bewerber zugehen und diesem die Entscheidung überlassen, die Unterlagen nachzureichen (und damit Daten über sich weiterzugeben) oder andernfalls eine Ablehnung der Bewerbung wegen unvollständiger Unterlagen in Kauf zu nehmen; auf eine solche drohende Ablehnung der Bewerbung hat das Personalamt den Bewerber bei der Nachforderung von Unterlagen hinzuweisen. Unabhängig davon darf sich das Personalamt wegen Daten über den Bewerber an die Ausländerbehörde wenden, wenn der Bewerber nach entsprechender Belehrung wirksam eingewilligt hat (§ 4 LDSG); die Ausländerbehörde darf dem Personalamt dann diese Daten mitteilen.

2. Volljährig – aber nicht für die Schule?

Dürfen Schulen die Eltern über schulische Angelegenheiten ihrer volljährigen Kinder unterrichten, auch wenn diese nicht eingewilligt haben? Diese Frage wurde nach dem Amoklauf eines ehemaligen Schülers an einem Erfurter Gymnasium laut, nachdem seine Eltern über seinen Schulverweis nicht informiert worden waren, weil er mit 19 Jahren bereits volljährig war.

In Baden-Württemberg stellt sich die Rechtslage wie folgt dar: Sobald ein Schüler volljährig ist, darf die Schule ohne seine ausdrückliche Einwilligung seine Eltern grundsätzlich nicht mehr über seine schulischen Angelegenheiten unterrichten, denn mit Vollendung des achtzehnten Lebensjahres (§ 2 des Bürgerlichen Gesetzbuches [BGB]) endet die elterliche Sorge (d. h. die Pflicht und das Recht der Eltern, für ihr Kind zu sorgen) und damit auch die gesetzliche Vertretung durch die Eltern (§ 1626 Abs. 1, § 1629 Abs. 1 BGB). Vor dem Hintergrund ihrer Fürsorgepflicht darf die Schule in extremen Ausnahmefällen die Eltern volljähriger Schüler jedoch auch ohne deren Einwilligung informieren. Dies gilt beispielsweise dann, wenn ein volljähriger Schüler selbstmordgefährdet ist und die Schule ihrer Fürsorgepflicht nur nachkommen kann, indem sie seine Eltern benachrichtigt. Gleiches gilt, wenn es nach den Umständen des konkreten Einzelfalls in absehbarer Zeit hinreichend wahrscheinlich ist, dass der volljährige Schüler die Rechte anderer Schüler oder Lehrer, etwa auf Leben oder körperliche Unversehrtheit, schwerwiegend beeinträchtigt, und die Schule die Eltern benachrichtigen muss, um diese Gefahr abzuwenden.

Eine weitergehende Benachrichtigung der Eltern volljähriger Schüler ist nach dem geltenden Recht in Baden-Württemberg nicht erlaubt. Sie wäre – als Eingriff in das Grundrecht der volljährigen Schüler auf informationelle Selbstbestimmung – nur auf Grund einer neuen gesetzlichen Regelung

zulässig. Dabei darf das berechtigte Anliegen, Rechtsgüter Dritter zu schützen, nicht den Blick darauf verstellen, dass eine solche Regelung im überwiegenden Allgemeininteresse liegen und dem Verhältnismäßigkeitsgrundsatz entsprechen muss. Dazu wäre u. a. zu fragen: Ist das Geschehen in Erfurt – als Grund für eine Gesetzesänderung – verallgemeinerungsfähig? Kann eine Benachrichtigung der Eltern in einer solchen Situation eine Straftat verhindern oder bewirkt sie – weil sie gegen den Willen des volljährigen Schülers erfolgt – eher das Gegenteil? Wie groß ist der Einfluss von Eltern auf ihr Kind, wenn dieses ihnen Schulprobleme nicht von sich aus mitteilt?

Nach unserer Auffassung ist keine Änderung des geltenden Rechts geboten. Der Staat sollte sich vielmehr aus dem Verhältnis der Eltern zu ihren volljährigen Kindern grundsätzlich heraushalten.

3. Datenschutz und Steuerrecht

Auch im Jahr 2002 hat der Bundesgesetzgeber eine Reihe von Steuergesetzen mit datenschutzrechtlichen Auswirkungen erlassen. Dass Steuergesetze oftmals mit finanziellen Belastungen für die Steuerpflichtigen verbunden sind, liegt in der Natur dieser Materie. Die jüngst erlassenen Steuergesetze enthalten darüber hinaus aber in zunehmendem Maße auch Vorschriften, die eine immer weiter gehende Überwachung der Bürger durch den Staat ermöglichen.

3.1 Steuergesetzgebung

So ist am 1. Juli 2002 das Gesetz zur weiteren Fortentwicklung des Finanzplatzes Deutschland (Viertes Finanzmarktförderungsgesetz) in Kraft getreten. Es befasst sich hauptsächlich mit der Änderung des Börsen- und Kapitalmarktrechts, um die rechtlichen Rahmenbedingungen für den Finanzplatz Deutschland zu modernisieren und dem raschen Strukturwandel der internationalen Kapitalmärkte anzupassen. Auch wollte der Gesetzgeber den Anlegerschutz stärken. Darüber hinaus sollte als Antwort auf die Terroranschläge in den USA ein Instrumentarium geschaffen werden, mit dem sich Konten terroristischer Organisationen und von Einzeltätern leichter aufdecken lassen. Deswegen hat das Vierte Finanzmarktförderungsgesetz dem Gesetz über das Kreditwesen einen § 24 c hinzugefügt, der alle Kreditunternehmen verpflichtet, Konten- und Depotnummern sowie Namen, Geburtstag und Anschrift sämtlicher Konteninhaber oder anderer Berechtigter in einem automatisierten Datenverarbeitungssystem zu speichern und zum Abruf durch die zuständige Aufsichtsbehörde bereitzuhalten. Diese darf die Datei insbesondere zum Aufspüren von Gewinnen aus schweren Straftaten und zur Bekämpfung der Geldwäsche nutzen. Eine derart weitgehende behördliche Zugriffsbefugnis auf Daten, die eigentlich dem Bankgeheimnis unterliegen, lässt nachteilige Auswirkungen auf das Vertrauensverhältnis zwischen den Kreditinstituten und ihren Kunden befürchten. Dabei drängen sich erhebliche Zweifel auf, ob diese Maßnahme überhaupt geeignet ist, den vom Gesetzgeber beabsichtigten Zweck zu erfüllen. Es ist eher folgende Konsequenz zu erwarten: Konten, die tatsächlich der Finanzierung terroristischer Aktivitäten oder der Geldwäsche dienen, werden künftig nur noch in Ländern unterhalten, in denen es derartige Kontrollen nicht gibt mit der Folge, dass in Deutschland von dem neuen Gesetz in weit geringerem Maß Konteninhaber mit hoher krimineller Energie, sondern in erster Linie nahezu alle unbescholtenen Bürgerinnen und Bürger betroffen sein werden.

Ein anderes Ziel, das der Bundesgesetzgeber im Jahr 2002 verfolgt hat, ist die Bekämpfung der Schwarzarbeit und des Leistungsmissbrauchs. Wenn diese Absicht auch begrüßenswert erscheinen mag, so war sie doch mit einer weiteren Einschränkung des Steuergeheimnisses verbunden. Es wurde nämlich mit Wirkung vom 1. August 2002 der § 31 a der Abgabenordnung so geändert, dass die Finanzämter nunmehr Daten, die grundsätzlich durch das Steuergeheimnis besonders geschützt sind, in Verfahren zur Bekämpfung der illegalen Beschäftigung oder der Schwarzarbeit sowie von Missständen bei der Arbeitnehmerüberlas-

sung den zuständigen Stellen in jedem Fall zwingend zugänglich machen müssen. Bisher durften sie das nur, wenn der Betroffene schuldhaft seine steuerlichen Pflichten verletzt hatte.

Auch das Kraftfahrzeugsteuergesetz hat eine Änderung erfahren. Schon bisher konnten die Landesregierungen bestimmen, dass bei der Zulassung eines Kraftfahrzeugs die Aushändigung des Fahrzeugscheins davon abhängig gemacht wird, ob der künftige Halter seine Kraftfahrzeugsteuer für einen bestimmten Zeitraum im Voraus bereits entrichtet oder eine Bankeinziehungsermächtigung für diese Abgabe erteilt hat. Nach der seit dem 8. August 2002 geltenden Novellierung neu hinzu gekommen ist, dass auch vorgeschrieben werden kann, dass die Aushändigung des Fahrzeugscheines nur in Frage kommt, wenn sicher ist, dass der Fahrzeughalter keine Kraftfahrzeugsteuerrückstände hat. Um dies zu überprüfen, soll es möglich sein, dass die Zulassungsbehörden bei einer Vielzahl von Finanzämtern nachfragen dürfen oder selbst unmittelbaren Zugriff auf die Kraftfahrzeugsteuerdaten des Betroffenen erhalten. Eine Regelung, nach der der Halter durch Vorlage einer Bescheinigung der Finanzverwaltung bei der Zulassungsstelle selbst belegen muss, dass er in der Vergangenheit liegende Steuerforderungen beglichen hat, wäre sicher der Intention des Gesetzgebers genauso gerecht geworden, hätte aber eher das Steuergeheimnis und den Grundsatz der Verhältnismäßigkeit gewahrt.

Bei den angesprochenen Steuergesetzen handelt es sich um Bundesgesetze. Sie werden vom Bundestag beschlossen, die Länder wirken aber in der Regel bereits bei der Erarbeitung der Referentenentwürfe in den Bundesministerien, spätestens jedoch über den Bundesrat am Gesetzgebungsverfahren mit. Um eine optimale Berücksichtigung von datenschutzrechtlichen Belangen beim Erlass von Bundesgesetzen zu gewährleisten, sind die zuständigen Ministerien unseres Landes gehalten, rechtzeitig mit dem Landesbeauftragten für den Datenschutz Verbindung aufzunehmen, um uns Gelegenheit zur Stellungnahme zu dem Gesetzgebungsvorhaben zu geben, damit die Ministerien unsere Bedenken und Anregungen gegenüber dem Bund vortragen können. Obwohl besagte Gesetze von erheblicher datenschutzrechtlicher Relevanz sind, hat es das für diesen Bereich in Baden-Württemberg zuständige Finanzministerium unterlassen, unser Amt einzuschalten. Das widerspricht nicht zuletzt wiederholten Zusagen der Landesregierung, uns unaufgefordert Referentenentwürfe von Bundesvorschriften zur Äußerung vorzulegen (so z. B. Stellungnahme der Landesregierung zum 5. Tätigkeitsbericht, LT-Drs. 9/1475, S. 37). Nur wenn eine frühzeitige Beteiligung am Erlass von Rechtsvorschriften auch des Bundes gewährleistet ist, ist es uns möglich, der unserem Amt nach § 31 LDSG übertragenen Beratungsaufgabe gerecht zu werden und darauf hinzuwirken, dass bei der Schaffung neuer Datenverarbeitungsregelungen dem Grundrecht auf Datenschutz in angemessener Weise Rechnung getragen wird. Wir haben uns deswegen an das Finanzministerium gewandt. Dort hat man erneut versichert, Referentenentwürfe von datenschutzrelevanten Gesetzgebungsvorhaben des Bundes im Bereich des Steuerrechts dem Landesbeauftragten für den Datenschutz wieder unaufgefordert zuzuleiten.

3.2 Offenbarung der Steuernummer

Bereits im Jahr 2001 sind zwei Steuergesetze ergangen, die die Bürger zwingen, ihre Steuernummern in großem Stil zu offenbaren. So verlangt der am 1. Januar 2002 in Kraft getretene § 48 b des Einkommensteuergesetzes, dass bestimmte Auftraggeber für Bauleistungen im Inland einen Steuerabzug von 15 % der Gegenleistung vorzunehmen und den Betrag an die zuständige Finanzkasse abzuführen haben, es sei denn, der Unternehmer hat dem Bauherrn eine vom Finanzamt ausgestellte Freistellungsbescheinigung vorgelegt. Die Richtigkeit dieser Freistellungsbescheinigung muss der Bauherr durch Rückfrage beim ausstellenden Finanzamt oder durch eine Anfrage beim Bundesamt für Finanzen per E-Mail überprüfen. War sie gefälscht, läuft er Gefahr, seinerseits für den nicht oder zu niedrig abgeführten Abzugsbetrag einste-

hen zu müssen. Dazu schreibt das Gesetz vor, dass in der Freistellungsbescheinigung Name, Anschrift und Steuernummer des Unternehmers, Geltungsdauer der Bescheinigung, Umfang der Freistellung, unter Umständen der Bauherr sowie das ausstellende Finanzamt anzugeben sind. Außerdem wird die Freistellungsbescheinigung mit einer 12-stelligen Sicherheitsnummer versehen. Diese und die Steuernummer des Unternehmers muss der Bauherr angeben, wenn er die Richtigkeit der Freistellungsbescheinigung beim Bundesamt für Finanzen per E-Mail abklären will.

Ein weiteres Gesetz mit vergleichbaren Auswirkungen ist das Steuerverkürzungsbekämpfungsgesetz. Dieses hat mit Wirkung vom 19. Dezember 2001 in § 14 des Umsatzsteuergesetzes einen Absatz 1a eingefügt, der die Unternehmer verpflichtet, ab dem 1. Juli 2002 ihre Steuernummer auf ihren Rechnungen anzugeben. Dadurch soll es den Finanzbehörden erleichtert werden, im Zuge von Außenprüfungen beim zuständigen Finanzamt festzustellen, ob der Rechnungsbetrag tatsächlich versteuert worden ist.

Dass die Steuernummer in immer größerem Umfang Dritten offenbart werden muss, stößt – wie mehrere Eingaben besorgter Geschäftsleute zeigen – nicht nur bei Datenschützern auf Kritik. Auch das Justizministerium hat Bedenken bekundet. Der § 48 b des Einkommensteuergesetzes erscheint uns nicht zuletzt deswegen problematisch, weil die Angabe der Steuernummer des Unternehmers auf der Freistellungsbescheinigung gar nicht erforderlich ist, damit der Bauherr seiner Verpflichtung nachkommen kann, die Richtigkeit einer ihm vorgelegten Freistellungsbescheinigung durch Rückfrage beim ausstellenden Finanzamt oder beim Bundesamt für Finanzen zu überprüfen. Dazu genügen nämlich die sonstigen auf der Freistellungsbescheinigung aufgeführten Personalien und die jeweils vergebene Sicherheitsnummer. Hinzu kommt, dass je größer der Kreis derjenigen ist, dem die Steuernummer eines Steuerpflichtigen bekannt ist, das Risiko desto größer wird, dass sich Dritte z. B. durch telefonische Anfragen beim Finanzamt Kenntnis von den steuerlichen Verhältnissen eines Steuerpflichtigen verschaffen können.

Diese Befürchtung haben wir zum Anlass genommen, der Sache nachzugehen. Dabei hat sich gezeigt, dass die Finanzämter in der Tat fernmündlich Auskünfte geben und Steuerfälle unter Umständen am Telefon besprechen. Allerdings wurde uns versichert, dass sie dies nur tun würden, wenn der Anrufer den Eindruck vermittelt, dass er über den Fall Bescheid weiß, andernfalls würde das Telefongespräch abgebrochen. Die bloße Angabe einer Steuernummer reiche dafür nicht aus. Auf diese Verfahrensweise könne man aus praktischen Gründen nicht verzichten, da es weder den Steuerbürgern noch den Mitarbeitern der Finanzämter zumutbar sei, sämtliche Steuerangelegenheiten schriftlich oder durch persönliche Vorsprache abzuwickeln. In der Tat ist uns bislang kein Fall bekannt geworden, in dem es ein Anrufer geschafft hat, etwas zu den Steuerangelegenheiten eines anderen in Erfahrung zu bringen, nachdem er dessen Steuernummer angegeben hatte.

