Landtag von Baden-Württemberg **Drucksache 13 / 2650**
13. Wahlperiode **01. 12. 2003**

Mitteilung

des Landesbeauftragten für den Datenschutz

Vierundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

Schreiben des Landesbeauftragten für den Datenschutz in Baden-Württemberg vom 1. Dezember 2003:

Anbei übersende ich Ihnen unseren 24. Tätigkeitsbericht, der nach § 31 Abs. 1 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 1. Dezember 2003 zu erstatten ist.

Zimmermann

Eingegangen: 01. 12. 2003 / Ausgegeben: 16. 12. 2003

Vierundzwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

INHALTSVERZEICHNIS

1. Teil: Zur Situation

Am 15. Dezember 2003 feiert das Volkszählungsurteil des Bundesverfassungsgerichts seinen 20. Jahrestag. Dieser Entscheidung kommt auch nach zwei Jahrzehnten noch immer wegweisende Bedeutung für die Stellung des Bürgers in einem immer mehr auf technische Kommunikation ausgerichteten Gemeinwesen zu. Aus den Grundrechten auf Achtung der Menschenwürde und des allgemeinen Persönlichkeitsrechts wurde das Recht auf informationelle Selbstbestimmung abgeleitet, das eine Gesellschaftsordnung erst ermöglicht, wie sie das Grundgesetz vor Augen hat. Es lohnt sich, die folgenden Kernsätze der Entscheidung nochmals in Erinnerung zu rufen:

> „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen ... Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“

Diese Erkenntnisse sollten nicht nur Erinnerungswert haben, sondern müssen auch heute noch unverändert Handlungsgrundlage für den Gesetzgeber und die öffentliche Verwaltung sein. Die Wirklichkeit wird diesem Anspruch jedoch noch lange nicht gerecht, vor allem wenn man die Entwicklung der letzten Jahre beobachtet. Zunehmend wird der Datenschutz von – wirklichen oder auch nur vermeintlichen – Sachzwängen in die Zange genommen. Dahinter können durchaus zu begrüßende Ziele stehen, wie etwa die gebotene Sparsamkeit der öffentlichen Haushalte oder das Bedürfnis nach umfassender Sicherheit der Bürger. Dass der Datenschutz sich nicht auf einer Insel der Seligen befindet und absolute Vorfahrt in allen Lebenslagen beanspruchen darf, hat auch das Bundesverfassungsgericht im besagten Volkszählungsurteil festgestellt:

> „Dieses Recht auf ‚informationelle Selbstbestimmung‘ ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‚seine‘ Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit ... Grundsätzlich muß daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen.“

Mit diesen Grundsatzaussagen ist aber ebenso belegt, dass das Grundrecht auf Datenschutz nur unter bestimmten Voraussetzungen hinter anderen, an sich ebenfalls schützenswerten Interessenlagen zurücktreten muss. Eingriffe in das Recht auf informationelle Selbstbestimmung müssen immer durch ein „überwiegendes Allgemeininteresse“ gerechtfertigt sein. Dieser Grundsatz scheint immer mehr vernachlässigt zu werden und dem Motto Platz zu machen: „Zweckmäßige und kostengünstige Erledigung von öffentlichen Aufgaben geht vor Datenschutz“. Dies wird dem Stellenwert des Grundrechts auf informationelle Selbstbestimmung in keiner Weise gerecht. Der Zweck heiligt eben nicht alle Mittel. Dies wird aber längst nicht durchgängig und allgemein so gesehen: Wie sonst ist es zu verstehen, dass maßgebliche Sicherheitspolitiker wieder einmal die Speicherung der Verbindungsdaten aller Internet-Nutzer auf Vorrat einfordern und nur noch darüber diskutieren, dass die deutsche Internet-Wirtschaft nicht mit zusätzlichen Kosten belastet werden darf, weil diese die internationale Wettbewerbsfähigkeit beeinträchtigen. Und wie sonst käme man beispielsweise auf die verschrobene und absurde Idee, den Unterricht schwänzende Schüler mit einer elektronischen Fußfessel versehen zu wollen. Zeigt die wenigstens in unserem Bundesland einigermaßen einheitliche und erfreulicherweise ablehnende Reaktion auf diesen Gedankenblitz noch, dass wenigstens in Extremfällen die Rückbesinnung auf das Selbstbestimmungsrecht der Bürger funktioniert, liegt die Sache bei etwas komplizierteren Sachverhalten schon anders. So wird in der öffentlichen Meinung kaum registriert, dass sich die staat-

lichen Eingriffe in das Selbstbestimmungsrecht der Bürger in der Gesamtschau in geradezu atemberaubender Weise verdichten. Sei es in Fragen der inneren Sicherheit (Telefon- und Videoüberwachung, Rasterfahndung, DNA-Analyse), der Steuerverwaltung (zunehmende Kontrollmöglichkeiten der Einkommens- und Vermögensverhältnisse) oder der Gesundheitsverwaltung (elektronische Gesundheitskarte) – nahezu flächendeckend wird der Bürger mit ständig verfeinerten Methoden in den Röntgenblick des Staates genommen. Keine Frage: Gegen eine wirksame Strafverfolgung, gegen eine möglichst gerechte Besteuerung oder gegen eine kostengünstige Gesundheitsverwaltung wird niemand etwas einzuwenden haben – im Gegenteil, gerade diese Lebensbereiche berühren die Interessensphäre der Bürger in hohem Maße und verlangen eine starke Präsenz der öffentlichen Hand. Aber es kommt auf die Art und Weise und die Intensität staatlichen Handelns an. So darf mit Fug und Recht nach der Sinnhaftigkeit gefragt werden, wenn man etwa sieht, dass eine mit großem personellen und sächlichen Aufwand durchgeführte Rasterfahndung bei allein in Baden-Württemberg sage und schreibe 1,8 Millionen Datensätzen letztlich zu keinem greifbaren Ergebnis geführt hat. Offensichtlich konnte trotz des enormen Aufwands nicht ein einziger Fahndungsansatz erarbeitet werden. Die oft bemühten so genannten „Trefferfälle“ beschreiben etwas ganz anderes, nämlich allein die Zahl der Übereinstimmungen mindestens zweier Rasterkriterien (Einzelheiten hierzu unten im 2. Teil, 1. Abschnitt), ohne dass hiermit zwangsläufig Erkenntnisse für Fahndung und Strafverfolgung verbunden wären. Unterhält man sich mit Polizeipraktikern, ist zu hören, man hätte die Rasterfahndung schon deshalb durchführen müssen, um sich nicht einem späteren Vorwurf ausgesetzt zu sehen, auch nur die kleinste Möglichkeit der Aufdeckung terroristischer Aktivitäten versäumt zu haben. Hier stellt sich allerdings die Frage nach Aufwand und Nutzen, zumal dieselben Polizeipraktiker auch einräumen, dass aus heutiger Sicht intelligentere und effizientere Fahndungsmethoden einer Rasterfahndung in der bislang praktizierten Form vorzuziehen wären. Für eine reine Alibi-Veranstaltung ist der Preis der – wenn auch nur vorübergehenden – massenhaften Erfassung völlig unbescholtener Personen jedenfalls zu hoch.

Delikaterweise profitiert der Datenschutz allerdings auch von der allgemeinen Finanzmisere. Auf manche Maßnahme, die in materiell besseren Zeiten in Angriff genommen wurde und für das Selbstbestimmungsrecht der Bürger nicht gerade als Wohltat anzusehen ist, muss wegen fehlender Mittel verzichtet werden. Ein hervorragendes Beispiel hierfür bietet die Videoüberwachung öffentlicher Örtlichkeiten. Manche dieser mit hohem Personal- und Finanzaufwand verbundenen und wegen Umfang und Intensität des Eingriffs in bürgerliche Freiheiten datenschutzrechtlich stets umstrittenen Maßnahmen im Land werden inzwischen schlicht deshalb eingestellt, weil sie nicht mehr zu finanzieren sind. Wesentliche Nachteile für die öffentliche Sicherheit und Ordnung auf unseren Straßen hatte dies bisher offensichtlich nicht.

Eine grundsätzlich neue Entwicklung scheint sich für die öffentliche Verwaltung insoweit anzubahnen, als auch sie sich – was für die private Wirtschaft schon lange Realität ist – verstärkt den Herausforderungen der Internationalisierung stellen muss. Ein in der Öffentlichkeit heiß diskutiertes Beispiel war die Vergabe der Arbeiten zur Ersterfassung von Daten für die Errichtung des elektronischen Grundbuchs. Hier bedient sich das Justizministerium eines Unternehmens in Bayern, das seinerseits unter anderem ein Subunternehmen in Rumänien einschaltete. Das Justizministerium musste daran erinnert werden, dass seine datenschutzrechtliche Verantwortung nicht bei dem mit der Vergabe bedachten Hauptunternehmen endet, sondern bis zur Endverarbeitung der Daten – wo auch immer diese stattfindet – reicht. Und hier hatte das Justizministerium wohl zunächst übersehen, dass es einen wesentlichen Unterschied ausmacht, ob die Datenverarbeitung im Inland bzw. in Mitgliedstaaten der Europäischen Union oder aber in Staaten erfolgt, die der Europäischen Union nicht angehören. Um das rechtlich geforderte „angemessene Datenschutzniveau“ auch für die Datenverarbeitung in Rumänien zu gewährleisten, war ein gründliches Überarbeiten der getroffenen Vereinbarungen erforderlich. Erfreulicherweise hat sich das Justizministerium den nötig gewordenen mühseligen Nacharbeiten nicht verschlossen. Es soll nicht verschwiegen werden, dass trotz der deutlichen Nachbesserungen zahlreiche Bürger ihr Unverständnis darüber äußerten, dass eine Datenverarbeitung personenbezogener Daten der öffent-

lichen Verwaltung überhaupt „nach außen“ und sogar ins Ausland vergeben werden kann. Tatsache aber ist, dass der Gesetzgeber diese Möglichkeit durchaus eröffnet hat, allerdings unter der Voraussetzung, dass das oben angesprochene „angemessene Datenschutzniveau“ gewährleistet bleibt. Dies festzustellen ist eine schwierige Angelegenheit. Nicht umsonst tut sich auch die EU-Kommission schwer, diese Voraussetzungen für andere Staaten allgemein anzuerkennen. Eine solche allgemeine Anerkennung ist bislang nur für Ungarn, die Schweiz und Argentinien sowie mit Einschränkungen für die USA und für Kanada ausgesprochen worden. Bei allen anderen Nicht-EU-Staaten muss mühevoll ermittelt werden, ob die Datenverarbeitung im konkreten Einzelfall ein nach unseren Maßstäben anzustrebendes angemessenes Datenschutzniveau erreicht hat. Angesichts dieser Entwicklungen wäre es dringend erforderlich, die mit der EU-Datenschutzrichtlinie innerhalb der Europäischen Union begonnene Harmonisierung des Datenschutzrechts auch auf den Bereich außerhalb der Europäischen Union auszuweiten – derzeit aber wohl eine utopische Wunschvorstellung.

Die organisatorischen Rahmenbedingungen für den Datenschutz sind in Baden-Württemberg – leider – unverändert geblieben. Die im vorangegangenen Tätigkeitsbericht angesprochene Zusammenlegung der Aufsicht für den öffentlichen und für den nichtöffentlichen Bereich fiel im parlamentarischen Raum zwar durchaus auf fruchtbaren Boden. Jedenfalls haben alle Landtagsfraktionen in direkten Gesprächen jeweils ihre Bereitschaft bekräftigt, entsprechende Überlegungen zu unterstützen. Leider steht ein vergleichbar kräftiges Bekenntnis zu einer ebenso wirksamen wie überfälligen Strukturveränderung des Datenschutzes seitens der Landesregierung bis heute aus. Vielleicht liegt dies daran, dass die Verwaltungsreform alle verfügbaren Kräfte insbesondere im Innenministerium beansprucht und keine Befassung mit zugegeben vergleichsweise bescheidenen Veränderungen in der Sparte Datenschutz zulässt. Dabei wäre es ein für jeden nachvollziehbarer Weg, gerade auch diesen Bereich unter dem Gesichtspunkt einer möglichst effizienten Aufgabenerledigung unter die Lupe zu nehmen und in umfassendere Maßnahmen zur Verwaltungsreform einzubinden. Dass bei einer Gesamtabwägung aller Umstände nur die Zusammenlegung beider Aufsichtsbereiche vernünftig ist, scheint mir außer Frage zu stehen.

Zum Stichwort Verwaltungsreform noch eine grundsätzliche Anmerkung: Die Kreativität beim Erfinden neuer Organisationsstrukturen ist bemerkenswert. So ist derzeit offenbar daran gedacht, so genannte „Gemeinsame Dienststellen“ einzurichten. In diesen auch als „Kompetenzzentren“ bezeichneten Einrichtungen sollen Bedienstete einzelner Behörden jeweils für ihre eigene Dienststelle tätig werden. Darüber hinaus soll aber auch ein „gemeinsamer Einsatz“ des Personals möglich sein. Dies bedeutet dann, dass jede Behörde auf das Personal der jeweils anderen Behörden zurückgreifen und dieses für die Erledigung der eigenen Aufgaben heranziehen kann. Diese Überlegungen hängen offensichtlich mit den Schwierigkeiten zusammen, die daraus entstehen, dass das Fachpersonal, das bisher für größere Gebietseinheiten zuständig war, im Zuge der Verwaltungsreform auf die Landratsämter verteilt werden muss und damit bisher bestehende Fachkompetenzen zerschlagen werden. In der Not will man wohl zunächst sowohl in der räumlichen Unterbringung wie auch personell alles beim Alten lassen und den aufzulösenden Ämtern lediglich ein neues Etikett verpassen. Aus Sicht des Datenschutzes ist dies jedoch nicht unproblematisch. Denn mit der Neuordnung der Zuständigkeiten verändern sich auch die datenschutzrechtlichen Verantwortlichkeiten. Der Bürger muss sich aber darauf verlassen können, dass auch innerhalb solcher Gemeinsamen Dienststellen grundsätzlich nur die örtlich für ihn zuständigen Mitarbeiterinnen und Mitarbeiter auf seine personenbezogenen Daten zugreifen können. Mit Datenschutzrecht nicht vereinbar wäre es deshalb, wenn in Gemeinsamen Dienststellen Aufgaben über örtliche Zuständigkeitsgrenzen hinweg nach dem Motto: „Jeder ist für alles zuständig“ erledigt werden sollen. Im Gegenteil: Um eine eindeutige Zuordnung des Personals zu den jeweils zuständigen Ämtern kommt man nicht herum. Jede sonstige Form der internen Zusammenarbeit bedarf einer klaren gesetzlichen Regelung der datenschutzrechtlichen Befugnisse. Ungeachtet dessen wäre es auf jeden Fall verfehlt, eine auf Dauer angelegte generelle Ermächtigung zur Einrichtung solcher Gemeinsamer Dienststellen zu schaffen. Wenn überhaupt, sollten solche Regelungen nur dort, wo dies sach-

lich auch wirklich gerechtfertigt ist, bereichsspezifisch in Fachgesetzen erfolgen und in Form einer Übergangslösung befristet sein.

Die Verwaltungsreform wirft auch wegen der geplanten Übertragung der IuK-Technik von staatlichen Stellen auf die Landratsämter sowie wegen der künftig geänderten Verantwortung für den Betrieb der genutzten DV-Verfahren zahlreiche Datenschutzfragen auf. Um den betroffenen Dienststellen eine Hilfestellung für die datenschutzgerechte Planung und Umsetzung der IuK-technischen Veränderungen zu geben, haben wir in Zusammenarbeit mit dem Innenministerium gemeinsame Hinweise zum datenschutzgerechten IuK-Einsatz bei der Verwaltungsreform erarbeitet (s. Anhang 1).

2. Teil: Öffentliche Sicherheit und Justiz

1. Abschnitt: Öffentliche Sicherheit

1. Die Rasterfahndung: Ende gut, alles gut?

Nachdem sich nach den Terroranschlägen vom 11. September 2001 auf das World Trade Center in New York und das Pentagon in Washington herausgestellt hatte, dass daran beteiligte Attentäter in Hamburg gelebt und an deutschen Universitäten studiert hatten, kam bundesweit eine Rasterfahndung nach so genannten Schläfern in Gang. Die Idee war, mit Hilfe von maschinellen Abgleichen diverser Datenbestände nach Personen zu suchen, die sich genauso unauffällig, wie dies die mutmaßlichen Attentäter in Hamburg getan hatten, in Deutschland aufhalten und darauf warten, ihren Einsatzbefehl zu erhalten. Das Landeskriminalamt ordnete im Benehmen mit dem Innenministerium gegenüber mehr als 250 Stellen die Herausgabe personenbezogener Daten an. Die Anordnungen richteten sich an Universitäten, Fachhochschulen, Berufsakademien und andere Einrichtungen wegen Daten von Studierenden und wissenschaftlichen Mitarbeitern, an Bürgermeisterämter und regionale Rechenzentren wegen Einwohnermeldedaten, an Flughäfen und Flugplätze wegen Daten von Flugplatzpersonal und von Personen, die in sicherheitsempfindlichen Bereichen arbeiten, an die Regierungspräsidien wegen Daten von Inhabern von Fluglizenzen, an Flugschulen wegen Daten von Flugschülern, an das Innenministerium wegen Daten von Asylbewerbern, an Energieversorgungsunternehmen wegen Daten von Mitarbeitern und Fremdpersonal, an die Regulierungsbehörde für Post und Telekommunikation wegen Daten von Personen, die eine Sprechfunklizenz besitzen, an die Industrie- und Handelskammern wegen Daten über Personen, die einen Gefahrgutführerschein beantragt haben, und an Bürgermeisterämter und Landratsämter wegen Daten von Sozialhilfeempfängern. Gefragt waren jeweils Daten von Männern bestimmten Alters aus bestimmten Staaten. Die angegangenen Stellen lieferten dem Landeskriminalamt Daten über 1,8 Millionen Personen. Bei zwei Dritteln davon entsprachen die Daten nicht den vom Landeskriminalamt in seinen Rasterfahndungsverfügungen vorgegebenen Kriterien. Diese so genannten überschießenden Daten und die Daten über Sozialhilfeempfänger hat das Landeskriminalamt im Zuge von Datenschutzkontrollen meines Amtes im April bzw. Juni 2002 gelöscht.

Anhand der Datensätze der übrigen 600 000 Personen hat das Landeskriminalamt maschinelle Datenabgleiche durchgeführt. Diese Datenabgleiche zogen sich bis November 2002 hin. Dabei und bei den Datenabgleichen, die beim Bundeskriminalamt von März 2002 bis März 2003 liefen und zu denen das Landeskriminalamt Daten von mehr als 25 000 Personen beigesteuert hatte, ergaben sich – wie es in amtlichen Verlautbarungen gerne hieß – 551 „Treffer“, was in der Öffentlichkeit den Eindruck beförderte, es handele sich um potenzielle „Schläfer“. Nüchtern betrachtet ging es freilich um praktische Mengenlehre: Der Begriff Trefferfälle bedeutete nämlich nichts anderes, als dass der Computer bei den maschinellen Datenabgleichen auf Personen gestoßen war, die mindestens in zwei zum Datenabgleich herangezogenen Datenbeständen vertreten, also beispielsweise Studenten bestimmten Alters und bestimmter Herkunft waren und zugleich am Flughafen arbeiteten oder einen Gefahrgutführerschein besaßen. Mit diesen 551 Personen befassten sich Landeskriminalamt und Staatsschutzdezernate von Polizeidirektionen und Polizeipräsidien näher. Dazu haben sie vor allem Akten von Ausländerämtern, Einbürgerungsbehörden und Asylbehörden beigezogen, bei Einwohnermeldeämtern nachgefragt und Erkundigungen bei Universitäten, Hochschulen und Fachhochschulen angestellt. Bei 180 Personen war die Arbeit bald erledigt: Sie waren entweder ins Ausland oder nach unbekannt verzogen oder bereits verstorben. Die übrigen 371 Personen haben Landeskriminalamt und Staatsschutzdezernate eingehend überprüft. Dabei haben sie sich ein detailliertes Bild über die näheren Lebensumstände dieser Personen verschafft und im Einzelfall auch deren persönliches Umfeld überprüft. Nach Abschluss der Überprüfungen haben Landeskriminalamt und Staatsschutzdezernate die 371 Personen angesprochen. Weder

dabei noch bei den jeweils vorangegangenen Überprüfungen hat sich, wie das Landeskriminalamt uns versichert hat, irgendein Anhaltspunkt dafür ergeben, eine dieser Personen könnte ein „Schläfer“ sein oder irgendetwas mit dem islamistischen Terrorismus zu tun haben. Bei dieser Sachlage war die Löschung aller Daten geboten. Nach § 40 Abs. 4 des Polizeigesetzes sind nämlich die übermittelten und die im Zusammenhang mit dem Abgleich zusätzlich angefallenen Daten zu löschen und die Unterlagen zu vernichten, wenn der Zweck der Rasterfahndung erreicht ist oder sich zeigt, dass er nicht erreicht werden kann. In Anbetracht dessen und weil die Daten und Unterlagen zudem in keinem einzigen Fall zur Verfolgung von Straftaten benötigt worden sind, hat das Landeskriminalamt die zu seinen maschinellen Abgleichen verwendeten Daten der 600 000 Personen im März 2003 auf seinen Computern gelöscht. Auf seine Aufforderung, mit den zu den maschinellen Abgleichen angelieferten Daten der 25 000 Personen ebenso zu verfahren, bedankte sich das Bundeskriminalamt für die Zusammenarbeit bei dieser an Zeit und Arbeit aufwendigen Aktion und ließ Ende April 2003 das Landeskriminalamt wissen, es habe die Daten inzwischen gelöscht und die angelieferten Datenträger vernichtet; Löschprotokolle gebe es jedoch nicht. Das Landeskriminalamt hat die bei ihm im Rahmen der Überprüfung der 551 Personen angefallenen Daten sukzessive nach Abschluss der Überprüfungen gelöscht und Hand in Hand die jeweils angefallenen Unterlagen vernichtet; mit den letzten Daten und Unterlagen ist es am 12. September 2003 so verfahren. Weil es nicht die Hand dafür ins Feuer legen konnte, dass die mit Überprüfungen befassten Staatsschutzdezernate ebenfalls reinen Tisch gemacht haben, versprach es uns, diese an die Löschungs- und Vernichtungspflicht zu erinnern.

Ende gut, alles gut? Wohl kaum. Mancher wird sich an die eilfertigen Erfolgsmeldungen erinnern, die die Rasterfahndung zu Beginn begleitet haben. Das Ergebnis der Rasterfahndung sah dann freilich, wie gerade zu lesen war, ganz anders aus. Doch nicht darum geht es hier, sondern darum, in Erinnerung zu rufen, dass mit einer Rasterfahndung gravierende Eingriffe in das Grundrecht auf Datenschutz einhergehen. Ihre Wirkungsweise besteht nämlich darin, dass personenbezogene Daten, die die Betroffenen in völlig anderem Zusammenhang einer staatlichen oder sonstigen Stelle zur Verfügung gestellt haben, zu ganz anderen Zwecken, nämlich zu Zwecken der vorbeugenden Straftatenbekämpfung, miteinander verbunden werden. Dadurch werden wesentliche Schutzgehalte des Rechts auf informationelle Selbstbestimmung ganz erheblich strapaziert, weil der Betroffene infolge der heimlichen Datenerhebung nicht mehr überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und weil das Zweckbindungsgebot, wonach der Bürger wissen muss, mit welchen Verwendungsmöglichkeiten seiner Daten er zu rechnen hat, praktisch ins Leere geht. Das besondere Ausmaß der durch die Rasterfahndung bewirkten Beeinträchtigung des Grundrechts auf Datenschutz erschließt sich aber erst dann, wenn man sich vor Augen führt, dass jemand allein schon deshalb in eine Rasterfahndung einbezogen werden kann, weil eine seiner Eigenschaften oder Verhaltensweisen als Gegenstand einer polizeilichen Hypothese dienen kann. Anknüpfungspunkt des polizeilichen Kontrollprozesses ist damit nicht mehr ein Verhalten, das die Annahme einer konkreten Gefahr oder den Anfangsverdacht einer Straftat rechtfertigt. Vielmehr werden regelmäßig die Daten einer Vielzahl von Unbeteiligten verarbeitet; im vorliegenden Zusammenhang fielen schlussendlich alle 600 000 Personen, deren Daten in die maschinellen Datenabgleiche einbezogenen waren, unter diese Rubrik. Sie alle waren, ohne letztlich einen konkreten Untersuchungsanlass gegeben zu haben, dem Prozess des Datenabgleichs unterworfen, an den sich bei Hunderten von ihnen weitere konventionelle Ermittlungen angeschlossen haben. Zwar konnten angesichts der gemeinsamen Lagebewertung der Sicherheitsbehörden des Bundes und der Länder, der zufolge zu befürchten gewesen ist, dass noch nicht identifizierte Personen in Baden-Württemberg als Reaktion auf die Planungen der USA und ihrer Verbündeter für eine militärische Intervention Vorbereitungen für terroristische Anschläge treffen, jedenfalls grundsätzlich gegen die Rasterfahndung aus datenschutzrechtlicher Sicht keine durchgreifenden Bedenken bestehen, wenngleich wir wegen des recht grobmaschigen Rasters von Anfang an Zweifel hatten, ob dabei etwas herauskommen kann

(vgl. 22. Tätigkeitsbericht, LT-Drs. 13/520, S. 13 f.). Jedoch muss man sich – so, wie die Rasterfahndung dann gelaufen ist – schon die Frage stellen, ob die Ausgangshypothesen der Rasterfahndung tatsächlich ausreichend fundiert waren. Immerhin hat sich trotz der Bedrohungslage die Rasterfahndung summa summarum über zwei Jahre hingezogen. Zudem war von Polizeipraktikern zu hören, an einer Rasterfahndung habe schon deshalb kein Weg vorbeigeführt, weil man sich nicht später im Falle eines tatsächlich erfolgten Anschlags dem Vorwurf ausgesetzt sehen wollte, man habe nicht alle zur Verfügung stehenden Register gezogen. Solches schwang auch mit, wenn angesichts des Null-Ergebnisses zur Rechtfertigung der Rasterfahndung nachträglich darauf verwiesen wurde, dass es mit Blick auf die damalige bundesweit mangelhafte Erkenntnislage der Sicherheitsbehörden unverantwortlich gewesen wäre, nicht jedes Instrument der präventiv-polizeilichen Gefahrenabwehr und der vorbeugenden Verbrechensbekämpfung zu nutzen. Für die Zukunft sollte man sich schon überlegen, ob derart pauschale Vorsorgeüberlegungen eine Rasterfahndung rechtfertigen, die zu einer hunderttausendfachen Beeinträchtigung der Datenschutzrechte der Bürger führten.

2. Noch einmal: Die polizeiliche Videoüberwachung – diesmal in Singen

Am 29. Dezember 2000 ist § 21 Abs. 3 des Polizeigesetzes, der die polizeiliche Videoüberwachung regelt, in Kraft getreten. Seitdem können – um es mit den Worten des Gesetzes zu sagen – der Polizeivollzugsdienst und die Ortspolizeibehörden zur Abwehr von Gefahren, durch die die öffentliche Sicherheit bedroht wird, oder zur Beseitigung von Störungen der öffentlichen Sicherheit die in § 26 Abs. 1 Nr. 2 des Polizeigesetzes genannten Orte, soweit sie öffentlich zugängliche Orte sind, offen mittels Bildübertragung beobachten und Bildaufnahmen von Personen anfertigen. Die Vorreiter für die polizeiliche Videoüberwachung spielten das Polizeipräsidium Mannheim und die Landespolizeidirektion Stuttgart II (vgl. 22. Tätigkeitsbericht, LT-Drs. 13/520, S. 19 ff.). Die Polizeidirektionen Heilbronn und Böblingen zogen nach. In Stuttgart hat die Polizei die Videoüberwachung nach 18 Monaten, in Böblingen nach drei Monaten wieder abgeschaltet, weil kein Kriminalitätsbrennpunkt mehr vorlag. Als wir Ende Mai 2003 in der Presse lasen, dass in Singen eine polizeiliche Videoüberwachung an den Start gehen soll, fragten wir die Stadt Singen und die für das Stadtgebiet Singen zuständige Polizeidirektion Konstanz, nach welchen Kriterien die für die Videoüberwachung vorgesehenen Straßen und Plätze ausgesucht worden sind, insbesondere welche Straftaten, die sich dort zugetragen haben, für die Auswahl maßgebend sind und inwiefern sich diese Straßen und Plätze hinsichtlich ihrer Kriminalitätsbelastung deutlich von anderen Orten in Singen unterscheiden. Die Polizeidirektion verwies uns an die Stadt. Am 2. Juni 2003 nahm die Stadt, wie wir in der Presse zu lesen bekamen, die Videoüberwachung, die ihr Oberbürgermeister mit Verfügung vom 26. Mai 2003 angeordnet hatte, in der Bahnhof- und August-Ruf-Straße in Betrieb. Mit ihrer Antwort auf unsere Fragen ließ sich die Stadt mehr Zeit. Mitte Juli 2003 erreichte uns ihr Schreiben. Darin bat die Stadt um Nachsicht, dass sie versäumt hatte, die Videoüberwachung einer Vorabkontrolle zu unterziehen. Wie notwendig eine solche Kontrolle gewesen wäre, stellte sich erst mit unserer Überprüfung heraus:

2.1 Das Grundproblem: Der Kriminalitätsbrennpunkt

Wie ein roter Faden zog sich durch das Gesetzgebungsverfahren, mit dem die Regelung über die Videoüberwachung in das Polizeigesetz eingefügt worden ist, dass die polizeiliche Videoüberwachung auf so genannte Kriminalitätsbrennpunkte zu begrenzen ist. Die Frage war allerdings: Was ist eigentlich unter einem solchen Brennpunkt zu verstehen? Der Verweis auf die „gefährlichen Orte“ des § 26 Abs. 1 Nr. 2 des Polizeigesetzes, an denen die Polizei eine Identitätsfeststellung durchführen darf, erschien ziemlich verunglückt. Dies sind Orte, an denen „erfahrungsgemäß Straftäter sich verbergen, Personen Straftaten verabreden, vorbereiten oder verüben, sich ohne die erforderliche Aufenthaltserlaubnis treffen oder der Prostitution nachgehen“. In dieser gesetzlichen Beschreibung findet das gesetzgeberische Motiv, die polizeiliche

Videoüberwachung auf Kriminalitätsbrennpunkte zu beschränken, wenn überhaupt, dann nur recht unzulänglich Ausdruck. So ist etwa der bloße Aufenthalt von Straftätern oder Personen, die keine erforderliche Aufenthaltserlaubnis besitzen oder der Prostitution nachgehen, schon nach der gesetzgeberischen Intention nicht ausreichend, um eine polizeiliche Videoüberwachung dieser Örtlichkeit zu rechtfertigen. Unsere Hinweise darauf und unser Vorschlag, im Polizeigesetz zu regeln, was unter einem Kriminalitätsbrennpunkt zu verstehen ist, fanden im Gesetzgebungsverfahren kein Gehör (vgl. 21. Tätigkeitsbericht, LT-Drs. 12/5740, S. 61 f.). Nähere Bestimmungen zu der Frage des Vorliegens eines Kriminalitätsbrennpunkts hat das Innenministerium dann in seiner Führungs- und Einsatzanordnung zur Videoüberwachung im öffentlichen Raum vom 22. Februar 2001 getroffen. Danach ist jedenfalls klar, dass eine polizeiliche Videoüberwachung einer Örtlichkeit nicht bereits dann zulässig ist, wenn sie als „gefährlicher Ort“ im Sinne von § 26 Abs. 1 Nr. 2 des Polizeigesetzes eingestuft wird. Vielmehr muss die Örtlichkeit eine besondere Kriminalitätsbelastung aufweisen. Maßgeblich sind dabei die Bereiche der Straßenkriminalität, des Vandalismus und offener Drogenszenen sowie anderer Straftaten, die sich in der Öffentlichkeit zutragen und das Sicherheitsgefühl der Bevölkerung besonders beeinträchtigen. In der schriftlichen Einsatzanordnung sind die Gründe, die den Einsatz der Videoüberwachung erforderlich machen, und die Tatsachen anzugeben, auf denen sie fußen; rein statistische Angaben genügen dafür nicht. Hierzu sind vielmehr anhand spezifischer Kriminalitätslagebilder die für die Annahme eines Kriminalitätsbrennpunkts maßgeblichen Umstände konkret darzulegen.