5. Teil: Technik und Organisation

1. Europäische Entwicklungen

Mehr und mehr beeinflussen Richtlinien und andere Entscheidungen von Rat und Parlament der Europäischen Union (EU) die rechtliche Entwicklung in den Mitgliedstaaten. Wer wissen will, welche Themen demnächst im nationalen Bereich oder auf Ebene der Bundesländer auf der Tagesordnung stehen, tut gut daran, sich über die entsprechenden europäischen Vorhaben zu orientieren. In folgenden Zusammenhängen erfolgen gegenwärtig wichtige Weichenstellungen für den Datenschutz:

1.1 Die neue Kommunikationsrichtlinie

Maßgeblichen Einfluss auf die nationale Gesetzgebung wird die Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2002 entfalten. Sie sieht unter anderem Folgendes vor:

– Information der Nutzer über Sicherheitsrisiken

Diensteanbieter werden verpflichtet, Sicherheitsmaßnahmen zu ergreifen und die Nutzer über alle besonderen Risiken der Verletzung der Netzsicherheit zu unterrichten.

– Schutz vor heimlichem Ausspionieren

In der Vergangenheit mehrten sich Meldungen über die Verwendung von Techniken, die beispielsweise als Spy-Ware, Web-Bugs oder Hidden Identifiers bezeichnet wurden und mit deren Hilfe sich das Verhalten von Internet-Nutzern sowie die auf deren PC gespeicherten Daten heimlich auskundschaften ließen. Die Verwendung dieser oder ähnlicher Techniken darf künftig nur mit Wissen der betreffenden Nutzer erfolgen. Der heimliche Einsatz wird damit untersagt.

– Verwendung von Cookies

Cookies, die möglicherweise auch genutzt werden können, um Interessenprofile von Internet-Nutzern zu erstellen, dürfen künftig nur verwendet werden, wenn der Nutzer dazu seine Einwilligung „in Kenntnis der Sachlage“ gegeben hat. Die Informationen darüber müssen klar und umfassend und sollen „so benutzerfreundlich wie möglich“ sein.

– Standortdaten in Mobilfunknetzen

Sofern es möglich ist, den Standort eines Teilnehmers in einem Mobilfunknetz präziser zu bestimmen, als der Betrieb des Netzes dies erfordert, dürfen solche Daten nur mit ausdrücklicher Einwilligung der Teilnehmer ermittelt, gespeichert und verarbeitet werden. Ferner sollen die Nutzer die Möglichkeit haben, die genauere Verarbeitung von Standortdaten zeitweise gebührenfrei zu unterbinden.

– Mehr Schutz vor SPAM-Mail, Telefax-Werbung und anderen Werbenachrichten

Unerbetene Werbung, vor allem solche, die per E-Mail (SPAM-Mail) oder per Telefax versandt wird, belästigt viele Teilnehmer. Die Richtlinie gestattet daher die Verwendung von automatischen Anrufsystemen, Faxgeräten oder elektronischer Post für die Zwecke der Direktwerbung nur nach vorheriger Einwilligung der Empfänger. Zweifellos stellt dies einen Fortschritt zum Schutz der Netzteilnehmer dar. Gleichwohl kann auch diese Richtlinie keinen umfassenden Schutz vor unerwünschten Werbesendungen bieten, denn sie eröffnet keine Möglichkeit, gegen Absender vorzugehen, die aus dem außereuropäischen Ausland tätig werden.

Die Richtlinie behandelt zum einen Telekommunikationsdienste (z. B. Angebot von Sprachtelefonie in Fest- oder Mobilnetzen) und zum anderen aber auch die Ebene der Tele- und Mediendienste. Diese beiden Bereiche werden bislang im deutschen Recht noch getrennt voneinander behandelt. In der Praxis führt dies immer wieder zu Abgrenzungsschwierigkeiten. Wenn die Richtlinie Anstoß gäbe, auch im nationalen Recht das Telekommunikations- sowie das Teledienstерecht zusammenzuführen oder zumindest besser als bisher aufeinander abzustimmen, könnte dies die praktische Handhabung erleichtern.

1.2 eEurope – eine Informationsgesellschaft für alle

Bereits seit einigen Jahren unterstützt die EU im Rahmen ihres Projekts „eEurope“ verschiedene Vorhaben zum Ausbau der Informationsgesellschaft. In diesem Jahr beschloss der Europäische Rat, dieses Projekt nun unter dem Titel „eEurope 2005“ für weitere drei Jahre fortzuführen. Lag der Schwerpunkt des Vorgängerprogramms noch auf der Verbreitung von Internet-Anschlüssen, so will das in diesem Jahr beschlossene Fortsetzungsprogramm unter anderem auch das Bewusstsein dafür schärfen, „dass die Online-Welt sicherer werden muss“, und ferner den Aufbau einer sicheren Informationsinfrastruktur fördern.

Dabei sollen Sicherheitslücken in Kommunikationsnetzen und -diensten sowie deren gegenseitige Abhängigkeiten untersucht und der Aufbau vertrauenswürdiger Netz- und Informationsinfrastrukturen unter besonderer Berücksichtigung neu aufkommender Technologien (z. B. Breitbandanschlüsse, drahtlose Übertragung) unterstützt werden.

Erklärtes Ziel des Projekts „eEurope 2005“ ist zudem, dass sich bis Ende 2005 durch Einführung entsprechend gestalteter Produkte und Arbeitsabläufe eine Sicherheitskultur „beim Entwurf und der Implementierung von Informations- und Kommunikationsprodukten“ eingestellt haben soll. Dabei sollen Projekte, bei denen es darum geht, „gute Praktiken und Standards“ bei der Entwicklung sicherer Produkte zu etablieren, ebenso gefördert werden wie Projekte, die darauf hinarbeiten, „die Sicherheitsrisiken allen Nutzern bewusst zu machen“.

Aus Sicht des Datenschutzes ist es sehr zu begrüßen, dass diese Ziele europaweit anerkannt und mit den Mitteln der EU gefördert werden. Nicht übersehen werden darf jedoch, dass das Projekt „eEurope 2005“ daneben auch Ziele anstrebt, die leicht mit dem Datenschutz in Konflikt geraten können. Insbesondere die auf eine Intensivierung der Strafverfolgung gerichteten Maßnahmen können vielfältige datenschutzrechtliche Probleme aufwerfen.

Die datenschutzrechtliche Ambivalenz des Projekts „eEurope 2005“ verhindert auch, dass sich gegenwärtig schon absehen ließe, wie die geplante Einrichtung eines „Sonderstabes für Computer- und Netzsicherheit“ datenschutzrechtlich zu bewerten ist. Klar ist jedenfalls, dass dieser Sonderstab ein Fachzentrum für Sicherheitsfragen werden, den Aufbau eines europäischen Warnsystems gegen Computerangriffe in die Wege leiten sowie die grenzüberschreitende Zusammenarbeit in Fragen der IT-Sicherheit unterstützen soll. Ganz im Sinne des Datenschutzes kann er dabei wirken, wenn er Sicherheitslücken aktuell verfügbarer oder gerade entwickelter Techniken untersucht und technische Entwicklungen fördert, die diese Lücken schließen. Sofern es dort jedoch nicht um die Beseitigung von Sicherheitslücken, sondern lediglich darum gehen sollte, deren Ausnutzung für unlautere oder strafbare Absichten entgegenzuwirken, etwa indem den Netzbetreibern und Diensteanbietern zusätzliche Unterstützungs- und Mitwirkungsleistungen gegenüber Strafverfolgungsbehörden oder Geheimdiensten auferlegt werden, so wird genau darauf zu achten sein, dass die dafür vorgesehenen Maßnahmen das Grundrecht der Bürger auf Datenschutz nicht unverhältnismäßig einschränken.

Auch wenn gegenwärtig noch manche Fragen in diesem Zusammenhang offen sind, ist doch zu begrüßen, dass die IT-Sicherheit als wesentliches Kriterium für den erfolgreichen Betrieb elektronischer Dienste und

Netze identifiziert und Maßnahmen auf verschiedenen Ebenen gefördert werden sollen, um das Sicherheitsniveau zu erhöhen.

2. Rund ums Internet

Die vielfältigen Nutzungsmöglichkeiten des Internets durch öffentliche Stellen und die von öffentlichen Stellen zusammengestellten Informationsangebote für die Bürger gaben auch in dieser Berichtsperiode Anlass zu Stellungnahmen, Beurteilungen und Beratungen. In diesem Abschnitt werden Einzelfälle getrennt nach Angeboten und Nutzung unter dem Blickwinkel des technischen Datenschutzes dargestellt.

2.1 Internet-Zugänge und Internet-Nutzung

2.1.1 Das Land und das Internet

Die Überlegungen des Staatsministeriums, jedem Mitarbeiter der Landesverwaltung den Zugriff auf das Internet am Arbeitsplatz zur Verfügung zu stellen, haben wir bereits im vorangegangenen Tätigkeitsbericht angesprochen (vgl. 22. Tätigkeitsbericht, LT-Drs. 13/520, S. 38). Auch in der Berichtsperiode beschäftigte uns das Thema in Form der „Konzeptionsstudie für eine sichere Internet-Anbindung der Landesbehörden Baden-Württembergs“. Die Endfassung dieser Studie hat Defizite, die angesprochen werden müssen. Im Einzelnen war zu der Studie Folgendes zu sagen:

- Die Studie ist technisch überholt und nicht auf zukünftige Entwicklungen ausgerichtet. Sie baut in wesentlichen Teilen auf Vorarbeiten auf, die Inhalt einer Diplomarbeit aus dem Jahr 1999 waren und orientiert sich an mittlerweile überholten Internet-Protokollen; so wird versäumt, neuere und aktuelle Protokolle und Techniken auf ihre Sicherheitsrelevanz zu begutachten. Gegenüber der Vorversion der Studie, die im letzten Tätigkeitsbericht angesprochen wurde, sind zwar Protokolle wie Internet-Telefonie, Peer-to-Peer und spezifische Microsoft-Protokolle wie beispielsweise Passport aufgenommen worden. Zweifel bleiben aber, ob man die sich dabei ergebenden Fragen in wenigen Textzeilen umfassend beantworten kann.
- Die Studie setzt sich – auch in der Endfassung – zwar seitenlang mit Sicherheitsproblemen von Internet-Protokollen auseinander. Im Blick hat die Studie aber vielfach das Betriebssystem UNIX. Dies geht an der Wirklichkeit der EDV-Infrastruktur der Landesverwaltung vollkommen vorbei. Hierzu muss man nämlich wissen, dass in der Landesverwaltung nur sehr wenige Systeme mit dem Betriebssystem Unix betrieben werden. Insbesondere an den Arbeitsplätzen werden, mit Ausnahme einer kleinen Dienststelle, nur die diversen Spielarten der Windows-Betriebssysteme eingesetzt. Der Inhalt der Studie befasst sich also sachlich mit einer Systemumgebung, die in Baden-Württemberg die absolute Ausnahme darstellt. Dass dann aus der Studie keine die Systemsicherheit fördernden Erkenntnisse gezogen werden können, liegt auf der Hand.

Ergebnis der Studie ist, dass die Verantwortlichkeit einer Sicherheitstechnik für alle Nutzer an einer zentralen Stelle gebündelt sein und dass man in besonders sensiblen Bereichen auf die Verschlüsselung als Sicherheitstechnik zurückgreifen solle. Dies ist zwar richtig, ist aber nichts umwerfend Neues und stand so auch schon im Projektauftrag. Zur Verschlüsselung ist überdies zu sagen, dass jeweils einzelne Dokumente durch Eingabe eines Schlüssels ver- und entschlüsselt werden müssen. Ob diese Methode dann praktikabel ist, wenn ein Mitarbeiter auf eine große Anzahl von Dokumenten zugreifen muss, wird sich erweisen müssen. Eine transparente Verschlüsselung beispielsweise der Festplatte oder einzelner Verzeichnisse jedenfalls ist wirkungs-

los, da Schaden induzierende Software hierauf den gleichen Zugriff wie der Benutzer haben würde.

Insgesamt ist leider festzustellen, dass eine wesentliche Verbesserung der Systemsicherheit durch die Studie nicht eingetreten ist.

Bei einer Besprechung mit der für die Realisierung des Internet-Zugriffs für die Innenverwaltung zuständigen Dienststelle wurde uns mitgeteilt, dass man zunächst auf die sicherheitstechnisch und datenschutzrechtlich äußerst kritisch einzuschätzenden aktiven Inhalte wie JavaScript, Active-X und Java verzichten wolle, indem man an einer zentralen Stelle die aktiven Inhalte in allen abgerufenen WWW-Seiten entfernt. Dadurch wird zwar das Risiko auf ein annehmbares Maß reduziert, fraglich ist aber, wie lange sich diese Politik durchhalten lässt. Die Erfahrung zeigt, dass in viele WWW-Seiten kleine, in der Programmiersprache JavaScript geschriebene Programme – so genannte Skripte – eingebaut sind und sich der Inhalt dieser Seiten erst erschließt, wenn diese Skripte ausgeführt werden. Hier wird abzuwarten sein, ob dem Druck der Benutzer standgehalten werden kann, wenn diese darlegen, dass sie den ungefilterten Zugriff haben müssen.

Abschließend muss darauf hingewiesen werden, dass sich mit den so genannten Terminalserver-Techniken sehr sichere, in der Funktionalität nicht nennenswert eingeschränkte Internet-Zugänge realisieren lassen. Uns wurde dann auch mitgeteilt, dass man diese Technik zunächst in Pilotinstallationen für die Mitarbeiter nutzen will, die auf Seiten zugreifen müssen, die mit Filterung nicht mehr darstellbar sind. Der Nachteil dieser Techniken besteht in einem finanziellen Mehraufwand. Wie im richtigen Leben gilt eben auch im Internet: Sicherheit gibt es nicht umsonst.

2.1.2 Virtuelle private Netzwerke für Kommunen

Land und Kommunen nutzen umfangreiche Netzwerke zur Datenkommunikation. Jedoch ist deren Ausbau nicht so weit fortgeschritten, dass jede Dienststelle direkt und wirtschaftlich an eines dieser Netzwerke angebunden werden könnte. Dennoch müssen auch die Rechner dieser Dienststellen mit anderen Dienststellen des Landes Daten austauschen können. Die Lösung besteht darin, die Strecke bis zum nächsten Knoten des Kommunalen Verwaltungsnetzes durch die Nutzung von Netzen kommerzieller Anbieter zu überbrücken. Unsere Dienststelle wurde im Berichtszeitraum um Unterstützung bei der unter dem Aspekt des technischen Datenschutzes korrekten Vorgehensweise gebeten. Beabsichtigt ist, Gemeinden an das Kommunale Verwaltungsnetz über das Internet anzubinden. Folgende Aufgabenstellungen sind hierbei zu lösen:

- Die Authentizität der Kommunikationspartner muss auch dann, wenn eine Verbindung nicht einem einzelnen Mitarbeiter an seinem Arbeitsplatz zugeordnet werden kann, gewährleistet werden. Da meistens kleinere Netze von Gemeinden auf diese Weise angebunden werden, bestehen die Verbindungen darüber hinaus über einen wesentlich längeren Zeitraum.
- Die Integrität der übertragenen personenbezogenen Daten muss gewährleistet sein. Unbefugte dürfen keine Kenntnis der Daten erlangen und es muss ausgeschlossen werden, dass Unbefugte die übertragenen Daten verändern können.
- Auf der Eingangsseite des Verwaltungsnetzes muss sichergestellt werden, dass nur Verbindungen mit autorisierten Gemeindenetzen zustande kommen.

Unsere Dienststelle hat eine von dem Betreiber des Kommunalen Netzwerks vorgestellte Lösung auf der Basis eines virtuellen pri-

vaten Netzwerks (VPN) auf die Einhaltung dieser Anforderungen geprüft. Dabei erwies es sich als vorteilhaft, dass die Systemsicherheit der Komponenten eines VPN-Systems im Gegensatz etwa zu einem Stand-alone-PC eines Heimarbeitsplatzes einfacher zu realisieren ist und flankierende Maßnahmen, welche die Systemsicherheit gewährleisten, auf Grund der wesentlich geringeren Anfälligkeit derartiger Systeme für Angriffe weniger aufwändig sind.