Daran haperte es bei der Videoüberwachung in Singen nicht nur, weil die Stadt fälschlicherweise offenbar davon ausgegangen ist, für die Annahme eines Kriminalitätsbrennpunkts reiche das Vorliegen eines so genannten „gefährlichen Ortes“ im Sinne von § 26 Abs. 1 Nr. 2 des Polizeigesetzes aus, sondern vor allem deshalb, weil nach den Einlassungen der Stadt und den uns dazu übersandten Unterlagen nicht belegt war, dass es sich bei den videoüberwachten Örtlichkeiten um einen Kriminalitätsbrennpunkt handelt. Zwar erschöpfte sich das Kriminalitätslagebild der Polizeidirektion, auf das die Stadt ihre Anordnung stützte, nicht allein in statistischen Angaben. Gleichwohl war das Vorliegen eines Kriminalitätsbrennpunkts an den videoüberwachten Örtlichkeiten in Singen nicht belegt. Die Zahlenangaben zu mutmaßlich oder tatsächlich begangenen Straftaten und zu polizeilichen Einsätzen konnten zur Frage des Vorliegens eines Kriminalitätsbrennpunkts schon deshalb wenig beitragen, weil sich diese Angaben nicht auf die überwachten Bereiche der Bahnhof- und August-Ruf-Straße, sondern praktisch auf die gesamte Innenstadt von Singen bezogen. Eine auf die videoüberwachte Örtlichkeit zugeschnittene Auswertung war der Polizeidirektion, wie sie in ihrem Kriminalitätslagebild einräumte, gar nicht möglich. Ihr Statistikprogramm konnte nur zwischen der gesamten Stadt und der Innenstadt von Singen unterscheiden, von der der videoüberwachte Bereich wiederum nur einen kleinen Teil ausmachte. Unter den in der statistischen Auswertung aufgeführten Delikten befanden sich zwar auch Delikte aus dem Bereich der Straßenkriminalität. Irgendetwas dazu, ob und, wenn ja, welche dieser Delikte – worauf es aber im vorliegenden Zusammenhang entscheidend ankommt – sich in dem videoüberwachten Bereich der Bahnhof-/August-Ruf-Straße zugetragen hatten oder ob sie sonst wo in der Innenstadt passiert waren, ließ sich dem Kriminalitätslagebild nicht entnehmen. Entsprechend verhielt es sich mit den in der Statistik erwähnten polizeilichen Einsätzen wegen Betäubungsmitteldelikten und Schlägereien. Die Hinweise der Polizeidirektion in ihrem Kriminalitätslagebild auf den multikulturellen Charakter des Gebiets um die Bahnhof-/August-Ruf-Straße und auf Einsätze wegen hilfloser Personen und Ruhestörungen oder Pöbeleien von Betrunkenen sowie darauf, dass es im Bereich des Bahnhofs regelmäßig zu Aufgriffen von Ausländern komme, die sich ohne die erforderliche Aufenthaltserlaubnis in Deutschland aufhalten, konnten schon deshalb nicht verfangen, weil sie keinen Aufschluss darüber geben, dass diese Örtlichkeit eine besondere Kriminalitätsbelastung vor allem im Bereich

der Straßenkriminalität aufweist. Soweit schließlich die Polizeidirektion in ihrem Kriminalitätslagebild darauf abstellte, in Lokalen im Bereich des Bahnhofs komme es zu Drogenhandel, illegalem Glücksspiel und Prostitution, war die Erforderlichkeit der polizeilichen Videoüberwachung nicht dargetan, zumal sich die Straftaten nach den Ausführungen der Polizeidirektion in den Lokalen und damit außerhalb des Blickwinkels der Videokameras zutrugen.

2.2 Eine problematische Amtshilfe

Wer sich mit der polizeilichen Videoüberwachung befasst hat, weiß: Zum Nulltarif ist sie nicht zu haben. Sie kostet nicht nur eine Stange Geld – und zwar ganz gleich, ob eine stationäre Anlage wie in Mannheim, Stuttgart und Heilbronn, oder die mobile Anlage, die das Land beschafft hat, wie in Singen zum Einsatz kommt. Daneben braucht man auch Personal: Zum einen so genannte Videosachbearbeiter, also Polizeibeamte, die ständig am Überwachungsmonitor sitzen, und zum anderen Interventionskräfte, also Polizeibeamte, die umgehend vor Ort sind, wenn der Videosachbearbeiter an seinem Überwachungsmonitor etwas Verdächtiges entdeckt hat. Weil wir ahnten, in welche Bredouille die Ortspolizeibehörden, also die Städte und Gemeinden, kommen können, weil sie gar kein Personal haben, das für die vorbeugende Bekämpfung von Straftaten und für die Verfolgung der Straßenkriminalität eingesetzt werden kann, hatten wir im Gesetzgebungsverfahren geraten, den Ortspolizeibehörden erst gar nicht die Befugnis zur Videoüberwachung einzuräumen. Gekommen ist es anders. Deshalb war die Stadt Singen als Ortspolizeibehörde von Gesetzes wegen befugt, die Anordnung selbst zu treffen. Personal für die Videoüberwachung hatte sie jedoch nicht. Deshalb kam sie mit der für ihr Stadtgebiet zuständigen Polizeidirektion Konstanz überein, dass eine aus Polizeibeamten des Polizeireviers und der Kriminalaußenstelle Singen sowie Beamten des Bundesgrenzschutzes und des Zolls gebildete Einsatzgruppe die Durchführung der Videoüberwachung in Amtshilfe erledigen soll.

Dies war schon deshalb problematisch, weil kennzeichnend für die Amtshilfe ist, dass sie zu einer Amtshandlung der ersuchenden Behörde beiträgt, mithin also unterstützenden Charakter hat. Die Herrschaft über die Maßnahme, zu der Hilfe erbeten wird, und über das Verfahren im Ganzen muss dagegen bei der ersuchenden Behörde verbleiben. Sie trägt dementsprechend die rechtliche Verantwortung für die Zulässigkeit der Maßnahme. Weil die Stadt der Einsatzgruppe gar keine Vorschriften gemacht hatte, wie sie bei der Videoüberwachung zu verfahren hat, die Einsatzgruppe dabei vielmehr völlig selbstständig vorgegangen ist, wird man kaum davon sprechen können, dass sie in Amtshilfe für die Stadt tätig geworden ist. Die Konstruktion der Stadt trägt auch deshalb nicht, weil sich die Verarbeitung personenbezogener Daten von vornherein nicht auf die Grundsätze der Amtshilfe stützen lässt. Gerade solches geschah jedoch im vorliegenden Zusammenhang, weil die infolge ihrer Anordnung für die Videoüberwachung verantwortliche Stadt Singen den an den Überwachungsmonitoren sitzenden Beamten – damit auch dem Bundesgrenzschutz und dem Zoll – die dort aufgelaufenen Videobilder und deshalb in der Terminologie des Datenschutzrechts personenbezogene Daten übermittelt hat. Für eine solche Datenübermittlung an den Bundesgrenzschutz und an den Zoll gab es keine Rechtsgrundlage. Wenn überhaupt, wäre ein Einsatz der Beamten des Bundesgrenzschutzes und des Zolls an den Überwachungsmonitoren nur in Frage gekommen, wenn sie so genannte Verwaltungshelfer der Stadt gewesen wären. Dafür hatte die Stadt jedoch weder etwas dargetan noch sprach sonst irgendetwas für eine solche Konstruktion.

2.3 Kamera läuft und niemand sitzt am Überwachungsmonitor

Soll die polizeiliche Videoüberwachung den mit ihr erklärtermaßen verfolgten Zweck, die Straßenkriminalität vorbeugend zu bekämpfen, überhaupt erreichen können, ist es unerlässlich, dass ständig Polizeibeamte an den Überwachungsmonitoren sitzen und die dort auflaufenden Videobilder verfolgen. Zudem muss ein unverzügliches Einschreiten

der Polizei im Ernstfall sichergestellt sein. Davon ist auch der Gesetzgeber ausgegangen. Er hat in der Begründung des Gesetzes, mit dem die Regelung über die polizeiliche Videoüberwachung in das Polizeigesetz eingefügt worden ist, betont, dass die Geschehnisse vor Ort auf dem Überwachungsmonitor zu beobachten sind. Auch das Innenministerium hat im Zuge des Gesetzgebungsverfahrens wiederholt betont, dass eine polizeiliche Videoüberwachung nur Sinn macht, wenn das, was sich vor Ort abspielt, am Monitor von der Polizei permanent beobachtet wird, und dass durch eine sinnvolle Einsatzkonzeption dafür gesorgt werden muss, dass die Einsatzkräfte möglichst schnell am Ort der Tat eintreffen, wenn am Monitor eine Straftat festgestellt wird. Bis nach Singen war das offenbar nicht durchgedrungen. Zwar liefen die Videokameras rund um die Uhr. Weil sich, wie es in der Einsatzkonzeption hieß, die Einsatzzeiten der Einsatzgruppe an der 40-Stunden-Wochenarbeitszeitregelung orientierten und Mehrarbeit nach Möglichkeit nicht anfallen sollte, waren die Überwachungsmonitore jedoch nur von 8.00 bis 18.00 Uhr besetzt; in den übrigen Zeiten saß niemand davor. Zudem war die Einsatzbereitschaft der Einsatzgruppe montags bis freitags nur von 10.00 bis 22.00 Uhr, samstags nur von 10.00 bis 17.00 Uhr und sonn- und feiertags je nach Einsatzlage gewährleistet. Deshalb vermittelten die Hinweisschilder, auf denen Stadt und Polizeidirektion den Bürgern versprochen hatten, dass die Bahnhof-/August-Ruf-Straße zu deren Sicherheit von der Polizei videoüberwacht wird, insoweit allenfalls ein trügerisches Sicherheitsgefühl. Sitzt nämlich niemand am Überwachungsmonitor, lassen sich mit der polizeilichen Videoüberwachung von vornherein weder Straftaten verhindern noch Gefahren für die öffentliche Sicherheit abwehren noch Störungen der öffentlichen Sicherheit beseitigen. Kurzum: Die Videoüberwachung verfehlte insoweit ihren Zweck und stand schon deshalb mit § 21 Abs. 3 des Polizeigesetzes nicht im Einklang.

Als wir Anfang August 2003 die Stadt Singen und die Polizeidirektion Konstanz auf diese Schwachstellen hinwiesen und um Abhilfe baten, ersuchte die Stadt Singen wegen der Ferienzeit und weil unsere Ausführungen vielschichtig ausgefallen seien um Geduld bis Anfang September. Als dann immer noch Funkstille herrschte, erinnerten wir Ende September schriftlich an die Erledigung. Eine Antwort haben wir gleichwohl nicht erhalten. Am 13. Oktober 2003 rief ein Mitarbeiter der Stadt bei uns an und kündigte den alsbaldigen Eingang der Stellungnahme an. Dabei sagte er auch, nach Lage der Dinge werde die polizeiliche Videoüberwachung zum 15. Oktober 2003 beendet. Der Stadt sei der finanzielle Aufwand zu groß; man habe auch Schwierigkeiten, das Vorliegen eines Kriminalitätsbrennpunkts zu begründen. Zudem binde die Videoüberwachung mehr Personal, als die Polizei dafür abstellen könne. Die angekündigte Stellungnahme hat ihren Weg zu uns immer noch nicht gefunden. Dass die Videoüberwachung dann tatsächlich eingestellt worden ist, haben wir der Presse entnommen. So kann man sich auch aus der Affäre ziehen. Die örtliche Presse feierte den erfolgten Einsatz der Videoüberwachung übrigens vor allem auch damit, dass man auf diese Weise der Unsitte mancher „Wandpinkler“ auf die Spur gekommen sei. Auch dieser Aspekt wird jedoch nicht reichen, einen Kriminalitätsbrennpunkt in dem überwachten Bereich wenigstens im Nachhinein zu begründen.

3. Das Lagebildinformationssystem (LABIS) der Polizei

Vorbeugen ist besser als Heilen. Diese alte Weisheit gilt auch im Datenschutz. Seit jeher steht deshalb – wenn auch an etwas versteckter Stelle – im Landesdatenschutzgesetz, dass mein Amt die Behörden und öffentlichen Stellen in Fragen des Datenschutzes beraten kann. In Anspruch genommen haben die Behörden dieses Angebot in der Vergangenheit freilich nicht allzu oft. Deshalb und obwohl mir klar war, dass eine fundierte Beratung viel Arbeitskapazität bindet, die woanders genauso dringend gebraucht wird, lag mir bei meinem Amtsantritt viel daran, diesen wichtigen Bereich aus seinem Dornröschenschlaf zu erwecken und die Behörden zu ermuntern, in Sachen Datenschutz unseren Rat einzuholen, ehe alles ins Werk gesetzt ist. So war es erfreulich, dass die Landespolizeidirektion Stuttgart I

mein Amt frühzeitig zum neuen LABIS-System konsultierte, das sie und die ihr nachgeordnete Polizeidirektion Böblingen erarbeitet hatten. Landespolizeidirektion und Polizeidirektion führten uns den Prototyp vor und legten dabei von Anfang an die Karten offen auf den Tisch. Auch das Innenministerium beteiligte sich an den Besprechungen.

3.1 LABIS – was es weiß, was es kann

Mit LABIS verfolgt die Polizei zweierlei Ziele: Zum einen ermöglicht LABIS, aktuelle und kleinräumig gegliederte Lagebilder zu erstellen. Zum anderen unterstützt LABIS die Polizei bei der Erfüllung ihrer Aufgaben, insbesondere bei der Verfolgung und vorbeugenden Bekämpfung von Straftaten, der Aufklärung und Verhinderung von Ordnungswidrigkeiten, der polizeilichen Präventionsarbeit, der Aufklärung und Verhütung von Unfällen im Straßenverkehr, der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung und zudem auch noch bei der Einsatzplanung und der Bewältigung des internen Geschäftsablaufs. Dazu verfügt LABIS über eine Lagebildkomponente und eine Abfrage-/Auswertungskomponente. Diese beiden Komponenten setzen auf einer Datenbank auf, in der die Polizeidirektion Vorkommnisberichte speichert, die ihre Polizeibeamten tagtäglich über Vorfälle fertigen, mit denen sie dienstlich befasst sind. Die Vorkommnisberichte betreffen ganz unterschiedliche Ereignisse. Dabei kann es um Ladendiebstahl, Betäubungsmitteldelikte oder andere Straftaten, um Ordnungswidrigkeiten, Verkehrsunfälle, Familienstreitigkeiten, vermisste Personen, Betrunkene oder Ruhestörungen gehen. Die Liste der Ereignisse ist nicht abschließend. Vielmehr eröffnet LABIS der Polizeidienststelle, die das System einsetzt, die Möglichkeit, den Ereigniskatalog zu ergänzen und damit die Weichen dafür zu stellen, welche Vorfälle in der LABIS-Datenbank erfasst werden. Je detaillierter der Ereigniskatalog ist, umso mehr gibt die LABIS-Datenbank jedem Polizeibeamten, der die Datenbank abfragen kann, einen Überblick darüber, mit welchen Vorfällen die Polizeidienststelle befasst ist oder gewesen ist und in welcher Eigenschaft die Person, mit der man es gerade zu tun hat, in den gespeicherten Vorkommnisberichten erwähnt ist, beispielsweise als Beschuldigter, Tatverdächtiger, Betroffener, Anzeigeerstatter, Geschädigter, Störer, Unfallverursacher/-beteiligter, Zeuge, Hinweisgeber oder als Auskunftsperson.

3.2 Wie steht es um den Datenschutz?

Klar ist: Wer ein so komplexes Datenverarbeitungssystem wie LABIS ins Werk setzen will, muss in puncto Datenschutz an mancherlei denken. Dessen waren sich Landespolizeidirektion und Polizeidirektion wohl bewusst. Ihre gemeinsamen Überlegungen hatten sie in einem Benutzerhandbuch und in einer vorläufigen Dienstanweisung zusammengefasst. Unsere Ratschläge dazu griffen beide auf. Dabei ging es uns vor allem um folgende Punkte:

3.2.1 Kurze Speicherfrist und zeitlich begrenzte Abfragemöglichkeiten

Ganz gleich, ob ein Polizeibeamter eine LABIS-Abfrage startet, weil er gegen einen Beschuldigten wegen des Verdachts einer Straftat ermittelt oder weil er gegen jemanden wegen eines Verkehrsunfalls oder einer Verkehrsordnungswidrigkeit tätig wird oder weil eine Person als vermisst gemeldet worden ist – in jedem Fall bekommt er alle Daten auf seinem Bildschirm angezeigt, die über die betreffende Person in der LABIS-Datenbank gespeichert sind. Diese Gestaltung der LABIS-Abfrage strapaziert das auch bei der polizeilichen Datenverarbeitung stets zu beachtende Gebot der Zweckbindung und den Grundsatz der Erforderlichkeit. Das Gebot der Zweckbindung besagt, dass die Polizei personenbezogene Daten grundsätzlich nur zu dem Zweck nutzen und verwenden darf, zu dem sie die Daten erlangt hat. Demzufolge darf die Polizei Daten, die sie beispielsweise für Zwecke der vorbeugenden Bekämpfung von Straftaten speichert, nur zu diesem Zweck und Daten, die sie zur Abwehr von Gefahren für

die öffentliche Sicherheit und Ordnung speichert, nur hierfür nutzen und verwenden. Für eine andere polizeiliche Aufgabe darf sie diese Daten ausnahmsweise verwenden, wenn die Polizei die Daten zu diesem Zweck erheben dürfte. Bei einer LABIS-Abfrage erhält ein Polizeibeamter jedoch zwangsläufig immer sämtliche Daten, die über den Betroffenen gespeichert sind, auf dem Bildschirm angezeigt – und zwar ganz gleich, ob die Daten zu dem polizeilichen Zweck, der Anlass für die Abfrage gewesen ist, oder ob sie für einen ganz anderen polizeilichen Zweck gespeichert sind. Dass er dabei auch Daten angezeigt bekommt, die er zur Erfüllung seiner Aufgabe, die ihn zu der LABIS-Abfrage veranlasst hat, gar nicht benötigt, liegt auf der Hand, wenn man sich einmal vor Augen führt, dass beispielsweise ein Polizeibeamter bei einer LABIS-Abfrage über einen Verkehrsunfallverursacher am Bildschirm auch darüber informiert wird, dass die Polizei wegen einer Ruhestörung oder wegen eines Familienstreits schon einmal mit ihm zu tun hatte. Solche Informationen helfen dem Polizeibeamten bei der Bearbeitung des Verkehrsunfalls nicht weiter; sie sind – um es mit den Worten des Datenschutzrechts zu sagen – zur Erfüllung seiner Aufgabe nicht erforderlich. Auf der anderen Seite ist die Polizei jedoch durchaus berechtigt, Vorkommnisberichte samt der darin enthaltenen personenbezogenen Daten zu Zwecken der Vorgangsbearbeitung in einem automatisierten Datenverarbeitungssystem für eine gewisse Zeit zu speichern und für diese Zeit die gespeicherten Daten zu diesem Zweck oder unter den geschilderten Voraussetzungen für einen anderen polizeilichen Zweck zu nutzen. Deshalb galt es mit der Landespolizeidirektion und der Polizeidirektion eine Lösung zu finden, die diese legitimen Interessen der Polizei und die beschriebenen Auswirkungen von LABIS-Abfragen auf das Zweckbindungsgebot und den Grundsatz der Erforderlichkeit möglichst unter einen Hut bringt. Sie sieht so aus: Die Polizeidirektion kann Vorkommnisberichte zwölf Monate lang in ihrer LABIS-Datenbank speichern. Die allermeisten Polizeibeamten können jedoch nur drei Monate lang auf die Vorkommnisberichte online zugreifen, einige wenige mit einer Sonderberechtigung ausgestattete Polizeibeamte auch noch darüber hinaus.

3.2.2 Maßgeschneiderte Zugriffsberechtigungen

Eine Polizeidirektion ist keine einheitliche Behörde. Sie ist vielmehr in verschiedene Bereiche mit unterschiedlichen Aufgaben gegliedert, man denke nur an die Kriminalpolizei oder die Verkehrspolizei. Zudem sind ihr Polizeireviere mit eigenen Aufgaben in ihrem Gebiet nachgeordnet. Weil aber im Datenschutz der Grundsatz gilt, dass nicht jeder Mitarbeiter einer Behörde alles wissen muss, was unter ihrem Dach läuft, sondern nur Zugang zu den Daten haben darf, die er zur Erfüllung seiner dienstlichen Aufgaben braucht, waren wir uns mit Innenministerium, Landespolizeidirektion und Polizeidirektion rasch einig, dass für LABIS dasselbe gilt und deshalb unterschiedliche Benutzergruppen einzurichten sind mit der Folge, dass die Mitglieder einer Benutzergruppe grundsätzlich nur auf die von ihrer eigenen Benutzergruppe eingespeicherten Vorkommnisberichte online zugreifen können. Deshalb können beispielsweise Polizeibeamte eines Polizeireviers, die eine Benutzergruppe bilden, nur die von ihrem Polizeirevier, nicht jedoch die von ihrem Nachbarrevier in LABIS eingespeicherten personenbezogenen Daten und Vorkommnisberichte an ihrem LABIS-Bildschirm aufrufen.

3.2.3 Vorsicht bei einer Datenweitergabe

Will die Polizeidirektion in LABIS gespeicherte Daten weitergeben, muss sie bedenken, dass LABIS immer nur ein mehr oder weniger unvollständiges Bild von den Einzelheiten eines gespeicherten Vorgangs gibt. Beispielsweise ist aus einem am Bild-

schirm angezeigten Vorkommnisbericht über eine Straftat insbesondere nicht zu erkennen, ob der Betroffene die ihm zur Last gelegte Straftat tatsächlich begangen hat, welches die näheren Tatumstände waren und welchen Ausgang das Ermittlungsverfahren genommen hat. Deshalb ist es ein eherner Grundsatz, dass keine Entscheidung allein aufgrund einer Bildschirmanzeige getroffen werden darf. Stets muss zudem anhand der Akten und schriftlichen Unterlagen geprüft werden, ob der Eindruck, den der Bildschirm vermittelt, auch tatsächlich zutrifft. Dies gilt umso mehr, wenn die Absicht besteht, aus den gespeicherten Daten irgendwelche Konsequenzen zu ziehen. Deshalb muss die Polizeidirektion vor der Weitergabe gespeicherter Daten diese auf ihre Speicherberechtigung und Relevanz überprüfen. Dies hat sie in ihrer LABIS-Dienstanweisung klargestellt.

3.2.4 Protokollierung der Abfragen

Wer personenbezogene Daten mit Hilfe von Computern verarbeitet, muss technische und organisatorische Maßnahmen ergreifen, um eine datenschutzgerechte Datenverarbeitung sicherzustellen. Zu den Standardmaßnahmen gehört dabei unter anderem eine effektive Protokollierung. Dies setzt wiederum voraus, dass ein Programm vorhanden ist, das Zugriffe auf gespeicherte personenbezogene Daten automatisch so protokolliert, dass die Protokolle Auskunft darüber geben, wer wann auf welche Daten zugegriffen hat. Das mussten wir der Landespolizeidirektion und der Polizeidirektion gar nicht lange erklären. Sie haben LABIS mit einem entsprechenden Protokollierungsprogramm nachgerüstet.

Inzwischen hat das Innenministerium LABIS für den Einsatz bei den Polizeidienststellen freigegeben. Ob es die großen Erwartungen erfüllt, die die Polizei damit verbindet, muss sich zeigen. Klar ist dagegen schon jetzt, dass für LABIS – ganz gleich wo es läuft – die datenschutzrechtlichen Standards gelten, die wir bei unserer Beratung mit der Landespolizeidirektion Stuttgart I, der Polizeidirektion Böblingen und dem Innenministerium für den Prototyp erarbeitet haben.

4. Einzelfälle

Tagtäglich wenden sich gerade auch im Bereich der Polizei Bürgerinnen und Bürger mit der Bitte um Rat und Hilfe an mein Amt. Ihre Anliegen sind vielfältig. Sie reichen von der allgemeinen Frage, wo man Auskunft über polizeiliche Datenspeicherungen erhalten kann, bis zur Bitte eines Autofahrers zu prüfen, was es mit dem Vorhalt eines Polizeibeamten bei einer Verkehrskontrolle auf sich hat, er sei als politisch motivierter Straftäter im Polizeicomputer registriert. Wie sehr die Bürgerinnen und Bürger angesichts der für sie kaum zu überblickenden Vielgestaltigkeit der polizeilichen Datenverarbeitung dabei auf mein Amt zählen, zeigen ihre Reaktionen. Manche halten die in ihrem Fall maßgeblichen Datenverarbeitungsvorschriften für zu weit gehend, andere lassen erkennen, für wie wichtig sie die Information und Unterstützung des Datenschutzbeauftragten halten: „Über Ihr Antwortschreiben habe ich mich sehr gefreut und möchte Ihnen sehr herzlich für Ihre Mühe danken.“

4.1 Wer war der Anonymus? oder: Kein Fall für die DNA-Datei

Ein Staatsanwalt war in einem anonymen Brief der fortgesetzten Strafvereitelung und Verfolgung Unschuldiger bezichtigt worden. Bei der Staatsanwaltschaft, der der Staatsanwalt selbst angehörte, erstattete dieser gegen den Anonymus Gegenanzeige. Weil sich in der anonymen Anzeige eine Formulierung fand, wie sie ein Mann in einem der Staatsanwaltschaft vorliegenden Schreiben verwendet hatte und weil die Staatsanwaltschaft annahm, der Mann habe sich von dem Staatsanwalt ungerecht behandelt gefühlt und deshalb ein Motiv für die anonyme Anzeige gehabt, leitete sie gegen ihn ein Ermittlungsverfahren wegen falscher Verdächtigung ein. Mit diesem Vorwurf konfrontiert, stellte der Mann ganz entschieden in Abrede, der anonyme Anzeigeerstatter zu

sein. Um anhand einer DNA-Analyse feststellen zu können, ob die Speichelanhaftungen an der Briefmarke des anonymen Briefs von dem Mann stammen, bat die Staatsanwaltschaft ihn gleichwohl, eine Speichelprobe abzugeben. Dieser Bitte kam der Mann nicht nach. Auf Antrag der Staatsanwaltschaft ordnete das Amtsgericht an, dem Mann eine Blutprobe zu entnehmen und die Blutprobe samt den an der Briefmarke des anonymen Briefs gefundenen Speichelantragungen einer DNA-Analyse zu unterziehen. Mit dem Vollzug der amtsgerichtlichen Anordnungen befasste die Staatsanwaltschaft die in ihrem Sprengel ansässige Polizeidirektion. In Anbetracht der amtsgerichtlichen Anordnungen gab der Mann zur Abwendung der Entnahme einer Blutprobe bei der Polizeidirektion schließlich eine Speichelprobe ab und willigte schriftlich darin ein, dass die Speichelprobe zur Klärung der Frage, ob er als derjenige in Betracht kommt, von dem die Speichelspuren an der Briefmarke des anonymen Briefs stammen, verwendet werden kann. Die DNA-Analyse gab die Polizeidirektion beim Kriminaltechnischen Institut des Landeskriminalamts in Auftrag. Das Ergebnis der Analyse war: keine Übereinstimmung. Dennoch war der Mann für zehn Jahre bis Dezember 2010 in der DNA-Analyse-Datei erfasst worden. Um zu verstehen, wie es dazu kam, muss man Folgendes wissen:

Die DNA-Analyse-Datei läuft seit 1998 auf dem Rechner des Bundeskriminalamts. Mittlerweile haben die Polizeien des Bundes und der Länder in dieser Datei zu Zwecken der Identitätsfeststellung in künftigen Strafverfahren die DNA-Identifizierungsmuster von mehr als 250 000 Personen erfasst. Will eine baden-württembergische Polizeidienststelle eine Person mit ihrem DNA-Identifizierungsmuster in die DNA-Analyse-Datei einspeichern, muss sie den extra dafür geschaffenen „Meldebogen DNA-Analyse-Datei“ ausfüllen und dem Landeskriminalamt zuleiten, das die Datenerfassung in der DNA-Analyse-Datei anhand dieser Meldebögen zentral für alle Polizeidienststellen im Lande erledigt. Deshalb staunten wir nicht schlecht, als uns die Polizeidirektion auf unsere Frage zunächst wissen ließ, der Mann sei im Zuge der besagten DNA-Analyse tatsächlich in der DNA-Analyse-Datei erfasst worden; wie es dazu gekommen ist, sei für sie jedoch nicht nachvollziehbar. Als wir daraufhin in die Akten der Polizeidirektion schauten, war rasch klar, dass sie selbst die Speicherung in der DNA-Datei veranlasst hatte. Die Polizeidirektion hatte nämlich mit ihrem DNA-Untersuchungsauftrag dem Landeskriminalamt einen „Meldebogen DNA-Analyse-Datei“ zugeleitet und darin angekreuzt, dass der Mann mit seinem DNA-Identifizierungsmuster, das bei der DNA-Analyse aus Anlass der ihm zur Last gelegten falschen Verdächtigung festgestellt worden ist, bis Dezember 2010 in der DNA-Analyse-Datei zu registrieren ist, was das Landeskriminalamt sodann auftragsgemäß erledigte.

Diese Datenspeicherung stand von Anfang an mit den dafür geltenden Vorschriften nicht im Einklang. Deshalb tat die Polizeidirektion gut daran, dass sie ihre Entscheidung sofort revidierte und die Löschung der Daten des Mannes in der DNA-Analyse-Datei in die Wege leitete, als wir sie darauf ansprachen. In dieser Datei dürfen DNA-Identifizierungsmuster von Beschuldigten gespeichert werden, gegen die wegen des Verdachts einer Straftat von erheblicher Bedeutung ein strafrechtliches Ermittlungsverfahren geführt wird, wenn wegen Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig Strafverfahren wegen einer Straftat von erheblicher Bedeutung – dazu zählen insbesondere Verbrechen, Vergehen gegen die sexuelle Selbstbestimmung, gefährliche Körperverletzung, Diebstahl in besonders schwerem Fall oder Erpressung – zu führen sind. An diesen Voraussetzungen fehlte es hier. Bei der dem Mann zur Last gelegten falschen Verdächtigung handelte es sich – einmal abgesehen davon, dass das Ergebnis der DNA-Analyse dagegen sprach, er sei der Anonymus – nun wirklich nicht um eine Straftat von erheblicher Bedeutung, weil dieser Tatvorwurf nach Art und Schwere weder mit den genannten Regelbeispielen vergleichbar noch sonst geeignet war, den Rechtsfrieden empfindlich zu stören. Zum anderen fehlte es an einer Prognose, der Mann

werde künftig Straftaten von erheblicher Bedeutung begehen. Irgendwelche Überlegungen dazu hatte die Polizeidirektion erst gar nicht angestellt.

Mancher wird sich noch fragen, ob die Anordnung der DNA-Analyse durch das Amtsgericht angesichts der Tatsache, dass mit einer DNA-Analyse ein tiefgreifender und nachhaltiger Eingriff in das Recht auf informationelle Selbstbestimmung einhergeht, gerechtfertigt war. Die Beantwortung dieser Frage muss ich jedem selbst überlassen, weil ich infolge der Regelungen des Landesdatenschutzgesetzes solche richterliche Anordnungen aus datenschutzrechtlicher Sicht nicht überprüfen kann. Die Staatsanwaltschaft, die die richterliche Anordnung beantragt hatte, ließ uns jedenfalls wissen, sie habe unsere Hinweise zu dem Fall des Mannes zum Anlass genommen, ihre Dezernenten zur besonders sorgfältigen Prüfung des Verhältnismäßigkeitsgrundsatzes anzuhalten.

4.2 Ein misslungener Zeugenaufruf und seine fehlgeschlagene Wiedergutmachung

Wenn die Polizei bei ihren Ermittlungen nicht recht vorankommt, schaltet sie manchmal in der Presse einen Zeugenaufruf in der Hoffnung, dass sich Personen melden, die zu dem fraglichen Vorfall aus eigener Anschauung etwas sagen können. Wie die Polizei dabei mit dem Datenschutz in Konflikt geraten und wie leicht man sich noch weiter verheddern kann, wenn man versucht, einen dabei unterlaufenen Fehler via Presse wieder auszubügeln, zeigt der folgende Fall:

Eine junge Frau erstattete wegen eines Vorfalls, der sich knapp eine Woche zuvor mitten in der Nacht zugetragen hatte, bei einem Polizeirevier Anzeige gegen drei junge Männer wegen Körperverletzung und Bedrohung. Das Polizeirevier nahm die Angaben der jungen Frau für bare Münze und schaltete folgenden Zeugenaufruf in der örtlichen Presse:

„Bereits am ..., ..., (Wochentag, Datum) befand sich eine ... (Altersangabe)-jährige Frau auf dem Nachhauseweg vom ... (Bezeichnung der Veranstaltung), als sie in der ...straße von einem unbekannten Mann von hinten an den Oberarmen gepackt und zu Boden geworfen wurde. Dabei erlitt sie leichtere Verletzungen. Der Unbekannte soll ca. ... cm groß, ca. ... bis ... Jahre alt, ... (Beschreibung der Statur) sein und ... (Angaben zum Haarschnitt und zur Haarfarbe) Haare tragen. Der Unbekannte soll in Begleitung zweier namentlich bekannter Brüder gewesen sein, wovon einer anschließend die Geschädigte mit einer silberfarbenen Pistole bedrohte. Der Grund der Auseinandersetzung ist nicht bekannt. Zeugen des Vorfalls werden gebeten, sich mit dem Polizeirevier ... in Verbindung zu setzen."

Im Zuge seiner Ermittlungen stellte das Polizeirevier fest, dass zwei Polizeibeamte des Polizeireviers in der besagten Nacht mit dem Vorfall bereits befasst gewesen waren und dass nach deren Feststellungen der angezeigten Tat ein völlig anderer Sachverhalt zugrunde lag. Die Mutter der beiden in dem Zeugenaufruf erwähnten Brüder bat bei ihrer Anhörung die Polizeidirektion um eine Klarstellung des Sachverhalts in den Medien. Die Pressemitteilung der Polizeidirektion, die ebenfalls in der örtlichen Presse veröffentlicht worden ist, sah so aus:

„... (Wohnort der jungen Frau und der beiden Brüder). Die junge Frau, die am ... (Datumsangabe) eine Bedrohung und Körperverletzung bei der Polizei angezeigt hatte, schilderte dabei nur einen Teil des Sachverhalts, der dann Grundlage für den Pressebericht vom ... (Datumsangabe des Zeugenaufrufs) war. Nicht geschildert hat sie, dass sie vor der angezeigten Tat, in der Nacht zum ..., mit Steinen und einem Holzknüppel auf geparkte Autos in der ...-Straße eingeschlagen hat. Um weitere Sachbeschädigungen an ihren Fahrzeugen zu unterbinden, hatten die beiden Brüder und ein weiterer Mann die Frau festgehalten. Als dann Polizeibeamte eintrafen, hat sich die ...-Jährige, die auch deutlich alkoholisiert war, gegen die Mitnahme zur Dienststelle heftig gewehrt. Zunächst hatten in dieser Nacht alle

Beteiligten von einer Anzeigeerstattung abgesehen. Erst am ... entschloss sich die Frau, die Anzeige zu erstatten."

Weder der Zeugenaufruf des Polizeireviers noch die Pressemitteilung der Polizeidirektion waren datenschutzkonform, weil die Polizei beides Mal unzulässigerweise personenbezogene Daten über die junge Frau und die beiden Brüder weitergegeben und dabei zudem nicht das Gebot der Wahrheit und Sachlichkeit beachtet hatte. Dass die Polizei in dem Zeugenaufruf und in der Pressemitteilung wenigstens den Namen der jungen Frau und der beiden Brüder nicht genannt hat, spielt dabei keine Rolle. Denn personenbezogene Daten werden bereits dann weitergegeben, wenn die Bezugsperson mit Hilfe anderer Informationen objektiv festgestellt werden kann. Dies ist umso leichter möglich, je weiter Angaben über eine Person gestreut werden. Gehen sie nur einem bestimmten Adressatenkreis zu, lässt sich noch einigermaßen zuverlässig abschätzen, ob die Adressaten über das zur Identifizierung der betreffenden Personen erforderliche Zusatzwissen verfügen. Weit weniger lässt sich das bei der Weitergabe von Daten an einen größeren Kreis von Adressaten abschätzen. Gehen Angaben gar zur Veröffentlichung an die Presse und werden sie dann einem unüberschaubaren Personenkreis zugänglich, hat es praktisch niemand mehr in der Hand, dass Zeitungsleser mit Hilfe ihres vorhandenen oder des beschaffbaren Zusatzwissens auf die betreffenden Personen schließen können. Gerade so war es hier: Um wen es sich bei der erwähnten jungen Frau und den beiden Männern handelte, war in dem kleinen Ort für interessierte Zeitungsleser wegen der detaillierten Angaben über sie in dem Zeugenaufruf und in der Pressemitteilung rasch klar. Deshalb und weil die Polizei dabei Angaben über strafbares Verhalten in der Öffentlichkeit so ausbreitete, dass der Schluss auf die junge Frau und die beiden namentlich bekannten Männer leicht möglich war, verletzte sie deren schutzwürdige private Interessen. Viel gravierender war jedoch, dass der Zeugenaufruf und die Pressemitteilung zudem dem Gebot der Wahrheit und Sachlichkeit nicht entsprachen. Nach diesem Gebot, das alle Behörden zu beachten haben, wenn sie sich an die Medien wenden, dürfen an die Öffentlichkeit gerichtete Äußerungen von Behörden keine einseitigen Bewertungen enthalten. Die Angaben müssen insbesondere inhaltlich zutreffen. Wesentliche Aspekte, wie z. B. einen Beschuldigten entlastende Umstände, dürfen nicht weggelassen werden. Ferner ist darauf zu achten, dass die Mitteilung so abgefasst ist, dass sie keinen unzutreffenden Eindruck bei den Empfängerkreisen hervorruft, an die die Medien sich wenden. Dabei ist insbesondere dafür Sorge zu tragen, dass bei noch nicht abgeschlossenen strafrechtlichen Verfahren der Unschuldsvermutung Rechnung getragen wird. Diesen Anforderungen des Gebots der Wahrheit und Sachlichkeit trugen das Polizeirevier und die Polizeidirektion nicht hinreichend Rechnung: In dem Zeugenaufruf wurden die beiden Männer als Personen hingestellt, die nachts auf offener Straße zusammen mit einem dritten Mann die junge Frau praktisch überfallen und mit einer Pistole bedroht haben. Deshalb musste jeder, der den Zeugenaufruf in der Zeitung gelesen hat, davon ausgehen, dass die beiden Brüder eine schwere Straftat begangen haben. In Wahrheit hatte sich der Vorfall jedoch ganz anders abgespielt. Deshalb hätte das Polizeirevier in seinem Zeugenaufruf die beiden Brüder nicht als Straftäter hinstellen dürfen. Aber auch die Pressemitteilung, mit der die vorgesetzte Polizeidirektion diese Scharte auswetzen wollte, entsprach nicht dem Gebot der Sachlichkeit und Wahrheit. In der Pressemitteilung wird die junge Frau als jemand hingestellt, der nachts in betrunkenem Zustand auf offener Straße randaliert und mit Steinen um sich geworfen und mit einem Holzknüppel auf geparkte Autos eingeschlagen und sich auch noch gegen die herbeigerufenen Polizeibeamten heftig zur Wehr gesetzt hat. Das damit von der jungen Frau in der Öffentlichkeit gezeichnete Bild fand indes in mehrfacher Hinsicht in dem Vermerk, den die Polizeibeamten über ihren Einsatz gefertigt hatten, keine Entsprechung: Entgegen der Darstellung in der Pressemitteilung war darin nicht davon die Rede, dass die junge Frau mit Steinen geworfen und einem Holzknüppel auf geparkte Autos eingeschlagen und dabei – wie die Pressemitteilung suggeriert – erhebliche Schäden an mehreren Autos ange-

richtet hatte. Solches hatten dem Vermerk zufolge nicht einmal die Personen behauptet, die die Polizei herbeigerufen hatten. Zudem hatte die junge Frau entschieden bestritten, Autos beschädigt zu haben. Dass die Polizeidirektion in ihrer Pressemitteilung die junge Frau in der Öffentlichkeit auch noch als jemanden hinstellte, der gegen die herbeigerufenen Polizeibeamten – was durch deren Vermerk nicht bestätigt war – auch noch Widerstand geleistet hat, passte ins Bild. Weil nach alledem die Voraussetzungen der §§ 161, 163 der Strafprozessordnung bzw. des § 4 des Landespressegesetzes nicht vorlagen und dem Gebot der Wahrheit und Sachlichkeit nicht Rechnung getragen war, gingen der Zeugenaufruf des Polizeireviers und die Pressemitteilung der Polizeidirektion zu weit.

4.3 Ein unzulässiger Freundschaftsdienst

Mehr Publicity, als ihr lieb war, hatte eine Polizeidirektion. Einer ihrer Polizeibeamten hatte bei der benachbarten Landespolizeidirektion angerufen und bei der dortigen Gemeinsamen Ermittlungsgruppe Rauschgift (GER) unter Vorspiegelung dienstlicher Belange eine Person im Informationssystem des Zolls (INZOLL) abchecken lassen. Darum hatte ihn der Sicherheitsbeauftragte einer Firma gebeten, der früher einmal selbst Polizist gewesen war und den Polizeibeamten aus jener Zeit gut kannte und auf diese Weise in Erfahrung bringen wollte, ob der Zoll den Mitarbeiter und die Firma im Visier hat. Auf diesem Weg erfuhr der Sicherheitsbeauftragte von dem Polizeibeamten, dass der Zoll tatsächlich gegen den Mitarbeiter der Firma ermittelt. Diese INZOLL-Abfrage kam ans Licht, weil bei einer Durchsuchung der Firma Unterlagen darüber gefunden wurden. Als wir davon in der Presse lasen, stellte sich für uns die Frage, was tun eigentlich die Polizeidirektion und die Landespolizeidirektion, um solche unbefugten Computerabfragen zu verhindern.

In den bei den Landespolizeidirektionen eingerichteten Gemeinsamen Ermittlungsgruppen Rauschgift arbeiten Polizeibeamte mit Beamten der Zollfahndung zusammen. Die Beamten der Zollfahndung können dabei INZOLL online abfragen. INZOLL ist das Informations- und Auskunftssystem über Straftaten und Ordnungswidrigkeiten im Bereich der Zollverwaltung. In diesem Informationssystem werden personenbezogene Daten von ermittelten Verdächtigen sowie Sachverhalts- und Firmendaten erfasst. Dass sich Polizeibeamte solche Informationen nur zu dienstlichen Zwecken beschaffen und dass diese Informationen nicht in fremde Hände gelangen dürfen, liegt auf der Hand. Deshalb hätte der Polizeibeamte dem Ansinnen des Sicherheitsbeauftragten nicht nachkommen, keine INZOLL-Abfrage veranlassen und erst recht nicht das Abfrageergebnis an den Sicherheitsbeauftragten weitergeben dürfen. Zum kleinen Einmaleins des Datenschutzes gehört aber auch, dass die Polizei Vorsorge dafür treffen muss, dass Abfragen in (polizeilichen) Datenverarbeitungssystemen wirklich nur zu dienstlichen Zwecken gestartet werden. Dazu gibt es verschiedene Möglichkeiten: Schriftliche Belehrungen und von Zeit zu Zeit erfolgende Hinweise auf die für solche Abfragen geltenden Vorschriften sind durchaus hilfreich; sie haben jedoch nur Appellcharakter. Bei telefonischen Bitten um die Abfrage eines Datenverarbeitungssystems kann mit Hilfe eines dafür vereinbarten Codeworts oder durch Rückruf bewirkt werden, dass die Daten an abfrageberechtigte Personen gelangen. Wichtig ist dabei auch, dass der Kreis dieser Personen so eng wie möglich gezogen und dass zudem am besten automatisch oder zur Not von Hand protokolliert wird, wer wann wie eine Computerabfrage durchgeführt oder veranlasst hat. Solche Protokolle und Aufzeichnungen sind durchaus geeignet, unbefugten Abfragen entgegenzuwirken. Denn immerhin muss jeder, der die Abfrage eines Datenverarbeitungssystems veranlasst, damit rechnen, dass seine Abfrage in der einen oder anderen Weise festgehalten wird. Der damit einhergehende Abschreckungseffekt würde jedoch verpuffen, wenn es mit der Protokollierung sein Bewenden hätte. Vielmehr muss anhand der Protokolle und Aufzeichnungen hin und wieder stichprobenweise überprüft werden, ob bei solchen Computerabfragen alles

korrekt läuft. Denn nur dann kann davon gesprochen werden, dass jemand, der unbefugterweise ein Datenverarbeitungssystem abfragt oder abfragen lässt, einem nennenswerten Entdeckungsrisiko ausgesetzt ist. Deshalb war es richtig, dass die Polizeidirektion auf unsere Hinweise die Befugnis zu schriftlichen und telefonischen Ersuchen um eine INZOLL-Abfrage auf den Leiter einer bestimmten Kriminalinspektion oder dessen Vertreter beschränkt und bestimmt hat, dass solche Ersuchen in der Regel schriftlich zu stellen sind und nur in eiligen Fällen telefonisch erfolgen dürfen. Zudem hat die Polizeidirektion festgelegt, dass in Eilfällen ein schriftliches Auskunftsersuchen nachzureichen ist und dass die Auskunftsersuchen in der jeweiligen Akte abzuheften sind. Die Landespolizeidirektion hat Näheres dazu bestimmt, wie ihre Gemeinsame Ermittlungsgruppe Rauschgift bei solchen Ersuchen zu verfahren hat. Weil dabei eine mustergültige Lösung herausgekommen ist, haben wir das Landeskriminalamt gebeten sicherzustellen, dass bei den Gemeinsamen Ermittlungsgruppen Rauschgift der anderen Landespolizeidirektionen entsprechend verfahren wird.

2. Abschnitt: Justiz

1. Grundbuchdaten nach Rumänien

Wie bereits im 1. Teil dieses Tätigkeitsberichts angesprochen, waren wir in diesem Berichtsjahr im Zusammenhang mit einer in der Öffentlichkeit heiß diskutierten Angelegenheit erstmalig mit dem Thema der Datenverarbeitung in einem nicht der Europäischen Union angehörenden Staat befasst.

Im Juni dieses Jahres war in den Medien bekannt geworden, dass das Justizministerium für die geplante Einrichtung des Elektronischen Grundbuchs Grundbuchdaten durch eine Firma in Rumänien erfassen lassen will. Das Justizministerium hatte uns hierüber nicht informiert. Nachdem wir aus der Presse hiervon erfahren hatten, setzten wir uns unverzüglich mit ihm in Verbindung. Die Prüfung der uns zur Verfügung gestellten Unterlagen ergab Folgendes:

Für die Einrichtung des Elektronischen Grundbuchs müssen die bisher in Papierform vorliegenden Grundbücher elektronisch erfasst werden. Das Justizministerium will dies durch private Firmen erledigen lassen. Zunächst ging es dabei um die Erfassung von etwa 10 Millionen Grundbuchseiten. Hierfür hatte ein bayerisches Unternehmen im Rahmen eines europaweiten Ausschreibungsverfahrens den Zuschlag erhalten. Dieses beabsichtigte, einen Teil der Grundbuchdaten einem Subunternehmer zu überlassen, der seinen Sitz in Timisoara in Rumänien hat. Dabei sollten zwar nicht die persönlichen Kenndaten der Eigentümer (Name, Anschrift) übermittelt werden, wohl aber Daten über Lage und Nutzungsart des jeweiligen Grundstücks sowie Angaben darüber, zu wessen Gunsten das Grundstück mit einem Nießbrauch oder einem Wegerecht oder mit welchen Hypotheken, Grundschulden oder Rentenschulden es belastet ist.

Die Beauftragung der bayerischen Firma unter Mitwirkung von Subunternehmen stellt eine Datenverarbeitung im Auftrag dar, die nach dem Landesdatenschutzgesetz grundsätzlich zulässig ist. Lässt eine öffentliche Stelle eigene Aufgaben im Auftrag erledigen, bleibt der Auftraggeber, hier also das Justizministerium, für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich und zwar unabhängig davon, ob – beziehungsweise wie viele – Subunternehmer in die Auftragsabwicklung einbezogen werden. Der Auftragnehmer fungiert lediglich als verlängerter Arm oder als ausgelagerte Abteilung des Auftraggebers, der die volle Verfügungsgewalt behält und damit auch allein über die Datenverarbeitung bestimmt. Der Auftraggeber muss im Rahmen seiner Verantwortung deshalb dafür Sorge tragen, dass seine Daten entsprechend der für ihn selbst geltenden Datenschutzvorschriften verarbeitet werden.

Nach dem Landesdatenschutzgesetz ist es nicht von vornherein ausgeschlossen, Daten auch in Staaten verarbeiten zu lassen, die nicht der Europäischen Union angehören. In diesem Fall ist jedoch sorgfältig zu prüfen, ob sichergestellt ist, dass das in den Mitgliedstaaten der Europäischen

Union vorgeschriebene Datenschutzniveau nicht unterlaufen wird. Die betroffenen Bürger müssen davon ausgehen können, dass mit ihren Daten im Empfängerland vorschriftsgemäß umgegangen wird. Das Gesetz verlangt hierfür, dass im Empfängerland ein „angemessenes Datenschutzniveau“ herrscht. Mit der Frage des Datenschutzniveaus in Drittstaaten setzt sich regelmäßig die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie auseinander. Sie hat zum einen Richtlinien zur Angemessenheit ausgearbeitet. Zum anderen prüft sie selbst anhand dieser Kriterien, bei welchen Ländern von einem angemessenen Datenschutzniveau auszugehen ist, und legt diese Länder listenmäßig fest. Rumänien ist in dieser „Angemessenheitsliste“ bisher nicht aufgeführt. Allerdings kann eine Angemessenheit auch für den Einzelfall festgestellt werden. Hierzu können insbesondere die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den Empfänger geltenden Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden. Das Landesdatenschutzgesetz lässt es aber auch genügen, wenn der Datenempfänger im Einzelfall ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist. Solche Garantien können sich auch aus Vertragsklauseln ergeben. Die Europäische Kommission hat hierfür Standardvertragsklauseln erarbeitet.

Den uns vom Justizministerium im Juni 2003 überlassenen Unterlagen war nicht zu entnehmen, dass das Justizministerium entsprechende Feststellungen über ein angemessenes Datenschutzniveau in Rumänien getroffen hatte oder dass nach den vorgenannten Maßstäben ausreichende Garantien für ein angemessenes Datenschutzniveau gegeben waren.

Auch hinsichtlich weiterer Forderungen des Landesdatenschutzgesetzes, insbesondere was die konkrete Festlegung technischer und organisatorischer Datenschutzmaßnahmen betrifft, zu denen sich der Auftragnehmer verpflichten muss, enthielten die uns vom Justizministerium vorgelegten Unterlagen Mängel. Unzureichend geregelt war etwa, wer beim Auftragnehmer im Einzelnen auf die Daten zugreifen und wie ein Missbrauch der Daten verhindert werden kann. Nach den ursprünglichen Vereinbarungen war zudem nicht sichergestellt, dass die Daten nach Abschluss der Arbeiten datenschutzgerecht gelöscht werden.

Nach Abschluss unserer Prüfung haben wir das Justizministerium daher darüber informiert, dass die Abwicklung des Auftrags datenschutzrechtlich erst dann zulässig ist, wenn es nachweist, dass die genannten rechtlichen Anforderungen, insbesondere an die Beauftragung eines Unternehmens aus dem Nicht-EU-Bereich, sichergestellt sind. Außerdem haben wir das Justizministerium aufgefordert, die bei der Vereinbarung der erforderlichen technischen und organisatorischen Maßnahmen aufgetretenen Mängel zu beheben.

Diesen Datenschutzanforderungen hat das Justizministerium zwischenzeitlich durch eine umfassende Überarbeitung der Auftragsunterlagen sowohl im rechtlichen als auch im technisch-organisatorischen Bereich Rechnung getragen. Insbesondere hat das Justizministerium vertraglich vereinbart, dass bei der Verarbeitung der Grundbuchdaten in Rumänien die von der Europäischen Kommission für eine Datenweitergabe in Nicht-EU-Staaten erarbeiteten Standardvertragsklauseln gelten. Darin wird unter anderem geregelt, dass die Verarbeitung der Grundbuchdaten in Rumänien entsprechend den Bestimmungen des Landesdatenschutzgesetzes durchgeführt wird. Klargestellt ist nun auch, dass das Justizministerium die datenschutzrechtliche Gesamtverantwortung für das Projekt trägt. Auch für die von uns gerügten Mängel im technisch-organisatorischen Bereich konnten Lösungen gefunden werden. So wurde z. B. durch technische Maßnahmen Vorsorge dagegen getroffen, dass Grundbuchdaten auf dafür nicht bestimmte Datenträger kopiert oder ins Internet übertragen werden können. Inzwischen ist auch sichergestellt, dass die Daten nach Abschluss der Arbeiten datenschutzgerecht gelöscht werden.

Nach alledem kann nun davon ausgegangen werden, dass für die Datenverarbeitung in der beauftragten rumänischen Firma ein angemessenes Schutzniveau gegeben ist, wie dies das Landesdatenschutzgesetz fordert. Wir hät-

ten uns allerdings eine frühere Beteiligung unserer Dienststelle durch das Justizministerium gewünscht. Hierdurch hätten nicht nur die mühseligen Nacharbeiten, sondern auch die in der Öffentlichkeit entstandenen Irritationen vermieden werden können.

2. Der Modellversuch des Justizministeriums zur Auslagerung der Gerichts- und Bewährungshilfe auf private Träger

In den am 30. April 2003 der Presse vorgestellten Vorschlägen zur Justizreform führte das Justizministerium unter anderem aus, dass die Bewährungshilfe unter Einbeziehung der Gerichtshilfe privatisiert werden soll. Das Justizministerium verspricht sich hiervon erhebliche finanzielle Einsparmöglichkeiten. Vor einer flächendeckenden Privatisierung soll jedoch zunächst ein zeitlich und räumlich begrenzter Modellversuch durchgeführt werden. Von diesem werden Erkenntnisse darüber erwartet, ob in privatrechtlichen Strukturen – auch bei noch weiter steigender Arbeitsbelastung – die Qualität der Bewährungs- und Gerichtshilfe eher sichergestellt werden kann als im bestehenden staatlichen System, ohne den finanziellen Aufwand für die Bewährungs- und Gerichtshilfe erhöhen zu müssen.

Mit dem Gesetzentwurf über die Durchführung eines Pilotprojekts der Bewährungs- und Gerichtshilfe in freier Trägerschaft soll die Grundlage für diesen Modellversuch geschaffen werden. Der Entwurf sieht vor, dass die Aufgaben der Gerichts- und Bewährungshilfe im Bezirk des Landgerichts und Amtsgerichts Stuttgart, die bisher von Sozialarbeitern der Justiz wahrgenommen werden, durch Vertrag für die Dauer von drei Jahren auf einen freien Träger übertragen werden können.

Es liegt zwar im öffentlichen Interesse, dass das Justizministerium angesichts der schwierigen Haushaltslage nach Wegen sucht, wie der erwarteten Steigerung der Arbeitsbelastung der Gerichts- und Bewährungshilfe bei gleichzeitiger, nachhaltiger Sicherung der Qualität der bislang geleisteten Arbeit in Zukunft am besten begegnet werden kann. Im Zusammenhang mit der Frage, ob die Aufgaben der Bewährungs- und Gerichtshilfe an freie Träger ausgelagert werden sollen, spielen jedoch auch andere Aspekte eine wichtige Rolle.

Schon bei Durchsicht des Gesetzentwurfs über die Durchführung des Pilotprojekts wird deutlich, dass eine Änderung der derzeitigen Struktur auch erhebliche Auswirkungen auf das Datenschutzrecht verschiedener Personengruppen haben würde. Nach § 2 des Gesetzentwurfs sollen dem freien Träger die Arbeitsergebnisse der Mitarbeiterinnen und Mitarbeiter der Gerichts- und Bewährungshilfe überlassen werden. Ferner soll der Vorstand des freien Trägers zur Ausübung der Dienstaufsicht über die Gerichts- und Bewährungshelfer, die für die Dauer des Modellversuchs Landesbedienstete bleiben, und zur Ausübung des dienstlichen Weisungsrechts ermächtigt werden.

Die Wahrnehmung dieser Aufgaben durch den freien Träger ist ohne die Verarbeitung personenbezogener Daten nicht denkbar. Ziel der Gerichtshilfe ist es, den Strafverfolgungsbehörden ein der Wahrheit entsprechendes Persönlichkeitsbild des Beschuldigten zu vermitteln. Zu diesem Zweck werden durch die Gerichtshilfe die persönlichen Verhältnisse des Beschuldigten erforscht. Dabei geht es vor allem um die Entwicklung und das Umfeld des Beschuldigten, also insbesondere um seine Entwicklungsschwierigkeiten, seine sozialen Kontakte und seine konkrete Lebenssituation zur Tatzeit. Der Gerichtshelfer fasst das Ergebnis seiner Erhebungen in einem schriftlichen Bericht zusammen, der zu den Akten genommen und damit deren Bestandteil wird. Zu den Aufgaben der Bewährungshilfe gehört einerseits die Kontrolle des Verurteilten, sodass der Bewährungshelfer dem Gericht gegebenenfalls zusätzliche Erkenntnisse zur Persönlichkeit des Verurteilten, aber auch Hintergründe vermitteln kann, die zu dessen Versagen beigetragen haben. Andererseits steht der Bewährungshelfer dem Verurteilten helfend und betreuend zur Seite. Dass er in beiden Bereichen seiner Tätigkeit weitreichende Einblicke in vielerlei Lebensbereiche des Probanden bekommt und dabei oftmals recht sensible Informationen über ihn erhält, liegt auf der Hand. Ebenso offensichtlich ist, dass dem freien Träger Personaldaten auch über die Mitarbeiter der Gerichtshilfe und Bewährungshilfe, die

in das Modellprojekt integriert werden sollen, zur Kenntnis gelangen werden, zumal der Begründung des Gesetzentwurfs zu entnehmen ist, dass dem freien Träger Dienstherrenbefugnisse bis hin zur Genehmigung von Nebentätigkeiten und der Erstellung dienstlicher Beurteilungen übertragen werden sollen.

Kurzum: Der beabsichtigte Modellversuch wird dazu führen, dass einerseits personenbezogene Daten über Beschuldigte, Verurteilte und über andere Personen aus deren Lebensumfeld durch die Gerichts- und Bewährungshilfe und andererseits personenbezogene Daten über die in das Modellprojekt integrierten Mitarbeiter der Gerichts- und Bewährungshilfe an den freien Träger weitergegeben und von diesem verarbeitet werden.

Maßstab für die Zulässigkeit dieser Datenverarbeitungsmaßnahmen ist das Recht auf informationelle Selbstbestimmung. Dieses gewährleistet dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten entscheiden zu können. Einschränkungen dieses Rechts muss der Einzelne jedoch im überwiegenden Allgemeininteresse hinnehmen. Solche Beschränkungen bedürfen allerdings einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entsprechen. Bei derartigen Regelungen hat der Gesetzgeber außerdem den Grundsatz der Verhältnismäßigkeit zu beachten und organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, die einer Verletzung des Persönlichkeitsrechts entgegenwirken. Diesen Anforderungen wird der Gesetzentwurf über die Durchführung eines Modellversuchs nicht gerecht.

Wir haben das Justizministerium daher aufgefordert, im Gesetzentwurf auch die Weitergabe personenbezogener Daten über Beschuldigte, Verurteilte und andere Personen im Rahmen der Gerichts- und Bewährungshilfe wie auch die Weitergabe von Personaldaten der Mitarbeiter der Gerichts- und Bewährungshilfe an den freien Träger zu regeln und dabei auch festzulegen, dass der freie Träger die übermittelten Daten jeweils nur für den Zweck verwenden darf, für den sie ihm übermittelt worden sind, und dass die Daten nach Abschluss des Modellversuchs komplett zurückzugeben sind.

3. DNA-Analyse im Ermittlungsverfahren oder: Kein Ende der Begehrlichkeiten

Als der Gesetzgeber im Jahr 1997 in der Strafprozessordnung die molekulargenetische Untersuchung von Körperzellen zur Aufklärung von Straftaten regelte, sah er die zentrale Speicherung der dabei gewonnenen DNA-Identifizierungsmuster nicht vor. Das änderte sich eineinhalb Jahre später. Seit dem DNA-Identitätsfeststellungsgesetz vom 7. September 1998 dürfen zum einen dem Beschuldigten, der einer Straftat von erheblicher Bedeutung, insbesondere eines Verbrechens, eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls in besonders schwerem Fall oder einer Erpressung verdächtig ist, Körperzellen entnommen und zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersucht werden. Voraussetzung ist zudem, dass wegen der Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen einer der vorgenannten Straftaten zu führen sind. Zum anderen dürfen die so gewonnenen DNA-Identifizierungsmuster in der beim Bundeskriminalamt eingerichteten DNA-Analyse-Datei gespeichert werden. Inzwischen sind in dieser Datei die DNA-Identifizierungsmuster von mehr als 250 000 Personen erfasst; tagtäglich kommen die Muster weiterer Personen hinzu. Dem Entwurf eines Gesetzes zur Änderung der Vorschriften über Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften zufolge soll bei Straftaten gegen die sexuelle Selbstbestimmung im Gegensatz zum geltenden Recht nicht mehr vorausgesetzt werden, dass die mutmaßlich oder tatsächlich begangene Anlasstat von erheblicher Bedeutung ist. Damit soll vor allem in Fällen exhibitionistischer Handlungen und bei anderen Delikten gegen die sexuelle Selbstbestimmung, die im Hinblick auf die jeweils dafür vorgesehenen

Strafrahmen in der Regel noch nicht dem mittleren Kriminalitätsbereich zuzurechnen sind und deshalb regelmäßig auch keine Straftaten von erheblicher Bedeutung darstellen, die Möglichkeit einer DNA-Analyse eröffnet werden. Dies geht manchen offenbar noch immer nicht weit genug. Derzeit gibt es diverse Forderungen aus dem politischen Raum und Gesetzesinitiativen, die darauf abzielen, die rechtlichen Anforderungen für die Entnahme von Körperzellen und deren DNA-Analyse sowie für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster in der zentralen DNA-Analyse-Datei der Polizei noch weiter herabzusetzen. Danach soll zum einen eine DNA-Analyse künftig nicht nur – wie nach geltendem Recht – bei einer Straftat von erheblicher Bedeutung oder – wie nach dem erwähnten Gesetzentwurf zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung – bei einer Straftat gegen die sexuelle Selbstbestimmung, sondern auch bei Straftaten mit sexuellem Hintergrund oder sogar bei jedweder Straftat möglich sein. Zum anderen soll die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung einer DNA-Analyse durch den Richter entfallen und statt dessen die Polizei über die Anordnung einer DNA-Analyse entscheiden.

Keine Frage: Wäre die DNA-Analyse und der dabei gewonnene genetische Fingerabdruck tatsächlich mit einem herkömmlichen Fingerabdruck vergleichbar, wäre hier nicht viel Aufhebens zu machen. Dieser Vergleich, den die Befürworter einer Ausweitung der DNA-Analyse anstellen, hinkt jedoch erheblich. Er verkennt nicht nur die unterschiedlichen Ausgangspunkte, sondern lässt auch die enorme Entwicklung außer Acht, die die DNA-Analyse in den letzten Jahren genommen hat. Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nicht-codierenden Teile der DNA untersucht werden, können dabei nämlich über das DNA-Identifizierungsmuster hinausgehende Zusatzerkenntnisse anfallen. So wird bei der derzeit verwendeten Untersuchungsmethode praktisch zwangsläufig das Geschlecht der Person bestimmt, von der das molekulargenetische Material stammt. Zudem erlaubt sie Wahrscheinlichkeitsaussagen über deren Alter und ethnische Zugehörigkeit. Möglicherweise sind einzelne Krankheiten wie Diabetes oder das Klinefelter-Syndrom zu erkennen. Ein genetischer Fingerabdruck lässt sich schon deshalb mit einem herkömmlichen Fingerabdruck nicht vergleichen. Dabei gilt es auch noch Folgendes zu bedenken: Zwar ermöglichen derzeit die automatisiert gespeicherten Informationen, die zum Zweck der Identitätsfeststellung in künftigen Strafverfahren erstellt worden sind, keine über die Identifizierung hinausgehenden Aussagen zu der jeweiligen Person oder deren Erbgut. In Einzelfällen können die analysierten nicht-codierenden DNA-Merkmale jedoch mit codierenden Merkmalen korrespondieren. In Anbetracht der weltweiten intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, dass künftig auch auf der Basis der Untersuchung von bisher als nicht codierend angesehenen Merkmalen weitere konkrete Aussagen über genetische Dispositionen der betroffenen Personen getroffen werden können. Angesichts dieser Wirkungen und Gefahrenpotenziale sowie der mit einer DNA-Analyse einhergehenden tiefgreifenden und nachhaltigen Eingriffe in das Recht auf informationelle Selbstbestimmung betonten die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 16. Juli 2003 (s. Anhang 9), dass die DNA-Analyse nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Instrument im Rahmen der Aufklärung und Verhütung von Straftaten werden und deshalb auf das Erfordernis der Prognose erheblicher Straftaten ebenso wenig verzichtet werden darf wie auf den Richtervorbehalt für die Anordnung einer DNA-Analyse.

4. Telekommunikationsüberwachung

Die Telekommunikationsüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Der Schutz des Telekommunikationsgeheimnisses ist deshalb seit Jahren ein besonderes Anliegen der Datenschutzbeauftragten des Bundes und der Länder. Angesichts der Weiter-

entwicklung der Technik zur Telekommunikationsüberwachung (z. B. IMSI-Catcher, stille SMS) und der hiermit einhergehenden Zunahme der Gefährdung der freien Telekommunikation gilt dies umso mehr. Die Forderung der Datenschutzbeauftragten nach aussagekräftigen Statistiken oder nach Forschungsvorhaben zur Wirksamkeit und Verhältnismäßigkeit der Telekommunikationsüberwachung war jedoch zunächst wenig erfolgreich. Im August 1999 hat das Bundesministerium der Justiz jedoch ein Forschungsvorhaben ausgeschrieben und an das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg vergeben, durch das Erkenntnisse über Umfang, Wirkungsweise und Erfolgseignung der Überwachung der Telekommunikation gewonnen werden sollten.

Im Mai dieses Jahres hat das Max-Planck-Institut sein Gutachten „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b der Strafprozessordnung (StPO) und anderer verdeckter Ermittlungsmaßnahmen“ vorgelegt.