2.1.3 Von guten und schlechten Nachrichten: SPAM-Mails

Wer ein elektronisches Postfach hat, dessen E-Mail-Adresse in einem öffentlichen Verzeichnis aufgeführt wird oder sonst eine entsprechende Verbreitung gefunden hat, kann ein Lied davon singen: Fast täglich wird man mit Nachrichten zugedeckt, deren Inhalt von Angeboten zum Kauf von Alkoholtestgeräten über Tätigkeiten als millionenschwerer Finanzagent bis hin zu zweifelhaften Angeboten vermeintlich junger Damen reicht. Diese so genannten SPAM-Mails, die über einen Verteiler an eine Vielzahl von Empfängern geschickt werden, sind nicht nur lästig, sondern nehmen, da man sie zumindest rudimentär bearbeiten muss, personelle und technische Ressourcen in Anspruch.

Wird der Austausch der E-Mail mit dem Internet über ein zentrales System durchgeführt, dann kann die Flut von SPAM-Mails zur Bedrohung der Funktionsfähigkeit des Nachrichtensystems werden. Auch wirken sich SPAM-Mails auf das Übertragungsvermögen der Leitungen aus und stören die notwendige Kommunikation möglicherweise so sehr, dass Systemfunktionen unterbunden oder Benutzer durch lange Antwortzeiten beeinträchtigt werden.

Man ist daher in der Landesverwaltung dazu übergegangen, sobald es Anzeichen für eine die Stabilität der Netze und Rechner beeinträchtigende SPAM-Mail-Flut gibt, die E-Mails auf einem zentralen System zu filtern. Hierzu wird der Betreff und der Inhalt gegen einen Katalog häufig in diesen Nachrichten auftretender Begriffe abgeglichen und bei einer bestimmten Trefferquote die Nachricht nicht dem Empfänger zugestellt. Anstatt auf den Inhalt abzuheben, kann die Filterung auch auf die Absenderadresse angewandt werden. Hierzu ist aus der Sicht des Datenschutzes Folgendes zu sagen:

- Eine nicht unerhebliche Anzahl von Mitarbeitern der Landesverwaltung, beispielsweise in der Steuerverwaltung oder im sozialen Bereich, unterliegt der besonderen Geheimhaltungspflicht. Nachrichten an diese Mitarbeiter dürfen unter keinen Umständen von Dritten gelesen werden, da sie Informationen und Daten enthalten könnten, die dieser Geheimhaltungspflicht unterliegen.
- Erlaubt der Dienstherr eine private Nutzung der E-Mail, dann wird er dadurch zum Anbieter von Telekommunikationsdiensten. Er hat dann die entsprechenden Regelungen des Telekommunikationsgesetzes (TKG) und der Telekommunikations-Datenschutzverordnung (TDSV) zu beachten.
- Wegen der gewählten Filtermethode kann nicht ausgeschlossen werden, dass Nachrichten mit beispielsweise finanziellem Bezug als SPAM-Mails klassifiziert werden, obwohl es sich um reguläre Nachrichten handelt. Eine Löschung der Nachricht darf daher erst dann durchgeführt werden, wenn zweifelsfrei feststeht, dass es sich um eine SPAM-Nachricht handelt.
- Wenn die Filterung auf die Absenderadresse abzielt, ist zu berücksichtigen, dass der Absender eine gefälschte, aber tatsächlich existierende Adresse verwenden könnte. Reguläre Nachrichten dieses Absenders werden dann auch als SPAM-Mails klassifiziert.

Die zuständige Dienststelle unterhält einen Zwischenspeicher, in dem sie gefilterte Nachrichten mehrere Tage vorhält, um bei Rückfragen die entsprechenden Nachrichten wieder zustellen zu können. Sie unterrichtet die Benutzerbetreuer außerdem darüber, wann und welche Filter eingesetzt werden beziehungsweise wann die Filterung ausgesetzt wird. Zu befürchten ist, dass uns weitere Auswüchse des SPAM-Unwesens auch künftig beschäftigen werden. Es bleibt zu hoffen, dass den Bestrebungen von Betroffenen, auf dem Klageweg der Verbreitung von SPAM-Mails entgegenzuwirken, Erfolg beschieden ist.

2.1.4 Wer darf ins Netz? – Internet-Surfen am Arbeitsplatz

Vorausgesetzt, eine Dienststelle hat ihr Computernetz mit dem Internet gekoppelt, stellt sich die Frage, welchen Mitarbeitern die Möglichkeit eröffnet wird, von ihrem Arbeitsplatz aus im Internet zu surfen. Dies war auch Gegenstand einer Kontrolle im Sozialdezernat eines Landratsamtes. Dort konnten alle Nutzer im Internet surfen, obwohl nur einzelne diese Zugriffsmöglichkeit dienstlich benötigten. Bei der Beurteilung dieses Sachverhalts ist Folgendes zu berücksichtigen: Auch wenn moderne Sicherheitstechniken wie Firewalls eingesetzt werden, die den Anschluss an das Internet an zentraler Stelle absichern, bleibt ein gewisses Restrisiko bestehen. Dies kann sich so auswirken, dass beim Surfen im Internet Schaden stiftende Programme auf den Computer gelangen und dort mitunter Daten ausspionieren, Hintertüren für Hackerangriffe öffnen oder sich wie ein Computervirus auf allen zur Verfügung stehenden Wegen weiterverbreiten. Um das damit akzeptierte Restrisiko so gering wie möglich zu halten, dürfen Berechtigungen zur Nutzung des WWW wie auch anderer Dienste des Internets nur in dem Umfang gewährt werden, wie dies dienstlich erforderlich ist.

2.1.5 Verwaltungs-PC der Schulen und Internet-Nutzung

Besondere Aspekte sind zu berücksichtigen, wenn schulische Verwaltungs-PC mit einem Internet-Anschluss versehen werden sollen. Die Besonderheiten ergeben sich daraus, dass zwar das Kultusministerium landesweit ausgerichtete EDV-Projekte plant, die EDV-Ausstattung den Schulen jedoch von den Kommunen zur Verfügung gestellt wird und daher sehr unterschiedlich sein kann. Da die PC der Schulverwaltung sowohl mit einem Netz des kommunalen Schulträgers als auch mit dem Netz der Kultusverwaltung gekoppelt sein können, muss ein Internet-Zugang solcher PC so gestaltet werden, dass er mit den Sicherheitsanforderungen der Kultusverwaltung wie auch mit denen des Schulträgers in Einklang steht. Dass dies nicht immer reibungslos klappt, illustriert folgendes Beispiel, das eine Stadt an uns herangetragen hat:

Die Stadt hatte als Schulträger Verwaltungs-PC der Schulen mit dem städtischen Netz gekoppelt, das seinerseits über einen geschützten zentralen Anschluss (Firewall) mit dem Internet verbunden war. Auf diesem Weg waren auch die Schulen aus dem Internet per E-Mail erreichbar. Unabhängig davon bot das Informationstechnische Fachzentrum der Kultusverwaltung (IFK) den Schulen die Möglichkeit, zentral beim IFK eingerichtete E-Mail-Postfächer für die Kommunikation im Internet zu nutzen. Der Zugriff auf diese E-Mail-Postfächer sollte seinerseits über das Internet erfolgen. Die Stadt war der Ansicht, dass die vom IFK bereitgestellte Möglichkeit zur E-Mail-Kommunikation nur eine geringere Sicherheit biete als die Anbindung der Schulen über das kommunale Netz. So eindeutig sahen wir die Dinge allerdings nicht. Unabhängig von der Art des Anschlusses sind in jedem Fall folgende Gesichtspunkte zu berücksichtigen:

– Setzen die Schulen Verwaltungs-PC ein, auf denen personenbezogene oder andere schutzbedürftige Daten gespeichert sind,

so müssen sie technische und organisatorische Maßnahmen ergreifen, um zu verhindern, dass unberechtigt auf diese Daten zugegriffen werden kann.

– Werden diese PC mit Computernetzen außerhalb des Verwaltungsbereichs der Schule verbunden, so gehen damit besondere Risiken für die gespeicherten Daten einher. Solche Koppelungen dürfen daher stets nur dann vorgenommen werden, wenn sie zur Aufgabenerfüllung der Schulen erforderlich sind und auch dafür entsprechende Schutzmaßnahmen ergriffen wurden. Dies gilt sowohl im Hinblick auf eine mögliche Koppelung der Schulverwaltungs-PC mit einem städtischen Netz wie auch für eine Koppelung mit Netzen der Schulverwaltung oder dem Internet.

Wenn eine Schule das Angebot der Kultusverwaltung nutzen und via Internet auf ihr beim IFK bereitgehaltenes Schulmail-Postfach zugreifen will, dürfen weder auf dem PC, an dem der Internet-Anschluss besteht, noch auf PC, mit denen dieser PC vernetzt ist, personenbezogene Daten gespeichert werden. Dies ist durch einen Erlass des Kultusministeriums entsprechend geregelt. Sofern auf dem mit dem Internet verbundenen Verwaltungs-PC keine personenbezogenen Daten gespeichert werden, wäre es keineswegs „äußerst unbefriedigend“, wie die Stadt meinte, sondern ein durchaus akzeptabler Lösungsweg, wenn über diesen PC die Schulmail-Post abgerufen würde.

Wird dagegen ein Schulverwaltungs-PC, auf dem personenbezogene Daten gespeichert sind, mit einem städtischen oder dem Landesverwaltungsnetz gekoppelt, so ist z. B. durch geeignete Filterregeln in einem zum Anschluss benutzten Router sowie durch datenschutzgerechte Nutzung von Wählverbindungen sicherzustellen, dass kein unbefugter Verbindungsaufbau möglich ist und nur die benötigten Dienste (hier insbesondere zum E-Mail-Versand und -Abruf), aber keine weiteren Dienste zum Informationsaustausch, genutzt werden können. Die zum Schutz der gespeicherten Daten erforderlichen technischen und organisatorischen Maßnahmen sind nicht zuletzt auch im Verfahrensverzeichnis gemäß § 11 LDSG schriftlich zu dokumentieren.

Werden per E-Mail über das Internet personenbezogene oder andere schutzbedürftige Daten versandt, sind diese zu verschlüsseln. Erfolgt auch der Datenaustausch zwischen Mail-Client und Mail-Server via Internet, sollte dafür ein Protokoll verwendet werden, bei dem die Passwörter nicht im Klartext übertragen werden.

Die hier dargestellten Überlegungen werden in einem anderen Licht erscheinen, wenn das landesweit angelegte Projekt „Schulverwaltung am Netz“ (SVN) umgesetzt wird. Damit soll den Schulverwaltungen ein sicherer Anschluss ans Internet ermöglicht werden, der beispielsweise sicherstellt, dass die zwischen Schulen oder auch zwischen Schulen und Schulverwaltung ausgetauschten E-Mails standardmäßig ebenso verschlüsselt werden wie Schulstatistikdaten, die die Schulen künftig elektronisch an die Schulverwaltung sowie das Statistische Landesamt übermitteln sollen.

2.2 Bausteine für e-Government

Im Jahr 2005 sollen sich, so hat es sich neben dem Bund auch Baden-Württemberg zum Ziel gesetzt, alle wesentlichen Dienstleistungen der Behörden auch elektronisch abwickeln lassen. Mit diesem Ziel vor Augen führen Bund, Länder und Gemeinden zahlreiche Projekte durch, die künftig als Bausteine zum Aufbau der im Internet rund um die Uhr erreichbaren „virtuellen Behörden“ dienen sollen. In diesem Jahr hatten wir Gelegenheit, uns mit einigen dieser Bausteine datenschutzrechtlich näher zu befassen:

2.2.1 Das e-Bürgerdienste-Portal des Landes

Wer künftig elektronische Bürgerdienste erledigt, soll, so ist es Wunsch der Landesregierung, nicht lange überlegen müssen, welche Behörde für sein Anliegen zuständig ist und wie er das dafür vorgesehene Internet-Angebot erreichen kann. Er soll vielmehr, ganz gleich, welches Anliegen er hat, zunächst eine zentrale Anlaufstelle, das so genannte e-Bürgerdienste-Portal, ansteuern können, das ihm beim Auffinden der zuständigen Stelle behilflich sein und ihn direkt mit dem Bürgerdienst verbinden soll. Datenschutzrechtlich von Bedeutung ist das Portal zum einen deshalb, weil vorgesehen ist, dass die Bürger darin personenbezogene Daten hinterlegen können, die sie für künftige behördliche Anträge immer wieder benötigen. Zum anderen ist datenschutzrechtlich von Belang, dass auch ein privates Unternehmen in die Verarbeitung personenbezogener Bürgerdaten einbezogen wird. Die mit dem Projekt insgesamt einhergehenden Datenschutzprobleme werden, dem schrittweisen Aufbau des Portals folgend, erst im Laufe der Zeit umfassend zu Tage treten. Aber bereits bisher wurde eine Reihe datenschutzrelevanter Aspekte dieses Vorhabens deutlich:

– Eckpunkte zum Datenschutz umsetzbar?

  Der zwischen Land und Auftragnehmer geschlossene Projektauftrag enthält mehrere datenschutzrechtlich positive Zielvorstellungen. So wurde vereinbart, dass

  • der Auftragnehmer beim Umgang mit personenbezogenen Daten den Grundsatz der Datensparsamkeit einzuhalten hat,

  • die Bürger die Möglichkeit erhalten sollen, ihre Daten, wo immer möglich, eigenverantwortlich zu verarbeiten,

  • die Bürger dazu beispielsweise einen personalisierten Zugang zu den über sie im Portal verschlüsselt gespeicherten Daten erhalten sollen, die weder von den beteiligten Behörden noch vom privaten Auftragnehmer, der das Portal betreibt, „ohne Zutun des Bürgers entschlüsselt werden können“.

  Führt man sich vor Augen, dass einige dieser Ziele in einem Spannungsverhältnis zueinander und zu den geplanten Funktionen des Portals stehen, so bleibt abzuwarten, in welchem Maß das Portal diesen Zielen gerecht werden wird. Um beispielsweise einem Nutzer nur die für ihn und seine Lebenssituation zuständigen Stellen und behördlichen Ansprechpartner nennen zu können, muss der Betreiber des Portals für einen geraumen Zeitraum im Klartext auf die vom Bürger hinterlegten personenbezogenen Daten zugreifen können. Dabei ist zumindest technisch nicht auszuschließen, dass die Daten des Bürgers kopiert und danach auch ohne dessen Mitwirkung von Dritten gelesen oder auf andere Weise verarbeitet werden können.

– Hinweise an Nutzer

  Gerade die Tatsache, dass das Portal zum einen die Möglichkeit zur eigenverantwortlichen Datenverarbeitung bieten, zum anderen aber auch behördliche Datenverarbeitungsvorgänge abwickeln und unterstützen soll, unterstreicht, wie wichtig es ist, den Bürgerinnen und Bürgern verständlich zu erläutern, welche personenbezogenen Daten auf welche Weise in dem Portal verarbeitet werden können. Dabei ist anzugeben, welche personenbezogenen Daten bei der Nutzung des Angebots oder auch nur einzelner Teilfunktionen verarbeitet werden, ob und wenn ja für welche Funktionen und für welche Zwecke Cookies verwendet werden sowie ob und wenn ja für welche Funktionen aktive Inhalte wie Java, JavaScript oder Active-X ge-

nutzt oder Techniken verwendet werden, die nur mit Hilfe spezieller Zusatzprogramme (z. B. Plug-Ins für den heimischen Browser) nutzbar sind. Damit die Nutzer u. a. ihr Recht auf Auskunft über die zu ihrer Person gespeicherten Daten geltend machen können, muss im Angebot außerdem, etwa in Form eines Impressums, angegeben werden, wer für den Inhalt des Angebots verantwortlich ist.

Bei einem so umfassend angelegten Vorhaben kommt es zudem darauf an, nicht nur einmalig geeignete Datenschutzhinweise zu formulieren, sondern durch geeignete Abläufe zu gewährleisten, dass bei allen künftigen Änderungen des Angebots, die von unterschiedlichen Beteiligten vorgenommen werden können, auch eine entsprechende Anpassung der Datenschutzhinweise sichergestellt wird.