Darin wird unter anderem festgestellt, dass sich die Zahl der Ermittlungsverfahren, in denen Telekommunikationsüberwachungsanordnungen erfolgten, zwischen 1996 und 2001 um 80 % erhöht hat (1996: 2 149; 2001: 3 868), sich die Gesamtzahl der Telekommunikationsüberwachungsanordnungen pro Jahr von 1994 bis 2000 versechsfacht hat (1990: 2 494; 2000: 15 741) und sich die Zahl der jährlich hiervon Betroffenen zwischen 1994 und 2001 fast verdreifacht hat (1994: 3 730; 2001: 9 122). In 21 % der Anordnungen wurden zwischen 1 000 und 5 000 Gespräche abgehört, in 8 % der Anordnungen sogar mehr als 5 000 Gespräche. Obwohl die Telekommunikationsüberwachung ganz erheblich in das Persönlichkeitsrecht der Betroffenen eingreift, waren nur 24 % der Anordnungsbeschlüsse substanziell begründet. Darüber hinaus sind 73 % der betroffenen Anschlussinhaber nicht über die Maßnahme unterrichtet worden und schließlich sind nur in 17 % der Fälle Ermittlungserfolge erzielt worden, die sich unmittelbar auf den die Telefonüberwachung begründenden Verdacht bezogen.

Der aus diesen Zahlen ableitbare Trend sollte nachdenklich stimmen. So kann der Anstieg der Überwachungsanordnungen sicher nicht allein darauf zurückgeführt werden, dass immer mehr Kriminelle mehrere Festnetz- und Handyanschlüsse benutzen, um ihre Spuren zu verwischen. Es liegt vielmehr die Vermutung nahe, dass sich die Überwachung der Telekommunikation langsam aber sicher von einem nur im äußersten Fall zulässigen Rechtseingriff zu einem Standardmittel der Strafverfolgung wandelt. Angesichts der Bedeutung des Rechts auf unbeobachtete Kommunikation können Eingriffe in dieses Recht jedoch nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden, das lediglich mit der Verfolgung schwerwiegender Straftaten begründet werden kann. Die Telekommunikationsüberwachung muss daher Ultima Ratio bleiben. Die geltenden gesetzlichen Bestimmungen können dies jedoch nicht hinlänglich gewährleisten.

Sowohl die gesetzliche Regelung wie auch die gegenwärtige Praxis der Telekommunikationsüberwachung bedürfen einer grundlegenden Nachbesserung. So sind etwa die Benachrichtigungspflichten gegenüber überwachten Personen gesetzlich klar zu regeln und die Verwertung von Gesprächen mit Zeugnisverweigerungsberechtigten zu verbieten. Auch macht die Feststellung des Max-Planck-Instituts, die Begründung der richterlichen Beschlüsse ergehe nicht eigenständig, sondern in Übernahme von Formulierungen der Staatsanwaltschaften, auf der Basis nur unzureichender eigener richterlicher Recherchen und nach unzureichendem Aktenstudium, deutlich, dass die derzeitige Handhabung dieser Maßnahmen dem damit verbundenen Eingriff in das Persönlichkeitsrecht Betroffener nicht ausreichend Rechnung trägt.

Die Datenschutzbeauftragten des Bundes und der Länder sind daher der Auffassung, dass sich die Qualität der Entscheidungen insgesamt deutlich verbessern muss, dabei aber in keinem Fall an eine Abschaffung des Richtervorbehalts gedacht werden darf. Sie haben diese Forderungen auf ihrer 66. Konferenz am 25. und 26. September 2003 in einer Entschließung zu datenschutzrechtlichen Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation zusammengefasst (s. Anhang 7).

Erfreulich ist, dass sich das Justizministerium des Landes den Problemen offen stellt und diese zum Gegenstand seines 24. Triberger Symposiums gemacht hat. Es ist zu hoffen, dass einige dort auch unter Beteiligung des Datenschutzes gewonnene Erkenntnisse in die Gesetzesarbeit auf Bundesebene und in die Praxis der Telekommunikationsüberwachung im Land einfließen.

5. Strafvollzug

Im 23. Tätigkeitsbericht für das Jahr 2002 hatten wir verschiedene Themen aus dem Strafvollzugsbereich angesprochen. Da zum damaligen Zeitpunkt entweder noch keine abschließende Stellungnahme von Seiten des Justizministeriums vorlag oder aber die vom Justizministerium bzw. von der betreffenden Strafvollzugsanstalt vertretenen Auffassungen aus datenschutzrechtlicher Sicht unbefriedigend waren, haben wir diese Angelegenheiten auch dieses Jahr weiterverfolgt. Da sich das Justizministerium zwischenzeitlich in weiten Teilen unserer Argumentation angeschlossen hat, konnten auch in Fragen, für die im letzten Jahr keine Einigung in Sicht war, Lösungen gefunden werden.

5.1 Anstaltsinterner Umgang mit Gefangenendaten

Im letzten Tätigkeitsbericht hatten wir ausführlich über einen in einer Justizvollzugsanstalt durchgeführten Kontrollbesuch berichtet, der im Bereich der anstaltsinternen Informationsverarbeitung verschiedenste Mängel offenbart hatte. Dabei ging es unter anderem um die Organisation des anstaltsinternen Postlaufs und den Umgang mit Gefangenenpersonalakten.

§ 183 Abs. 1 Satz 1 des Strafvollzugsgesetzes (StVollzG) sieht vor, dass sich der einzelne Vollzugsbedienstete von personenbezogenen Daten nur Kenntnis verschaffen darf, 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 in Verbindung mit § 9 des Bundesdatenschutzgesetzes 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 unterbinden. Die Verfahrensweise der von uns damals kontrollierten Justizvollzugsanstalt entsprach diesen Vorgaben nicht. Es fehlten Vorkehrungen, die sicherstellen, dass Beschäftigte nur in dem für die Erledigung der konkret anstehenden Aufgaben notwendigen Maß auf personenbezogene Daten zugreifen können.

So war der anstaltsinterne Postlauf der Justizvollzugsanstalt dergestalt organisiert, dass die für einen Gefangenen bestimmten hausinternen Vorgänge, wie z. B. Genehmigungen, Aufstellungen über finanzielle Angelegenheiten usw., unkuvertiert in das Postfach des für den jeweiligen Gefangenen zuständigen Stockwerksbeamten eingelegt worden sind. Der Stockwerksbeamte konnte sich daher über sämtliche den Gefangenen betreffende Angelegenheiten informieren. Da sich die Postfächer in der für alle Beschäftigten der Justizvollzugsanstalt zugänglichen Poststelle befanden und außerdem nicht abschließbar waren, hatte diese Vorgehensweise auch zur Folge, dass im Grunde jeder Beschäftigte die offen in den Postfächern liegenden Schreiben einsehen konnte.

Der Umgang mit den Gefangenenpersonalakten entsprach ebenfalls nicht den Vorgaben des Strafvollzugsgesetzes. Sie enthalten eine Vielzahl personenbezogener Daten über den jeweiligen Gefangenen, z. B. über das religiöse Bekenntnis, den Familienstand, die Kinderzahl, den während der Haft anfallenden Schriftverkehr usw., aber auch Daten über Dritte, wie z. B. Angehörige. In der von uns kontrollierten Justiz-

vollzugsanstalt konnte praktisch jeder Beschäftigte auf jede Gefangenenpersonalakte zugreifen. Man musste lediglich einen Anforderungszettel ausfüllen, die Akte wurde dann – für jeden zugänglich – in das offene Postfach des Bediensteten gelegt, der sie angefordert hatte.

Zunächst sahen weder die betroffene Justizvollzugsanstalt noch das Justizministerium Anlass, an den beschriebenen Zuständen etwas zu ändern. Nach weiterem Schriftverkehr und nach Kontrollen unserer Dienststelle bei zwei weiteren Justizvollzugsanstalten, über deren Ergebnis wir das Justizministerium jeweils informiert hatten, machte sich das Justizministerium jedoch einen Großteil der von uns gemachten Vorschläge zur Verbesserung der Organisation des Postlaufs und des anstaltsinternen Umgangs mit Gefangenenpersonalakten zu Eigen und forderte alle Justizvollzugsanstalten per Runderlass auf, bestimmte Maßnahmen umzusetzen, um so einen datenschutzgerechten Umgang mit personenbezogenen Daten zu gewährleisten.

So sieht der Erlass z. B. vor, dass die Justizvollzugsanstalten verschließbare Postverteilerschränke einrichten. Unberechtigte Zugriffe auf Vorgänge, wie sie bei offenen Postfächern möglich sind, werden hierdurch ausgeschlossen. Auch der Zugriff auf Gefangenenpersonalakten wird durch den Erlass eingeschränkt. So ist unter anderem vorgesehen, dass Mitarbeiter, die zur Aufgabenerledigung Informationen aus einer Gefangenenpersonalakte benötigen, lediglich in den Räumen der Vollzugsgeschäftsstelle, wo die Gefangenenpersonalakten normalerweise aufbewahrt werden, Einsicht in die Akte erhalten. Bei dieser Vorgehensweise kommt man nicht in Versuchung, sich länger mit einer Gefangenenpersonalakte zu befassen und sich mehr Informationen daraus zu beschaffen als tatsächlich nötig. Nur noch in den Fällen, in denen eine Akteneinsicht bei der Vollzugsgeschäftsstelle nicht ausreicht, soll die Herausgabe einer Akte erfolgen. Die Gefangenenpersonalakte ist dann jedoch persönlich von dem Mitarbeiter, der sie benötigt, abzuholen und zurückzubringen oder von einem Boten zu überbringen. Überlassene Gefangenenpersonalakten sollen außerdem am gleichen Tag wieder zurückgebracht werden. Unberechtigte Zugriffe während des anstaltsinternen Transports von Gefangenenpersonalakten und durch eine längere Aufbewahrung außerhalb der Vollzugsgeschäftsstelle sind bei dieser Vorgehensweise nicht mehr möglich.

Sowohl die Einsichtnahmen in als auch die Mitnahme von Gefangenenpersonalakten sind außerdem unter Angabe des Zwecks zu dokumentieren, um den datenschutzgerechten Umgang mit Gefangenenpersonalakten überwachen zu können.

In einem Punkt, dessentwegen uns viele Strafgefangene im Laufe des Berichtsjahrs angeschrieben haben, ist das Justizministerium unseren Forderungen dagegen nicht nachgekommen. Da nicht nachvollziehbar ist, dass der Stockwerksbeamte über die in seinem Zuständigkeitsbereich untergebrachten Gefangenen umfassend informiert sein muss, hatten wir – unter Bezugnahme auf eine entsprechende Entscheidung der Strafvollstreckungskammer des Landgerichts Karlsruhe vom 18. Februar 2002 – gefordert, für Gefangene bestimmte Einzahlungsbelege, Kontoauszüge usw. nicht mehr offen an den jeweiligen Stockwerksbeamten auszuhändigen, sondern diese zu kuvertieren. Das Justizministerium sah und sieht hierfür keinen Bedarf, da der mit dem Einkuvertieren verbundene Aufwand nicht in einem angemessenen Verhältnis zu dem damit angestrebten Schutzzweck stehe. Zu diesem Thema existieren auf der Ebene der Strafvollstreckungskammern der Landgerichte zwar mehrere Entscheidungen, die unsere Auffassung vertreten. Da zwischenzeitlich jedoch auch Entscheidungen des Hanseatischen Oberlandesgerichts vom 7. April 2003, Az. 3 Vollz (Ws) 31/03 609 Vollz 251/02, und des Oberlandesgerichts Koblenz vom 21. Juli 2003, Az. 1 Ws 303/03, vorliegen, die das Einkuvertieren wegen des damit verbundenen Aufwands nicht für erforderlich halten, besteht wohl – zumindest bis eine hiervon abweichende Entscheidung eines anderen Oberlandesgerichts vorliegt – keine Aussicht, das Justizministerium von der von unserer Dienststelle vertretenen Auffassung zu überzeugen.

5.2 Einzelfragen

Neben den Kontrollen bei Justizvollzugsanstalten zu den vorgenannten Themen beschäftigten wir uns auch dieses Jahr mit einer großen Zahl von Einzelfällen im Bereich des Strafvollzugs. Bei der Bearbeitung dieser Eingaben konnten wir – überschlägig betrachtet – feststellen, dass die Justizvollzugsanstalten die von uns angeforderten Stellungnahmen zügiger abgaben als noch im Vorjahr.

Allerdings konnten wir einen bereits im 23. Tätigkeitsbericht angesprochenen Fall, der auf der Eingabe eines Strafgefangenen aus dem Jahr 2002 beruhte, erst vor einigen Monaten abschließen. Es ging dabei um die Frage, wie bei kostenlosen Überweisungen von dem von den Justizvollzugsanstalten verwalteten Einkommen der Strafgefangenen vermieden werden kann, dass die Justizvollzugsanstalt als Kontoinhaber genannt wird. Diese Vorgehensweise hat zur Folge, dass Dritte, wie z. B. die Firma, bei der der Gefangene etwas bestellt hat, überflüssigerweise erfahren, dass es sich bei dem Kunden, der lediglich eine Rechnung bezahlen will, um einen Strafgefangenen handelt.

Nachdem die betroffene Justizvollzugsanstalt das Justizministerium eingeschaltet hatte, teilte dieses zu Beginn des Jahres mit, dass in den meisten Justizvollzugsanstalten auf den Überweisungsträgern die Justizvollzugsanstalt namentlich als Absender genannt sei. Entsprechende Rückfragen der Justizvollzugsanstalten bei den jeweiligen Kreditinstituten hätten ergeben, dass dies aus EDV-technischen Gründen derzeit nicht zu vermeiden sei. Nach Auskunft einiger Kreditinstitute sei eine eindeutige Zuordnung unerlässlich, um bei etwaigen Falschbuchungen den Auftraggeber zweifelsfrei ermitteln zu können. Das Justizministerium teilte weiter mit, dass die Möglichkeit, kostenlose Überweisungen vom Dienstkonto der jeweiligen Justizvollzugsanstalt vorzunehmen, eine freiwillige Dienstleistung seitens der Justizvollzugsanstalt darstelle, die die Gefangenen nicht in Anspruch nehmen müssten. Die Gefangenen hätten den Umstand der Bekanntgabe des Kontoinhabers gegenüber dem Zahlungsempfänger daher hinzunehmen, wenn das Kreditinstitut keine Möglichkeit der Unkenntlichmachung sieht. Die Alternative wäre, diese Serviceleistung für die Gefangenen insgesamt einzustellen. Obwohl die Justizvollzugsanstalten dennoch bemüht seien, eine Lösung des Problems zu finden, sei es bislang lediglich in einer Justizvollzugsanstalt möglich gewesen, mit dem betreffenden Kreditinstitut eine individuelle Absprache dahin gehend zu treffen, dass auf Wunsch des Gefangenen die entsprechenden Überweisungen nicht mittels Beleglesern, sondern manuell bearbeitet werden.

Darüber hinaus sei auch die kontoführende Bank der Justizvollzugsanstalt, auf die sich die Eingabe bezog, die die Angelegenheit ins Rollen gebracht hatte, zwischenzeitlich in Ausnahmefällen bereit, als Absender nicht die Justizvollzugsanstalt namentlich zu benennen. Kurze Zeit später ließ uns die letztgenannte Justizvollzugsanstalt jedoch die genau gegenteilige Information zukommen: Es sei nicht möglich gewesen, mit der Bank eine individuelle Absprache zu treffen. Die Nennung der Justizvollzugsanstalt als Absender könne nicht vermieden werden. Die endgültige Klärung dieser Angelegenheit nahm zwar noch einige Monate in Anspruch. Letztendlich konnten wir jedoch zumindest einen Teilerfolg erzielen: Inzwischen besteht in dieser Justizvollzugsanstalt tatsächlich die Möglichkeit, Überweisungen zu tätigen, ohne dass beim Empfänger als Absender die Justizvollzugsanstalt erscheint. Hierzu kann der Gefangene einen Zahlschein bei der Zahlstelle anfordern. In diesem Fall erscheint beim Empfänger der Name des jeweiligen Gefangenen als Absender. Allerdings ist diese Vorgehensweise leider nicht gebührenfrei.

Eine überraschend große Zahl der diesjährigen Anfragen und Eingaben bezog sich auf die Überwachung des Schriftverkehrs von Gefangenen durch die Justizvollzugsanstalten. Zum Teil fragten Betroffene allgemein an, unter welchen Bedingungen ihr Schriftverkehr überwacht werden darf, teils bezogen sich die Schreiben auf konkrete Vorkommnisse. Zur letztgenannten Gruppe gehörte der Fall, in dem eine Justizvollzugs-

anstalt ausgerechnet eine von unserer Dienststelle an einen Gefangenen gerichtete Postsendung geöffnet und damit gegen das Überwachungsverbot des § 29 Abs. 2 StVollzG verstoßen hatte. Nach dieser Vorschrift dürfen Schreiben der Gefangenen an bestimmte Stellen, wie z. B. an Volksvertretungen des Bundes oder der Länder sowie an deren Mitglieder, aber auch solche an die Datenschutzbeauftragten des Bundes und der Länder, nicht überwacht werden. Auch die Schreiben dieser Stellen an Gefangene unterliegen einem Überwachungsverbot.

Die betroffene Justizvollzugsanstalt räumte den Fehler auch unverzüglich ein und entschuldigte sich für den Vorfall. Eine Wochenendvertretung habe die Briefsendung aus Unkenntnis der einschlägigen gesetzlichen Bestimmungen geöffnet. Auf unsere Empfehlung hin hat die Justizvollzugsanstalt ihre Hausverfügung zur Überwachung des Schriftverkehrs zwischenzeitlich überarbeitet und ausführlicher gestaltet. Hierdurch soll sichergestellt werden, dass auch Bedienstete, die nur vertretungsweise mit der Briefüberwachung beauftragt sind, mit der gesetzeskonformen Verfahrensweise vertraut sind.

6. Die Odyssee eines korrekt adressierten Schreibens

Auch andere Behörden gehen mit Schreiben unserer Dienststelle nicht immer datenschutzgerecht um. So kam es im Berichtsjahr zu folgendem Vorfall:

Nach Bearbeitung der Eingabe eines Bürgers, der sich bei uns über die Vorgehensweise einer Staatsanwaltschaft beschwert hatte, wollten wir die betroffene Staatsanwaltschaft über das Ergebnis unserer Prüfung informieren. (Diese hatte – nebenbei erwähnt – ergeben, dass die Staatsanwaltschaft korrekt gehandelt hatte.) Wir leiteten unsere Mitteilung, die auch personenbezogene Daten des Betroffenen enthielt, vollständig adressiert der Staatsanwaltschaft zu. Im Bezug verwiesen wir auf die Stellungnahme der Staatsanwaltschaft, die diese in der Angelegenheit unserer Dienststelle gegenüber abgegeben hatte, und nannten außerdem das vollständige Aktenzeichen der Staatsanwaltschaft.

Das im Bezug unseres Schreibens genannte Aktenzeichen der Staatsanwaltschaft war den Bediensteten der Poststelle der Staatsanwaltschaft jedoch nicht bekannt. Nach Auskunft der Staatsanwaltschaft lag dies daran, dass die unter diesem Aktenzeichen erfassten Beschwerdevorgänge nicht im EDV-System der Behörde erfasst, sondern in ein im Vorzimmer des Leitenden Oberstaatsanwalts geführtes Register eingetragen werden und die ausgehende Post in diesen Verfahren ebenfalls durch das Vorzimmer des Leitenden Oberstaatsanwalts bearbeitet wird, sodass die Poststelle mit derartigen Vorgängen nur wenig zu tun habe. Da die Bediensteten der Poststelle das Aktenzeichen nicht als solches der Staatsanwaltschaft erkannten, brachten sie auf unserem Schreiben daher den Vermerk an „Dieser Schriftsatz kann ohne nähere Angabe nicht bearbeitet werden“ und wollten es an unsere Dienststelle zurückschicken. Dort kam es jedoch erst auf Umwegen an. Denn das für die Zurücksendung bestimmte Schreiben wurde – wahrscheinlich war es in der Poststelle der Staatsanwaltschaft falsch zugeordnet worden – zusammen mit anderen Poststücken versehentlich der Stadt zugeleitet, in der die Staatsanwaltschaft ihren Sitz hat. Vom dortigen behördlichen Datenschutzbeauftragten wurde es schließlich an uns weitergeleitet.

Bei diesem Vorgang sind der Staatsanwaltschaft gleich zwei Fehler unterlaufen: Zum einen stellt die Zusendung des Schreibens an die Stadt, die überhaupt nichts mit der Angelegenheit zu tun hatte, eine unzulässige Übermittlung personenbezogener Daten dar. Aber auch der Umstand, dass die Bediensteten, die im Bereich des Posteingangs mit unserer Mitteilung befasst waren, das im Bezug unseres Schreibens angegebene Aktenzeichen der Staatsanwaltschaft nicht gekannt haben, stellt einen datenschutzrechtlichen Mangel dar. Denn nach dem Landesdatenschutzgesetz müssen öffentliche Stellen, die personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um eine dem Landesdatenschutzgesetz entsprechende Datenverarbeitung zu gewährleisten, soweit der damit verbundene Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Der Begriff der technischen

und organisatorischen Maßnahmen umfasst dabei die gesamte Palette potenzieller Datensicherheitsmaßnahmen. Öffentliche Stellen müssen daher sicherstellen, dass eingehende Post – auch innerhalb einer Dienststelle – nicht unnötig hin und her geschickt wird. Nur so kann verhindert werden, dass unzuständige Personen vom Inhalt Kenntnis nehmen. Auf den konkreten Fall bezogen bedeutet dies, dass den in der Poststelle Beschäftigten Informationen zur Verfügung stehen müssen, anhand derer sie eindeutig feststellen können, ob es sich bei einem angegebenen Aktenzeichen um ein solches der Staatsanwaltschaft handelt und wer für die Bearbeitung der Angelegenheit zuständig ist.

Die Staatsanwaltschaft, die beide Fehler einräumte, hat Maßnahmen ergriffen, um derartige Vorfälle künftig zu vermeiden. So wurde eine Liste der bei der Staatsanwaltschaft gebräuchlichen Registerzeichen zusammengestellt, die unter anderem den Mitarbeiterinnen und Mitarbeitern der Poststelle bekannt gegeben wurde.

7. Der Entwurf eines Forderungssicherungsgesetzes

Der Entwurf eines Gesetzes zur dinglichen Sicherung von Werkunternehmeransprüchen und zur verbesserten Durchsetzung von Forderungen sieht für die Bereiche des Zivilprozessrechts, des Sozialrechts sowie des Straßenverkehrsrechts Regelungen vor, die aus Sicht des Datenschutzes bedenklich sind:

- In die Zivilprozessordnung soll unter anderem ein § 750 a neu eingefügt werden, der sich auf die Ausschreibung des Schuldners zur Aufenthaltsermittlung bezieht. Danach soll das Gericht auf Antrag des Gläubigers die Ausschreibung unter bestimmten Voraussetzungen anordnen können. In der Begründung zum Gesetzentwurf wird zu Recht betont, dass mit den beabsichtigten Ausschreibungen der Schuldner zur Aufenthaltsermittlung in den Fahndungshilfsmitteln der Polizei ein schwerwiegender Eingriff in das Grundrecht der Schuldner auf informationelle Selbstbestimmung einhergeht. Dieser wäre nur gerechtfertigt, wenn er erforderlich ist, um den angestrebten Zweck zu erreichen. Die Erforderlichkeit der beabsichtigten Ausschreibung von Schuldnern wäre nur dann gegeben, wenn die bisherige Praxis und die bisher dem Gläubiger für die Ermittlung des Aufenthaltsorts des Schuldners eingeräumten Möglichkeiten zu Unverträglichkeiten bei der Vollstreckung von Forderungen geführt haben. Konkrete Hinweise darauf sind im Gesetzentwurf indes nicht dargetan. Abgesehen davon würde die beabsichtigte Regelung zu einer systemwidrigen Nutzung der polizeilichen Fahndungshilfsmittel führen und zudem die Polizeibeamten mit fachfremden Aufgaben befassen, nämlich mit der Ermittlung des Aufenthalts von Schuldnern, gegen die kein Haftbefehl ergangen ist.
- Mit § 68 a des Zehnten Buchs des Sozialgesetzbuchs (SGB X) soll eine Befugnis zur Übermittlung von Daten zum Zweck der Vollstreckung privatrechtlicher Titel geschaffen werden. Dies würde im Regelungsbereich zum Schutz der Sozialdaten einen Systembruch darstellen und zu einer weiteren – abzulehnenden – Aushöhlung des Sozialgeheimnisses führen. Insbesondere ist aus § 74 SGB X zu folgern, dass eine Übermittlung von Sozialdaten zur Verfolgung privatrechtlicher Ansprüche grundsätzlich ausgeschlossen sein soll. Diese Vorschrift, die sich auf familienrechtliche Ansprüche einschließlich des Versorgungsausgleichs bezieht, lässt die Übermittlung von Sozialdaten an Privatpersonen nämlich lediglich eingeschränkt und ausnahmsweise nur deshalb zu, weil Leistungen wie Unterhalt in ihrer sozialen Funktion mit Sozialleistungen und deren Aufgaben vergleichbar sind. Eine solche Sachnähe ist bei der geplanten Neuregelung gerade nicht gegeben.
- § 39 des Straßenverkehrsgesetzes zur Übermittlung von Fahrzeugdaten und Halterdaten zur Verfolgung von Rechtsansprüchen soll um einen neuen Absatz 4 erweitert werden. Damit soll das Auskunftsrecht systemwidrig auf privatrechtliche Titel erstreckt werden, die nicht im Zusammenhang mit der Teilnahme am Straßenverkehr stehen. Nach geltendem Recht setzt eine Übermittlung von Fahrzeugdaten und Halterdaten zur Verfolgung von Rechtsansprüchen grundsätzlich voraus, dass diese im

Zusammenhang mit der Teilnahme am Straßenverkehr stehen; soweit der Gesetzgeber bereits jetzt Ausnahmen davon zugelassen hat, betreffen diese lediglich öffentlich-rechtliche oder bestimmte auf die öffentliche Hand nach dem Unterhaltsvorschussgesetz oder dem Bundessozialhilfegesetz übergegangene Ansprüche. Abgesehen von der Systemwidrigkeit der vorgesehenen Regelung ist – neben weiteren Ungereimtheiten – nicht ersichtlich, inwieweit die vorgesehene Auskunft die Position eines Vollstreckungsgläubigers überhaupt verbessern könnte, zumal das Fahrzeugregister jedenfalls in Baden-Württemberg regelmäßig keine aktuelleren Daten enthalten wird als das Melderegister und nach der Gesetzesbegründung ein Ersuchen an die Meldebehörde ohnehin vorrangig ist.

Wir haben die zuständigen Ministerien über unsere Auffassung informiert. Das Justizministerium hat unsere Bedenken dem Bundesministerium der Justiz sowie den übrigen Landesjustizverwaltungen mitgeteilt. Es bleibt aus Sicht des Datenschutzes zu hoffen, dass diese systemwidrigen und zum Schutz der Gläubiger zum Teil auch ungeeigneten Regelungen nicht Gesetz werden.

3. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheit

Im Gesundheitswesen gibt es eine Vielzahl von Akteuren. Das Spektrum reicht vom Arzt über die Krankenhäuser, Apotheken, die gesetzlichen Krankenkassen und die privaten Krankenversicherungen bis hin zu den Rentenversicherungsträgern, die sich in weiten Bereichen ebenfalls mit medizinischen Fragestellungen beschäftigen müssen. Nicht zu vergessen auch der öffentliche Gesundheitsdienst mit seinen ganz speziellen Aufgaben. Nicht für alle diese Personen und Einrichtungen ist der Landesbeauftragte für den Datenschutz zuständig. Er hat sich nur um die öffentlichen Stellen zu kümmern. „Nur“ bedeutet indes nicht, dass es sich dabei um Randbereiche handelt. Insbesondere die Zuständigkeit für die als öffentlich-rechtliche Körperschaften organisierten Träger der Sozialversicherung mit ihren Millionen Mitgliedern stellt erhebliche Anforderungen an die Leistungsfähigkeit des Personals der Dienststelle. Ein Tätigkeitsbericht kann und soll dabei kein vollständiges Bild dessen zeichnen, womit wir uns tatsächlich zu beschäftigen hatten. Die nachfolgende Darstellung bildet insoweit erneut nur einen Querschnitt aus der praktischen Arbeit.

1. Das Gesundheitsamt

Die Kombination der Worte „Gesundheit“ und „Amt“ ruft bei manchem Zeitgenossen düstere Assoziationen hervor. Darin zeigt sich nicht nur die verbreitete Skepsis, der Bürokratie Einblick in einen der intimsten Bereiche, der eigenen körperlichen und geistigen Verfassung, zu gewähren. Meist sucht man den Weg zum Gesundheitsamt ja auch nicht freiwillig, man wird „geschickt“ und „vorgeladen“. Umso wichtiger ist es für die Betroffenen, sicher sein zu können, dass das Amt die strengen Geheimhaltungspflichten penibel beachtet. Um beurteilen zu können, ob dies tatsächlich der Fall ist, gehen wir von Zeit zu Zeit vor Ort. In diesem Jahr besuchten wir das Gesundheitsamt der Landeshauptstadt Stuttgart.

1.1 Kontrollbesuch beim Gesundheitsamt Stuttgart

Aufgrund der langjährigen Erfahrungen erwartet man förmlich bei jedem neuen Kontrollbesuch, Mängel beim Umgang mit den personenbezogenen Daten festzustellen. Umso misstrauischer ist man, wenn nichts Nachteiliges auffällt. Selbstkritisch fragt man dann zunächst, ob datenschutzrechtlich tatsächlich alles in Ordnung ist oder ob lediglich etwas übersehen wurde. Andererseits mag man sich bei solchen „erfolglosen“ Kontrollen damit beruhigen, dass jedenfalls grobe Mängel offensichtlich nicht bestehen. Auch dies kann aus Sicht des Datenschutzes schon als ein erfreuliches Ergebnis gewertet werden.

Als Fazit aus einem Kontrollbesuch beim Gesundheitsamt Stuttgart lässt sich feststellen, dass dort datenschutzrechtlich im Großen und Ganzen alles so läuft, wie es sein sollte. Es ist jedenfalls nichts aufgefallen, was tatsächlich zu beanstanden gewesen wäre. Im Gegenteil: Manches war vorbildlich organisiert. So ist das Gesundheitsamt Stuttgart das bisher einzige von uns besuchte Gesundheitsamt, bei dem keine „Personenakten“ geführt werden. Zur Erinnerung: Schon seit Jahren besteht die Forderung des Datenschutzes, dass die Gesundheitsämter nicht alles, was sie über eine Person im Laufe der Jahre erfahren und dokumentieren, in einer einzigen Akte zusammenfassen. Die Anlässe, aus denen sich eine Person an das Gesundheitsamt wendet, haben in aller Regel nichts miteinander gemeinsam. Es ist deshalb auch nicht gerechtfertigt, die bei diesen aus unterschiedlichen Untersuchungen gewonnenen Erkenntnisse so miteinander zu verknüpfen, dass jeder im Gesundheitsamt, der die Akte in die Hand nimmt, zwangsläufig die gesamte „Gesundheitsamtskarriere“ der betreffenden Person erfährt. Gerade bei einem Gesundheitsamt mit mehreren Amtsärzten muss auch untereinander die ärztliche Schweigepflicht gewahrt bleiben. Im Gesundheitsamt Stuttgart führt tatsächlich jede Organisationseinheit ihre Akten selbst und bewahrt sie so auf, dass nur die in der Einheit beschäftigten zustän-

digen Mitarbeiterinnen und Mitarbeiter auf die Dokumentation zugreifen können. Vorbildlich insoweit auch die Vernichtung der Unterlagen, deren Aufbewahrungsfrist abgelaufen ist: Wie uns versichert wurde und auch tatsächlich festgestellt werden konnte, werden die medizinischen Unterlagen generell nach zehn Jahren ausgesondert und datenschutzrechtlich korrekt vernichtet. Der Aufwand hierfür ist beträchtlich, da alle Akten und Karteikartensammlungen jährlich vollständig durchforstet werden. Hier verspricht die Umstellung auf eine elektronische Aktenführung, die derzeit im Gange ist, eine wesentliche Vereinfachung und Entlastung zu bringen. Positiv zu erwähnen ist schließlich, dass die vom Gesundheitsamt angebotenen Beratungen (etwa zu AIDS, Geschlechtskrankheiten, Drogen) durchweg in einer Form stattfinden, die den Betroffenen ein hohes Maß an Anonymität und Unbeobachtetheit garantieren.

Nur wenig getrübt wird dieses Bild durch zwei Punkte, die aus datenschutzrechtlicher Sicht zu kritisieren waren:

Der eine Punkt betraf den Bereich Drogenberatung. Hier ergab sich, dass die Beraterinnen und Berater ihre schriftlichen Unterlagen zwar verschlossen in Aktenschränken aufbewahren. Allerdings konnte jeder ungehindert und, ohne dass dies vermerkt wurde, jederzeit auf die Schlüssel auch der anderen zugreifen. Hier sind wir der Auffassung, dass die Verschwiegenheitspflicht, der jeder Berater und jede Beraterin persönlich unterliegt, Maßnahmen zum Schutz des Vertrauens der Klienten erfordert. Auch wenn es unbestritten möglich sein muss, dass sich Berater gegenseitig vertreten, wenn akuter Beratungsbedarf entsteht und der bisherige Ansprechpartner gerade nicht zur Verfügung steht, darf es doch nicht so sein, dass die Möglichkeit einer Kenntnisnahme der sehr sensiblen Angaben völlig ins Belieben des Beratungspersonals gestellt wird. Das Gesundheitsamt ist unserer Aufforderung, hier etwas zu ändern, mittlerweile nachgekommen. Die Schrankschlüssel werden nun vom Sekretariat verwaltet.

Der andere Punkt betraf das eingesetzte Software-Programm Octoware. Hier wurde festgestellt, dass mitunter Zugriffe auf gespeicherte Daten möglich waren, die sich fachlich nicht rechtfertigen ließen. So sind im Gesundheitsamt Stuttgart etwa der Bereich Tuberkulose und der Bereich der weiteren Meldungen nach dem Infektionsschutzgesetz organisatorisch völlig voneinander getrennt. Gleichwohl war es so, dass die in den jeweiligen Bereichen beschäftigten Amtsärzte immer auch sehen konnten, was in dem jeweils anderen Bereich zu den betroffenen Patienten gespeichert war. Es widerspricht aber dem datenschutzrechtlichen Grundsatz der Erforderlichkeit, wenn ein Zugriff auf personenbezogene Daten ermöglicht wird, ohne dass diese Daten für die Erledigung der konkret übertragenen Aufgaben benötigt werden.

Das Gesundheitsamt sieht dies datenschutzrechtlich zwar ebenso, hat aber dargelegt, dass es sich hier um ein Software-Problem handle, das allenfalls der Hersteller lösen könne. Dies kann naturgemäß nicht zufrieden stellen. Wegen der vom Gesundheitsamt allein nicht zu behebenden technischen Mängel wurde zwar von einer Beanstandung abgesehen. Gleichwohl müssen sich die für den Einsatz von Octoware Verantwortlichen Gedanken darüber machen, wie dieses Programm datenschutzgerecht ausgestaltet werden kann. Von den Herstellern muss mit Nachdruck die Umsetzung der notwendigen Änderungen gefordert werden.

1.2 Wer im Glashaus sitzt ...

Gerade in wirtschaftlich schwierigen Zeiten hat regelmäßig ein Schlagwort Konjunktur, nämlich das der „Entbürokratisierung“. Wurde gestern noch laut nach Maßnahmen des Gesetzgebers gerufen, überbietet man sich heute mit der Forderung, nahezu sämtliche normativen Vorgaben über Bord zu werfen. In schöner Regelmäßigkeit trifft diese Forderung auch den Datenschutz. So konnte man Anfang des Jahres der Tagespresse die Forderung eines Landrats entnehmen, der Datenschutz müsse „heruntergeschraubt“ werden. Ironie des Schicksals: Nahezu

zeitgleich mit dieser Forderung flatterten uns zwei Datenschutzbeschwerden ins Haus, die Einrichtungen gerade desselben Landkreises betrafen.

Im einen Fall wandte sich ein Bürger an uns und teilte mit, er habe von einem Kreiskrankenhaus einen Arztbrief erhalten, in dem auf die gesundheitlichen Umstände eines mit Name und Adresse gekennzeichneten Patienten eingegangen wurde. Obwohl der Bürger das Kreiskrankenhaus schriftlich darauf hinwies, dass er gar kein Arzt sei und den betroffenen Patienten schon gar nicht behandle, erhielt er kurz darauf erneut einen diesen Patienten betreffenden ärztlichen Entlassungsbericht.

Unsere Recherchen ergaben, dass der betroffene Patient bei seiner Einlieferung ins Krankenhaus seinen behandelnden Arzt angegeben hatte. Das Krankenhaus hatte es, als es dessen Adresse aus dem Telefonbuch ermittelte, allerdings versäumt, auf die richtige Schreibweise des Namens zu achten. So kam es, dass ein gleichklingender Name herausgesucht und die Post dorthin verschickt wurde. Der darauf folgende Hinweis des Empfängers auf die offensichtliche Namensverwechslung war dann zwar in den Akten vermerkt worden. Im Computer unterblieb allerdings die Berichtigung. So kam es, dass der Entlassungsbericht erneut an den falschen Empfänger adressiert wurde.

Der Schaden war natürlich nicht mehr gutzumachen, wobei der Betroffene von Glück sagen konnte, dass die Schreiben an einen verantwortungsbewussten Zeitgenossen geraten waren. Für mich ist dieser Fall ein Paradebeispiel dafür, wozu es führen kann, wenn datenschutzrechtliche Standards „heruntergeschraubt“ werden.

Gleiches gilt für den anderen Fall. Dort beschwerte sich eine Bürgerin darüber, dass das Gesundheitsamt ein Schreiben, das sie vom Sozialministerium erhalten und welches sich auch in den Akten des Gesundheitsamts befunden habe, von diesem mit ihrem Namen und ihrer Adresse an Dritte weitergegeben worden war. Nachdem das Landratsamt der Betroffenen gegenüber zunächst noch gemeint hatte, das sei ja nun wirklich „keine gravierende Verletzung des Datenschutzes“, zeigte man sich nach meiner Intervention etwas reumütiger und versprach, „zukünftig in Fragen des Datenschutzes größere Sorgfalt walten zu lassen“. Gut und schön, aber auch hier wurde das Vertrauen eines Bürgers in den sorgsamen Umgang einer öffentlichen Stelle mit vertraulichen Informationen stark beschädigt.

Vor diesem Hintergrund kann ich nur davor warnen, datenschutzrechtliche Standards abzubauen. Dies zu fordern mag zwar bisweilen populär sein. Wer jedoch einmal, wie in den dargestellten Fällen, selbst Opfer einer Datenschutzverletzung wurde, wird solchen Forderungen sicher nicht viel abgewinnen können. Und treffen kann es schließlich jeden einmal.

2. Krankenversicherung

Die Finanzierung der sozialen Sicherungssysteme gehört zu den drängendsten und auch am schwierigsten lösbaren Problemen der heutigen Zeit. Fast täglich liest und hört man neue Vorschläge, die Auswege aus der Krise aufzeigen sollen. So unterschiedlich die jeweiligen Ansätze auch sein mögen, eines jedenfalls haben sie gemeinsam: Alle sind mit einer quantitativen und qualitativen Erweiterung der Datenverarbeitungsbefugnisse der Akteure im Gesundheitswesen verbunden. Im Geflecht der verschiedenen betroffenen Interessen ist das Interesse der Versicherten an der Wahrung ihres Datenschutzrechts dasjenige, das offensichtlich die geringste Rolle spielt. Dies zeigt sich unter anderem auch darin, dass die Meinung der Datenschutzbeauftragten im Gesetzgebungsverfahren immer weniger gefragt ist. Ein Beispiel hierfür ist das jüngst verabschiedete Gesetz zur Reform der gesetzlichen Krankenversicherung. Hier wurde der Datenschutz bei der Erarbeitung wesentlicher Teile des Gesetzentwurfs schlicht nicht beteiligt und auch nachträglich war eine Änderung des zwischen Regierung und Opposition gefundenen Kompromisses zugunsten eines besseren Datenschutzes poli-

tisch nicht mehr gewollt. Und dies angesichts des Umstands, dass mit dieser Novelle eine grundsätzliche Abkehr vom bisherigen System erfolgte. War es bisher so, dass die Krankenkassen die Behandlungsdaten ihrer Versicherten jedenfalls aus dem ambulanten Bereich nicht personenbezogen erhalten hatten, wird dies zukünftig anders sein. Als Folge der Neuregelung des vertragsärztlichen Vergütungssystems, das eine Übernahme des so genannten Morbiditätsrisikos durch die Krankenkassen beinhaltet, wird es den Krankenkassen ermöglicht, jede für die Behandlung eines Versicherten jeweils abgerechnete Leistung zu überprüfen. Damit erhält die Krankenkasse erstmals einen vollständigen Überblick über die Krankheitsverläufe ihrer Versicherten und ist durch die auf den Versicherten bezogene Zusammenführung der abgerechneten Leistungen in der Lage, individuelle Krankheitsprofile zu erstellen. Damit rückt der vielfach befürchtete „gläserne Patient“ in greifbare Nähe. Angesichts dieses schwerwiegenden Eingriffs in das Persönlichkeitsrecht der Betroffenen wäre es dringend erforderlich gewesen, vor einer abschließenden Entscheidung die datenschutzrechtlichen Fragen und vor allem die möglichen Alternativen zu diskutieren. Gelegenheit hierzu wurde bedauerlicherweise nicht gegeben.

In dieser Situation hat eine Datenschutzkontrollinstanz oft nur die Möglichkeit, dafür zu sorgen, dass der Datenschutz jedenfalls im Kleinen funktioniert. Zu tun gibt es hier immer noch einiges, wie die folgende Darstellung zeigt.

2.1 Die Kassenärztlichen Vereinigungen

Die in den 30er-Jahren des zwanzigsten Jahrhunderts aus Interessenvertretungen der Ärzteschaft entstandenen und seither immer wieder hinsichtlich ihrer Existenzberechtigung hinterfragten Kassenärztlichen Vereinigungen standen auch im Berichtszeitraum wieder im Blickpunkt unseres Interesses. Kein Wunder, laufen bei ihnen doch die Behandlungsdaten von Millionen von Versicherten, aber auch viele persönliche Daten der Vertragsärzte zusammen, werden dort verarbeitet und archiviert. Mit Blick auf die besondere Schutzwürdigkeit und Schutzbedürftigkeit insbesondere von Gesundheitsdaten bedarf es hier der besonderen Sorgfalt beim Umgang mit diesen Daten. Nicht immer wird die Praxis dem gerecht.

2.1.1 Kontrollbesuch bei der Kassenärztlichen Vereinigung Südbaden

Nachdem der Besuch einer Kassenärztlichen Vereinigung durch meine Dienststelle schon mehrere Jahre zurücklag, war es an der Zeit, auch dort einmal wieder zu prüfen, wie sich die Datenverarbeitung mittlerweile weiter entwickelt hat. Die Wahl fiel auf die Kassenärztliche Vereinigung Südbaden. Was dort zum Teil vorgefunden wurde, konnte nicht zufrieden stellen.

Durfte nach den Ausführungen der Geschäftsführung in der Eingangsbesprechung noch davon ausgegangen werden, dass der Betriebsablauf im Großen und Ganzen dem entsprach, wie es aus Sicht des Datenschutzes sein sollte, stellte sich bei der anschließenden Besichtigung einzelner Arbeitsplätze schnell heraus, dass zwischen Anspruch und Wirklichkeit doch Lücken klafften:

– Die von den Vertragsärzten (meist in Form einer Diskette) eingereichten Abrechnungsunterlagen müssen, damit sie elektronisch weiterverarbeitet werden können, zunächst eingelesen werden. Hierfür ist im Wesentlichen eine Mitarbeiterin zuständig. Nach Abschluss dieser Arbeiten und zuzüglich einer gewissen Karenzzeit werden die Original-Datensätze an diesem Arbeitsplatz nicht mehr benötigt. Nach Aussage der Kassenärztlichen Vereinigung sollte deshalb ein Zugriff auf diese Daten spätestens nach jeweils zwei Quartalen nicht mehr möglich sein. Tatsächlich ergab sich jedoch, dass die Mitarbeiterin die Disketten über die letzten acht Quartale in einem Stahlschrank aufbewahrt. Darüber hinaus werden die Abrechnungsdaten auf eine CD-ROM gebrannt und ebenfalls über mehrere Quartale hinweg gesammelt. Nach Aussage der Mitarbeiterin

werden diese CDs auch für die anderen Bezirksstellen hergestellt. Eine sachliche Notwendigkeit für die Aufbewahrung der Abrechnungsunterlagen in dieser Form konnte nicht begründet werden.

– Bei der Besichtigung eines weiteren Arbeitsplatzes in der Abrechnungsabteilung, in der die Original-Abrechnungsdaten der Vertragsärzte zentral verarbeitet werden, wurde festgestellt, dass dort nicht nur auf die Quartalsdatenbanken des laufenden und des vorangegangenen Quartals zugegriffen werden konnte, wie zunächst behauptet worden war, sondern vielmehr auf die Daten der letzten sechs Quartale. Diese Zugriffsmöglichkeit stand allen Mitarbeiterinnen der Abrechnungsabteilung offen. Indes konnte niemand erklären, wozu diese Daten gebraucht werden.

– Auch außerhalb der Abrechnungsabteilung sind nach Auskunft der Kassenärztlichen Vereinigung 51 Bedienstete berechtigt, auf für Zwecke der Leistungsabrechnung gespeicherte versichertenbezogene Daten zuzugreifen. Der Geschäftsführer räumte ein, dass einige dieser Personen die Zugriffsmöglichkeiten nicht benötigen.

– Die Kassenärztliche Vereinigung betreibt bei ihren Bezirksstellen (Freiburg, Offenburg, Konstanz) für unterschiedliche Zwecke jeweils mehrere Windows NT-Server. Eine stichprobenweise Prüfung ergab, dass eine Vielzahl personenbezogener Dokumente ohne weiteres von allen Mitarbeitern, die eine zur Anmeldung am NT-Netzwerk dienende Benutzerkennung hatten, gelesen oder sogar geändert werden konnte.

– Ein Verzeichnis enthielt zahlreiche gescannte Akten aus dem von der Kassenärztlichen Vereinigung geführten Arztregister. So konnte beispielsweise auf 37 DIN-A4-Seiten der berufliche Werdegang eines Arztes nachvollzogen werden. Die Akte enthielt unter anderem den Antrag auf Eintragung in das Arztregister, die Einbürgerungsurkunde, das ärztliche Approbationszeugnis, die Urkunde über die Anerkennung als Facharzt für Allgemeinmedizin sowie einen Auszug aus dem Familienbuch, aus dem nicht nur Angaben über den Arzt selbst, sondern auch über seine und die Angehörigen seiner Ehefrau hervorgingen.

– Ein anderes Verzeichnis enthielt 183 Unterverzeichnisse, in denen sich ebenfalls jeweils eine Reihe von gescannten Unterlagen befanden.

– Auf einem Server befanden sich Daten über die per Beleg (Behandlungsscheine) gemeldeten ärztlichen Leistungen ab dem zweiten Quartal 2000.

– In einem Verzeichnis waren 488 Dateien gespeichert. Die Überprüfung ergab, dass es sich dabei um Schreiben an Ärzte aus dem Bereich der Bezirksstelle Konstanz handelt, in denen diese unter Nennung der Patientennamen und der vom Arzt genannten Gebührennummern auf Fehler in ihrer Abrechnungsmitteilung hingewiesen wurden.

Die Zugriffsberechtigungen aller überprüften Dokumente waren auf „Vollzugriff für Jedermann“ eingerichtet. Damit können die Mitarbeiter der Kassenärztlichen Vereinigung auf alle genannten Dokumente des gesamten Bezirks zugreifen, unabhängig davon, ob sie in der Landesstelle in Freiburg oder einer der Bezirksstellen tätig sind.

Dieser Zustand widerspricht einer ordnungsgemäßen Datenverarbeitung. Diese setzt voraus, dass eine Datennutzung nur so weit ermöglicht wird, wie dies zur Aufgabenerfüllung erforderlich ist. Das Sozialgeheimnis, dem die hier betroffenen Arzt- und Versichertendaten unterliegen, gilt grundsätzlich auch innerhalb der

Kassenärztlichen Vereinigung. Um es zu wahren, muss sie sicherstellen, dass die Sozialdaten nur entsprechend der jeweiligen Aufgabenstellung zugänglich sind. Die festgestellten Zugriffsberechtigungen gehen weit über das hinaus, was die einzelnen Mitarbeiter der Kassenärztlichen Vereinigung zur Erledigung ihrer jeweiligen Aufgaben benötigen. Um diesen Mangel zu beseitigen, haben wir die Kassenärztliche Vereinigung aufgefordert, sich zunächst einmal darüber Kenntnis zu verschaffen, wie tatsächlich mit den Datenträgern verfahren wird und welche Zugriffsberechtigungen jeweils bestehen. Nicht erforderliche Berechtigungen müssen umgehend entzogen werden. Eng verknüpft damit ist die Notwendigkeit, dafür zu sorgen, dass der Zugriff auf Datenbestände zeitlich nur so lange zugelassen wird, wie dies für die Erfüllung der zu erledigenden Aufgaben konkret erforderlich ist. Dies bedeutet etwa, dass Zugriffsmöglichkeiten auf die Quartalsdatenbanken durch Mitarbeiterinnen der Abrechnungsabteilung auszuschließen sind, soweit sie über die letzten beiden Quartale hinausreichen. Die Sammlung ganzer Jahrgänge von Abrechnungsdaten auf Diskette und auf CD-ROM in den Räumen der Abrechnungsabteilung ist zu unterbinden, mit Ausnahme der Daten, die aktuell in der Bearbeitung sind. Dabei müssen die Datenträger so aufbewahrt werden, dass ein Zugriff unbefugter Dritter sicher ausgeschlossen ist. Auch dies war nicht gewährleistet, da die Schlüssel für den Stahlschrank und die Schiebeschränke nach Dienstende in den Diensträumen aufbewahrt werden und der Aufbewahrungsort dieser Schlüssel einer unbestimmten Zahl von Personen bekannt ist.

Deutliche Kritik musste sich die Kassenärztliche Vereinigung auch hinsichtlich ihrer Praxis der Altpapierbeseitigung gefallen lassen. Obwohl der Blick in die Altpapiercontainer mittlerweile zu den „Klassikern“ einer Datenschutzkontrolle zählt, verwundert es, dass immer wieder die gleichen Resultate zu verzeichnen sind. Das war hier nicht anders. Im Außenbereich des Gebäudes der Kassenärztlichen Vereinigung befindet sich ein Verschlag, in dem die Behälter zur Abholung bereitgestellt sind. Zwar kann der Verschlag mit einem Gitter verschlossen werden; zum Zeitpunkt des Besuchs stand er jedoch offen. So konnte sich jedermann (der Standort liegt unmittelbar neben einer Tankstelle) nach Belieben bedienen; und auch fündig werden. Mit einem Griff konnten so Schreiben an Ärzte entnommen werden, die beispielsweise Widerspruchsbescheide oder Leistungsübersichten zum Inhalt hatten. Damit verstößt die Kassenärztliche Vereinigung gegen das Sozialgeheimnis, das auch dazu verpflichtet, Unterlagen mit Sozialdaten so zu vernichten, dass Unbefugte keine Möglichkeit haben, diese Daten zur Kenntnis zu nehmen.

Aufgrund der Vielzahl der Datenschutzmängel und in einzelnen Bereichen auch wegen der Schwere des Verstoßes sah ich mich veranlasst, eine förmliche Beanstandung auszusprechen. Die Kassenärztliche Vereinigung hat dies akzeptiert und die erforderlichen Maßnahmen zum Teil bereits ergriffen, zum Teil arbeitet sie noch daran.

2.1.2 Der „gläserne Patient“ bei der Kassenärztlichen Vereinigung?

Wurde in der Vergangenheit mit Sorge vor dem „gläsernen Patienten“ gewarnt, so betraf dies meistens die Krankenkassen. Völlig unbeachtet blieb dabei, dass auch die Kassenärztlichen Vereinigungen in großem Umfang patientenbezogene Daten erheben und speichern. Denn alle Vertragsärzte rechnen die von ihnen erbrachten ambulanten Leistungen über „ihre“ Kassenärztliche Vereinigung ab. So verfügen die Kassenärztlichen Vereinigungen im Laufe der Zeit über eine enorme Fülle von Informationen über die gesundheitlichen Verhältnisse der Patienten in ihrem Bezirk. Und je länger sie diese Daten patientenbezogen speichern, desto brisanter wird das Datenmaterial.

Schon in unserem 22. Tätigkeitsbericht (LT-Drs. 13/520, S. 67 f.) war ein Problem angesprochen worden, das bis heute noch nicht zufrieden stellend gelöst wurde. Bei der Kassenärztlichen Vereinigung Südbaden sind wir darauf gestoßen, dass die Abrechnungsdaten der Vertragsärzte bis zu zehn Jahre gespeichert werden, wobei der Versichertenbezug über die gesamte Speicherdauer bestehen bleibt. Wir hatten dies damals kritisiert, weil das Sozialgesetzbuch die versichertenbezogene Speicherung im Regelfall allenfalls zwei Jahre lang erlaubt. Nur wenn sich innerhalb dieses Zeitraums Zweifel an der Richtigkeit der abgerechneten Leistungen ergeben, darf längerfristig versichertenbezogen gespeichert werden, und zwar grundsätzlich so lange, bis der Vorgang insgesamt abgeschlossen ist.

Die Kassenärztliche Vereinigung hatte sich auf den Standpunkt gestellt, die Rechtsvorschrift des Sozialgesetzbuchs, welche die Löschung nach zwei Jahren vorschreibt, gelte für sie überhaupt nicht. Das Sozialministerium Baden-Württemberg hatte sie in dieser Rechtsauffassung unterstützt, wobei es sich damit in Widerspruch zur Meinung des Bundesministeriums für Gesundheit und Soziale Sicherung setzte.

Zwischenzeitlich haben wir eine Umfrage zur jeweiligen Praxis bei den Kassenärztlichen Vereinigungen im Land durchgeführt. Das Ergebnis ist uneinheitlich:

- Die Kassenärztliche Vereinigung Südbaden speichert die Abrechnungsdaten insgesamt zehn Jahre lang. Über die letzten sechs Jahre erfolgt die Speicherung auf Datenträgern, die extern in einem Tresor untergebracht sind und auf die nur der interne Datenschutzbeauftragte zugreifen kann.
- Die Kassenärztliche Vereinigung Nordbaden bewahrt die Originalunterlagen – je nach verwendetem Medium – unterschiedlich lange auf: Krankenscheine reichen derzeit zurück bis ins Quartal 1/2001, Disketten werden nach acht Quartalen vernichtet. Die auf der Grundlage der Originalunterlagen erzeugten Datenbestände enthalten keinen Versichertenbezug mehr.
- Die Kassenärztliche Vereinigung Nord-Württemberg speichert die eingelesenen oder eingescannten Abrechnungsdaten für den jederzeitigen Zugriff über einen Zeitraum von zwei Quartalen in einer Datenbank. Gleichzeitig werden die Daten über fünf Quartale archiviert.
- Bei der Kassenärztlichen Vereinigung Südwürttemberg gehen die Abrechnungsdaten auf das Quartal 1/1996 zurück. Bis zum Quartal 4/1998 angefallene Daten sind gesperrt.

Als Fazit lässt sich feststellen, dass sich – legt man die Auskunft der Kassenärztlichen Vereinigungen zugrunde – derzeit allein die Kassenärztliche Vereinigung Nord-Württemberg datenschutzgerecht verhält. Bei der Kassenärztlichen Vereinigung Nordbaden wäre dabei allenfalls zu kritisieren, dass die Krankenscheine länger als zwei Jahre aufbewahrt werden, da die elektronisch gespeicherten Daten keinen Personenbezug mehr aufweisen. Ganz eindeutig zu lange speichert die Kassenärztliche Vereinigung Südwürttemberg die Daten versichertenbezogen. Die Situation ist hier ähnlich wie bei der Kassenärztlichen Vereinigung Südbaden.

Wir hatten uns in der Angelegenheit mit dem Sozialministerium besprochen. Dort sagte man zu, sich zu gegebener Zeit näher mit dieser Problematik zu befassen. Bewegung in die Sache scheint nun durch das GKV-Modernisierungsgesetz zu kommen. Vorgesehen ist zum einen, die Kassenärztlichen Vereinigungen nun ausdrücklich auch im Text des § 304 SGB V, nicht wie bisher nur in der Überschrift, aufzuführen. Damit dürfte es künftig ausgeschlossen sein zu behaupten, die spezielle Löschungsvorschrift des SGB V gelte für die Kassenärztliche Vereinigung schon über-

haupt nicht. Zum anderen wird bestimmt, dass „Daten, die für die Prüfungsausschüsse und ihre Geschäftsstellen für die Prüfungen nach § 106 erforderlich sind, spätestens nach vier Jahren“ zu löschen sind. Damit dürfte der überlangen Aufbewahrung von Behandlungsdaten der Patienten endgültig ein Riegel vorgeschoben sein. Ob sich die Kassenärztlichen Vereinigungen daran halten werden, bleibt abzuwarten.

2.1.3 Eine falsch verstandene Fürsorge

In seinem Volkszählungsurteil hatte das Bundesverfassungsgericht ausgeführt, eine Gesellschafts- und Rechtsordnung, in welcher der Bürger nicht mehr wissen könne, wer was wann und bei welcher Gelegenheit über ihn weiß, sei mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar. Der datenschutzrechtliche Auskunftsanspruch spielt deshalb für die Sicherung der persönlichen Handlungsfreiheit eine zentrale Rolle. Nicht selten haben öffentliche Stellen jedoch Hemmungen, ihre Daten offen zu legen, insbesondere dann, wenn damit gleichzeitig Informationen über Dritte preisgegeben würden. Mit dieser Problematik hatten wir in folgendem Fall zu tun:

Ein Patient begab sich zur Behandlung zu einem Facharzt. Da der Patient kurz zuvor die Krankenkasse gewechselt und seine neue Krankenversichertenkarte noch nicht erhalten hatte, erklärte er sich zunächst bereit, sich wie ein Privatpatient behandeln zu lassen. Unklar blieb, ob er den behandelnden Arzt darauf hingewiesen hatte, dass er seine Krankenversichertenkarte nach deren Erhalt nachreichen werde und dann die Behandlung als Sachleistung der gesetzlichen Krankenversicherung abgerechnet werden solle.

Obwohl der Patient tatsächlich seine Krankenversichertenkarte nachträglich in der Praxis vorgelegt hatte, erhielt er eine Rechnung des Arztes, die er dann letztlich auch bezahlte. Da er aber vermutete, der Arzt habe die Behandlung zusätzlich auf Kosten der gesetzlichen Krankenversicherung abgerechnet, wandte er sich an die Kassenärztliche Vereinigung Nordbaden und bat darum, ihm mitzuteilen, ob solche Leistungen tatsächlich abgerechnet wurden. Die Kassenärztliche Vereinigung lehnte die Auskunft ab, um den Arzt davor zu bewahren, von seinem Patienten des Abrechnungsbetrugs bezichtigt zu werden.

Diese Fürsorge zugunsten des Arztes ging zu weit. Die Kassenärztliche Vereinigung war nach § 83 SGB X verpflichtet, dem Patienten Auskunft auch über die zu seiner Person gespeicherten Abrechnungsdaten zu geben. Keine Rolle spielt es, dass die Kassenärztliche Vereinigung diese Daten vom Arzt erhalten hat. Für die Auskunftspflicht entscheidend ist, dass die Kassenärztliche Vereinigung mit den Abrechnungsdaten zugleich Informationen über den Versicherten erhält und speichert, nämlich etwa darüber, welchen Arzt der Versicherte wann aufgesucht hat und worauf er vom Arzt behandelt wurde. Sich hierüber Klarheit zu verschaffen ist das gute Recht eines jeden Versicherten.

Unzutreffend war in diesem Zusammenhang das von der Kassenärztlichen Vereinigung vorgebrachte Argument, § 305 SGB V räume dem Versicherten ja bereits einen Anspruch gegen die Krankenkasse darauf ein, über die im jeweils letzten Geschäftsjahr in Anspruch genommenen Leistungen und Kosten unterrichtet zu werden. Zwar gehen § 305 SGB V und § 83 SGB X formal in die gleiche Richtung, inhaltlich verfolgen sie aber unterschiedliche Zwecke. § 305 SGB V soll das Kostenbewusstsein der Versicherten stärken und die Transparenz der Leistungserbringung und der Leistungsabrechnung erhöhen und dadurch letztlich einen wirtschaftlicheren Umgang mit den Ressourcen der gesetzlichen Krankenversicherung fördern. § 83 SGB X dagegen ist Ausfluss der verfassungsrechtlich garantierten informationellen

Selbstbestimmung und soll es dem Betroffenen ermöglichen zu erfahren, was die Kassenärztliche Vereinigung über ihn weiß, um gegebenenfalls die Zulässigkeit der Verarbeitung überprüfen zu lassen. Wegen dieser unterschiedlichen Normzwecke stehen § 305 SGB V und § 83 SGB X nicht in einem Rangverhältnis zueinander. Dies entspricht auch der herrschenden Meinung.

Diese Rechtslage hatten wir der Kassenärztlichen Vereinigung Nordbaden schriftlich mitgeteilt. In ihrer Antwort bestreitet sie nach wie vor eine Auskunftspflicht. Sie meint, die von den Vertragsärzten im Rahmen der Abrechnung übermittelten Daten seien keine die Person des Versicherten betreffende Daten und deshalb sei § 83 Abs. 1 Satz 1 Nr. 1 SGB X nicht anwendbar, wenn ein Versicherter wissen wolle, was die Kassenärztliche Vereinigung über ihn speichere. Zudem würde ein Auskunftsanspruch nach § 83 SGB X durch § 305 SGB V verdrängt. Und selbst wenn § 83 Abs. 1 anwendbar wäre, sei sie nach § 83 Abs. 4 Nr. 3 SGB X zur Auskunft schon deshalb nicht verpflichtet, weil die Gefahr bestehe, der Betroffene könne die gewonnenen Erkenntnisse dazu nutzen, den Arzt eines Abrechnungsbetrugs zu bezichtigen. Dabei verkennt die Kassenärztliche Vereinigung allerdings, dass das Verschleiern eines Abrechnungsbetrugs gerade in der heutigen Situation der gesetzlichen Krankenversicherung kaum als „berechtigtes Interesse“ akzeptiert werden kann.

Im Ergebnis ist die Rechtsauffassung der Kassenärztlichen Vereinigung Nordbaden schlichtweg falsch. Sie beraubt den Versicherten seines verfassungsmäßigen Rechts zu wissen, wer was über ihn weiß. Von weiteren Maßnahmen haben wir derzeit nur deshalb abgesehen, weil sich die Angelegenheit im konkreten Fall bereits anderweitig erledigt hat und die Kassenärztliche Bundesvereinigung – so die Auskunft durch die Kassenärztliche Vereinigung – noch über dieser Rechtsfrage brütet. Letztlich muss in dieser Frage jedoch Klarheit für alle Beteiligten geschaffen werden, da mit vergleichbaren Auskunftsersuchen auch künftig zu rechnen ist.

2.2 Die Krankenkasse: Gut gemeint ist nicht immer richtig

Immer wieder muss man Daten verarbeitende Stellen darauf hinweisen, dass ausschlaggebend dafür, wie mit personenbezogenen Daten umgegangen werden darf, einzig und allein das Gesetz ist. Nicht einfach ist es, dafür Verständnis zu erhalten, wenn eine bestimmte Form der Datenverarbeitung eigentlich gut gemeint ist. Diese Erfahrung mussten wir in folgender Angelegenheit wieder einmal machen:

Wird jemand arbeitsunfähig krank, hat er für die Dauer von sechs Wochen gegen seinen Arbeitgeber einen Anspruch auf Entgeltfortzahlung. Seine Arbeitsunfähigkeit muss der Arbeitnehmer dem Arbeitgeber allerdings unverzüglich mitteilen. Hierzu erhält er, wenn es um eine ambulante Behandlung geht, von seinem Arzt den Durchschlag der Arbeitsunfähigkeitsbescheinigung. Begibt er sich dagegen zur stationären Behandlung ins Krankenhaus, erhält er von dort keine solche Bescheinigung, jedenfalls nicht ungefragt. Deshalb und weil es gerade bei einer stationären Aufnahme die konkrete körperliche Verfassung oft nicht zulässt, kann es vorkommen, dass die unverzügliche Benachrichtigung des Arbeitgebers über die Arbeitsunfähigkeit unterbleibt.

Aus dem Gedanken heraus, das Mitglied in dieser Situation zu entlasten, war es bei der AOK Baden-Württemberg und der Innungskrankenkasse Baden-Württemberg üblich, den Arbeitgeber vom Krankenhausaufenthalt seines Arbeitnehmers zu unterrichten, sobald der Krankenkasse die Aufnahmeanzeige durch das Krankenhaus vorlag. Dieser Service wurde auch von den Arbeitgebern dankbar angenommen. Allein, die gute Absicht reicht nicht aus. Denn das Ganze muss auch rechtlich zulässig sein. Und das war es tatsächlich nicht.