– Umgang mit den im Portal hinterlegten Bürgerdaten

Das Portal soll den Bürgern die Möglichkeit bieten, persönliche Daten darin zu hinterlegen und darauf bei späteren elektronischen Behördengängen immer wieder zurückzugreifen. Dabei stellt sich das Problem der Löschung dieser Daten: Grundsätzlich sollten diese Daten nur so lange im Portal hinterlegt sein, wie der Bürger sie dort noch benötigt. Was aber tun, wenn ein Bürger etwa nach einem Umzug in ein anderes Bundesland die hinterlegten Daten nicht mehr für behördliche Anträge benötigt, er es aber versäumt, selbst die Löschung der Daten zu veranlassen? Sinnvoll ist es daher, wie von dem hier federführenden Innenministerium vorgesehen, die hinterlegten Daten mit einem Zeitstempel zu versehen, dem zu entnehmen ist, wann die Daten zuletzt genutzt wurden, und vorzusehen, dass diese gelöscht werden, sofern darauf über einen gewissen Zeitraum hinweg nicht zugegriffen wurde. Der vom Innenministerium dafür vorgesehene Zeitraum von zehn Jahren erscheint uns allerdings zu lang. Wir halten es für zweckmäßig, die Bürger nach einem Zeitraum von sechs bis zwölf Monaten ohne Zugriff über die bevorstehende Löschung zu informieren und ihnen dabei Gelegenheit zu geben, die Speicherdauer um weitere sechs bis zwölf Monate zu verlängern. Erfolgt darauf keine Antwort, so sollten die Daten nach Ablauf einer weiteren Frist von zwei bis drei Monaten gelöscht werden. Daneben sollten die Nutzer die Möglichkeit haben, ihre Daten jederzeit teilweise oder vollständig zu löschen.

– Problematik der Gästebuchfunktion

Internet-Angebote bieten gelegentlich „Gästebücher“, in die jeder Nutzer beliebige und für jeden Internet-Nutzer lesbare Mitteilungen eintragen kann. Auch das e-Bürgerdienste-Portal, so sieht es die Planung des Innenministeriums vor, soll eine Gästebuchfunktion bieten. Solche Gästebücher werden, das lehrt die Erfahrung, immer wieder auch dazu benutzt, verunglimpfende oder in anderer Weise die Persönlichkeitsrechte anderer Personen beeinträchtigende Äußerungen zu veröffentlichen. Da sich eine solche missbräuchliche Nutzung zum einen nicht zuverlässig verhindern lässt und die Funktion des Gästebuchs zum anderen nicht für die Abwicklung von Bürgerdiensten erforderlich ist, rieten wir davon ab, ein solches Gästebuch bereitzustellen.

– Rahmenkonzeption mit Lücken:

Für Projekte wie das e-Bürgerdienste-Portal muss ein schriftliches Datenschutz- und Sicherheitskonzept erstellt werden. Das Land als Auftraggeber verständigte sich mit dem privaten Auftragnehmer darauf, dieses Konzept schrittweise zu entwickeln. Bislang sind uns lediglich eine Rahmenkonzeption

zum Datenschutz sowie ein so genanntes Strukturkonzept im Entwurf bekannt. Folgende Aspekte sind in diesem Zusammenhang von Bedeutung:

- Geplante Verarbeitungsvorgänge und die dafür einschlägigen Rechtsvorschriften bleiben im Dunkeln

  Eine Rahmenkonzeption sollte erkennen lassen, welche Angebote das Portal im Einzelnen bieten wird und welche Rechtsvorschriften dafür einschlägig sind. Im Hinblick auf die angebotenen Dienstleistungen führte die Rahmenkonzeption jedoch lediglich aus, dass „eine Vielzahl an Verarbeitungsvorgängen“ stattfinde, bei denen „verschiedene personenbezogene Daten verarbeitet werden“. Solche vagen Aussagen sind jedoch nicht einmal als Grundlage für eine Rahmenkonzeption ausreichend. Auch die Zusammenstellung der für einzelne Dienstleistungen einschlägigen Rechtsvorschriften wirkte alles andere als systematisch und durchdacht.

- Leitlinien zur Verwendung von Cookies und aktiven Inhalten fehlen

  Zu erwarten wäre, dass eine Rahmenkonzeption auch Leitlinien für die mit Risiken für den Datenschutz verbundene Verwendung von Cookies und sog. aktiven Inhalten erkennen lässt. Cookies bergen kurz gesagt das Risiko, dass mit ihrer Hilfe Interessen- und Nutzerprofile erstellt werden können, während von aktiven Inhalten das Risiko ausgeht, dass beim Surfen fremde Programme unbemerkt auf den eigenen Computer gelangen und im schlimmsten Fall die auf dem eigenen Computer gespeicherten Daten ausspionieren oder Hintertüren öffnen können, durch die sich Hacker unbemerkt Zugang zum System verschaffen können. Leider geht die Rahmenkonzeption auf die mit aktiven Inhalten verbundene Problematik überhaupt nicht ein. Cookies werden zwar mehrfach erwähnt, allerdings stets nur im Zusammenhang mit isolierten Einzelfalllösungen. Die grundlegende Frage, ob und in welchen Fällen Cookies überhaupt genutzt werden müssen, klammert die Rahmenkonzeption jedoch aus. Gerade von einem Projekt, das wie das e-Bürgerdienste-Portal erklärtermaßen auch im Hinblick auf die Umsetzung der Datenschutzmaßnahmen vorbildlich sein soll, ist aber zu erwarten, dass diese Fragestellung in der Rahmenkonzeption aufgegriffen und innovative Lösungen gesucht werden, die die angestrebte Funktionalität bieten, dazu aber so weit wie möglich auf die Verwendung von Cookies und aktiven Inhalten verzichten.

- Schutz vor Zusammenführen von in unterschiedlichem Zusammenhang erhobenen personenbezogenen Daten

  Das Rahmenkonzept sieht vor, dass die in einem Zusammenhang erhobenen Daten „getrennt von an anderer Stelle erhobenen persönlichen Daten gespeichert“ werden. Diese Festlegung ist zumindest missverständlich: Denn die getrennte Speicherung allein bietet noch keinen erhöhten Schutz – schließlich können auch Daten, die beispielsweise in unterschiedlichen Datenbanktabellen oder getrennt gespeichert sind, mühelos wieder zusammengeführt werden. Entscheidend ist vielmehr, ob die getrennt gespeicherten Daten über gemeinsame Datenfelder verfügen, anhand derer eine spätere Zusammenführung wieder möglich ist oder ob solche Datenfelder nicht existieren.

2.2.2 Sicherer E-Mail-Austausch

Viele e-Government-Lösungen sehen auch eine Möglichkeit zum Austausch von elektronischen Postsendungen vor. Werden dabei personenbezogene oder andere schutzbedürftige Daten übermittelt, so sind diese zu verschlüsseln. Daneben kann es auch notwendig sein, die Authentizität des Absenders nachzuweisen, etwa mit Hilfe einer digitalen Signatur. Dafür bieten sich unterschiedliche Realisierungsmöglichkeiten:

– Eine Möglichkeit besteht darin, E-Mails nach wie vor mit einem gängigen E-Mail-Programm zu versenden und dabei den Mail-Inhalt sowie die Anlagen mit einem dafür vorgesehenen Zusatzprogramm zu verschlüsseln. Vorteil dieser Verfahren ist, dass damit auch Nachrichten mit qualifizierten Signaturen versehen werden können, die mittlerweile vielfach an die Stelle eigenhändiger Unterschriften treten können. Voraussetzung dafür ist allerdings, dass die Teilnehmer zunächst die für die Verschlüsselung und die Signatur erforderliche Soft- und zum Teil auch Hardware an ihrem PC installieren und sich die erforderlichen Schlüssel beschaffen, bevor sie mit dem Austausch verschlüsselter Nachrichten beginnen können. Im Hinblick auf die Kommunikation zwischen Bürgern und Behörden ist zu bedenken, dass nur ein Teil der Bürger diesen Aufwand auf sich nehmen dürfte, um E-Mails gesichert im Internet austauschen zu können.

– Um die damit verbundenen Einschränkungen zu umgehen und von Anfang an eine verschlüsselte Kommunikationsmöglichkeit für praktisch alle Internet-Nutzer zu bieten, kommt auch eine sog. Web-Mail-Lösung in Betracht, wie sie beispielsweise von der AOK Baden-Württemberg im Rahmen des Projekts AOK24 angeboten wird *(www.aok24.de)*. Die AOK sah sich damit konfrontiert, dass Versicherte ihr zunehmend unverschlüsselte E-Mails sandten und darin auch sensible Sozial- und Gesundheitsdaten ansprachen. Ihr Anliegen war, allen Versicherten die Möglichkeit zu bieten, verschlüsselte Nachrichten mit ihr austauschen zu können, ohne dass sie zuvor zusätzliche Software auf ihrem PC installieren, sich die Schlüssel beschaffen oder um deren Erzeugung kümmern müssen. Ein Versicherter, der diese Möglichkeit nutzen will, muss sich zuvor lediglich registrieren und freischalten lassen. Danach kann er verschlüsselte Nachrichten an die AOK senden, indem er mit seinem Browser die entsprechende Web-Seite aufruft, seine Mitteilung dann in einer Eingabemaske erfasst und diese anschließend versendet. Dabei werden die erfassten Daten mit der in allen gängigen Browsern eingebauten SSL-Technik (SSL: Secure Sockets Layer) verschlüsselt und anschließend an die AOK übertragen. Deren Antwort wird in einem von der AOK bereitgestellten elektronischen Briefkasten abgelegt, auf den der Versicherte wiederum mit Hilfe seines Web-Browsers geschützt zugreifen kann. Um unberechtigte Zugriffe auf diese Briefkästen zu verhindern, muss sich der Versicherte mit einer nach der Registrierung zugewiesenen Benutzerkennung und einem von ihm gewählten persönlichen Passwort identifizieren.

2.2.3 Elektronischer Rechtsverkehr

Die Justizminister des Bundes und der Länder haben in diesem Jahr organisatorisch-technische Leitlinien verabschiedet, die sich mit der Frage befassen, wie Bürger und Justizbehörden künftig mit der nötigen Sicherheit und Rechtsverbindlichkeit miteinander elektronisch kommunizieren können. Inhaltlich sehen diese Leitlinien vor, dass elektronische Dokumente zwischen Bürgern und Dienststellen stets verschlüsselt und digital signiert übertragen

werden sollen. Daneben geht es auch um die Frage, welche Arten von Textdokumenten für den elektronischen Rechtsverkehr in Frage kommen. Im Hinblick auf das insbesondere von dem Textverarbeitungsprogramm Word verwendete Dokumentenformat (*.doc) wird dabei eine Reihe von Eigenschaften erwähnt, die einer Verwendung für den elektronischen Rechtsverkehr entgegenstehen. Im Kern geht es darum, dass es sein kann, dass das Programm nicht alle Textpassagen am Bildschirm darstellt, die in dem entsprechenden Dokument enthalten sind. In einem solchen Dokument können, je nach eingesetzter Version und den Einstellungen des Programms, noch Textabschnitte zu finden sein, die der Bearbeiter längst schon „gelöscht“ hat, die durch das Löschen aber nicht aus dem Dokument, sondern nur aus dem angezeigten Teil verschwinden. Wird nun ein solches Dokument digital signiert, so stellt sich die Frage, ob die zwar vorhandenen, aber nicht ohne weiteres angezeigten Textabschnitte als autorisiert gelten sollen oder nicht. Diese Problematik, die auch aus anderem Grund datenschutzrechtliche Probleme aufwirft, haben wir unter der Überschrift „Was Texte so alles verraten können“ in unserem 20. Tätigkeitsbericht (LT-Drs. 12/4600, S. 27 f.) genauer dargestellt. Obwohl die Justizministerien diese Problematik erkannt haben, sollen entsprechende Dokumente im Hinblick auf deren weite Verbreitung gleichwohl zum elektronischen Rechtsverkehr zugelassen werden. Wir hätten es begrüßt, wenn die Justizministerien ihre eigenen Überlegungen zum Anlass genommen hätten, nur solche Dokumententypen zum elektronischen Rechtsverkehr zuzulassen, bei denen Zweifelsfälle der beschriebenen Art gar nicht erst auftreten können.

Nicht nur in Baden-Württemberg erfordern e-Government-Projekte neue Antworten für die datenschutzgerechte Gestaltung der Systeme. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder richtete daher eine Arbeitsgruppe ein, die Möglichkeiten darstellen sollte, wie e-Government datenschutzgerecht zu gestalten ist. Die Ergebnisse der Arbeitsgruppe sind in einer Broschüre mit dem Titel „Datenschutzgerechtes e-Government“ zusammengefasst, die der Konferenz der Datenschutzbeauftragten dieser Tage zur abschließenden Beschlussfassung vorgelegt wird. Danach ist die Broschüre in elektronischer Form unter
www.baden-wuerttemberg.datenschutz.de/material-aks/aks-index.html
abrufbar.

Gedruckte Exemplare der Broschüre können kostenlos bei uns angefordert werden.

3. Ausgewählte Fragen des technischen Datenschutzes

Im Laufe des Jahres hatten wir im Rahmen unserer Beratungstätigkeit mit unterschiedlichsten Fragen aus dem Bereich des technisch-organisatorischen Datenschutzes zu tun. Folgende Projekte illustrieren, worum es dabei unter anderem ging:

3.1 Super, machet's – aber nicht so

Eine Gemeinde hat sich die Steigerung der Attraktivität des ländlichen Raums auf die Fahnen geschrieben. In einem Dienstleistungszentrum bietet sie mittelbar durch eine Betreibergesellschaft eine Reihe von privaten und öffentlichen Dienstleistungen an. Von dem Vorhaben war der Innenminister anscheinend so begeistert, dass er sich laut Presseberichten zu der euphorischen Äußerung „Super, machet's“ hinreißen ließ. Dass die Gemeinde, getragen von solcher Zustimmung, mit dieser Form der Bürgernähe unter dem Aspekt des technischen Datenschutzes dann allerdings über das Ziel hinausschoss, davon wird in diesem Abschnitt die Rede sein.

Die EDV-Infrastruktur dieses Zentrums bestand aus drei PC, die untereinander sowie mit der EDV der Gemeinde vernetzt waren. Alle drei PC waren über ein Firewall-System mit dem Internet verbunden. Ein PC

wurde ausschließlich von einer Mitarbeiterin des Dienstleistungszentrums genutzt. Die beiden anderen, von denen einer in einer so genannten Diskretionszone, der andere für jedermann zugänglich im Raum stand, wurden sowohl von Mitarbeiterinnen als auch von der Bevölkerung genutzt. Die PC wurden mit dem Betriebssystem Windows 98 betrieben, d. h. eine Benutzeranmeldung mit einem Passwort war nicht notwendig; lediglich der Bildschirmschoner musste am Publikums-PC, wenn er denn eingeschaltet war, durch ein biometrisches Fingerabdrucksystem von einer der Mitarbeiterinnen deaktiviert werden. Da die Mitarbeiterinnen auch mit dem System arbeiteten, waren ständig Verzeichnisse, die sich auf den Festplatten eines Gemeinde-Servers befanden, ebenfalls auf den einzelnen PC eingebunden. Dadurch konnte am Publikums-PC nicht nur auf die Dateien der Mitarbeiterinnen zugegriffen werden, sondern – lesend und schreibend – auf alle Dateien aller Bediensteten, weil auf dem Gemeinde-Server kein Zugriffsschutz realisiert war. Die Gemeinde verwendet nämlich ein Dokumentmanagementsystem, das die Dokumente in einem separaten Zweig des Dateisystems speichert. Unsere Mitarbeiter waren erstaunt, als sie entgegen ihrer Vorstellung, jeder Mitarbeiter könne nur auf seine Dokumente zugreifen, entdeckten, dass jedermann vom Publikums-PC aus hätte alle Dokumente des Dokumentmanagementsystems auf dem Gemeinde-Server lesen, verändern oder löschen können. Bei der Kontrolle förderten wir unter anderem Dokumente zu Verwaltungsverfahren in Erbangelegenheiten und etwa zu Rentenversicherungsauskünften zu Tage.

Aber nicht nur in der Dateiablage des Dokumentmanagementsystems, sondern auch im normalen Dateisystem konnten wir Dokumente finden, die personenbezogene Daten enthielten, von denen man annehmen würde, dass nicht Hinz und Kunz sie lesen können sollte. Unter anderem handelte es sich um Eingänge zu Angebotsaufforderungen und Einschätzungen zur Gebäudequalität des Ortskerns, ferner um für Abrechnungen notwendige minutiöse Aufstellungen aller erbrachten Dienstleistungen mit Namen der die Dienstleistung in Anspruch nehmenden Bürger sowie um Altersstatistiken über ausländische Mitbürger.

Erschwerend kommt hinzu, dass es unterlassen wurde, die Diskettenlaufwerke der PC zu sperren. So konnten nicht nur die Dokumente eingesehen werden, sondern Unbefugte hätten sich eine Kopie anfertigen und diese auf Diskette mit nach Hause nehmen können. Sie hätten aber, was noch schwerer wiegt, auch von zu Hause Programme mitbringen können, die dazu hätten dienen können, aus der Ferne die mit diesen Programmen infizierten PC auszuspionieren. Der Installation auf den durch die Öffentlichkeit nutzbaren PC und einer Weiterverbreitung bis in das Netz des Rathauses hätte jedenfalls nichts entgegengestanden, und zwar deshalb nicht, weil man der Auffassung war, durch das Firewall-System würden derartige Programme abgewehrt und deshalb müsse auf den einzelnen Arbeitsplatz-PC kein Virenschutzprogramm installiert werden. Diese Auffassung erwies sich schon deshalb als falsch, weil wir auf dem Publikums-PC noch Spuren eines Programms namens „Hackers-Welt“ fanden. Nur nebenbei sei noch erwähnt, dass sich auch jemand an den Einstellungen des WWW-Browsers auf dem Publikums-PC zu schaffen gemacht hatte. Im Gegensatz zu den zwei anderen PC war auf dem Publikums-PC eine niedrige Sicherheitsstufe konfiguriert.

Auch sonst baute man keine nennenswerten Hürden auf, um Manipulationen der Systeme und unberechtigte Zugriffe auf personenbezogene Daten zu verhindern. So war beispielsweise die Benutzerverwaltung des Gemeinde-Servers so konfiguriert, dass fehlgeschlagene Versuche, sich an den Systemen der Gemeinde anzumelden, nicht wie üblich zu einer Sperrung der Benutzerkennung führten. Eine Mindestlänge für Benutzerkennworte war auch nicht eingestellt, was erfahrungsgemäß dazu führt, dass Benutzer besonders einfache Kennworte wählen, die von Hackern unter Einsatz spezieller Programme leicht zu erraten sind. Und das alles wäre wohl unbeobachtet geblieben, da man wegen der unzureichend vorgesehenen Protokollierung aus den entsprechenden Aufzeichnungen keine Anhaltspunkte für Eindringversuche hätte entnehmen können.

Unsere Bedenken und Ausführungen konnten die Gemeinde davon überzeugen, dass weit reichende Änderungen an der EDV des Dienstleistungszentrums notwendig sind, um einen Betrieb zu ermöglichen, der mit datenschutzrechtlichen Regelungen in Einklang steht.

3.2 Verschlüsselung

Mit der Verschlüsselungstechnik steht ein leistungsfähiges Werkzeug zur Verfügung, um Daten vor unberechtigter Kenntnisnahme sowie vor unbemerkten Änderungen zu schützen.

– Schutz der Daten einer Psychologischen Beratungsstelle

Ein Mitarbeiter einer organisatorisch dem Landratsamt zugeordneten Psychologischen Beratungsstelle bat um Rat, wie sich erreichen lässt, dass nicht einmal die Systemverwalter des Landratsamtes auf die von der Beratungsstelle bearbeiteten Daten zugreifen können, die im Netz des Landratsamtes übertragen und auf dessen Servern gespeichert werden. Dabei ist zu bedenken, dass medizinische Daten, um die es hier geht, zum einen der ärztlichen Schweigepflicht unterliegen und zum anderen zu den besonders sensiblen Datenarten zählen, die nur unter besonders engen Voraussetzungen verarbeitet werden dürfen. Insbesondere muss vor deren erstmaliger Verarbeitung eine so genannte Vorabkontrolle durchgeführt werden. Die für den Einsatz oder die wesentliche Änderung des entsprechenden EDV-Verfahrens zuständige Stelle muss dabei untersuchen, ob von dem Verfahren besondere Gefahren für das Persönlichkeitsrecht ausgehen, und darf das Verfahren erst einsetzen, wenn sie nachgewiesen hat, dass dies nicht der Fall ist oder dass die Gefahren durch technische und organisatorische Schutzmaßnahmen verhindert werden können. Inhaltlich ist dabei unter anderem zu berücksichtigen, dass spezielle LAN-Verschlüsselungsprodukte den Schutz der von der Beratungsstelle verarbeiteten Daten auch dann ermöglichen können, wenn deren Daten auf Servern des Landratsamtes gespeichert sind. Damit ist es möglich,

- die Daten in verschlüsselter Form auf einem Server im lokalen Netz zu speichern,
- die Daten verschlüsselt vom Server über das lokale Netz an die Arbeitsplatz-PC (Clients) der Beratungsstelle zu übertragen und
- die Daten erst auf einem Arbeitsplatz-PC der Beratungsstelle zu entschlüsseln.

Will man mit dem Einsatz des Verschlüsselungsprodukts erreichen, dass auch Server- und Netzadministratoren nicht auf die Daten zugreifen können, so muss die Schlüsselverwaltung von anderen Personen wahrgenommen werden.

– Durchgängiger Schutz durch Verschlüsselung

Betrachtet man Verschlüsselungsprojekte wie das oben erwähnte Projekt zum Schutz der Daten einer Beratungsstelle oder das in Nr. 2.2.2 dieses Teils genannte Beispiel der durch Verschlüsselung geschützten E-Mail-Kommunikation, so stellt man fest, dass diese Projekte stets nur einen Teil der Datenverarbeitungsvorgänge einer öffentlichen Stelle schützen können. Lösungen, bei denen personenbezogene Daten praktisch während aller vorstellbarer Verarbeitungsphasen geschützt werden, sind bislang nur selten anzutreffen. Wie die verschiedenen Anwendungsbereiche der Verschlüsselung miteinander verbunden werden können, soll ein von der Stadt Stuttgart geplantes Projekt aufzeigen.

Angefangen von den ein- und ausgehenden E-Mails über die Kommunikation im lokalen Netzwerk der Stadt bis hin zur Bearbeitung der Daten in Fachverfahren und der Ablage elektronischer Unterlagen auf den städtischen Servern: Alle diese Bereiche sollen durch die Verschlüsselung geschützt werden. Aber nicht nur das: Die zur Verschlüsselung eingesetzten kryptografischen Verfahren sollen in

Verbindung mit Chipkarten auch dazu dienen, die Anmeldung der Benutzer und die zur korrekten Zuweisung der individuellen Zugriffsberechtigung erforderliche Prüfung der Authentizität dieser Anmeldung mit höherer Zuverlässigkeit vornehmen zu können, als dies mit den bislang gängigen Passwortverfahren möglich ist. Ziel des Gesamtprojekts ist dabei unter anderem, dass die Schlüsselverwaltung für alle diese Anwendungsbereiche möglichst einheitlich erfolgen kann. Die ebenfalls angestrebte Möglichkeit, auch innerhalb der Verwaltung digital signierte Vorgänge zu verarbeiten, soll die Grundlage für die vollelektronische Abwicklung interner Arbeitsabläufe bilden. Zu hoffen ist, dass die Stadt dieses Projekt wie geplant zügig angeht und dass dessen Ergebnisse möglichst bald dazu beitragen, einen durchgängigen Schutz personenbezogener Daten zu gewährleisten.

3.3 Das ressortübergreifende Active Directory

Wer Computersysteme betreibt, muss bei einem Personalwechsel den Namen des ausscheidenden Mitarbeiters, dessen Benutzerkennungen und E-Mail-Konten sowie eine Reihe weiterer personenbezogener Angaben aus Mitarbeiter- und Benutzerverzeichnissen, aus Telefonlisten sowie aus etlichen anderen elektronischen Verzeichnissen löschen und den neuen Mitarbeiter entsprechend in all diese Verzeichnisse aufnehmen. Zentrale Verzeichnisdienste, die das Ziel haben, den mit einem Stellenwechsel verbundenen Änderungsaufwand zu reduzieren, haben daher Konjunktur. Ein solches zentrales Verzeichnis soll künftig das so genannte Active Directory des Landes sein, in dem Informationen über die Benutzer der lokalen Computersysteme, über deren Zugriffsberechtigungen sowie über deren E-Mail-Konten erfasst und verwaltet werden. Dabei wird angestrebt, dass sich möglichst viele Behörden diesem zentralen Verzeichnis anschließen.

Datenschutzrechtlich ist dabei die Rolle der zentralen Administratoren von Bedeutung. Deren Zugriffsberechtigungen können zwar so gestaltet werden, dass sie nicht unmittelbar auf Daten aller mit diesem Active Directory verbundenen Computersysteme zugreifen können. Dieser Schutz ist allerdings in sofern unzulänglich, als die Administratoren diese Beschränkung selbst aufheben und sich umfassende Zugriffsberechtigungen für beliebige, daran angeschlossene Computersysteme verschaffen können. Man muss sich vergegenwärtigen, dass in den angeschlossenen Systemen auch schutzbedürftige personenbezogene Daten, inklusive besonders sensibler Daten der Polizei, der Staatsanwaltschaften, der Gerichte, der Steuerverwaltung, der Personalverwaltung sowie mitunter auch Gesundheits- und Sozialdaten verarbeitet werden können. Hieraus wird deutlich, dass Schutzmaßnahmen erforderlich sind, um zu gewährleisten, dass die zentralen Administratoren nicht auf die in den angeschlossenen Computern gespeicherten Daten zugreifen können. Dabei ist eine Lösung zu favorisieren, die dies technisch sicherstellt. Neben der Möglichkeit, die eingesetzte Software entsprechend zu modifizieren, lässt sich dies auch durch die Verschlüsselung der schutzbedürftigen Daten erreichen. Zudem sollte durch eine sog. Terminalbeschränkung sichergestellt werden, dass sich die Administratoren nur von einzelnen, wenigen Arbeitsplatz-PC aus anmelden können. Eine solche Lösung wirkt auch dem Risiko entgegen, dass es Unberechtigten gelingt, auf Grund von Programmierungs-, Konfigurations- oder Betriebsfehlern in die Rolle eines „allmächtigen“ Administrators zu schlüpfen und damit unberechtigt personenbezogene Daten zu lesen oder zu ändern.

Daneben stellt sich beim Active Directory, wie bei anderen elektronischen Verzeichnisdiensten auch, die Frage, welche personenbezogenen Daten darin über die einzelnen Bediensteten gespeichert werden dürfen und wer auf welche dieser Daten zugreifen darf.

All dies macht deutlich, dass die Einführung eines Active-Directory in jedem Fall eines zwischen allen beteiligten Stellen abgestimmten Datenschutz- und Sicherheitskonzeptes bedarf. Mittlerweile gab der mit

Vertretern aller Ministerien besetzte Arbeitskreis Informationstechnik ein solches Sicherheitskonzept in Auftrag.

3.4 Die Fernwartung – näher betrachtet

Die Bedienung eines PC ist in den vergangenen Jahren durch die Verwendung von graphischen Bedienoberflächen immer einfacher geworden. Daneben ist zu beobachten, dass die so genannten Backoffice-Systeme wie beispielsweise Datenbanksysteme, Bürokommunikationssysteme, Terminalsysteme oder geographische Informationssysteme, die der Benutzer nicht sieht, auf die er bei seiner Arbeit aber ständig zugreift, immer komplexer werden. Vielfach ist für die Installation, Fehlerbehebung und Wartung detailliertes Expertenwissen notwendig. Deshalb gehen viele öffentliche Stellen dazu über, darauf spezialisierte Unternehmen mit Aufgaben der Wartung und Instandhaltung zu beauftragen. Zur datenschutzrechtlich korrekten Gestaltung und Durchführung dieser Auftragsverhältnisse wurden an uns im Berichtszeitraum mehrere Ersuchen um Beratung herangetragen.

Bei der Wartung von Systemen durch ein Unternehmen handelt es sich regelmäßig um eine Datenverarbeitung im Auftrag. Hierzu bedarf es immer des Abschlusses eines Vertrags, dessen Inhalt sich unter anderem an § 7 LDSG ausrichten muss.

Bei der Durchführung von Installations- und Wartungsarbeiten greift das Wartungspersonal meist über Weitverkehrsnetzwerkverbindungen auf die zu wartenden Rechner-Systeme zu. Aus der Sicht des technischen Datenschutzes ist für diese Netzwerkverbindungen zu fordern:

- Der Aufbau einer Verbindung durch Unbefugte darf nicht möglich sein. Dies kann bei dedizierten Verbindungen dadurch erreicht werden, dass ein Verbindungswunsch durch einen Rückruf erfüllt wird. Ebenso sollte von der Möglichkeit, die Verbindung über eine Benutzerkennung und ein Passwort abzusichern (CHAP), Gebrauch gemacht werden.
- Der gesamte Datenverkehr zwischen zu wartendem Rechner-System und Rechner des Wartungspersonals muss verschlüsselt erfolgen, soweit dabei personenbezogene Daten übermittelt werden. Kein Kennwort darf unverschlüsselt übertragen werden. Bei Verbindungen über das Internet sollte die Schlüssellänge mindestens 128 Bit betragen.
- Bei Verbindungen über das Internet wird die Kommunikation am zweckmäßigsten über so genannte virtuelle private Netzwerke (VPN) abgewickelt. Die Prüfung der Authentizität eines Kommunikationspartners sollte sich nicht auf das Wissen einer Benutzerkennung und eines Kennworts beschränken, sondern auch den Besitz eines physischen Merkmals wie beispielsweise einer Chipkarte umfassen.
- Der Aufbau einer Verbindung darf auf der Netzwerkebene nur unter Mitwirkung eines Mitarbeiters der Dienststelle möglich sein. Dies kann dadurch geschehen, dass die Verbindung beispielsweise erst in einem Firewall-System freigeschaltet werden muss oder dass auf dem entsprechenden Telekommunikationsendgerät keine eingehende Verbindung angenommen wird. Eine permanente Verbindung darf nur in Ausnahmefällen wie beispielsweise besonders schwieriger Fehlerbehebung gestattet werden.
- Der passive oder aktive Aufbau einer weiteren Netzwerkverbindung durch den Rechner des Wartungspersonals darf während der Wartungsarbeiten nicht möglich sein.

Bei den Zugriffen durch externes Wartungspersonal sind unterschiedliche Vorgehensweisen anzutreffen. Es sind dabei allerdings immer gewisse Regeln einzuhalten und Maßnahmen zu ergreifen, wenn personenbezogene Daten mit im Spiel sind. Im Einzelnen sind aus der Sicht des technischen Datenschutzes auf der Programmebene folgende Anforderungen zu erfüllen:

– Es muss nachvollziehbar sein, auf welche personenbezogenen Daten während der Wartungsarbeiten zugegriffen wurde. Werden die Wartungsarbeiten mit Programmen durchgeführt, die eine Kopie des Bildschirminhalts des zu wartenden Systems auf den Rechner des Wartungspersonals übertragen, dann kann der Mitarbeiter im Allgemeinen am Bildschirm des zu administrierenden Rechners die Zugriffe beobachten.

– Werden für die Arbeiten spezielle Administrationsprogramme eingesetzt, dann sollte die Protokollierung dieser Programme so umfangreich sein, dass später nachvollzogen werden kann, auf welche Daten zugegriffen wurde. Gegebenenfalls muss einem Mitarbeiter der Behörde der Zugriff auf die Protokollierung des Rechners des Wartungspersonals eingeräumt werden. Unter diesen Protokollierungsbedingungen können auch Terminaldienste eingesetzt werden.