Die Information der Krankenkasse durch das Krankenhaus, dass sich ein Versicherter in stationärer Behandlung befindet, unterliegt dem Sozial-

geheimnis. Dieses darf in zulässiger Weise nur durchbrochen werden, wenn und soweit das Sozialgesetzbuch selbst dies gestattet. Im Sozialgesetzbuch gibt es aber keine Regelung, die eine solche Information des Arbeitgebers zulässt. Insbesondere ist § 69 Abs. 4 SGB X keine solche Vorschrift. Danach ist die Krankenkasse lediglich befugt, dem Arbeitgeber mitzuteilen, ob die Fortdauer einer Arbeitsunfähigkeit oder eine erneute Arbeitsunfähigkeit eines Arbeitnehmers auf derselben Krankheit beruht. Die dort geregelte Übermittlungsbefugnis betrifft also nicht die Mitteilung einer erstmaligen Erkrankung, sondern es geht darum, dem Arbeitgeber die Möglichkeit zu geben festzustellen, ob ein Anspruch des Arbeitnehmers auf Entgeltfortzahlung im Krankheitsfall ausnahmsweise entfällt. Dies ist dann der Fall, wenn die aktuelle Erkrankung als Fortsetzung einer früheren anzusehen und deshalb die frühere Arbeitsunfähigkeit für die aktuelle Arbeitsunfähigkeit noch relevant ist. Geht es dagegen nicht um eine Fortsetzungs-, sondern um eine Ersterkrankung, scheidet die Anwendbarkeit von § 69 Abs. 4 SGB X seinem Wortlaut nach aus. Nach dem Entgeltfortzahlungsgesetz ist in solchen Fällen allein der Arbeitnehmer verpflichtet, dem Arbeitgeber die Arbeitsunfähigkeit und deren voraussichtliche Dauer unverzüglich mitzuteilen. Die Krankenkasse darf das nicht für den Betroffenen erledigen, ohne diesen vorher zu fragen.

Auch wenn die AOK Baden-Württemberg zunächst etwas Mühe hatte, diese Rechtslage zu akzeptieren, weil sie bei einer Umstellung der bisherigen Praxis negative Reaktionen der Arbeitgeber befürchtete (nicht zu Unrecht, wie sich herausstellte), kam sie unserer Aufforderung schließlich – ebenso wie auch die Innungskrankenkasse Baden-Württemberg – doch nach. Wie es bei den einzelnen landesunmittelbaren Betriebskrankenkassen aussieht, entzieht sich unserer Kenntnis. Der Landesverband der Betriebskrankenkassen teilt jedenfalls unsere Rechtsauffassung und hat seine Mitglieder entsprechend informiert.

Interessant war übrigens die Eingabe eines Unternehmens, das sich kritisch mit unserer Auffassung auseinander setzte. Bezeichnend sein Argument für die Beibehaltung der Benachrichtigungspraxis: „Hierbei [Anm.: Gemeint ist die Information über die Dauer des Krankenhausaufenthalts] kann man sich nun mal nicht immer auf die Aussagen des Mitarbeiters verlassen, z. B. kann der Mitarbeiter angeben, er sei fünf Tage im Krankenhaus gewesen, statt dessen waren es aber nur drei Tage und die restlichen Tage hat er einfach frei genommen. Wie kommt man als Arbeitgeber zuverlässig an diese sehr wichtige Information?“ Nun, jedenfalls nicht durch die Krankenkasse!

2.3 Der Medizinische Dienst der Krankenversicherung: Gutachten mit Augenmaß

Immer wieder gibt es Einzelfälle, in denen die Krankenkasse Zweifel daran hat, ob Leistungen zu Recht geltend gemacht werden. Spielen in diesem Zusammenhang medizinische Sachverhalte eine Rolle, darf die Krankenkasse diese Fragen nicht selbst zu klären versuchen und sich hierzu Angaben über die gesundheitlichen Verhältnisse des Versicherten beschaffen. Für solche Fälle hat der Gesetzgeber nämlich eigens eine mit Ärzten besetzte Einrichtung vorgesehen, den Medizinischen Dienst der Krankenversicherung (MDK). Die Krankenkasse muss sich deshalb in solchen Fällen an den MDK wenden. Dieser allein ist berechtigt, sich an die Leistungserbringer zu wenden und von diesen nähere Einzelheiten über den Gesundheitszustand des Versicherten zu erheben. Der MDK erstellt auf der Grundlage der erhobenen Daten sein Gutachten. Nach § 277 Abs. 1 SGB V ist er dann verpflichtet, der Krankenkasse „das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund“ mitzuteilen.

Uns war nun berichtet worden, beim MDK Baden-Württemberg sei es gängige Praxis, in Erfüllung seiner Mitteilungspflicht den Krankenkassen regelmäßig das komplette Gutachten, also einschließlich der Angaben zur Krankengeschichte (Anamnese), zu übermitteln. Wir haben uns deswegen an den MDK gewandt und um Aufklärung gebeten.

Dabei hatten wir die Auffassung vertreten, dass in der Medizin grundsätzlich zwischen Anamnese, Befund und Diagnose unterschieden werde. Diese Begriffe kennzeichnen jeweils eigene Inhalte der ärztlichen Dokumentation. Auch das SGB V unterscheide begrifflich jedenfalls zwischen Befunden und Diagnosen. Es sei wenig plausibel anzunehmen, der Gesetzgeber habe – abweichend von anderen Vorschriften – gerade in § 277 Abs. 1 SGB V einen umfassenden Befundbegriff im Sinn gehabt, der alle Bestandteile einer ärztlichen Dokumentation einschließe. Vielmehr sei davon auszugehen, dass die Beschränkung des Gesetzes auf die Übermittlung der notwendigen Befundangaben bewusst erfolgt sei. Es könne sich dabei nur um Angaben handeln, die es der Krankenkasse ermöglichen, das vom MDK mitgeteilte Begutachtungsergebnis (laienhaft) nachzuvollziehen. Keinesfalls müsse der Krankenkasse die Datenbasis eines ärztlichen Sachverständigen zur Verfügung stehen. Im Übrigen würde eine solche Auffassung dem jüngst auch vom Bundessozialgericht bestätigten Verbot der Erhebung von Behandlungsunterlagen durch die Krankenkasse widersprechen.

Weiter haben wir darauf hingewiesen, dass nach dem Wortlaut des § 277 Abs. 1 Satz 1 SGB V nur die Übermittlung der „erforderlichen“ Befundangaben zulässig sei. Damit sei eine routinemäßige Übermittlung des vollständigen Befunds nicht zu vereinbaren. Der MDK müsse vielmehr vor jeder Datenweitergabe an die Krankenkasse prüfen, welche und wie viele Informationen die Krankenkasse braucht, um im konkreten Fall ihre Entscheidung treffen zu können. Dies setze regelmäßig eine kritische und verantwortliche Auswahl der mitzuteilenden Angaben voraus.

In seiner Stellungnahme teilte der MDK mit, die ärztlichen Gutachter seien verpflichtet worden, den Umfang der Mitteilungen nach § 277 Abs. 1 SGB V einzuschränken, wenn es um besonders sensible Sachverhalte gehe (kritische berufliche und familiäre Verhältnisse, Betroffenheit Dritter, psychiatrische Sachverhalte, bestimmte Erkrankungen). Allerdings legt der MDK die Worte „erforderliche Angaben über den Befund“ weiter aus als wir. Der Befundbegriff sei nicht streng medizinisch zu verstehen. Denn soweit eine Begutachtung allein auf der Grundlage von Akten erfolge, würde der MDK eigentlich keine Befunde erheben. Dann könnte er aber auch keine Befunde übermitteln, wie dies in § 277 Abs. 1 SGB V vorgesehen sei. Daraus ergebe sich, dass der Befundbegriff anders zu verstehen sei. Der Sache nach müsse es darum gehen, der Krankenkasse die Informationen zur Verfügung zu stellen, die es ihr ermöglichen, zu treffende Sachentscheidungen inhaltlich zu begründen. Dazu könne es im Einzelfall erforderlich sein, auch bestimmte Angaben aus der Anamnese zu kennen.

Dies haben wir akzeptiert. Dabei gehen wir davon aus, dass sich der MDK an die selbst auferlegten Beschränkungen hinsichtlich des Umfangs und der Inhalte seiner Befundmitteilungen an die Krankenkasse halten wird.

3. Rentenversicherung

Die gesetzliche Rentenversicherung ist das größte soziale Sicherungssystem in der Bundesrepublik Deutschland. In ihr sind alle Personen kraft Gesetzes versichert, die als Arbeitnehmer gegen Entgelt beschäftigt sind. Ihr Leistungskatalog umfasst nicht nur Altersrenten, sondern auch medizinische, berufsfördernde und ergänzende sowie sonstige Rehabilitationsleistungen. Damit solche Leistungen erbracht werden können, muss der Versicherte dem Rentenversicherungsträger zahlreiche persönliche Daten zur Verfügung stellen. Dabei darf er zu Recht darauf vertrauen, dass mit diesen Angaben, die teilweise intime Lebenssachverhalte betreffen, verantwortungsvoll umgegangen wird. Bei der Landesversicherungsanstalt Baden-Württemberg, die unserer Kontrollzuständigkeit untersteht, kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass dem so ist; dies jedenfalls legen die Erfahrungen aus der Kontrollpraxis der letzten Jahre nahe. Damit soll indes nicht gesagt sein, dass es im Einzelfall nicht doch zu Mei-

nungsverschiedenheiten kommen kann. Mitunter bedarf es dann einiger Mühe, die Feinheiten des Datenschutzrechts plausibel zu machen. Dazu nachfolgender Fall.

3.1 Die falsch verstandene Zeugenpflicht

Ein Unternehmen wandte sich an uns und behauptete, die Landesversicherungsanstalt Baden-Württemberg wolle es dazu drängen, einen umfangreichen Fragebogen auszufüllen, der einen bestimmten Mitarbeiter betraf. Dies erfordere einen bürokratischen Aufwand, den zu erbringen man ohne rechtliche Verpflichtung hierzu weder in der Lage noch bereit sei.

In der Sache ging es darum, dass im Rahmen eines Scheidungsverfahrens der Versorgungsausgleich durchgeführt werden sollte. Das Familiengericht benötigte dazu eine Information über die Rentenanwartschaften des Versicherten. Zu diesem Zweck wandte es sich an die Landesversicherungsanstalt und bat um entsprechende Auskunft. Der Landesversicherungsanstalt lagen die erbetenen Informationen zu diesem Zeitpunkt allerdings nicht vor. Deshalb übersandte sie dem Arbeitgeber des Versicherten zwecks „Klärung des Versicherungsverhältnisses“ einen (standardisierten) Fragebogen mit der Aufforderung, Angaben zum Beruf des Versicherten sowie über die Beitragsentrichtung, die Unterbrechungstatbestände und die Krankenkasse zu machen.

Datenschutzrechtlich ist es so, dass die Landesversicherungsanstalt nach § 74 Satz 1 Nr. 1 Buchst. b SGB X und § 53 b Abs. 2 Satz 3 des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit zwar zur Übermittlung der vom Familiengericht angeforderten Angaben verpflichtet war. Diese Übermittlungspflicht besteht jedoch nur, soweit die Daten, um die es geht, schon vorliegen. Liegen sie nicht vor, können sie auch nicht übermittelt werden. Eine gesetzliche Übermittlungspflicht berechtigt nicht gleichzeitig und zwangsläufig auch dazu, Daten, die man selbst nicht hat, eigens zu dem Zweck zu erheben, um sie an denjenigen, der sie gefordert hat, weiterleiten zu können. Die Erhebungsbefugnisse der Landesversicherungsanstalt ergeben sich vielmehr abschließend aus § 148 Abs. 1 Satz 2 SGB VI. Da die Informationsbeschaffung zum Zweck der Durchführung eines Verfahrens über den Versorgungsausgleich dort nicht genannt ist, hätte die Landesversicherungsanstalt sich deshalb auch nicht an den Arbeitgeber des Versicherten wenden dürfen.

Die Landesversicherungsanstalt hatte dies verkannt und ging fälschlich davon aus, durch das Auskunftsersuchen des Familiengerichts berechtigt und sogar verpflichtet zu sein, sich an den Arbeitgeber des Versicherten zu wenden. Ob es uns gelungen ist, ihr dieses datenschutzrechtliche Grundprinzip klarzumachen, dass nämlich datenschutzrechtlich jede einzelne Phase der Datenverarbeitung, hier also etwa Datenerhebung und Datenübermittlung, jeweils für sich einer eigenen gesetzlichen Rechtfertigung bedarf, wissen wir nicht. Die Schreiben der Landesversicherungsanstalt erwecken diesbezüglich gewisse Zweifel. So hat sie etwa auch darauf verwiesen, dass der Versicherte nachträglich einen Antrag auf Kontenklärung gestellt habe. Aber selbst mit Zustimmung des Versicherten wäre eine Datenerhebung, die nicht zur Erfüllung einer Aufgabe nach § 148 Abs. 1 Satz 2 SGB VI dient, nicht zulässig. Denn §§ 67 ff. SGB X in Verbindung mit § 148 SGB VI sehen nicht vor, dass eine solche Erhebung mit Einwilligung rechtens sei; eine Einwilligung genügt nach dem Gesetzeswortlaut nur für die Verarbeitung und Nutzung von Sozialdaten (§ 67 b Abs. 1 und 2 SGB X; so auch: Bundessozialgericht vom 28. November 2002 – RDV 2003, 142). Und auch mit dem Argument, man sei jederzeit berechtigt gewesen, ein Kontenklärungsverfahren durchzuführen, kann die Landesversicherungsanstalt ihr Vorgehen im konkreten Fall nicht rechtfertigen. Denn zum Zeitpunkt der Anfrage beim Arbeitgeber hatte sie keinen objektiven Anlass, dies zu tun. Motiv für das Tätigwerden war allein die gerichtliche Aufforderung, wie sich aus mehreren Schriftsätzen der Landesversicherungsanstalt eindeutig ergab. Dies ist allerdings ein Ge-

sichtspunkt, der bei der Ermessensabwägung keine tragende Rolle spielen durfte.

3.2 Gemeinsam geht's besser

Unterschiedliche Auffassungen darüber, wie datenschutzrechtliche Bestimmungen auszulegen sind und wie Datenschutz und Verwaltungspraxis am besten in Übereinstimmung gebracht werden können, gibt es immer wieder. In der Regel kommt man am Ende häufig doch zu einem Ergebnis, das gemeinsam getragen werden kann. Ein Beispiel für ein solches konstruktives Zusammenwirken ist folgender, mit der Landesversicherungsanstalt Baden-Württemberg erörterter Sachverhalt:

Wer Leistungen der gesetzlichen Rentenversicherung begehrt, muss nachweisen, dass die Voraussetzungen hierfür vorliegen. Häufig geht es dabei um medizinische Fragen. Um das Vorbringen von Versicherten fachkundig prüfen zu können, unterhält die Landesversicherungsanstalt Baden-Württemberg einen Sozialmedizinischen Dienst. Kommt dieser nach Prüfung der Unterlagen zum Ergebnis, dass es einer körperlichen Untersuchung des Versicherten bedarf, lädt er in der Regel hierzu ein. Es gibt allerdings auch Fälle, in denen der Sozialmedizinische Dienst selbst die Begutachtung nicht durchführen kann, entweder weil es an den personellen Ressourcen fehlt oder aber weil der Dienst keine Ärzte der speziellen Fachrichtung beschäftigt. Dies sind die Fälle, in denen man externen Sachverstand hinzuziehen muss.

Bisher war es so, dass der interne Prüfarzt in den Fremdbegutachtungsfällen einen Gutachter auswählte und diesem die vorhandenen Unterlagen übersandte. Der Gutachter wandte sich dann an den Versicherten und lud ihn zu einer Untersuchung ein. Fand diese statt, erstellte der Facharzt sein Gutachten und übermittelte es der Landesversicherungsanstalt.

Aus Sicht der Betroffenen hatte diese Praxis die nachteilige Folge, dass sie zum einen keinen Einfluss darauf hatten, durch welchen Arzt sie begutachtet wurden. Und datenschutzrechtlich war problematisch, dass der Gutachter die der Landesversicherungsanstalt vorliegenden medizinischen Unterlagen erhielt, ohne dass endgültig feststand, ob sich der Versicherte überhaupt begutachten lassen wollte oder ob er sich gerade durch den von der Landesversicherungsanstalt ausgewählten Facharzt begutachten lassen wollte. Denn jedenfalls kann nie ganz ausgeschlossen werden, dass ein Versicherter eine Begutachtung ablehnt, wenn auch um den Preis, dass sein Antrag auf Leistungen dann abgelehnt wird.

Datenschutzrechtlich ist immer dann, wenn es um die Weitergabe personenbezogener Daten an Dritte geht, zu fragen, ob der angestrebte Erfolg auch auf eine Weise erreicht werden kann, die mehr Rücksicht auf die Belange des Betroffenen nimmt. In diesen Begutachtungsfällen hielt ich dies für möglich. Denn der gleiche Erfolg kann erreicht werden, wenn man dem Versicherten aufgibt, selbst einen Gutachter vorzuschlagen oder sich bei einem von der Landesversicherungsanstalt vorgeschlagenen Gutachter vorzustellen, wobei diesem die Unterlagen erst dann zugesandt werden, wenn sich der Versicherte bereit erklärt hat, diesen tatsächlich aufzusuchen. Es geht hier um den Grundsatz der Erforderlichkeit einer Datenverarbeitung, konkretisiert in der Frage, wie viel Selbstbestimmung man bereit ist, dem Betroffenen einzuräumen.

In ausführlichen Besprechungen mit der Landesversicherungsanstalt Baden-Württemberg konnte ein Ergebnis erzielt werden, das den gegenseitigen Bedürfnissen gerecht wird: Die Landesversicherungsanstalt wird künftig jeden Versicherten, der von einem Konsiliararzt untersucht werden soll, vor dessen Beauftragung schriftlich davon unterrichten, dass eine solche Untersuchung erforderlich ist und welchen Arzt die Landesversicherungsanstalt vorgesehen hat. Der Versicherte hat dann die Möglichkeit, Gründe zu benennen, die aus seiner Sicht gegen die Begutachtung an sich oder gegen den speziellen Gutachter bestehen. Er wird auch darüber informiert, dass die Landesversicherungsanstalt die

ihn betreffenden Unterlagen dem ausgewählten Gutachter übersenden wird, wenn innerhalb einer bestimmten Frist keine Einwände erhoben werden.

Wir halten dies für ein gutes Ergebnis, das wieder einmal zeigt, dass in der Verwaltung durchaus die Bereitschaft besteht, auch etablierte Verfahren zugunsten einer datenschutzfreundlicheren Sachbehandlung abzuändern. Nötig hierfür ist ein Verständnis für die Belange der jeweils anderen Seite, das hier – wie das Ergebnis zeigt – gegenseitig vorhanden war. Selbstverständlich ist dies allerdings nicht.

2. Abschnitt: Soziales

Einen Schwerpunkt unserer (Kontroll-)Tätigkeit, den wir z. B. im Jahr 2001 bei den Jugendämtern gesehen haben, haben wir im abgelaufenen Berichtsjahr nicht gesetzt. Gleichwohl gab es zahlreiche Vorgänge, denen wir nachzugehen hatten. So versuchten wir, einem Datenabgleich auf seinen verschlungenen und oftmals schwer durchschaubaren Pfaden zu folgen, bemühten uns um die Kontrolle wissenschaftlicher Begleituntersuchungen und fanden auch in der täglichen Arbeit der Sozial- und Jugendämter reichlich Berichtenswertes.

1. Datenabgleich der BAföG-Verwaltung mit dem Bundesamt für Finanzen

Wenn die BAföG-Ämter bei den Studentenwerken und den Kommunen einen Datensatz ihrer Leistungsempfänger dem Bundesamt für Finanzen übermitteln und die Bundesbehörde ihre Informationen mit diesem Datensatz abgleicht – was kommt dabei wohl heraus? Zumindest jede Menge Wirbel, aber auch eine überraschend hohe Rückforderungssumme. Von einem Skandal war die Rede, von „Mogelstudenten“, die bei dem bundesweit durchgeführten Datenabgleich ihre Vermögensverhältnisse aufhellen lassen mussten; die Gegenseite sprach gar von einer „Rasterfahndung“ nach Auszubildenden. Einige Studenten wandten sich Hilfe suchend an meine Dienststelle, nachdem die BAföG-Ämter sie im Rahmen einer förmlichen Anhörung mit dem Ergebnis des Abgleichs konfrontiert hatten. Dieses Ergebnis wiederum mag sogar das in Baden-Württemberg zuständige Ministerium für Wissenschaft, Forschung und Kunst verblüfft haben, als es meine Dienststelle im Oktober wissen ließ, dass bis dato in rund 1 800 Fällen bereits 8,7 Millionen Euro an Ausbildungsförderung von den Empfängern zurückgefordert worden seien und dies noch nicht das Ende bedeute. Es vermeldete zudem, dass auf die Rückforderungsmaßnahme bislang 3,8 Millionen Euro eingegangen seien.

Dabei hatte eigentlich alles ganz harmlos begonnen. Ein Kollege aus einem anderen Bundesland wies im Jahr 2002 darauf hin, dass auf Veranlassung des dortigen Wissenschaftsministeriums ein Abgleich durch die Ämter für Ausbildungsförderung beim Bundesamt für Finanzen durchgeführt werde. Dabei gehe es um die tatsächlich in Anspruch genommenen Freistellungsaufträge aller Leistungsempfänger nach dem Bundesausbildungsförderungsgesetz. Im Juli 2002 wandten wir uns also an das Landesamt für Ausbildungsförderung beim Regierungspräsidium Stuttgart, zunächst nur, um herauszufinden, ob sich denn die hiesigen Ämter auch an diesem Abgleich beteiligten. Die Antwort kam nicht gerade spontan, denn erst im September erfuhren wir, dass das Ministerium für die Beantwortung unserer Anfrage zuständig sei, und man kam überein, dass unser Schreiben deshalb dorthin weiterzuleiten sei. Das kann passieren, dachten wir – schade nur, dass kurz zuvor, nämlich im August, just dieser Abgleich rasch durchgeführt wurde. Von dieser Durchführung erfuhren wir allerdings erst im Dezember 2002.

Erst nach einigen weiteren Monaten wussten wir, wer genau was gemacht hat oder hätte tun sollen:

Nach dem „Steuerentlastungsgesetz 1999/2000/2002“ sind die Kreditinstitute gehalten, dem Bundesamt für Finanzen (BfF) Mitteilung zu machen, in welcher Höhe Freistellungsaufträge tatsächlich in Anspruch genommen werden. Das Einkommensteuergesetz (EStG) bietet zudem die Möglichkeit, diese Informationen des Bundesamts über tatsächliche Zinseinkünfte aus Kapitalvermögen mit Daten von Sozialleistungsträgern automatisiert abzu-

gleichen (§ 45 d EStG). Die obersten Landesbehörden für Ausbildungsförderung hatten sich daher gemeinsam mit der zuständigen Bundesbehörde darauf verständigt, einen solchen Abgleich durchzuführen und zwar für alle Leistungsfälle, erstmalig im Jahr 2002. Nach erfolgtem Abgleich sollten den Ämtern für Ausbildungsförderung durch das Bundesamt für Finanzen die Zinserträge mitgeteilt werden. Vereinbart wurde eine Mindestgrenze von 200 DM für die Anzeige der Summe der mitgeteilten Zinserträge.

In Baden-Württemberg erfolgte dieser Datenabgleich für das Meldejahr 2001. Da der Vermögensfreibetrag der Auszubildenden im Bundesausbildungsförderungsgesetz im Laufe des Jahres 2001 aber auf 10 000 DM erhöht wurde, wich das Ministerium für Wissenschaft, Forschung und Kunst von der Vorgabe des Bundes ab. Die Grenzsumme zugeflossener Zinserträge wurde auf 350 DM erhöht. Für die Durchführung des automatisierten Abgleichs übermittelte das Zentrum für Informationstechnik bei der Oberfinanzdirektion Stuttgart (ZfI) dem Bundesamt für Finanzen Nachname, Vorname, Geburtsdatum und Postleitzahl der Leistungsbezieher, damit das Bundesamt sie mit seinen Informationen über tatsächlich in Anspruch genommene Freistellungsaufträge vergleiche. Die Rückspieldaten ergänzten dann die genannten Angaben zu den geförderten Auszubildenden lediglich um den Hinweis, dass Freistellungsaufträge für das Jahr 2001 in Anspruch genommen wurden. Diese Informationen waren auf einem Datenträger gespeichert, der wiederum beim ZfI ausgewertet wurde. Auswertung hieß, dass das verwendete Programm für alle Förderfälle, in denen die genannte Grenzsumme von 350 DM erreicht wurde, einen Aktenvermerk auswarf. Diese Vermerke wurden postalisch vom ZfI an die für die betroffenen Auszubildenden jeweils zuständigen BAföG-Ämter versandt. Anhand der Aktenvermerke haben die Ämter dann geprüft, ob die mitgeteilten Zinseinkünfte im maßgeblichen Bewilligungszeitraum mit dem vom Auszubildenden angegebenen Vermögen übereinstimmen. Ergab sich eine Abweichung, wurden die Auszubildenden hierzu angehört und um neuerliche Sachaufklärung hinsichtlich ihres Kapitalvermögens gebeten. Stellte sich dabei heraus, dass die Angaben in den Antragsunterlagen unvollständig waren, wurde der Bewilligungsbescheid aufgehoben; zu Unrecht erbrachte Leistungen wurden zurückgefordert. In diesen Fällen war zusätzlich auch zu prüfen, ob die Voraussetzungen für die Einleitung eines Ordnungswidrigkeitenverfahrens vorliegen. Tatsächlich waren bis Oktober dieses Jahres 575 solcher Bußgeldverfahren eingeleitet.

So weit zum nicht ganz unkomplizierten tatsächlichen Ablauf. Rechtlich ist die Sache auch nicht ganz einfach, schon weil die Rechtsgrundlage für den Datenabgleich im Einkommensteuergesetz nach der überwiegenden Meinung der Landesdatenschutzbeauftragten nicht ausreichend ist. Zum anderen traten im geschilderten Verfahrensablauf etliche Ungereimtheiten zu Tage, die darauf hindeuten, dass die Aktion wohl nicht bis zum Letzten durchdacht war.

Eines vorweg: Es geht uns keineswegs darum, einen derartigen Abgleich von vornherein auszuschließen; denn ein Leistungsmissbrauch ist vor allem in einer solchen Größenordnung nicht hinnehmbar. Wir müssen aber auf einem rechtlich ordnungsgemäßen Verfahren auf rechtlich sicherer Grundlage bestehen. Das ist derzeit (noch) nicht gewährleistet:

Die zuständigen Ministerien der Länder und des Bundes erblicken im Einkommensteuergesetz die Rechtsgrundlage für den geschilderten automatisierten Datenabgleich. Tatsächlich sieht § 45 d EStG die Vornahme eines solchen Abgleichs von Sozialdaten mit Daten des Bundesamts für Finanzen ausdrücklich vor. Das Bundesamt ist danach zudem berechtigt, das Ergebnis des Abgleichverfahrens, wie geschehen, den Sozialleistungsträgern, also hier den BAföG-Ämtern, mitzuteilen. Die BAföG-Verwaltung agierte somit nicht im „rechtsfreien Raum“, um einmal bildhaft zu sprechen, denn in der Tat hat ja der Gesetzgeber seinen Willen zu einem solchen automatisierten und kompletten Abgleich kundgetan.

Aus der Sicht des Datenschutzes bestehen an der Vollständigkeit der genannten gesetzlichen Regelung allerdings erhebliche Zweifel. Es fehlt hier nämlich an einer ausdrücklichen Datenerhebungsbefugnis für die Sozialleistungsträger, also die BAföG-Ämter, und an einer entsprechenden gesetz-

lichen Befugnis zur Weitergabe von Sozialdaten an das Bundesamt für Finanzen. Dass die Bestimmung des § 45 d EStG diese Anforderungen als „notwendige Vorfrage voraussetzt und abdeckt“, wie das Wissenschaftsministerium meinte, ist nach den vom Bundesverfassungsgericht entwickelten Grundsätzen gerade nicht ausreichend. Im so genannten Volkszählungsurteil hat es nämlich unter anderem entschieden, dass Einschränkungen des Rechts auf informationelle Selbstbestimmung einer klaren gesetzlichen Grundlage bedürfen.

So hat der Gesetzgeber für den Datenabgleich des Sozialhilfeträgers in § 117 des Bundessozialhilfegesetzes eben diese Erhebungs- und Übermittlungsbefugnis an das Bundesamt für Finanzen ausdrücklich vorgesehen. Von der Notwendigkeit einer solchen gesetzlichen Regelung geht auch der Entwurf der Bundesregierung eines Vierten Gesetzes für moderne Dienstleistungen am Arbeitsmarkt (Bundesratsdrucksache 558/03, 15. August 2003) in seinem § 52 und der hierzu gegebenen Begründung aus. Wir haben deshalb gefordert, zunächst eine ausreichende gesetzliche Regelung für diesen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht aller Beteiligten zu schaffen.

Diese Forderung wird unterstrichen durch die Erfahrungen, die wir gerade bei der Aufarbeitung des Abgleichvorgangs mit den zuständigen Behörden machen mussten. Zunächst fällt auf, dass von einer entscheidenden Mitwirkung der BAföG-Ämter, die ja bekanntlich die Daten verarbeitenden Stellen sind und als gesetzliche Leistungsträger die „Herrschaft über die Sozialdaten“ haben sollten, nur selten die Rede ist. Sie kommen erst ins Spiel, wenn die Auswertung erfolgt ist und die Anhörungen anstehen. Der Rolle verantwortlicher Leistungsträger nach dem Sozialgesetzbuch wird das nicht gerecht. Stattdessen ist in den uns vorliegenden Unterlagen ausschließlich die Rede von einer Weisung des Bundesministeriums für Bildung und Forschung, einem entsprechenden Auftrag des Wissenschaftsministeriums an die Datenzentrale Baden-Württemberg, der nachfolgenden Bitte der Datenzentrale an das ZfI und der anschließenden Weitergabe von Daten an das BfF. In dieses Bild passt, dass das ZfI die Daten für die BAföG-Ämter zwar seit Jahren verarbeitet, hierüber aber bislang noch nicht einmal der vom Gesetzgeber geforderte schriftliche Auftrag erteilt wurde. Bereits im Jahr 1997, als die Daten noch durch das Zentrum für Kommunikation und Datenverarbeitung verarbeitet wurden, wiesen wir auf das Fehlen einer solchen schriftlichen Vereinbarung hin. Im Jahr 1999 legte das Wissenschaftsministerium dann einen Mustervertrag vor und teilte mit, dass eine Auftragserteilung – nun an das ZfI – beabsichtigt sei. Wir haben diesen Entwurf datenschutzrechtlich bewertet, jedoch wurde er nie in Kraft gesetzt.

Nachdem das Ministerium jüngst wiederholt darauf hingewiesen worden ist, bemüht sich die Behörde nun intensiv um einen solchen ordnungsgemäßen Auftrag. Neben einem solchen von § 80 SGB X geforderten schriftlichen Auftragsverhältnis mangelt es auch an einer Freigabe des zum Abgleich eingesetzten EDV-Verfahrens. Man bewegt sich also rechtlich und auch in der praktizierten Umsetzung auf unsicherem Boden. Daher überrascht es umso mehr, dass uns die oberste Landesbehörde, allen Hinweisen auf die Notwendigkeit einer ausreichenden Rechtsgrundlage zum Trotz, bereits weitere Abgleichverfahren ankündigte. So soll der Datenabgleich für das Meldejahr 2001 wiederholt werden, diesmal allerdings für Zinseinkünfte zwischen 200 und 349 DM. Das erstaunt, hatte doch das Ministerium selbst mit Rücksicht auf den Vermögensfreibetrag eine Mindestsumme von 350 DM festgelegt. Somit müssten sich die Rückmeldungen doch regelmäßig im Bereich des Vermögensfreibetrags bewegen. Auch hier warten wir noch auf eine Erklärung des Wissenschaftsministeriums.

2. Datenschutz beim Sozialamt

Der Sozialdatenschutz sollte ständiger Begleiter der Mitarbeiter/innen des Sozialamts sein. Deshalb ist es anzuraten, sich diese Vorschriften im Sozialgesetzbuch immer wieder zu vergegenwärtigen. Ob die Behörde ihre Daten automatisiert verarbeitet, Material für eine Untersuchung zur Verfügung stellt, als Auskunftei Privater in Anspruch genommen werden soll oder einfach nur Unterlagen in einem Leistungsfall sammelt, regelmäßig ist das

Grundrecht auf informationelle Selbstbestimmung der Beteiligten betroffen. Deshalb muss eine Frage immer lauten: Sieht der Gesetzgeber für diese Vorgänge jeweils eine Datenverwendungsbefugnis vor?

2.1 Tücken bei der Beschränkung von Zugriffsberechtigungen im Sozialamt

Wer personenbezogene Daten verarbeitet, muss dafür sorgen, dass nur diejenigen Bediensteten darauf zugreifen können, die dies für ihre Aufgaben benötigen. Dass dabei an ganz unterschiedlichen Stellen Schwierigkeiten auftreten können, zeigte sich exemplarisch bei einem Kontrollbesuch, den wir in einem Sozialamt durchführten. Teils war bereits die Festlegung unzulänglich, welche Bediensteten auf welche Daten zugreifen dürfen, teils haperte es an der technischen Umsetzung der Zugriffsbeschränkungen.

– Leseberechtigungen zu weitgehend

Die Zugriffskonzeption des Sozialamts sah vor, dass jede Sachbearbeiterin und jeder Sachbearbeiter Sozialdaten nur für solche Personen erfassen und ändern kann, für die sie dienstlich unmittelbar oder im Rahmen einer Vertretungsregelung zuständig sind. Demgegenüber gestattete das Sozialamt allen Bediensteten, im Wege des lesenden Zugriffs auf Daten sämtlicher Hilfeempfänger zuzugreifen. Das Sozialamt hielt diese umfassende Leseberechtigung für erforderlich, um feststellen zu können, ob eine Person früher unter anderem Namen einmal Sozialhilfe erhalten hat. Aber selbst für diesen Zweck hätte keine uneingeschränkte Zugriffsmöglichkeit auf alle zu der Person gespeicherten Sozialdaten eröffnet werden dürfen. Wir forderten das Sozialamt daher zu einer entsprechend restriktiven Vergabe der Zugriffsberechtigungen auf.