Aus der Sicht des organisatorischen Datenschutzes ist bei Zugriffen auf personenbezogene Daten während Wartungsarbeiten Folgendes zu fordern:

– Grundsätzlich ist der Zugriff auf das Erforderliche zu beschränken. Dies bedeutet, dass dann keine Rechte eines Systemadministrators an externe Personen vergeben werden dürfen, wenn dies wegen des zu administrierenden Gegenstandes nicht erforderlich ist. Datenbanksysteme beispielsweise verfügen über eine leistungsfähige Benutzerverwaltung, die von der Benutzerverwaltung des Betriebssystems entkoppelt ist. Ein Datenbankadministrator muss nicht zwingend auch die Rolle eines Systemadministrators einnehmen. Es empfiehlt sich daher, dass für unterschiedliche Teilsysteme wie beispielsweise Datenbanksysteme oder Bürokommunikationssysteme unterschiedliche Benutzerkennungen zur Wartung benutzt werden.

– Es sollten für die Administration durch externes Wartungspersonal spezifische Benutzerkennungen angelegt werden. Diese Benutzerkennungen müssen nach erfolgter Administration deaktiviert werden. Die Kennwörter von Benutzerkennungen, die nicht deaktiviert werden können und die zur Kenntnis des externen Wartungspersonals gelangt sind, müssen nach erfolgter Wartung geändert werden.

– Wird parallel zum Produktionssystem ein Testsystem eingesetzt, auf dem die Wartungseingriffe zunächst auf ihre Wirksamkeit hin geprüft werden, dann dürfen auf diesem Testsystem nur personenbezogene Daten in anonymisierter Form oder reine Testdaten gespeichert und verarbeitet werden.

Es versteht sich von selbst, dass daneben noch Maßnahmen wie der lückenlose Einsatz von Virenschutzprogrammen auf allen beteiligten Systemen und die Verwendung von Firewall-Systemen bei Verbindungen über das Internet getroffen sein müssen.

3.5 Chipkarteneinsatz an Hochschulen

Auch in diesem Jahr legten uns mehrere Hochschulen die Ergebnisse von Vorabkontrollen vor, die sie im Zuge des von ihnen geplanten Chipkarteneinsatzes vorgenommen hatten. Eine solche Vorabkontrolle muss durchführen, so sieht es das Landesdatenschutzgesetz vor, „wer für den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten zuständig ist, das mit besonderen Gefahren für das Persönlichkeitsrecht verbunden sein kann“. Neben automatisierten Abrufverfahren und Verfahren, mit denen besonders schutzbedürftige Daten verarbeitet werden, zählen dazu auch Projekte, bei denen Chipkarten ausgegeben und genutzt werden. Die Vorabkontrollen belegten durchweg, dass die jeweiligen Hochschulen die damit verbundene Aufgabe ernst nehmen und sich darum bemühten, die mit dem Chipkarteneinsatz zusammenhängenden datenschutzrechtlichen Fragestellungen und die dazu gehörenden Schutzmaßnahmen herauszuarbeiten. Gleichwohl machten wir eine Reihe von Vorschlägen zur Verbesserung der Vorabkontrollen. Dabei spielten unter anderem folgende Punkte eine Rolle:

– In einer Vorabkontrolle sollten nur solche Aspekte behandelt werden, die für den geplanten Betrieb relevant sind. Möglichkeiten für zukünftige Lösungen und Funktionen gehören nicht dorthin. Auf der anderen Seite ist es unzureichend, wenn Lösungen zu Sicherheitsfragen nur in Aussicht gestellt, nicht aber beschrieben werden.

– Nicht-personalisierte Chipkarten sollen zum Teil an Gäste der Hochschule ausgegeben werden, damit diese in der Mensa oder an anderen Stellen bezahlen können. Auf Wunsch sollten aber auch Studierende oder Mitarbeiter neben einer personalisierten Karte, die ihnen als Studierenden- oder Mitarbeiterausweis dient, eine anonyme Karte erhalten können, die sie zum Bezahlen oder für andere Nutzungen einsetzen können, die keine persönliche Identifikation erfordern.

– Bei einigen der personenbezogenen Daten, die auf den Chipkarten oder in den Hintergrundsystemen gespeichert werden sollten, wurde nicht klar, wofür diese benötigt werden.

– Zum Teil war auch nicht erkennbar, wie lange die Daten im Einzelnen gespeichert, wer darauf Zugriffsmöglichkeiten erhalten und welchen anderen Stellen sie mitgeteilt werden sollen.

– Fragen ergaben sich dazu, wie bei der Erstvergabe sowie im Fall einer notwendig werdenden Rücksetzung von PIN-Nummern, die die Chipkarteninhaber in manchen Fällen eingeben müssen, vorzugehen ist.

– Weiterer Klärungsbedarf ergab sich etwa im Hinblick auf den Schutz der computerbasierten Selbstbedienungsstationen oder im Hinblick auf die Wirksamkeit der Zugriffsschutzmaßnahmen, die gewährleisten sollen, dass unter mehreren Organisationseinheiten, die die Chipkarten nutzen, jede nur auf die Daten zugreifen kann, die sie benötigt.

3.6 Die unzulänglichen Verfahrensverzeichnisse

Jede öffentliche Stelle führt, so sieht es das Landesdatenschutzgesetz vor, ein Verzeichnis der automatisierten Verfahren, mit denen sie personenbezogene Daten verarbeitet. Eine Reihe von Verfahrensverzeichnissen, mit denen wir in diesem Jahr zu tun hatten, erwies sich als unzulänglich. Oft sind die darin enthaltenen Angaben zu allgemein formuliert und lassen es daher nicht zu, sich davon zu überzeugen, dass die Daten verarbeitende Stelle ausreichende technische und organisatorische Schutzmaßnahmen vorsieht. Folgende allgemeine Hinweise sollten bei der Erstellung des Verfahrensverzeichnisses beachtet werden:

– Bezeichnung des Verfahrens

  Mitunter kommt es vor, dass Verfahren als „Liste“ oder „Datei“ bezeichnet werden, wobei nicht erkennbar ist, ob der Begriff „Datei“ edv-technisch gemeint ist, das gemeldete Verfahren also beispielsweise lediglich aus einer Word- oder Excel-Datei besteht, oder ob das Verfahren etwa trotz der Bezeichnung „Datei“ als datenbankbasierte Fachanwendung programmiert wurde. Die Bezeichnung des Verfahrens sollte daher so gewählt werden, dass derartige Missverständnisse gar nicht erst entstehen können.

– Zugriffsberechtigte Personen oder Personengruppen

  Hier werden gelegentlich Bezeichnungen wie „Mitarbeiter der XY-Abteilung“ verwendet. Solche Angaben lassen jedoch offen, ob alle oder nur einige Mitarbeiter dieser Abteilung einen Zugriff benötigen. Dies sollte der Beschreibung der zugriffsberechtigten Personen oder Personengruppen zu entnehmen sein. Die entsprechenden Personen müssen dazu nicht einzeln namentlich genannt werden, sondern können durch die Fachaufgaben beschrieben werden, zu deren Bearbeitung sie die elektronischen Zugriffsmöglichkeiten benötigen. Sofern die zugriffsberechtigten Mitarbeiter auf unterschiedliche Datenarten zugreifen können, sollte auch dies erkennbar sein.

– Beschreibung der eingesetzten Hard- und Software sowie der Vernetzung

  Gelegentlich wird die vorhandene EDV-Infrastruktur allein mit Begriffen wie „Windows-Netzwerk“ oder „Stand-alone-PC“ beschrieben. Solche Angaben allein reichen nicht aus, um die technische Infrastruktur zu beschreiben. Da sich die einzelnen Windows-Varianten in sicherheitstechnischer Hinsicht ganz erheblich unterscheiden, ist die Angabe „Windows“ zur Beschreibung des Betriebssystems unzureichend. Die Beschreibung sollte in jedem Fall erkennen lassen, welches Betriebssystem auf wie vielen der eingesetzten Clients, Server sowie etwa vorhandenen unvernetzten PC eingesetzt wird.

– Technisch-organisatorische Schutzmaßnahmen

  In ein Verfahrensverzeichnis sind auch die von der Daten verarbeitenden Stelle zu treffenden technischen und organisatorischen Datenschutzmaßnahmen aufzunehmen. Viele Verfahrensverzeichnisse erweisen sich insbesondere in diesem Punkt als ergänzungsbedürftig:

  • Gelegentlich werden im Zusammenhang mit den Maßnahmen der Zugriffskontrolle, die einen unberechtigten Zugriff auf personenbezogene Daten verhindern sollen, lediglich Stichwörter wie „Passwortschutz“, „Zugriffsberechtigungen“ oder „Dienstanweisung“ genannt. Diese Maßnahmen sind zwar in der Regel allesamt notwendig, offen bleibt jedoch, wie sie umgesetzt werden. Um auch das zu verdeutlichen, sollte im Zusammenhang mit dem Passwortschutz beispielsweise die technisch sichergestellte Mindestlänge und das Höchstalter der Passwörter genannt werden. Auch im Hinblick auf weitere Gestaltungsmöglichkeiten des Passwortschutzes, wie sie beispielsweise in unserem Merkblatt zum Umgang mit Passwörtern beschrieben sind (im Internet unter *www.baden-wuerttemberg.datenschutz.de/material-lfd/passwort.html* abrufbar), sollte dargestellt werden, welche Optionen in den jeweiligen Installationen gewählt wurden und welche Anforderungen an Passwörter technisch und welche organisatorisch sichergestellt werden.

    Im Hinblick auf die Gestaltung der Zugriffsberechtigungen sollte auch angegeben werden, welches Dateisystem gewählt wird. In Abhängigkeit vom Datenhaltungskonzept sollte dargelegt werden, welche Zugriffsberechtigungen dafür erforderlich sind (z. B. individuelle Ablagen, Ablagen für Gruppenverzeichnisse, Ablagen für Daten der Anwendungsprogramme).

  • Es sollte erkennbar sein, ob und wofür Verzeichnisfreigaben (Shares) verwendet werden. Nach Möglichkeit sollten Benutzer keine Freigaben vornehmen oder vorhandene nutzen können.

  • Soweit die Anwendungsprogramme selbst sicherheitsrelevante Funktionen bieten (z. B. einen eigenen Passwortschutz oder eigene Zugriffsberechtigungsverwaltung), ist auch darauf einzugehen und zu beschreiben, wie diese Funktionen genutzt werden.

  • Auch im Hinblick auf weitere, sicherheitsrelevante Einstellungen der Betriebssysteme und Anwendungsprogramme sollte angegeben werden, wie davon Gebrauch gemacht wird.

  • Was eventuell vorgesehene Fernsteuerungs- und Fernwartungsmaßnahmen betrifft, so sollte erwähnt werden, wie dieser Zugriff jeweils erfolgen soll (z. B. über Landesverwaltungsnetz, ISDN-Wählverbindung oder über Internet) und welche sicherheitsrelevanten Parameter und welche sonstigen Schutzmaßnahmen dafür getroffen werden (z. B. Option zur Einwahl von außen deaktiviert, Mitwirkung der Systemverantwortlichen vor Ort beim Verbindungsaufbau, Protokollierung der durchgeführten Arbeiten).

  • Im Zusammenhang mit der Anbindung lokaler Computer und Netzwerke an Verwaltungsnetze oder öffentliche Netze (z. B.

ISDN-Netz, Internet) ist auch darzustellen, was getan wird, um einen unberechtigten Verbindungsaufbau zu verhindern.

- Sofern über die lokalen Netze auch E-Mails ausgetauscht oder im Internet gesurft werden soll, sind auch dafür entsprechende Sicherheitsmaßnahmen vorzusehen.
- Soweit ein Teil der Datenverarbeitung von einem externen Auftragnehmer, etwa einem regionalen Rechenzentrum ausgeführt wird, kann das Verfahrensverzeichnis auf Datenschutz- und Sicherheitskonzepte des Rechenzentrums verweisen, sofern deren Umsetzung zwischen Auftraggeber und Auftragnehmer vereinbart ist. Wichtig ist dabei dann allerdings, dass die Auftraggeber diese Konzeptionen vor Auftragserteilung und auch später jederzeit einsehen können, dass die Verweise auf konkrete Inhalte (also z. B. Gliederungsnummern oder Kapitel von genau bezeichneten Dokumenten – Angabe des genauen Titels und Stand) gerichtet sind und dass die Umsetzung der genannten Maßnahmen zwischen Auftraggeber und Auftragnehmer vertraglich vereinbart ist.

Die hier genannten Punkte können nur beispielhaft für Fragestellungen stehen, die im Verfahrensverzeichnis zu berücksichtigen sind. Je nach der Nutzungssituation vor Ort kann die Behandlung weiterer Punkte im Verfahrensverzeichnis erforderlich sein. Weitere in Frage kommende Maßnahmen werden etwa in unseren Merkblättern zu folgenden Themen angesprochen:

- Einsatz von PC und lokalen Netzwerken
  www.baden-wuerttemberg.datenschutz.de/material-lfd/pcln.html
- Fernsteuerung
  www.baden-wuerttemberg.datenschutz.de/material-lfd/fernsteuerung.html
- Fernwartung
  www.baden-wuerttemberg.datenschutz.de/material-lfd/fernwartung.html
- Internet und Datenschutz
  www.baden-wuerttemberg.datenschutz.de/material-lfd/internet.html

Ist es im Einzelfall unklar, ob und mit welcher Ausführlichkeit bestimmte Fragestellungen im Verfahrensverzeichnis angesprochen werden sollen, so kann es hilfreich sein, sich in die Rolle eines Lesers zu versetzen, der der öffentlichen Stelle nicht angehört, aber anhand des Verfahrensverzeichnisses darüber informiert werden soll, welche Datenverarbeitungsvorgänge ablaufen, auf welcher Rechtsgrundlage dies erfolgt und ob dafür ausreichende technische und organisatorische Schutzmaßnahmen ergriffen wurden.

Vor dem Hintergrund dieser praktischen Erfahrungen haben wir auch unser Merkblatt zum Führen eines Verfahrensverzeichnisses überarbeitet. Die aktuelle Fassung ist unter
www.baden-wuerttemberg.datenschutz.de/material-lfd/verfahrensverzeichnis.html
abrufbar.

Inhaltsverzeichnis des Anhangs

Anhang 1

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24./25. Oktober 2002

zur systematischen verdachtslosen Datenspeicherung
in der Telekommunikation und im Internet

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnisses grundlegend in Frage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedsstaaten in den Bereichen „Justiz und Inneres“ entsprechende Maßnahmen – allerdings unter weitgehendem Ausschluss der Öffentlichkeit – diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des World Wide Web), wie sie jetzt erwogen wird, ist ebenso wenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weiter gehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

Anhang 2

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 7./8. März 2002

Biometrische Merkmale in Personalausweisen und Pässen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solcher Maßnahme nennt, zustimmend zur Kenntnis genommen. Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.
2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z. B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.
3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.
4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.
5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

zu Anhang 2

63. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 7. März – 8. März 2002

Positionspapier der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen

1. Ausgangslage

Mit dem Terrorismusbekämpfungsgesetz wurden in § 4 Passgesetz und § 1 Personalausweisgesetz nahezu gleichlautende Regelungen folgenden Inhalts aufgenommen:

– Pässe und Personalausweise dürfen neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von
  - Fingern,
  - Händen oder
  - Gesicht

  des Inhabers enthalten.
– Alle biometrischen Merkmale und die Angaben über die Person dürfen auf den Ausweispapieren verschlüsselt gespeichert werden. Durch ein Bundesgesetz ist Folgendes zu regeln:
  - Arten der biometrischen Merkmale,
  - Einzelheiten der Einbringung von Merkmalen und Angaben in verschlüsselter Form,
  - Art der Speicherung und
  - Art ihrer sonstigen Verarbeitung und Nutzung.
– Die biometrischen Merkmale dürfen nur verwendet werden, um die Echtheit des Dokumentes und die Identität des Inhabers zu prüfen.
– Eine bundesweite Datei darf nicht eingerichtet werden.

Um beurteilen zu können, ob diese Maßnahmen geeignet und angemessen sind, müssen die verschiedenen biometrischen Verfahren aus Datenschutzsicht bewertet werden. Im Folgenden werden verschiedene Verfahren beschrieben und die Risiken aufgezeigt, die im Zusammenhang mit einem flächendeckenden Einsatz biometrischer Merkmale in Ausweisdokumenten zu erkennen sind.

2. Technische Möglichkeiten

2.1 Nutzung vorhandener biometrischer Merkmale

Bevor neue Merkmale in Ausweisen gespeichert werden, sollte geklärt werden, ob die vorhandenen nicht bereits ausreichen, um die Identität des Ausweisinhabers zu prüfen. Auf die Erhebung neuer personenbezogener Daten muss dann verzichtet werden. Könnten Verfahren eingesetzt werden, die bereits vorhandene biometrische Merkmale nutzen, wäre eine geringere Eingriffstiefe in das Recht auf informationelle Selbstbestimmung als bei der Verwendung eines völlig neuen Merkmals ausreichend.

Lichtbild

Mit dem Foto des Inhabers enthalten deutsche Ausweisdokumente bereits biometrische Daten. Mit heute vorhandener Technik ist es grundsätzlich möglich, das Foto auf dem Personalausweis automatisch mit dem Gesicht der Person zu vergleichen, die den Ausweis vorlegt.

Möglicherweise können die zurzeit verwendeten Passbilder die Qualitätsanforderungen an eine automatisierte Verarbeitung nicht in vollem Umfang erfüllen. Bisher gibt es allerdings keine verlässlichen Aussagen über die Bildqualität, die für biometrische Verfahren erforderlich ist. Ebenso wenig ist bisher geklärt, wie sich biometrische Merkmale im Laufe der Zeit ändern. Möglicherweise müsste die Gültigkeitsdauer von Personalausweisen wesentlich verkürzt werden, damit die Verifikation anhand des Passbildes im Ausweis über die gesamte Gültigkeitsdauer sichergestellt werden kann.

Unterschrift

Die Unterschrift des Inhabers ist ein weiteres biometrisches Merkmal, das schon jetzt auf jedem deutschen Ausweisdokument vorhanden ist. Ein automatischer Vergleich der vorhandenen mit einer bei der Kontrolle geleisteten Unterschrift wäre jedoch wenig sinnvoll, weil die zur Erkennung erforderlichen dynamischen Daten der Unterschrift (Druckverlauf, Schreibpausen) im Ausweis nicht gespeichert sind.

2.2 Biometrische Vermessung des Gesichtes

Sollen biometrische Daten des Gesichtes neu erhoben und in den Ausweispapieren maschinenlesbar beispielsweise als Barcode oder elektronischer Datensatz gespeichert werden, sind hohe Qualitätsanforderungen an die Erfassungs- und Kontrollsysteme zu stellen, um eine ausreichende Wiedererkennungsrate sicherzustellen. Für gute Ergebnisse sind gleichmäßig ausgeleuchtete Frontalaufnahmen von Gesichtern erforderlich. In der Praxis werden diese Anforderungen nur mit hohem Aufwand realisierbar sein.

2.3 Papillarmuster der Finger

Werden nur die Merkmale eines bestimmten Fingers genutzt, entstehen Probleme, wenn dieser bei der Erfassung oder bei Vergleichen verletzt oder anderweitig stark beansprucht ist (z. B. bei Bauarbeitern). Die Erfassung von Daten mehrerer Finger und alternative Vergleiche bei Kontrollen sind sehr aufwändig. Außerdem zeigen Tests, dass ein signifikanter (statistisch aber noch nicht abschließend verifizierter) Prozentsatz von Papillarmustern aus physiologischen Gründen nicht nutzbar ist (siehe Punkt 3.2).

2.4 Handgeometrie und Handlinien

Bei der Vermessung der Handgeometrie handelt es sich um ein System, das in den USA bereits im Einsatz ist. Über die Erkennungsqualität gibt es keine verlässlichen Angaben. Über die Möglichkeiten der Nutzung der Handlinien gibt es ebenfalls keine gesicherten Erkenntnisse. Die Problematik der Verletzungen oder sonstigen Einschränkungen der Nutzung einer Hand und der sich daraus ergebenden Notwendigkeit der Alternativdaten ist vergleichbar mit der bei der Papillarmusterverwendung. Unklar ist zurzeit auch die Wiedererkennungsqualität bei Handveränderungen durch Arbeits- und Alterungsprozesse.

2.5 Iris- und Retinastruktur

Die gesetzliche Formulierung „Gesicht“ lässt eine Erfassung detaillierter Merkmale der Augen nicht zu. Ungeachtet dessen ist festzustellen, dass diese Verfahren bisher noch nicht im größeren Stil eingesetzt worden sind. Sie sind sowohl technisch als auch organisatorisch sehr aufwändig. Bisher ist eine genaue Kopfpositionierung erforderlich, so dass fraglich ist, ob sie durch „Ungeübte“ in den Erfassungsstellen und an den Kontrollstellen praktiziert werden können. Sofern das Gesicht, die Iris oder die Retina durch ein Infrarot- oder Lasersystem abgetastet wird, ist damit zu rechnen, dass derartige Systeme auf eine signifikante Ablehnung durch die Betroffenen stoßen.

2.6 Weitere biometrische Merkmale

Aus technischer Sicht ist nicht auszuschließen, dass zur Prüfung der Identität Betroffener auch andere biometrische Merkmale verwendet werden könnten (z. B. Stimme, Bewegungsmuster). Diese Merkmale werden hier jedoch nicht weiter betrachtet, weil laut Pass- und Personalausweisgesetz neben dem Lichtbild und der Unterschrift nur biometrische Merkmale von Fingern, Händen oder dem Gesicht des Inhabers verwendet werden dürfen (siehe 1).

3. Allgemeine technische Randbedingungen

3.1 Vorgaben aus der bestehenden Rechtslage

Aus dem rechtlichen Rahmen ergeben sich für die zu schaffenden Regelungen aus technischer Sicht, unabhängig von der Art der genutzten biometrischen Merkmale, folgende Vorgaben:

– Die Kontrollsysteme bestehen aus vier Komponenten, die untrennbar und unbeeinflussbar miteinander verknüpft sein müssen:
  • Leseeinheit für die aktuellen biometrischen Merkmale,
  • Leseeinheit für die Ausweispapiere,
  • Entschlüsselungs- und Vergleichseinheit und
  • Einheit zur Freigabe bzw. Sperrung der Passage.
– Um Manipulationen ausschließen zu können, müssen die biometrischen Systeme bei der Kontrolle stand-alone arbeiten.
– Die enthaltenen Softwarekomponenten sollten zertifiziert (z. B. nach Common Criteria oder ITSEC) und signiert sein. Das gilt auch für Hardwarekomponenten, soweit mit ihnen Entschlüsselungen vorgenommen werden.
– Eine Speicherung von personenbezogenen Daten auf den Datenträgern der Kontrollsysteme über den Abschluss des Kontrollvorgangs hinaus ist nicht zulässig.
– Die Zahl der Personen, die Kontrollen trotz falscher Identität passieren können, muss möglichst gering sein (vgl. FAR unter 3.2).
– Eine regelmäßige Falsch-Rückweisung durch Unzulänglichkeiten bei den gespeicherten Daten muss vor der Ausgabe der Ausweise und Pässe schon durch die örtlichen Ausweisbehörden ausgeschlossen werden. Bevor die ausgebende Stelle den Ausweis aushändigt, muss sie ihn daher mit einem entsprechenden Referenz-Kontrollsystem prüfen.
– Die Verschlüsselung kann wahlweise bei der örtlichen Behörde oder in der Bundesdruckerei erfolgen.
– Der Verschlüsselungsalgorithmus muss wissenschaftlich anerkannt sein und dem Stand der Technik entsprechend als sicher gelten (mindestens für den Zeitraum der Gültigkeit der Ausweise).
– Der Schlüssel darf Unbefugten nicht bekannt werden.
– Wird auf eine Verschlüsselung der Daten verzichtet, müssen die gespeicherten Werte auf andere Weise gegen Missbrauch gesichert werden.

3.2 Stand der wissenschaftlichen Erkenntnisse zu biometrischen Verfahren

– Bisher gibt es keine wissenschaftlich gesicherten Erkenntnisse zu biometrischen Verfahren bei großen Anwendergruppen. Es können lediglich Erfahrungen mit kleineren Systemen (z. B. die automatisierte Kontrolle der Einwanderungsbehörde auf amerikanischen Flughäfen [Handgeometrie] oder auf den Flughäfen Schiphol und Frankfurt [Irisscan]) herangezogen werden.
– Die Leistungsfähigkeit biometrischer Systeme wird durch ihre Zurückweisungsrate berechtigter Personen (FRR False Rejection Rate) und ihre Überwindungssicherheit gegenüber unberechtigten Personen (FAR False Acception Rate) beschrieben. Beide Raten stehen in einem engen Zusammenhang. Je größer die Überwindungssicherheit ist, um so mehr berechtigte Personen werden abgewiesen. Die Ermittlung der FAR und der FRR und der Beziehung zueinander ist sehr aufwändig. Für große Anwendergruppen gibt es deshalb bisher keine herstellerneutralen Untersuchungen.
– Biometrische Systeme sind bislang hinsichtlich der FRR und der FAR nicht ausreichend überprüft, um flächendeckend eingesetzt zu werden. Das betrifft auch Fragen der Manipulationssicherheit des Gesamtsystems. Von besonderer Bedeutung ist die Verbindung zwischen Rechner und Sensor, da bei unzureichender Sicherung biometrische Merkmale durch Einspielen (Replay) entsprechender Datensätze vorgetäuscht werden können.

– Auch die Lebenderkennung ist bisher wenig ausgereift. Es ist deshalb nicht auszuschließen, dass biometrische Systeme durch die Präsentation nachgebildeter Merkmale (Silikonabdruck eines Fingerabdrucks, Foto eines Gesichtes usw.) überwunden werden können.

– Zur FER (False Enrollment Rate), die den Anteil der Personen nennt, bei denen das jeweilige biometrische Merkmal nicht geeignet ist oder nicht zur Verfügung steht, gibt es bisher keine gesicherten wissenschaftlichen Erkenntnisse. Eine FER von 1 % bedeutet beispielsweise bei bundesweiten Ausweisdokumenten, dass mehr als 500.000 Personen bei Kontrollen immer mit Fehlermeldungen rechnen müssen, da sie durch das System nicht erkannt werden. In jedem Fall muss ein Rückfallsystem für die Nutzer vorhanden sein, die eine sehr schlechte Merkmalsausprägung besitzen oder überhaupt nicht erfasst werden können.

4. Einheitliches Personenkennzeichen

Mit neu erfassten biometrischen Merkmalen bzw. mit den daraus generierten Datensätzen lässt sich eine Vielzahl unterschiedlicher Dateien erschließen und verknüpfen. Deshalb muss ausgeschlossen werden, dass die zusätzlichen biometrischen Merkmale der Ausweise sowohl für weitere staatliche Zwecke (z. B. Strafverfolgung) als auch im privatrechtlichen Bereich (z. B. für Vertragsabschlüsse) verwendet werden. Ein derartiges Merkmal käme sehr schnell einem einheitlichen Personenkennzeichen gleich, das gemäß dem Volkszählungsurteil des Bundesverfassungsgerichts unzulässig ist (BVerfGE 65,1, -53-).

In Bereichen, in denen Biometrie für andere als die in § 4 Passgesetz und § 1 Personalausweisgesetz genannten Zwecke zum Einsatz kommt (z. B. Zugangskontrolle), wäre eine Verknüpfung der verschiedenen Daten technisch möglich. Dies könnte zum einen durch Verwendung der im Ausweis gespeicherten Daten als Referenzmaterial für solche Zwecke erfolgen. Zum anderen könnten gespeicherte biometrische Daten mit denen abgeglichen werden, die zum Zwecke der Ausweiserstellung verwendet werden. Dies wäre, auch wenn es keine durchgängig verwendeten Standards für die Codierung biometrischer Daten gibt, verfahrensübergreifend prinzipiell durchführbar.

5. Speicherung biometrischer Daten

Zur Vermeidung der unbefugten Nutzung von Ausweisdokumenten ist nur eine biometrische Verifikation erforderlich, d. h. der Abgleich der biometrischen Merkmale einer konkreten Person mit den auf einem Ausweis gespeicherten Daten. Eine Speicherung außerhalb des Ausweises ist dafür nicht erforderlich. Das Ziel der Erkennung von „Doppelidentitäten“ durch Abgleich biometrischer Daten einer unbekannten Person mit denjenigen anderer Personen (Identifikation) setzt die Speicherung personenbezogener Daten in zentralen Referenzdateien voraus. Aus Sicht des Datenschutzes ist eine solche Datensammlung insbesondere im Hinblick auf die Bildung eines einheitlichen Personenkennzeichens und die unvermeidlichen Missbrauchsmöglichkeiten jedoch abzulehnen.

Für die Ausweise selbst besteht die Möglichkeit, die Referenzdaten als Rohdaten oder als biometrischen Datensatz zu speichern. Während Rohdaten ggf. auch grafisch gespeichert werden können (z. B. das Bild eines Fingerabdrucks), muss für elektronische Biometriedaten („Template“, „Vektor“) der Ausweis mit einem maschinenlesbaren Datenträger (Barcode, Speicherchip etc.) versehen werden. Um einen Missbrauch dieser Daten zu verhindern, kommt insbesondere eine verschlüsselte Speicherung in Betracht. Während dies gegen einen alltäglichen Zugriff schützen mag, kann bei der Vielzahl von Geräten, in denen der Entschlüsselungsschlüssel vorhanden sein muss (bei Polizei und Grenzkontrollbehörden), jedoch kaum davon ausgegangen werden, dass die verschlüsselt gespeicherten Daten auf Dauer vor interessierten Dritten verborgen bleiben (siehe 3.1).

6. Überschießende Daten

Einige biometrische Merkmale lassen neben der Nutzung zur Identifizierung auch völlig andere Auswertungen zu. So kann möglicherweise auf bestimmte gesundheitliche Zustände oder Dispositionen, auf Faktoren wie Stress, Betrunkenheit oder Müdigkeit geschlossen werden. Bekannt ist dies von Bildern des Gesichts, der Hand und des Augenhintergrunds, von verhaltensbasierten biometrischen Merkmalen (Sprache, Unterschrift) sowie in besonderer Weise von genetischen Daten.

In der Regel sind nur aus den biometrischen Rohdaten solche Zusatzinformationen ableitbar, nicht aber aus den daraus gewonnenen Templates. Aus diesem Grund dürfen insbesondere die Rohdaten selbst nicht zentral gespeichert werden. Außerdem sind im Verarbeitungsprozess einer biometrischen Kontrolle die Rohdaten möglichst früh zu löschen, um die Gefahr einer Zweckentfremdung zu verringern.

7. Eignung für die Überwachung

Die Speicherung biometrischer Merkmale außerhalb des Ausweises birgt neue Gefahren für das Grundrecht auf informationelle Selbstbestimmung. Gelingt es, biometrische Daten im Alltag zu erfassen und diese mit einer zentralen Datenbank abzugleichen, können weitgehende Bewegungsprofile der Betroffenen erstellt werden. Im Gegensatz zu einer Erfassung eines biometrischen Merkmals unter Mitwirkung des Betroffenen handelt es sich hierbei um nicht-kooperative Vorgänge, die dem Betroffenen womöglich nicht einmal bewusst sind. Dafür sind Merkmale geeignet, die kontaktlos und über eine gewisse Distanz erfasst werden können. Dies trifft zur Zeit vor allem auf die Gesichtserkennung zu, die bei geeignetem Blickwinkel mittels gewöhnlicher Kameras erfolgen kann. Da es datenschutzrechtlich geboten ist, sensitive Daten nur in Kenntnis der Betroffenen zu erheben, sind nichtkooperative passive Systeme abzulehnen.

Demgegenüber ist die flächendeckende Erfassung des Fingerabdrucks oder der Handgeometrie ohne Wissen und Mitwirkung des Betroffenen nicht oder nur unter sehr großem Aufwand möglich. Zwar können Fingerabdrücke auch heimlich von berührten Gegenständen abgenommen werden. Dies eignet sich jedoch – wegen des hierfür erforderlichen Aufwands – nur zur Behandlung von Einzelfällen und ist daher mit einer Überwachung nicht vergleichbar.