– Nicht nur Dialogberechtigungen berücksichtigen

Um die notwendige Beschränkung durchzuführen, müssen die Berechtigungen in der programmeigenen Berechtigungsverwaltung angepasst werden. Als problematisch erwies sich dabei, dass neben Berechtigungen für die interaktive Fallbearbeitung im Bildschirmdialog auch Berechtigungen existierten, die sich auf die so genannte Listenauswertung beziehen. Damit lassen sich anhand vorgegebener Kriterien Listen derjenigen Hilfeempfänger erzeugen, auf die diese Kriterien zutreffen. Ändert man nur die Berechtigungen für den interaktiven Zugriff, wirkt sich dies nicht auf die Berechtigungen zur Listenauswertung aus. Notwendig ist es daher, auch die Berechtigungen für die Listenauswertung anzupassen. Das Sozialamt will seinen Bediensteten als Konsequenz daraus die Berechtigung zur Listenauswertung entziehen.

– Zugriffsmöglichkeit auf Dateiebene

Auch wenn alle programminternen Berechtigungen korrekt vergeben sind, können immer noch zu weitgehende Zugriffsmöglichkeiten bestehen. Auch dafür bot das überprüfte Sozialamt ein Beispiel:

Dazu muss man Folgendes wissen: Die mit dem Programm erfassten und bearbeiteten Sozialdaten werden in einer Reihe von Dateien auf einem Server abgelegt. Alle Nutzer dieses Programms konnten diese Dateien auf Betriebssystemebene, die nicht der programminternen Berechtigungsverwaltung unterliegt, lesen und ändern. Dies war zwar nicht mit Hilfe der Sozialamts-Fachanwendung möglich, jedoch ließen sich die Dokumente, beispielsweise mit gängigen Textverarbeitungsprogrammen wie dem auf vielen PCs standardmäßig vorhandenen Notepad, öffnen. Bei der stichprobenweisen Ansicht einzelner solcher Dateien mit Hilfe von Notepad ergab sich, dass diese zwar unstrukturiert und die gespeicherten Werte zum Teil durch Zahlwerte codiert waren, dass die übrigen, im Klartext lesbaren Daten aber immer noch eine Reihe personenbezogener Informationen über namentlich genannte Hilfeempfänger offenbarten.

– Zugriffsmöglichkeit auf Protokolldateien

Das im Sozialamt eingesetzte Programmpaket protokolliert bei einer Reihe von Verarbeitungsschritten, wer diese wann ausgeführt hat. Es ist nicht nur ein Gebot des Sozial-, sondern auch des Personaldatenschutzes, dabei darauf zu achten, dass nur die notwendigen Daten erfasst und diese auch nur solchen Bediensteten zugänglich gemacht werden können, die dies dienstlich benötigen. In einer Dienstanweisung für das Sozialamt wurde daher festgelegt, dass diese Protokolldaten nur mit Zustimmung des Personalrats ausgewertet werden dürfen. Diese Regelung lief praktisch jedoch dadurch ins Leere, dass jeder Bedienstete des Sozialamts wie oben beschrieben auf Dateiebene auch auf diese Protokolldaten zugreifen konnte.

– Auch Sicherungskopien berücksichtigen

Aus Gründen der Datensicherung legt das Sozialamt von Zeit zu Zeit sowie vor Systemänderungen eine Sicherungskopie der aktuellen Softwareinstallation inklusive der darin gespeicherten personenbezogenen Daten an. Das Sozialamt hatte diese wie die Daten des Produktivsystems auf dem Server gespeichert. Da es auch die Zugriffsberechtigungen wie im Produktivsystem eingerichtet hatte, konnten alle Nutzer dieses Verfahrens auf Dateiebene auch auf diese historischen Daten zugreifen.

Um die auf Dateiebene bestehenden, zu weitgehenden Zugriffsberechtigungen beschränken zu können, bedarf das Sozialamt der Unterstützung durch den Programmhersteller. Nach Auskunft des Sozialamts wird sich das Problem mit Übergang auf eine neue, bislang aber noch nicht freigegebene Version des Programms ausräumen lassen. Das Sozialamt hat sich ferner mit dem Hersteller in Verbindung gesetzt, um schon in der Übergangsphase eine Beseitigung des Mangels in Angriff nehmen zu können.

2.2 Missklang bei MoZArT?

Die Rückkehr arbeitsloser Menschen auf den Arbeitsmarkt ist ein Problem, das selbstverständlich auch den Gesetzgeber beschäftigte und auch weiterhin zu immer neuen Anstrengungen animiert. Mit dem „Gesetz zur Verbesserung der Zusammenarbeit von Arbeitsämtern und Trägern der Sozialhilfe“ vom 20. November 2001 schuf der Gesetzgeber auf Initiative der Bundesregierung im Sozialgesetzbuch mit den so genannten Experimentierklauseln die rechtlichen Voraussetzungen für Modellprojekte in diesem Bereich. Im Rahmen dieser Projekte sollen, gefördert durch das Bundesministerium für Wirtschaft und Arbeit, auf regionaler Ebene neue Formen der Zusammenarbeit zwischen Arbeits- und Sozialämtern erprobt werden, kurz MoZArT. Der Name soll offensichtlich Wohl- und Gleichklang symbolisieren und bedeutet nichts anderes als *Mo*dellprojekte zur Verbesserung der *Z*usammenarbeit zwischen *A*rbeitsämtern und *T*rägern der Sozialhilfe. Ziele sind die Optimierung der Vermittlung in Arbeit, eine Steigerung der Wirksamkeit der Hilfen zur Eingliederung in eine Erwerbstätigkeit und eine Vereinfachung des Verwaltungsverfahrens. Diese Verbesserungen sollen vor allem bei arbeitslos gemeldeten Empfängern von Hilfe zum Lebensunterhalt nach dem Bundessozialhilfegesetz und bei Beziehern von Arbeitslosenhilfe zum Tragen kommen. Auch in Baden-Württemberg gibt es einen derartigen Modellversuch, bei dem ein Arbeitsamt und der zuständige Sozialhilfeträger eine Kooperationsvereinbarung geschlossen haben.

So viel zum Hintergrund. Denn nicht etwaige datenschutzrechtliche Probleme bei der Ausgestaltung dieser Zusammenarbeit sollen hier besprochen werden, vielmehr haben wir unser Augenmerk auf die vorgesehene wissenschaftliche Begleituntersuchung gerichtet. Nach dem Willen des Gesetzgebers sind die Modellvorhaben entsprechend ihrer Zielsetzung so auszuwerten, dass sie eine bundesweite Bewertung zulassen. Beauftragt mit der Begleitforschung zu MoZArT ist das Institut

für angewandte Sozialwissenschaft GmbH, kurz infas. Damit das, was Evaluation heißt, auch Hand und Fuß bekommt, benötigte das Institut Sozialdaten: einmal von dem am Modellversuch mitwirkenden Sozialamt, außerdem von weiteren Sozialämtern, die lediglich als Vergleichsstichprobe Kontrollgruppen bilden sollten. Konkret geht es dabei neben codierten Daten auch um Informationen wie Name, Adresse und Telefonnummer von Hilfeempfängern zum Zweck einer telefonischen Befragung durch infas. Damit die Sozialämter solche personenbezogenen Angaben in größerer Anzahl für Zwecke der wissenschaftlichen Forschung an ein Unternehmen weitergeben können, bedurfte es einer vorherigen Genehmigung durch die oberste Landesbehörde, also des Sozialministeriums (§ 75 Abs. 2 SGB X). Diese Genehmigung erfolgte auch im Juni 2002.

Zur Ziehung der Vergleichsstichprobe hatte infas verschiedene Städte im ganzen Bundesgebiet benannt. Die Genehmigung erstreckte sich somit auch auf die Datenübermittlung durch zwei Städte in Baden-Württemberg „als Träger der Sozialhilfe im Wege der Delegation durch den jeweiligen Kreis, soweit diese bereit sind, sich zu beteiligen“, wie es im Genehmigungsschreiben des Sozialministeriums an infas heißt. Bei unseren Nachfragen erfuhren wir, dass beide Städte überhaupt keine Zuständigkeit für Sozialhilfeaufgaben besaßen. Infas wandte sich kurzerhand an die tatsächlich zuständigen Sozialhilfeträger, also die jeweiligen Landkreise. Ein Leistungsträger lehnte die Mithilfe ab, der andere leistete der Bitte Folge, was wir leider zu spät erfuhren. Im Hinblick auf die vorgelegte Genehmigung übermittelte er nämlich Name, Vorname, Geburtsjahr, Geschlecht und Anschrift von 1 490 Hilfeempfängern, die infas mittels einer kennwortgeschützten Excel-Datei zugeleitet wurden. Auf der Grundlage dieses Datenmaterials wurden durch infas 395 Personen angeschrieben und danach 129 telefonische Interviews geführt. Die Sache hat allerdings einen Haken: Denn sowohl in den Unterlagen von infas als auch in der Genehmigung wurden allein und ausschließlich die beiden Städte angesprochen und damit wurden auch nur diese beiden zur Datenübermittlung ermächtigt. Diese Befugnis sollte zudem auch noch von der Bereitschaft der beiden Kommunen zur Mitwirkung abhängen. Keinesfalls kann daher davon ausgegangen werden, dass bei etwa mangelnder Bereitschaft oder, wie hier, bei tatsächlicher Unmöglichkeit der Mitwirkung ersatzweise der jeweilige „wirkliche“ Sozialhilfeträger zur Übermittlung berechtigt sein sollte, zumal es sich bei den Betroffenen auch um einen ganz anderen Personenkreis handelt. Andernfalls hätte dies in der Genehmigung deutlich zum Ausdruck kommen müssen. Genau genommen erfolgten die Datenübermittlungen ohne Genehmigung und damit ohne rechtliche Grundlage.

Infas und der Behörde stand allerdings ein Rettungsanker zur Verfügung, den sie aber nicht ergriffen. Mit dem § 118 wurde am 27. April 2002 eine Vorschrift in das Bundessozialhilfegesetz eingefügt, die bereits am 1. Mai 2002 in Kraft trat. Danach darf der Sozialhilfeträger einer wissenschaftlichen Einrichtung, die im Auftrag des Bundes ein Forschungsvorhaben im Sozialleistungsbereich durchführt, Sozialdaten übermitteln, ohne dass es hierzu einer Genehmigung bedarf. Allerdings treffen den Leistungsträger umfangreiche Verfahrenspflichten, die er vor der Übermittlung zu erfüllen hat. Mangels wirksamer Genehmigung hätte der Sozialhilfeträger somit nur aufgrund dieser Bestimmung der Bitte von infas nachkommen können.

Es war offensichtlich, dass sowohl infas als auch das Sozialamt in ihrem Festhalten an der Genehmigung einem Missverständnis unterlagen. Deshalb sahen wir auch von einer Beanstandung der unberechtigten Übermittlung ab. Zudem wäre es auch nicht angezeigt, wenn Sozialämter nun auf eine Mitwirkung bei solchen wissenschaftlichen Begleituntersuchungen verzichten würden. Wir haben aber das betroffene Amt zu mehr Sorgfalt bei der Prüfung von Unterlagen und das Sozialministerium zu mehr Kontrolle bei solchen Maßnahmen angehalten.

2.3 Aus der Praxis verschiedener Sozialämter

Die alltägliche Arbeit der Sozialämter ist immer eine Fundgrube für datenschutzrechtliche Fragestellungen aller Art, wie die anschließenden Beispiele zeigen.

– Bereits im Sommer des Jahres 2002 wandte sich ein Bürger mit der Bitte an unsere Dienststelle, für ihn in seiner Sache tätig zu werden. Das zuständige Sozialamt verlangte von ihm die Vorlage mehrerer Unterlagen und er fragte sich und uns, ob diese Forderungen berechtigt seien. Ein Routinefall also, dachten wir zunächst, und nahmen Kontakt mit dem Sozialhilfeträger auf, nicht ahnend, dass sich diese Angelegenheit zu einer Geduldsprobe entwickeln würde. So tauschten wir ein ganzes Jahr lang Meinungen mit dem zuständigen Sozialamt aus, versuchten dieses zu einer datenschutzfreundlichen Vorgehensweise zu bewegen und appellierten schließlich an Verhältnismäßigkeit und Sensibilität im Umgang mit personenbezogenen Daten. Umsonst: Im Juli dieses Jahres mussten wir den Fall zum Leidwesen des Bürgers und leider mit einem für uns unbefriedigenden Ausgang zu den Akten geben.

  Was war geschehen? Der Bürger bezog vom Sozialamt laufende Hilfe zum Lebensunterhalt nach dem Bundessozialhilfegesetz, einschließlich der Kosten für seine Unterkunft, die sich aus den tatsächlichen Miet- und den Mietnebenkosten zusammensetzen. Im Anschluss an die Zeit des Sozialhilfebezugs war der Bürger bei der Kommune selbst in einem auf ein Jahr befristeten Beschäftigungsverhältnis tätig. Dies dank einer Kostenzusage des Sozialamts, sodass die Aufwendungen für die Beschäftigung letztlich wieder aus Sozialhilfemitteln bestritten wurden. Kurz vor Ablauf der Zeit seiner Beschäftigung erreichte ihn die noch ausstehende Nebenkostenabrechnung. Mit dieser erst nachträglich erstellten Rechnung wurde für einen Zeitraum, in dem der Bürger noch nicht sozialversicherungspflichtig beschäftigt, also noch Hilfeempfänger war, eine Nachzahlung in Höhe von 712 DM gefordert. Die Abrechnung umfasste Positionen wie Müllentsorgung, Gebäudeversicherung, Allgemeine Versicherung, Außenanlagen/Winterdienst, Wartung, Brandschutz usw.

  Sich an eine Vereinbarung mit dem Sozialamt erinnernd, legte der Bürger die Abrechnung der Behörde vor. Überraschend für den Antragsteller und für uns nicht minder war die Reaktion des Sozialamts. Dabei soll hier außer Betracht bleiben, ob die Mietnebenkosten für einen Zeitraum, in dem der Berechtigte einen Anspruch auf Sozialhilfe hat, diesem diese Kosten nur deshalb nicht mehr erstattet werden dürfen, weil diese lange zuvor entstandenen Nebenkosten leider erst zu einem Zeitpunkt abgerechnet wurden, zu dem der Bürger bereits bei der Stadtverwaltung beschäftigt war und somit nicht mehr von Sozialhilfe lebte. Gestört haben wir uns vielmehr daran, dass die Behörde – obgleich es nur um eine rückwirkende Teilabwicklung von Sozialhilfeansprüchen ging – ihr komplettes Überprüfungsprogramm ablaufen ließ:

  Zur Bearbeitung des Antrags auf einmalige Beihilfe verlangte sie die Vorlage von Kontoauszügen für den Zeitraum März bis einschließlich Juni 2002, also für vier Monate, was damit begründet wurde, dass die Sozialbehörde von allen Erstantragstellern auf Sozialhilfe die lückenlose Vorlage der Kontoauszüge der letzten drei Monate verlange. Auf die „Zugabe“ von einem Monat angesprochen, erklärte das Sozialamt, es sei erforderlich zu klären, ob der Bürger die Kostennachforderung nicht doch unmittelbar vor Antragstellung noch selbst beglichen habe. Zum Nachweis der Einkünfte, die, warum auch immer, offensichtlich nicht diesen Kontoauszügen entnommen werden konnten, forderte das Sozialamt die Vorlage von Verdienstabrechnungen für den Zeitraum Mai bis einschließlich Juli 2002, also für drei Monate. Dies sollte deshalb notwendig sein, weil der Bürger während seiner Beschäftigung bei der Kommune ein schwankendes

Einkommen aufgrund ebenso schwankender Dienstzeiten erzielte. Damit aber nicht genug: Zusätzlich sollte ein Nachweis erbracht werden, aus dem ersichtlich war, ob sich die Miete geändert hat. Dies könne einmal eine ausdrückliche Bestätigung des Vermieters sein, dass keine Änderung eingetreten ist, andernfalls eine vom Vermieter zu erstellende Mietbescheinigung. Auch diese Position mochte das Amt nicht aus den vorgelegten Kontoauszügen entnehmen, vielmehr musste in jedem Fall eine dritte Person, hier also der Vermieter, einbezogen werden. Aus einem Kontoauszug schloss das Sozialamt dann, dass sich der Mietzins, den der Bürger zu entrichten hatte, mittlerweile wohl doch um rund 20 Euro erhöht hatte, sodass nun auch die Zusammensetzung dieser Mietzahlung durch den Vermieter aufzuschlüsseln war. Es sei daran erinnert, dass es dem Bürger keineswegs um die Übernahme seines Mietzinses ging. Um es kurz zu machen: Wir haben an der grundsätzlichen Berechtigung der Sozialbehörde, zur Überprüfung der Einkommens- und Vermögensverhältnisse die Vorlage von Kontoauszügen zu verlangen, nicht gerüttelt, ihr aber dringend empfohlen, sich gerade im vorliegenden Fall neben der letzten Verdienstbescheinigung allenfalls auf die Anforderung des aktuellen Kontoauszugs zu beschränken. Aus diesem kann dann auch die Höhe der Miete entnommen werden, ohne dass gleichzeitig dem Vermieter der neuerliche Antrag des Bürgers zur Kenntnis gebracht wird. Das Sozialamt hielt aber an seiner Begründung und seinen Forderungen fest und lehnte den Antrag des zwischenzeitlich arbeitslos gewordenen Bürgers wegen fehlender Mitwirkung ab.

– Ein städtisches Klinikum (betrieben in der Rechtsform einer gGmbH), das wegen der von einem Bürger in Anspruch genommenen Pflege und Behandlung noch eine unbeglichene Forderung über Krankenhauskosten besaß, wollte den Anspruch geltend machen und übertrug die Besorgung dieses Geschäfts einem Anwalt. Diesem war bekannt, dass der Bürger zum damaligen Zeitpunkt Sozialhilfe bezog. Der Bevollmächtigte des Klinikums wandte sich nun an das zuständige Sozialamt mit der Bitte um Mitteilung, ob die Tatsache des Leistungsbezugs noch immer zutraf.

  Wir rieten der Behörde, auf diese Frage keine Auskunft zu erteilen. Dies deshalb, weil es sich bei dem Gegenstand der Anfrage um Sozialdaten handelt, die ein Leistungsträger eben nur unter engen Voraussetzungen weitergeben darf. Dem Sozialamt war es aber gesetzlich nicht erlaubt, die gewünschten Informationen zu übermitteln.

  Daran ändert sich nicht etwa bereits deshalb etwas, weil dem Klinikum und dessen anwaltlichem Vertreter ja schon bekannt war, dass der Betroffene zu einem früheren Zeitpunkt soziale Leistungen erhalten hatte und damit zumindest sein damaliger Kontakt zum Sozialamt für den Gläubiger offenkundig ist; bei dem Sozialdatum, das es zu schützen gilt, muss es sich nämlich nicht um ein Geheimnis handeln. Es geht vorliegend nicht um eine strafbewehrte Schweigeverpflichtung für bestimmte Berufsgruppen, denen in ihrer Eigenschaft, z. B. als Arzt oder Psychologe, Umstände anvertraut wurden, wie wir dies aus dem Strafgesetzbuch kennen (§ 203 Abs. 1). Es geht vielmehr darum, dass Eingriffe in das Grundrecht auf informationelle Selbstbestimmung, hier durch Übermittlung von Sozialdaten durch einen Sozialleistungsträger, eben einer gesetzlichen Grundlage bedürfen. Somit kommt eine Weitergabe solcher Informationen nur in Betracht, wenn eine im Sozialgesetzbuch verankerte Übermittlungsbefugnis dies dem Leistungsträger gestattet.

  Zwar erlaubt der Gesetzgeber der Sozialleistungsbehörde die Herausgabe eines Standarddatensatzes zur Durchsetzung einer öffentlichrechtlichen Geldforderung in Höhe von mindestens 600 Euro (§ 68 Abs. 1 SGB X). Hierzu ist aber erforderlich, dass der geltend gemachte Anspruch seinen Rechtsgrund im öffentlichen Recht hat. Das ist bei einer Geldforderung aufgrund eines privatrechtlichen (Behandlungs-)Vertrags nicht der Fall. Dies gilt auch dann, wenn der Anspruch einer öffentlichen Stelle zusteht. Zulässig ist auch die Mit-

teilung von Schuldnerdaten an einen Gläubiger, der einen Anspruch auf Sozialleistungen pfändet, die so genannte Drittschuldnererklärung nach der Zivilprozessordnung (§ 71 Abs. 1 Satz 2 SGB X). Der für die Gewährung dieser Sozialleistung zuständige Träger hat dann nach Vorlage eines Pfändungsbeschlusses an der Pfändung mitzuwirken. Das war hier ebenfalls nicht der Fall.

Offensichtlich hat der Gesetzgeber eine Übermittlung von Sozialdaten durch einen Leistungsträger zur Verwirklichung privatrechtlicher Ansprüche – bislang jedenfalls – grundsätzlich nicht gewollt (vgl. hierzu aber auch die Ausführungen zum Forderungssicherungsgesetz im 2. Teil, 2. Abschnitt, Nr. 7). Er lässt insoweit nur dann eine Ausnahme und damit eine Durchbrechung des Sozialgeheimnisses zu, wenn die Datenübermittlung der Durchsetzung familienrechtlicher Unterhaltsansprüche und der Durchführung des Versorgungsausgleichs dient (§ 74 SGB X). Das hat seinen Grund darin, dass gerade Unterhaltsleistungen in ihrer Funktion den Sozialleistungen nicht unähnlich sind. Somit gehört es auch ganz allgemein nicht zu den Aufgaben des Sozialamts, jedwedem privatem Gläubiger bei der Geltendmachung seiner Forderungen behilflich zu sein (§ 69 Abs. 1 Nr. 1 SGB X).

– Das musste auch ein geprellter Vermieter erkennen, der sich an ein Sozialamt wandte, um dort die neue Anschrift eines Sozialhilfeempfängers in Erfahrung zu bringen. Der Vermieter wollte bei seinem ehemaligen Vertragspartner aufgelaufene Mietschulden einfordern. Werden die Mietschulden eines Hilfeempfängers aber sozialhilferechtlich nicht durch das Sozialamt übernommen, so gehört es auch nicht zu den Aufgaben des Leistungsträgers, einen Vermieter bei der Geltendmachung seiner Forderung durch die Mitteilung von Sozialdaten tatkräftig zu unterstützen. Das Sozialamt musste also den Vermieter auf einen anderen Weg, z. B. den zu der Meldebehörde, verweisen.

– Eine ganz andere Sachlage betraf die Arbeitsweise eines Sozialhilfeträgers, der sich bemühte, Empfänger von Sozialhilfe in den Arbeitsmarkt zu integrieren. Zu diesem Zweck legte er einer Hilfeempfängerin eine „Einverständniserklärung in die Datenweitergabe“ vor, mit der die Betroffene in die Übermittlung ihrer Sozialdaten an einen Arbeitsvermittlungsservice einwilligen sollte. Dass das Sozialamt hierzu das Einverständnis der Hilfeempfängerin benötigte, wurde bereits im 20. Tätigkeitsbericht (LT-Drs. 12/4600, Seite 65 f.) dargelegt. Der Hilfesuchende kann seiner Pflicht zur Selbsthilfe durch Arbeit nämlich auf unterschiedliche Weise nachkommen. Das gilt natürlich auch für den Sozialhilfeträger, der darauf hinzuwirken hat, dass der Hilfesuchende sich um Arbeit bemüht und diese auch findet. Auch hier gibt es mehrere Möglichkeiten; eine kann z. B. darin bestehen, den Antragsteller lediglich zum Arbeitsamt zu schicken. Deshalb ist es nicht notwendig, auf einen Arbeitsvermittlungsservice zurückzugreifen. Setzt die Behörde aber auf diesen Dienst, dürfen die für eine Vermittlung erforderlichen Informationen dann auch nur mit der Einwilligung des Betroffenen weitergegeben werden.

  Das besagte Sozialamt versah seinen Einwilligungsvordruck dann noch mit dem Hinweis, dass mangelndes Bemühen um Arbeit zum Verlust des Hilfeanspruchs führen kann. So weit, so gut. Nun geschah es aber, dass aus für die Behörde „nicht mehr nachvollziehbaren Gründen“ zwei weitere Vordrucke für Einverständniserklärungen versendet wurden, diese aber nun plötzlich mit unzutreffenden Angaben zum Familienstand, zur zuletzt ausgeübten Tätigkeit, zum Beginn der Arbeitslosigkeit und zur Dauer des Hilfebezugs. Die Hilfeempfängerin mochte diese Erklärungen nicht unterzeichnen. Diese Weigerung konnte jedoch keine Sanktionen wie etwa eine Kürzung der Hilfeleistung zur Folge haben. Denn es bestand jedenfalls keine Obliegenheit der Hilfeempfängerin, die unrichtigen Angaben, die Teil der nachträglichen Einwilligungsvordrucke waren, zu unterschreiben. Die Abgabe einer solchen Erklärung konnte nicht

verlangt werden. Da die Akte der Bürgerin offensichtlich auch noch Unrichtigkeiten enthielt, hatte sie sogar einen entsprechenden Berichtigungsanspruch gegen die Kommune.

2.4 Ist der Kontakt zur Sozialbehörde ein Sozialdatum?

In einem Beschluss vom Sommer dieses Jahres kommt das Verwaltungsgericht Karlsruhe zu folgenden Feststellungen: „Gemäß § 67 Abs. 1 Satz 1 SGB X sind Sozialdaten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person, die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden. Der Kontakt zum Sozialamt, der sich aus der Tatsache der Abtretung ergibt, ist keine solche Angabe; gemeint sind vielmehr dem Kontakt zum Sozialamt vorgelagerte Tatsachen, die zur Prüfung des vom Betroffenen geltend gemachten Anspruchs erforderlich sind."

Um was ging es bei dieser Entscheidung? Um dies zu erklären, müssen wir zunächst ein Jahr zurückblättern. In unserem 23. Tätigkeitsbericht (LT-Drs. 13/1500, S. 48) vertraten wir die Ansicht, dass die vom Sozialamt übernommene Mietkaution nicht generell und ausschließlich nur an den Vermieter ausbezahlt werden darf. Dies folgt bereits aus der entsprechenden gesetzlichen Regelung (§ 15 a BSHG), wäre aber auch aus dem informationellen Selbstbestimmungsrecht des Einzelnen abzuleiten. Mit der Auszahlung des Betrags direkt an den Vermieter wird diesem nämlich unweigerlich der Kontakt des Bürgers zur Sozialbehörde offenbart.

Wird die Kaution nur als Darlehen gewährt und dann an den Hilfeempfänger ausbezahlt, tritt der gleiche Effekt ein, wenn das Sozialamt sich den Rückzahlungsanspruch (für die Kaution) gegen den Vermieter vom Hilfeempfänger abtreten lässt und dem Vermieter diese Abtretung anzeigt.

Über einen solchen Fall hatte das Verwaltungsgericht zu befinden. Es ging davon aus, dass die Abtretung des Rückzahlungsanspruchs für die Kaution an den Sozialleistungsträger das einzige Sicherungsmittel für das Darlehen sei. Um die Wirksamkeit der Abtretung sicherzustellen, sei es auch erforderlich, sie dem Vermieter anzuzeigen, damit dieser nicht nach Ablauf des Mietverhältnisses die Kautionssumme dennoch an seinen Mieter ausbezahlt. In diesem Fall wäre es ungewiss, ob das Sozialamt von dem Hilfeempfänger sein darlehensweise hingegebenes Geld wiedererhalten würde. Insbesondere könne es dem Leistungsträger verborgen bleiben, dass der Antragsteller das Mietverhältnis beende, sodass die Realisierung des Anspruchs auf Darlehensrückzahlung ohne die genannte Sicherung unsicher sei.

Wenn es sich tatsächlich so verhält, so ist folgende Argumentation aus der Sicht des Datenschutzes denkbar: Ist die Gewährung der Sozialleistung „Übernahme der Mietkaution als Darlehen" tatsächlich und vernünftigerweise nicht anders erfüllbar als durch Anzeige der Abtretung an den Vermieter, dann wäre die damit verbundene Übermittlung von Sozialdaten zur Aufgabenerfüllung auch erforderlich und könnte nach § 69 SGB X zulässig sein.

Abzulehnen sind aber die eingangs genannten Ausführungen des Verwaltungsgerichts. Abgesehen davon, dass nicht deutlich wird, welche „dem Kontakt zum Sozialamt vorgelagerte Tatsachen" hier gemeint sind, widerspricht diese Auslegung auch den Ausführungen des Bundesarbeitsgerichts in seiner so genannten Telefondatenerfassungsentscheidung. Auf dieses richtungweisende Urteil aus dem Jahr 1987 haben wir ebenfalls in unserem 23. Tätigkeitsbericht auf Seite 48 f. hingewiesen. Hier sei nochmals einer der Kernsätze dieser Entscheidung wiedergegeben: „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."

Nun geht es beim Sozialdatenschutz nicht wie in § 203 des Strafgesetzbuchs um anvertraute Geheimnisse aber die Aussage des Bundesarbeitsgerichts ist auch auf den Sozialdatenschutz übertragbar. Geschützt werden sollen hierdurch nämlich alle denkbaren Informationen, die sich auf den persönlichen oder sachlichen Bereich einer natürlichen Person beziehen. Richtet das Sozialamt eine Anfrage an einen Dritten, um die Voraussetzungen für eine Leistungsbewilligung zugunsten des Antragstellers zu klären, so teilt es gleichzeitig mit, dass der Antragsteller in Kontakt mit dem Sozialamt steht, selbst wenn er am Ende keine Leistung erhalten sollte. Für diese Mitteilung, die die Kehrseite der Identifizierung des Antragstellers ist, benötigt die Behörde selbstverständlich eine Übermittlungsbefugnis. Dies deshalb, weil bereits die – auch nur vorübergehende – Beziehung einer Person zu einem Leistungsträger ein schützenswertes Sozialdatum ist.

3. Aus der Praxis der Jugendämter

Wir haben zur Arbeit der Jugendämter aus datenschutzrechtlicher Sicht drei Fallgestaltungen ausgewählt, die nicht ganz alltägliche Situationen betreffen.

3.1 Informationen der Unterhaltsvorschusskasse an das Sozialamt über möglichen Leistungsmissbrauch

Ein Jugendamt, bei dem die Unterhaltsvorschusskasse als zuständige Behörde für Leistungen nach dem Unterhaltsvorschussgesetz eingerichtet ist, trug folgendes Problem an unsere Dienststelle heran: Die Unterhaltsvorschusskasse erbrachte Leistungen für ein minderjähriges Kind, das bei einem Elternteil lebte, von dem anderen Elternteil aber trotz bestehender Verpflichtung keinen Unterhalt erhielt. Der Unterhaltsanspruch war zusammen mit dem entsprechenden Auskunftsanspruch auf das Land übergegangen. Der Verpflichtete berief sich gegenüber dem Jugendamt auf seine Unfähigkeit zur Unterhaltsleistung; als Beleg führte er den Bezug laufender Hilfe zum Lebensunterhalt durch das Sozialamt an. Aus den vorgelegten Nachweisen ergab sich aber auch, dass jener Elternteil zusätzlich „erhebliche finanzielle Zuwendungen“ von seiner Mutter erhielt, die er dem Sozialamt jedoch verschwiegen hatte und die der Unterhaltsvorschusskasse als durchaus relevant für die Frage der Sozialhilfegewährung erschienen.

Das Jugendamt, das einen Leistungsmissbrauch zulasten des Sozialamts vermutete, fragte nun, ob es die Nachweise an das zuständige Sozialamt weitergeben dürfe. Dies haben wir bejaht.

Klar ist, dass es sich bei den Feststellungen der Unterhaltsvorschusskasse um Sozialdaten handelt. Denn obwohl diese öffentliche Stelle selbst kein Sozialleistungsträger oder eine gleichrangige Stelle ist, sind für sie doch die Bestimmungen des Sozialdatenschutzes einschlägig. Das Unterhaltsvorschussgesetz gilt als besonderer Teil des Sozialgesetzbuchs und die zuständige Behörde ist damit in den Regelungsbereich der sozialgesetzlichen Datenschutzbestimmungen einbezogen. Sie darf somit auch nur nach diesen Vorschriften Daten übermitteln; denn um eine Übermittlung handelt es sich zweifellos, selbst wenn Unterhaltsvorschusskasse und Sozialamt Organisationseinheiten desselben Landratsamts sind.

Eine solche Übermittlung ist auch zulässig, wenn sie für die Erfüllung der Aufgabe eines Sozialleistungsträgers, an den die Informationen weitergegeben werden sollen, erforderlich ist. Das war hier zu bejahen.