8. Ergebnis

Im Ergebnis zeigt sich, dass keines der weiteren biometrischen Merkmale unproblematisch ist. Vor der Entscheidung, ob ein bestimmtes biometrisches Merkmal in Ausweise aufgenommen werden soll, müssen die verschiedenen Risiken daher sorgfältig gegeneinander abgewogen werden.

Vor der gesetzlicher Einführung neuer biometrischer Merkmale ist eine Evaluation durch einen Großversuch geboten. Dabei wären Ausweise mit zusätzlichen Sicherheitsmerkmalen (z. B. Hologramm) ohne biometrische Merkmale zu erproben und zu bewerten und mit Ausweisen zu vergleichen, die ebenso ausgestaltet sind, jedoch biometrische Merkmale enthalten. Zu prüfen wäre auch, wie hoch das Risiko für Bürgerinnen und Bürger wäre, wegen Gerätedefekten bei hard- oder softwaregestützter Erkennung der Merkmale bzw. wegen statistisch zu erwartenden Falscherkennungen bei der Ausweiskontrolle trotz eines echten eigenen Ausweises aufgehalten und intensiver überprüft zu werden, als sonst notwendig.

Anhang 3

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 7./8. März 2002

Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten

Mit der rasch wachsenden Nutzung des Internet kommt dem datenschutzgerechten Umgang mit den dabei anfallenden Daten der Nutzerinnen und Nutzer immer größere Bedeutung zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit (Entschließung der 59. Konferenz „Für eine freie Telekommunikation in einer freien Gesellschaft“) darauf hingewiesen, dass das Telekommunikationsgeheimnis eine unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft ist. Seine Geltung erstreckt sich auch auf Multimedia- und E-Mail-Dienste.

Die Datenschutzbeauftragten betonen, dass das von ihnen geforderte in sich schlüssige System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, nach wie vor fehlt. Die Strafprozessordnung (und seit dem 1. Januar 2002 das Recht der Nachrichtendienste) enthält ausreichende Befugnisse, um den Strafverfolgungsbehörden (und den Nachrichtendiensten) im Einzelfall den Zugriff auf bei den Anbietern vorhandene personenbezogene Daten zu ermöglichen. Für eine zusätzliche Erweiterung dieser Regelungen z. B. hin zu einer Pflicht zur Vorratsdatenspeicherung besteht nicht nur kein Bedarf, sondern eine solche Pflicht würde dem Grundrecht auf unbeobachtete Kommunikation nicht gerecht, weil damit jede Handlung (jeder Mausklick) im Netz staatlicher Beobachtung unterworfen würde.

In keinem Fall sind Anbieter von Tele-, Medien- und Telekommunikationsdiensten berechtigt oder verpflichtet, generell Daten über ihre Nutzerinnen und Nutzer auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen Nachrichteninhalte, Verbindungsdaten und bestimmte Daten (Nutzungsdaten), die sie ursprünglich für eigene Zwecke benötigt haben und nach den Bestimmungen des Multimedia-Datenschutzrechts löschen müssten, den Strafverfolgungsbehörden (oder Nachrichtendiensten) zu übermitteln.

Anhang 4

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24. Mai 2002

Geplanter Identifikationszwang in der Telekommunikation

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der geschäftsmäßig Telekommunikationsdienste erbringt, dazu zu verpflichten, Namen, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für Telekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift „Schließen von Regelungslücken“ stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig – teilweise nach jedem Telefonat – wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.
- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.
- Die Anbieter würden eine Reihe von Daten auf Vorrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.
- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.
- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z. B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereitgestellt werden und sie damit diese Daten auch für die Verknüpfung mit anderen Datenbeständen verwenden können.

- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das private Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.
- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weitreichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender Verordnungsentwurf bei der Beratung des Gesetzes vorliegt.

Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der Telekommunikationsunternehmen weitgehend vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikationsgesetzes zu verzichten und vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.

Anhang 5

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 7./8. März 2002

Neues Abrufverfahren bei den Kreditinstituten

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen können. Dies ist ein neuer Eingriff in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung dieses Abrufverfahrens eine Verpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine effektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten der Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mit Hilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (sog. „know your customer principle“). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

Anhang 6

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24./25. Oktober 2002

Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zur Zeit in verstärktem Maße in der öffentlichen Diskussion. Mehrere kommunale Spitzenverbände haben sich diesbezüglich bereits an die jeweiligen Landesdatenschutzbeauftragten gewandt. Unbeschadet bereits bestehender Landesregelungen und der Möglichkeit, Daten ohne Grundstücksbezug zu veröffentlichen, fordert die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf Grund der bundesweiten Bedeutung der Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden.

Dabei ist zu bestimmen, wie derartige Kataster erstellt werden sollen. Die gegenwärtige Regelung des Bundesimmissionsschutzgesetzes sieht keine ausdrückliche Ermächtigung zur Schaffung von Mobilfunkkatastern vor, so dass deren Erstellung und Veröffentlichung ohne Einwilligung der Grundstückseigentümer und -eigentümerinnen und der Antennenbetreiber keine ausdrückliche gesetzliche Grundlage hat. Bei der Novellierung ist insbesondere zu regeln, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist. Individuelle Auskunftsansprüche nach dem Umweltinformationsgesetz oder den Informationsfreiheitsgesetzen bleiben davon unberührt.

Anhang 7

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 24./25. Oktober 2002

zur datenschutzgerechten Vergütung für digitale Privatkopien im neuen Urheberrecht

Zur Umsetzung der EU-Urheberrechtsrichtlinie wird gegenwärtig über den Entwurf der Bundesregierung für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft beraten. Hierzu hat der Bundesrat die Forderung erhoben, das bisherige System der Pauschalabgaben auf Geräte und Kopiermedien, die von den Verwertungsgesellschaften auf die Urheberinnen und Urheber zur Abgeltung ihrer Vergütungsansprüche verteilt werden, durch eine vorrangige individuelle Lizenzierung zu ersetzen. Zugleich hat der Bundesrat die Gewährleistung eines ausreichenden Schutzes der Nutzerinnen und Nutzer vor Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzungsprofilen gefordert.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in diesem Zusammenhang auf Folgendes hin: Das gegenwärtig praktizierte Verfahren der Pauschalvergütung beruht darauf, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internets ihre Berechtigung. Die Datenschutzkonferenz bestärkt den Gesetzgeber, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Sollte der Gesetzgeber – wie es der Bundesrat fordert – jetzt für digitale Privatkopien vom Grundsatz der Pauschalvergütung (Geräteabgabe) tatsächlich abgehen wollen, so kann er den verfassungsrechtlichen Vorgaben nur entsprechen, wenn er sicherstellt, dass die urheberrechtliche Vergütung auf Grund von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte (Digital Rights Management) müssen datenschutzfreundlich gestaltet werden.

Anhang 8

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 7./8. März 2002

zur
datenschutzgerechten Nutzung von E-Mail- und
anderen Internet-Diensten am Arbeitsplatz

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat detaillierte Hinweise hierzu erarbeitet .

Insbesondere gilt Folgendes:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internet am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.
2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.
3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.
4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.
5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.
6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.
7. Die gleichen Bedingungen wie bei der Nutzung des Internet müssen prinzipiell bei der Nutzung von Intranets gelten.

Die Datenschutzbeauftragten fordern den Bundesgesetzgeber auf, auch wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben.

zu Anhang 8

Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

(Die Orientierungshilfe wurde unter Beteiligung des AK Personalwesen erstellt. Sie richtet sich in erster Linie an öffentliche Stellen des Bundes und der Länder. Die hier dargestellten Grundsätze können auch auf den nicht-öffentlichen Bereich übertragen werden.)

Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. E-Mail und andere Internetdienste sind geeignet, das Verhalten und die Leistung der Beschäftigten zu überwachen. Die Orientierungshilfe stellt die bei der Nutzung dieser Dienste geltenden datenschutzrechtlichen Anforderungen dar.

I. Allgemeines

a. Bei der Nutzung von E-Mail und anderen Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden (Grundsatz von Datenvermeidung und Datensparsamkeit). Hierzu bietet es sich an, datenschutzfreundliche Verfahren einzusetzen. Ebenso ist die Kontrolle der Nutzung dieser Dienste durch den Arbeitgeber (Zur Vereinfachung bezeichnet „Arbeitgeber“ sowohl den Arbeitgeber als auch den öffentlich-rechtlichen Dienstherren) so zu gestalten, dass sie zunächst ohne, zumindest aber mit so wenigen personenbezogenen Daten wie möglich durchgeführt wird. Dabei sind präventive Maßnahmen gegen unbefugte Nutzung nachträglichen Kontrollen vorzuziehen.

b. Die Bediensteten sind mit den technischen Möglichkeiten vertraut zu machen, wie die eingesetzten Verfahren datenschutzgerecht angewendet werden können. Um Art und Umfang der Verarbeitung ihrer personenbezogenen Daten nachvollziehen zu können, sind die Bediensteten umfassend darüber zu informieren (Grundsatz der Transparenz).

c. Es sind geeignete Maßnahmen zu treffen, um die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Insbesondere sollte jeder internetfähige PC mit leicht bedienbarer, auch bei den Kommunikationspartnern vorhandener Verschlüsselungssoftware ausgestattet sein, um zu verhindern, dass aus Bequemlichkeit personenbezogene oder andere sensible Daten unverschlüsselt übertragen werden.

d. Automatisierte zentrale und wegen einer Verschlüsselung auch lokale Virenchecks sind notwendig. Um aktive Inhalte zu überprüfen, empfiehlt sich der Einsatz von lokaler Sandbox-Software.

II. Dienstliche Nutzung

a. Gestattet der Arbeitgeber die Nutzung von E-Mail und Internet ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations- (TK-) bzw. Teledienstesrechts (vgl. § 1 Abs. 1 Nr. 1 Teledienstedatenschutzgesetz, TDDSG); die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den einschlägigen Vorschriften des Beamtenrechts bzw. des BDSG (für Tarifbediens-

tete des Bundes) oder den Landesdatenschutzgesetzen (für Tarifbedienstete der Länder).

b. Der Arbeitgeber hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. E-Mail-Versenden der Beschäftigten dienstlicher Natur ist. Eine automatisierte Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten hingegen nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Es wird empfohlen, über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der die Fragen der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig geregelt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

c. Bei Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen (z. B. Psychologen, Ärzte, Sozialarbeiter und -pädagogen), muss entsprechend der Rechtsprechung des Bundesarbeitsgerichtes zu Verbindungsdaten über dienstliche Telefonate eine Kenntnisnahme des Arbeitgebers vom Inhalt der Nachrichten und den Verbindungsdaten, die einen Rückschluss auf die betroffenen Personen zulassen, ausgeschlossen werden.

d. Der Arbeitgeber darf die Nutzungs- und Verbindungsdaten der Personalvertretung nur insoweit kontrollieren, als dies im Einzelfall aus Gründen der Kostenkontrolle erforderlich ist. Soweit allerdings nur unerhebliche Kosten bei der Nutzung von Internet und E-Mail anfallen – was überwiegend der Fall sein wird –, ist eine Auswertung dieser Daten unzulässig.

e. Soweit die grundlegenden Datenschutzprinzipien eingehalten werden, kann die Dienstvereinbarung Regelungen enthalten, die im Einzelfall hinter den unter a. genannten Vorschriften zurückbleiben. Weder das BDSG noch die Landesdatenschutzgesetze bzw. die beamtenrechtlichen Vorschriften schließen dies von vornherein aus. Nur wenn eine gesetzliche Regelung unabdingbar ist, kommt eine Abweichung zuungunsten der Beschäftigten nicht in Betracht.

f. Im Regelfall sollte darauf verzichtet werden, die Verarbeitung von Protokolldaten auf die Einwilligung der Beschäftigten zu stützen, da sie auf Grund des Abhängigkeitsverhältnisses zum Arbeitgeber nicht immer freiwillig entscheiden können. Nur ausnahmsweise ist auch die Einwilligung der Beschäftigten in eine Verarbeitung der Protokolldaten über die unter a. genannten Vorschriften hinaus möglich. Die Beschäftigten können z. B. die Verwertung ihrer Protokolldaten verlangen, um den Verdacht einer unbefugten Internet-Nutzung auszuräumen.

g. Soweit die Nutzung von E-Mail und Internet zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren protokolliert wird, dürfen diese Daten nach dem BDSG, den Landesdatenschutzgesetzen und dem Beamtenrecht des Bundes und der Länder auch nur zu diesen Zwecken genutzt werden, nicht aber zur Verhaltens- und Leistungskontrolle der Beschäftigten.

h. Von ein- und ausgehenden dienstlichen E-Mails seiner Beschäftigten darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von deren dienstlichem Schriftverkehr. Beispielsweise könnte der Vorgesetzte verfügen, dass ihm jede ein- oder ausgehende E-Mail seiner Mitarbeiter zur Kenntnis zu geben ist.

i. Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, die gefährlichen oder verdächtigen ausführbaren Code enthalten (also insbesondere html-Seiten als Mail-body, Dateien mit den Erweiterungen *.exe, *.bat, *.com oder gepackte Dateien wie *.zip, *.arj, *.lha).

III. Private Nutzung

1. Allgemeines

a. Wenn ein Arbeitgeber den Beschäftigten die private Nutzung von Internet oder E-Mail erlaubt, ist er ihnen gegenüber TK- bzw. Teledienste-Anbieter.

b. Vom Arbeitgeber beauftragte Zugangsanbieter (Access Provider) sind zwar diesem gegenüber TK- bzw. Teledienste-Anbieter, gegenüber den privat nutzenden Beschäftigten sind die Provider aber lediglich Auftragnehmer des dann als Anbieter zu qualifizierenden Arbeitgebers.

c. Der Arbeitgeber ist den Beschäftigten gegenüber zur Einhaltung des Telekommunikationsgeheimnisses verpflichtet. Daher gelten die gleichen Bedingungen wie beim privaten Telefonieren.

d. Es gelten die Regelungen der Telekommunikations-Datenschutzverordnung, des Teledienstedatenschutzgesetzes bzw. des Mediendienste-Staatsvertrages.

e. Der Arbeitgeber ist nicht verpflichtet, den Beschäftigten die private Nutzung des Internet zu erlauben. Entschließt er sich jedoch dazu, muss es ihm grundsätzlich möglich sein, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen (z. B. eine angemessene Art der Kontrolle durchzuführen). Beschäftigte, die diese Voraussetzungen nicht erfüllen wollen, können ihre Einwilligung ohne jeden dienstlichen Nachteil verweigern.

f. Der Umfang der privaten Nutzung, ihre Bedingungen sowie Art und Umfang der Kontrolle, ob diese Bedingungen eingehalten werden, müssen – am sinnvollsten durch Dienstvereinbarung oder -anweisung – unter Beteiligung des Personalrats eindeutig geregelt werden.

g. Eine Protokollierung darf ohne Einwilligung erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs der Verfahren oder zu Abrechnungszwecken erforderlich ist.

2. Besonderheiten bei E-Mail

a. Private E-Mails sind wie private schriftliche Post zu behandeln. So sind eingehende private, aber fälschlich als Dienstpost behandelte E-Mails den betreffenden Mitarbeitern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben.

b. Der Arbeitgeber sollte vor dem Hintergrund des von ihm zu wahrenden Telekommunikationsgeheimnisses entweder für die Beschäftigten separate E-Mail-Adressen zur privaten Nutzung einrichten oder – falls privates Surfen erlaubt ist – sie auf die Nutzung eines (kostenlosen) Web-Mail-Dienstes verweisen.

c. Wie bei der dienstlichen Nutzung (s. II.i.) dürfen aus Gründen der Datensicherheit eingegangene private E-Mails oder deren Anhänge unterdrückt werden, wenn sie ein Format aufweisen, das ausführbaren Code enthalten kann. Die Verfahrensweise ist den Beschäftigten zuvor bekannt zu geben. Generell sind die Beschäftigten darüber zu unterrichten, wenn an sie gerichtete oder von ihnen abgesendete E-Mails ganz oder teilweise unterdrückt werden oder virenverseucht sind. Eine Untersuchung von virenverseuchten E-Mails mit Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist nur unter Einbeziehung der betreffenden Beschäftigten zulässig.

d. Eine darüber hinaus gehende inhaltliche Kontrolle ist nicht zulässig.