Leistungen der Sozialhilfe sind nämlich nachrangig, d. h. diese Hilfeleistungen sollen grundsätzlich diejenigen nicht erhalten, denen eine ausreichende Unterstützung schon von dritter Seite zuteil wird. Der Sozialhilfeträger hat die Aufgabe, den jeweiligen Leistungsbegehrenden auf die etwaige vorrangige Deckung seines Bedarfs durch Leistungen Dritter zu verweisen und damit den vom Gesetzgeber gewollten Nachrang wieder herzustellen. Das gilt auch dann, wenn auf die tatsächliche Unterstützung durch die Mutter kein Rechtsanspruch bestehen sollte.

Hinzu kommt, dass den Sozialbehörden die Aufgabe zufällt, die Voraussetzungen einer bereits bewilligten Leistung zu überprüfen, wenn ein konkreter Verdacht für einen Missbrauch vorliegt. Das ist selbstverständlich nicht anders, wenn die zuständige Behörde erst durch eine andere Stelle auf solche Umstände aufmerksam gemacht wird. Die übermittelnde Stelle muss sich also ein Stück weit in die Rolle des Datenempfängers hineinversetzen. Wäre das Sozialamt angesichts solcher Hinweise zumindest zu einer Anfrage beim Hilfeempfänger aufgerufen, so darf die Unterhaltsvorschusskasse diese Informationen auch mitteilen. Sind sie bei dem Empfänger ganz offensichtlich nicht bereits aktenkundig und damit für ihn auch nicht erkennbar, ist die Übermittlung auch erforderlich. Dabei ist allerdings zu beachten, dass nur die Daten zur Verfügung gestellt werden dürfen, die dem Zweck der Übermittlung dienen. Auf den Nachweisen etwa befindliche weitere Angaben, die in keinem Zusammenhang mit dem gehegten Verdacht stehen, diesen also nicht begründen, sind vor einer etwaigen Weitergabe der Nachweise somit unkenntlich zu machen.

3.2 Automatisierte Datenverarbeitung durch eine Beratungsstelle des Landkreises

Die EDV-technische Entwicklung der Landratsämter macht natürlich auch vor den Beratungsstellen der Landkreise nicht Halt. Das ist auch nicht zwingend notwendig, finden wir; nur sind bei der technischen Integration solcher Psychologischen Beratungsstellen oder Beratungsstellen für Eltern, Kinder und Jugendliche bestimmte Voraussetzungen zu beachten.

Bei einem Jugendhilfeträger war geplant, die in einer Beratungsstelle anfallenden Daten, somit auch die Angaben, die im Rahmen eines Beratungsgesprächs erhoben werden, auf dem zentralen Server des Landratsamts zu speichern. Damit unterliegt es nicht mehr der Kontrolle, der Aufsicht und dem Einfluss der Daten verarbeitenden Stelle selbst, wer z. B. aus der EDV-Abteilung der Gebietskörperschaft als Administrator auf die gespeicherten sensiblen Informationen zugreifen kann.

Hier ist zunächst zu beachten, dass die Umstände, die Mitarbeitern einer solchen Beratungsstelle im Verlauf eines Beratungsgesprächs anvertraut werden, einer besonderen Geheimhaltungspflicht unterliegen. Nach § 203 Abs. 1 des Strafgesetzbuchs (StGB) ist es nämlich Berufspsychologen, staatlich anerkannten Sozialarbeitern und Sozialpädagogen sowie Ehe-, Familien-, Erziehungs- und Jugendberatern einer anerkannten Beratungsstelle unter Strafandrohung verboten, unbefugt die ihnen anvertrauten Geheimnisse ihrer Klienten zu offenbaren. Die Möglichkeit eines nicht dienstlich gebotenen – lesenden – Zugriffs auf solche elektronisch gespeicherten personenbezogenen Daten kann bereits einen Verstoß gegen diese gesetzliche Schweigepflicht darstellen.

Hinzu kommt, dass medizinische Daten, aber auch z. B. Daten, die sich auf das Sexualleben beziehen, durch das Landesdatenschutzgesetz der Gruppe besonders sensibler Angaben zugerechnet werden, die nur unter restriktiven Bedingungen verarbeitet werden dürfen. Insbesondere sieht dieses Gesetz in seinem § 12 vor, dass in diesen Fällen durch die für den Einsatz oder die wesentliche Änderung des EDV-Verfahrens zuständige Stelle eine so genannte Vorabkontrolle durchzuführen ist. Anzuwenden ist diese Regelung, wenn die automatisierte Verarbeitung personenbezogener Daten mit besonderen Gefahren für das Persönlichkeitsrecht verbunden sein kann.

Unabhängig davon ist zu sagen, dass im Falle einer weiteren EDV-technischen Integration der Beratungsstelle jedenfalls im Anwendungsbereich von § 203 Abs. 1 StGB die Daten vor unberechtigten Zugriffen auch der Administratoren zu schützen sind. Ein solcher Schutz ist durch den Einsatz von Verschlüsselungsverfahren möglich. In Betracht kommt hierfür ein so genanntes LAN-Verschlüsselungsprodukt. Der Einsatz eines solchen Produkts erfordert eine Schlüsseladministration. Diese Aufgabe darf dann allerdings nicht von den EDV-Administratoren der Körperschaft wahrgenommen werden, da hiermit das ange-

strebte Ziel gerade nicht erreicht werden könnte. Diese Funktion sollte stattdessen einem Angehörigen der Beratungsstelle übertragen werden.

Sich darum zu bemühen, ist eine Aufgabe der Beratungsstelle. Denn: Verantwortlich für die Prüfung der Zulässigkeit ihrer Datenverarbeitung bleibt die Beratungsstelle selbst. Das gilt einmal für die Begrenzung der Zugriffsberechtigung innerhalb der Stelle, aber auch gegenüber den Administratoren der Körperschaft des Leistungsträgers.

3.3 Unterrichtung der Eltern über eine Inobhutnahme

Das Achte Buch des Sozialgesetzbuchs (SGB VIII) sieht als Aufgabe der Jugendhilfe auch die Inobhutnahme von Kindern und Jugendlichen vor. Der Gesetzgeber sieht darin die vorläufige Unterbringung des Kindes oder des Jugendlichen bei einer geeigneten Person, in einer Einrichtung oder einer sonstigen betreuten Wohnform (§ 42 SGB VIII). Die Geeignetheit der Unterbringung ist zwar nur bei der ersten Alternative gesetzlich vorgesehen, dessen ungeachtet müssen aber alle drei Stellen die Gewähr dafür bieten, dass sie nicht nur Verwahranstalten sind, sondern in ihnen auch sozialpädagogischen Zielen Rechnung getragen wird. So wird insbesondere eine Krisenintervention häufig angezeigt sein.

Bei der Verpflichtung des Jugendamts zur Inobhutnahme wird herkömmlicherweise zwischen den so genannten „Selbstmeldern“ und „Fremdmeldern“ unterschieden. Bitten Minderjährige selbst um Obhut, entsteht für das Jugendamt eine entsprechende Pflicht zum Tätigwerden, da eine Gefahr für das Wohl des Kindes oder des Jugendlichen unterstellt wird. Werden Minderjährige von anderen Stellen wie Polizei oder Schule oder von Dritten wie Verwandten oder Nachbarn dem Jugendamt zur Inobhutnahme angezeigt oder der Behörde „zugeführt“, ist das Jugendamt ebenfalls zur Tätigkeit verpflichtet, wenn eine dringende Gefahr für das Wohl des Kindes oder des Jugendlichen die Inobhutnahme erfordert.

Beiden Lebenssachverhalten ist gemein, dass das Jugendamt den Personensorge- oder Erziehungsberechtigten unverzüglich über die vorgenommene Maßnahme der Inobhutnahme zu unterrichten hat. Was diese Unverzüglichkeit der Benachrichtigung über den bloßen Vorgang der Inobhutnahme angeht, so kann es das Kindeswohl im Einzelfall erfordern, dass zunächst eine Abklärung der Situation der Benachrichtigung vorausgeht. Hierzu muss dem Jugendamt eine angemessene Zeit verbleiben, um die Sachlage zu prüfen. Das ist insbesondere angeraten, wenn gerade ein Konflikt mit den Personensorge- oder Erziehungsberechtigten die Meldung mit verursacht hat. Dies darf aber keineswegs dazu führen, dass auf die Benachrichtigung im Interesse oder auf Wunsch des Minderjährigen verzichtet wird.

Wie sieht aber der erforderliche Umfang einer solchen Benachrichtigung aus? Diese Frage stellte sich ein Jugendamt, das eine 16-Jährige in Obhut nahm. Die Minderjährige bat die Behörde, den Eltern nicht die Schwangerschaft ihrer Tochter mitzuteilen. In der Tat ist der gebotene Inhalt einer Benachrichtigung in diesem Fall nicht ganz einfach zu bestimmen. Zumindest muss sie die bloße Tatsache einer Inobhutnahme umfassen. Regelmäßig wird die Nachricht auch die Anschrift der Einrichtung zu enthalten haben, wenn nicht die besondere Situation gerade diese Information im Hinblick auf das Wohl des Kindes verbietet. Unstreitig können aber Angaben über die Gründe und Motive der Minderjährigen, die Inobhutnahme zu erbitten, z. B. eine Schwangerschaft, im Rahmen dieser Benachrichtigung unterbleiben.

4. Wer ist Adressat einer Arbeitgeberanfrage durch das Sozial- oder Jugendamt?

Es kommt nicht allzu oft vor, dass sich ein privates Unternehmen mit einem Verbesserungsvorschlag an uns wendet. So geschehen aber im abgelaufenen Berichtsjahr durch eine Firma mit ca. 80 Beschäftigten. Eine der Mitarbeiterinnen, dort für Personalangelegenheiten zuständig, ist immer

wieder mit Arbeitgeberanfragen durch Sozialbehörden befasst. Dies hat seinen Grund darin: Nach § 116 des Bundessozialhilfegesetzes ist der Arbeitgeber verpflichtet, dem Träger der Sozialhilfe über die Art und Dauer der Beschäftigung, die Arbeitsstätte und den Arbeitsverdienst des bei ihm beschäftigten Hilfesuchenden oder Hilfeempfängers, Unterhaltspflichtigen und deren nicht getrennt lebenden Ehegatten sowie Kostenersatzpflichtigen Auskunft zu geben, soweit die Durchführung des Gesetzes es erfordert. In ähnlicher Weise ist die Auskunftsverpflichtung gegenüber dem Jugendhilfeträger (§ 97 a Abs. 4 SGB VIII) sowie die Pflicht der Arbeitgeber gegenüber der nach dem Unterhaltsvorschussgesetz zuständigen Stelle (§ 6 Abs. 2 UnterhVG) formuliert.

Die Mitarbeiterin besagter Firma schlug nun vor, dass die Sozialbehörden doch ihre Anfragen mit dem Zusatz „Personalabteilung“ versehen mögen. Schließlich sei diese Abteilung auch die einzige Stelle im Haus, die diese Anfragen behandeln könne. Werden sie jedoch nur an die Firma geschickt, sei eine unbefugte Kenntnisnahme innerhalb der Firma nicht auszuschließen. Dem konnten wir nur zustimmen.

Wenden sich die öffentlichen Stellen mit ihrem Auskunftsbegehren an einen privaten Arbeitgeber, so werden bei diesem Vorgang zwangsläufig Sozialdaten des Betroffenen an den Empfänger der Anfrage übermittelt. So kann der Arbeitgeber aus der behördlichen Anfrage z. B. schließen, dass ein bestimmter Beschäftigter selber Leistungsempfänger ist oder einem solchen gegenüber unterhaltspflichtig ist. Gelangen die Daten dergestalt in den Privatrechtsverkehr, ist die nicht-öffentliche Stelle zunächst einmal darauf hinzuweisen, dass sie die Daten in demselben Umfang geheim zu halten hat wie der Leistungsträger selbst und sie auch nur zu dem Zweck verwenden darf, zu dem sie ihr übermittelt wurden (§ 78 Abs. 2 SGB X). Der Datenempfänger hat diese Hinweise an die mit den Daten befassten Mitarbeiter weiterzugeben.

Aus ihrer Pflicht zur Datensicherung folgt für die Behörde aber auch im Rahmen einer Datenweitergabe die Aufgabe, die Risiken einer unbefugten Offenbarung von sensiblen Daten zu minimieren; dies verlangt z. B. einen gesicherten Datentransport. Diese „Nachsorge“ für das Datenmaterial muss somit auch bis zur zuständigen Stelle beim Empfänger reichen. Sozialdaten, die ausschließlich die Personalstelle eines Arbeitgebers betreffen und die mit dem entsprechenden Zusatz „Personalsache“ oder „Personalstelle“ von dem allgemeinen Postlauf ausgenommen werden können, sind damit an diese allein zuständige Organisationseinheit beim Arbeitgeber zu richten.

5. Einwilligung in Auskünfte der Behörde an Dritte?

Ob eine solche anzunehmen war, beschäftigte uns in einem Fall aus dem Leistungsbereich der Kriegsopferfürsorge. Nach der Darstellung der Behörde hatte die Leistungsempfängerin dort die Übernahme von Umzugskosten beantragt und zu diesem Zweck den Kostenvoranschlag eines Spediteurs vorgelegt. Das für die Leistungsbearbeitung zuständige Sozialamt war jedoch nur bereit, einen Teil der Summe zu bewilligen, und lehnte den Antrag im Übrigen ab. Die Bürgerin erteilte dem Spediteur den Auftrag demnach, beglich jedoch nicht dessen Rechnungen.

Der Unternehmer wiederum bevollmächtigte einen Rechtsanwalt mit der Wahrnehmung seiner Interessen. Der anwaltliche Vertreter nahm dann Kontakt mit der Behörde auf. Ihm sei im Wesentlichen Folgendes bestätigt worden: Ein entsprechender Vorgang ist dem Sozialamt bekannt, der Antrag wurde jedoch nur zum Teil bewilligt, die unbeglichenen Forderungen sind bei der Auftraggeberin geltend zu machen. Die Bürgerin war damit aber nicht einverstanden, insbesondere monierte sie die Auskunftserteilung per Telefon und die fehlende Einwilligung in die Datenweitergabe. Hierin konnten wir ihr leider nicht beipflichten.

Die Antragstellerin hatte die Firma zur Erfüllung der Forderungen schriftlich direkt und ausschließlich an die Behörde verwiesen und unter Angabe der dortigen Telefonnummer die Kommune als zuständig zur Begleichung des Anspruchs erklärt. Sie teilte dem Spediteur darüber hinaus mit, sie habe die Rechnungen umgehend weitergeleitet und um unverzügliche Erledigung

gebeten. Zudem hatte die Antragstellerin angeboten, auch die Forderung eventueller Verzugszinsen unverzüglich an die Behörde weiterzugeben.

Wer in dieser Form jegliche eigene Verantwortlichkeit für den eingeleiteten Vorgang bestreitet, muss damit rechnen, dass sich der Forderungsinhaber zur Klärung des Sachverhalts mit der angegebenen Stelle in Verbindung setzt und diese auch die notwendigen Auskünfte erteilt. Wird der Eindruck erweckt, man ist nur Bote oder Briefkasten für den allein zuständigen Ansprechpartner Sozialamt, ist an dem Vorliegen einer Einwilligung mit der Kontaktaufnahme nicht zu zweifeln. Da sich der Bevollmächtigte unter Berufung auf den ihm vorliegenden Schriftwechsel gegenüber dem Sozialamt außerdem durch Sachverhaltskenntnis ausgewiesen hatte, durften die erforderlichen Auskünfte auch telefonisch erteilt werden.

4. Teil: Kommunales und anderes

1. Abschnitt: Kommunales

1. Datenschutz nach Kassenlage

Mit der letzten Novellierung des Landesdatenschutzgesetzes im Jahr 2000 wurde auch für die öffentlichen Stellen im Lande etwas geregelt, was andernorts schon längst selbstverständlich war: Erstmals wurde in allgemeiner Form die Bestellung örtlicher Datenschutzbeauftragter vorgesehen. Dass dies nur auf freiwilliger Basis erfolgen sollte, hatte bereits mein Vorgänger mehrfach beklagt. An dieser Kritik halte auch ich fest. Ich möchte hier zwar nicht erneut in eine grundsätzliche Diskussion dieses Themas einsteigen. Für geboten halte ich es allerdings, die Entwicklungen nicht aus dem Auge zu verlieren und – wenn nötig – deutlich anzusprechen, wenn solche Entwicklungen aus Sicht des Datenschutzes in die falsche Richtung gehen.

Zunächst das Positive: Die unbestreitbaren Vorteile einer Datenschutzfachperson vor Ort haben offensichtlich viele überzeugt. Auch wenn keine genauen Zahlen vorliegen, so gibt doch die bei meiner Dienststelle eingehende wachsende Zahl von Anfragen zu Aus- und Fortbildungsmöglichkeiten durch neu bestellte behördliche Datenschutzbeauftragte einen deutlichen Hinweis darauf, dass sich ein Bewusstseinswandel vollzogen hat. Als Indiz hierfür sehe ich auch den Umstand, dass speziell für behördliche Datenschutzbeauftragte angebotene Grundlagenseminare aufgrund des enormen Andrangs kapazitätsmäßig ausgeweitet werden mussten. In persönlichen Gesprächen war festzustellen, dass die Betroffenen mit zum Teil großem Engagement an ihre neue Herausforderung herangehen. Zu hoffen bleibt, dass sie hierin von ihrer jeweiligen Dienststellenleitung nicht nur nicht gebremst, sondern vielmehr ausdrücklich unterstützt werden.

Dieses insgesamt eher positive Bild wird deutlich dadurch getrübt, dass sich gerade diejenigen, denen insoweit eine Vorbildfunktion zukommt, mehr oder weniger deutlich in Zurückhaltung üben. Zu denken ist hier konkret an die großen Städte im Land.

Konnte sich die Landeshauptstadt Stuttgart erst nach einem quälenden Prozess dazu durchringen, eine entsprechende Funktion einzurichten, gab es von anderen Städten Absagen (Karlsruhe, Ulm) oder hinhaltende Stellungnahmen (Baden-Baden, Mannheim). Nachzulesen ist dies in meinem 23. Tätigkeitsbericht (LT-Drs. 13/1500, S. 50). Weshalb erwähne ich dies nochmals? Nun, Anlass hierzu gibt mir ein neues Schreiben des Oberbürgermeisters der Stadt Mannheim. Darin wird auf die schwierige Haushaltslage der Stadt hingewiesen und schlicht festgestellt, diese lasse die Bestellung eines behördlichen Datenschutzbeauftragten nicht zu. Im Ergebnis macht dieses Schreiben wieder einmal deutlich, welcher Stellenwert dem Datenschutz in bestimmten Bereichen der Verwaltung eingeräumt wird: Datenschutz ist gut und wichtig, aber er darf nichts kosten! Natürlich sehe ich die finanziellen Probleme der Städte und Gemeinden. Selbstverständlich zwingen diese dazu, Prioritäten zu setzen. Aber weshalb muss dabei der Datenschutz häufig das erste Opfer sein? Liegt es vielleicht daran, dass die freiheitssichernde Bedeutung des Datenschutzes verkannt wird? Dass man die Aufgaben des Datenschutzes ernst nehme, wie die Städte unisono versichern, hört man gerne. Indes, dies zeigt die Erfahrung, lässt sich ein wirksamer Datenschutz nur dann hinreichend sicher gewährleisten, wenn eine konkrete Person, mit klaren Kompetenzen, den notwendigen Fachkenntnissen und der Unterstützung der Behördenleitung ausgestattet, hierfür zuständig ist. Nicht zuletzt die anlässlich einer Reihe von Kontrollen durch meine Dienststelle festgestellten Mängel im Umgang mit den verwalteten personenbezogenen Daten belegen dies nachdrücklich.

2. Besonderheiten bei der Baurechtsbehörde der Stadt Freiburg

Offensichtlich ganz nah am Bürger wollte sich die Stadt Freiburg präsentieren und hatte zu diesem Zweck auch die Verfahren bei der Baurechtsbehörde für die örtlichen Bürgervereine geöffnet. Aber vielleicht hat sie sich damit in Einzelfällen sogar von dem einen oder anderen Bürger ein

Stück weit entfernt. Ich sah jedenfalls Anlass, diese Freiburger Spezialität zu beanstanden.

Auf folgende Praxis war ich bei der Baurechtsbehörde der Stadt gestoßen: Das städtische Bauordnungsamt unterrichtete die örtlichen Bürgervereine der jeweiligen Stadtteile über alle beabsichtigten Bauvorhaben, indem es ihnen die entsprechenden Flurstücksnummern sowie die Straße (mit Hausnummer) mitteilte und in einer Beschreibung das geplante Bauvorhaben vorstellte. Diese Vorgehensweise praktizierte die Stadt bei allen Bauanträgen im Sinne der Landesbauordnung, bei Vorhaben im Kenntnisgabeverfahren nach der Landesbauordnung sowie bei Bauvoranfragen.

Dabei erhielt der Bürgerverein des von dem Bauvorhaben betroffenen Stadtteils jeweils eine schriftliche Mitteilung mit den genannten Fakten. Bei weiterem Informationsbedarf konnte sich der Verein zusätzlich an das Bauordnungsamt wenden, um dort einen Plansatz einzusehen, außerdem ein „Informationsgespräch“ mit der Amtsleitung führen. Die schriftlichen Mitteilungen der Stadt erfolgten an die jeweiligen Vereinsvorsitzenden. Die Einsichtnahme der Pläne war auf Personen begrenzt, die zuvor vom Bürgerverein gegenüber der Behörde namentlich benannt wurden. Die Bürgervereine hatten dann die Möglichkeit, eine Stellungnahme gegenüber der Stadt abzugeben, mit der sie Bedenken und Anregungen vorbringen konnten. In einer mir vorliegenden Stellungnahme ist etwa von einem Bürgerverein ein Vorhaben abgelehnt worden. Die Stadt teilte mit, dass sich die benachrichtigten Bürgervereine in vielen Fällen nicht geäußert hätten. Eingegangene Äußerungen wurden dann zu den jeweiligen Bauakten genommen.

Dass die Behörde damit personenbezogene Daten weitergab, war klar. Es war den Vereinen nicht zuletzt aufgrund ihrer Verankerung in den jeweiligen Stadtteilen leicht möglich, aufgrund der mitgelieferten Angaben auf die jeweiligen Personen der Bauherren zu schließen und diese somit zu identifizieren. Im Übrigen musste spätestens die Einsichtnahme in einen Plansatz regelmäßig zur Bekanntgabe des Namens des Bauherrn führen. Da es sich bei den geschilderten Vorgängen zweifellos um Datenübermittlungen handelte, bedurfte es hierfür einer Rechtsgrundlage. Da die Landesbauordnung zwar eine Angrenzerbenachrichtigung, aber eben nicht die geschilderte Form der Beteiligung von Vereinen vorsieht, konnte die Datenweitergabe nur auf der Grundlage der allgemeinen Regelungen des Landesdatenschutzgesetzes erfolgt sein. Die Beteiligung der Bürgervereine ist für die Aufgabenerfüllung der Baurechtsbehörde nicht erforderlich. Deshalb kann der Eingriff in das informationelle Selbstbestimmungsrecht des jeweiligen Bauherrn nur gerechtfertigt sein, wenn die Vereine, an die die Daten übermittelt wurden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegen konnten und der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hatte (§ 18 Abs. 1 Nr. 2 LDSG).

Wir vermochten bereits kein berechtigtes Interesse der Bürgervereine an der Kenntnis der übermittelten Daten auszumachen. Zwar wurde von Seiten der Stadt vorgebracht, dass die Unterstützung von Vereinstätigkeit öffentlichen Interessen entspreche und die Verfolgung solcher öffentlicher Interessen wiederum ein berechtigtes Interesse sei. Dieser Argumentation vermochten wir nicht zu folgen. Die Unterrichtung der Vereine erfolgte hier gerade nicht zur Förderung der Vereinstätigkeit, sondern offensichtlich wohl deshalb, um die dortige Meinungsbildung frühzeitig in die baurechtlichen Verfahren einfließen zu lassen. Im Ergebnis erhielt die Baurechtsbehörde eine Rückmeldung darüber, ob ein Bauvorhaben von Teilen der Bürgerschaft als unbeachtlich eingestuft, mitgetragen oder gar abgelehnt wurde. Deshalb sprach die Stadt wohlweislich auch von einer „Beteiligung der Bürgervereine“ und einer „vertrauensvollen Zusammenarbeit“, hingegen nicht von einer Unterstützung der Vereinstätigkeit. Die gewählte Verfahrensweise sollte der Erkenntnisgewinnung für die rechtliche Beurteilung von Bauvorhaben dienen. Diese Aufgabe der baurechtlichen Beurteilung ist jedoch gesetzlich der Baurechtsbehörde zugewiesen, die sie auch ohne Beteiligung der Bürgervereine zu erfüllen vermag. Auch über die Bestimmungen des Landesdatenschutzgesetzes konnten die Bürgervereine daher nicht als beratende Gremien in das Verwaltungsverfahren einbezogen werden. Die geschilderte Praxis war somit unzulässig.

In der Folge hatte die Stadt die kritisierte Vorgehensweise zunächst ausgesetzt und hat sie inzwischen gänzlich eingestellt.

3. Bürgermeisterwahlen und Datenschutz

3.1 Herausgabe von Adressen

Gleich mehrere Bürger einer Gemeinde haben sich unabhängig voneinander in derselben Sache an uns gewandt. Sie waren vor der Bürgermeisterwahl von einem der Bewerber angeschrieben und um ihre Stimme gebeten worden. Die Betroffenen wollten von uns wissen, wie der Bürgermeisterkandidat an ihre Adressen gekommen ist und ob die undichte Stelle womöglich bei der Gemeindeverwaltung liegt.

Der zur Stellungnahme aufgeforderte Bürgermeister teilte uns mit, ein Mitarbeiter habe die Adressen von Jungwählern und Senioren versehentlich aus dem Melderegister an den Ortsverein einer Partei herausgegeben. Er wolle diese Panne zwar nicht beschönigen, aber auch „zuständigen Stellen“ sei die in Baden-Württemberg geltende Rechtslage nicht bekannt gewesen.

Mit dieser Bemerkung kann der Bürgermeister weder das Innenministerium des Landes, das sowohl für das Einwohnermeldewesen als auch für den Bereich Kommunalwahlen zuständig ist, noch unsere Dienststelle gemeint haben. Wir stimmen nämlich darin überein, dass der eindeutige Wortlaut des § 34 Abs. 1 des Meldegesetzes die Herausgabe der Daten von Wahlberechtigten vor Bürgermeisterwahlen nicht zulässt. Nach dieser Vorschrift darf die Meldebehörde Parteien und anderen Trägern von Wahlvorschlägen im Zusammenhang mit allgemeinen Wahlen zu parlamentarischen und kommunalen Vertretungskörperschaften, allgemeinen Abstimmungen, Volks- und Bürgerbegehren in den sechs vorangehenden Monaten Auskunft aus dem Melderegister über Familiennamen, Vornamen, Doktorgrad und Anschriften von Gruppen von Wahl- oder Stimmberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist, soweit diese nicht widersprochen haben. Diese gesetzliche Bestimmung, in der die Bürgermeisterwahlen nicht aufgeführt sind, hat jedenfalls hinsichtlich der Herausgabe von Adressen für Zwecke der Wahlwerbung abschließenden Charakter. Im Übrigen gibt es bei Bürgermeisterwahlen weder eine Partei als Wahlvorschlagsträger noch einen anderen Wahlvorschlagsträger. Vielmehr reicht jede Person, die das Amt des Bürgermeisters anstrebt, ihre Bewerbung selbst ein.

Dass die Gemeinde trotz dieser klaren rechtlichen Regelung einer Partei vor der Bürgermeisterwahl Adressdaten aus dem Melderegister zur Verfügung gestellt hat, habe ich beanstandet. Gleichzeitig habe ich den Bürgermeister gebeten, die Rechtslage künftig zu beachten.

3.2 Die unzulässige Speicherung im Melderegister

Eine Petentin äußerte die Vermutung, anlässlich der Oberbürgermeisterwahl in einer Großen Kreisstadt sei zusammen mit den Daten der Unterstützer der Name des jeweiligen Kandidaten festgehalten worden. Die Petentin fragte uns, ob diese Vorgehensweise der Stadt datenschutzrechtlich in Ordnung ist.

Die Vermutung der Petentin sollte sich als zutreffend herausstellen. Die Stadt hat bestätigt, dass sie in ihrem Melderegister bei den betroffenen Wahlberechtigten vorübergehend gespeichert hatte, welchen Bewerber diese unterstützt haben. Wir haben den Sachverhalt datenschutzrechtlich wie folgt beurteilt:

Nach dem Kommunalwahlrecht muss in Gemeinden mit mehr als 20 000 Einwohnern jeder Bewerber mit Ausnahme des Amtsinhabers eine bestimmte Anzahl von Unterstützungsunterschriften beibringen, um zur Bürgermeisterwahl zugelassen zu werden. Ein Wahlberechtigter darf nur eine Bewerbung durch seine Unterschrift unterstützen. Unterzeichnet jemand mehr als eine Bewerbung, sind alle seine Unterschriften ungültig. Es begegnet deshalb keinen Bedenken, dass das mit der

Wahlvorbereitung beauftragte Wahlamt die Unterstützerdaten vorübergehend elektronisch gespeichert und in diese Datei zum Erkennen von Mehrfachunterschriften auch ein Kennzeichen für die jeweilige Bewerbung aufgenommen hat. Selbstverständlich war es auch erforderlich und damit datenschutzrechtlich zulässig, dass die Stadt ihr Bürgeramt, bei dem das Melderegister geführt wird, mit der Prüfung der Wahlberechtigung der Unterzeichner betraut hat. Zu diesem Zweck hätte es aber ausgereicht, wenn das Wahlamt dem Bürgeramt die Daten der Unterzeichner zur Verfügung gestellt hätte. Die Prüfung der Wahlberechtigung ist nämlich unabhängig davon, welche Bewerbung der einzelne Unterzeichner unterstützt. Aufgrund des Ergebnisses der vom Bürgeramt vorgenommenen Überprüfung der Wahlberechtigung der Unterzeichner wäre es dem Wahlamt mit Hilfe seiner elektronischen Datei ohne weiteres möglich gewesen, Mehrfachunterschriften festzustellen und entsprechend den kommunalwahlrechtlichen Vorschriften zu behandeln. Unzulässig war auch die Speicherung der Tatsache der Unterzeichnung und der unterstützten Bewerbung im Melderegister. § 4 des Meldegesetzes regelt abschließend, welche Daten im Melderegister gespeichert werden dürfen. In diesem Datenkatalog sind Unterstützer- und Bewerberdaten für Wahlen nicht aufgeführt.

Ich habe die Stadt gebeten, meine Hinweise bei künftigen Wahlen zu beachten. Von einer förmlichen Beanstandung habe ich im Hinblick darauf abgesehen, dass die Daten unverzüglich nach der Wahl gelöscht worden sind.

4. Datenschutzrechtliche Probleme beim Fremdenverkehr

Private Zimmervermieter in einer kleinen Fremdenverkehrsgemeinde wandten sich mit folgendem Anliegen an uns:

Die örtliche Tourist-Information GmbH, eine Eigengesellschaft der Gemeinde, biete einen Vordrucksatz an, der aus dem melderechtlich vorgeschriebenen „Meldeschein der Beherbergungsstätten“ (so genannter Hotelmeldeschein) und einem weiteren „Meldeschein“ bestehe, welcher der Erhebung der Kurtaxe diene. Die Petenten halten die formularmäßige Verknüpfung der beiden genannten Rechtsbereiche für datenschutzrechtlich bedenklich. Insbesondere bemängeln sie, dass der Hotelmeldeschein, der eigentlich beim Zimmervermieter aufbewahrt werden sollte, der GmbH zuzuleiten ist.

Ferner wenden sich die Petenten gegen die Aufforderung der GmbH an die Vermieter, für Zwecke der Zimmervermittlung einen 10-seitigen Fragebogen auszufüllen.

Die von uns eingeholten Stellungnahmen der Gemeinde und der GmbH und unsere rechtliche Prüfung haben zu folgenden Ergebnissen geführt:

4.1 Kurtaxe und Hotelmeldepflicht

Es hat sich herausgestellt, dass die GmbH tatsächlich einen Durchschreibesatz anbietet, der den melderechtlichen Bereich abdeckt und zugleich der Erhebung der Kurtaxe dient. Dagegen bestehen aus datenschutzrechtlicher Sicht keine grundsätzlichen Vorbehalte. Es muss aber sichergestellt sein, dass auf jedem Vordruck nur diejenigen Daten erfragt werden, die zur Erfüllung der jeweiligen Aufgabe benötigt werden. Das wurde hinsichtlich des Hotelmeldescheins im vorliegenden Fall ohne Einschränkung beachtet. Dieser Teil des Vordrucksatzes entsprach in vollem Umfang dem vom Innenministerium als Verordnungsgeber vorgeschriebenen amtlichen Muster. Ein paar Haare in der Suppe fanden wir dagegen in dem Kurtaxevordruck. Dieses Formular stimmte zwar mit dem von der Gemeinde herausgegebenen Vordruck überein. Dennoch mussten wir verschiedene Fragen, z. B. nach dem Grad der Behinderung des Gastes und ob dieser auf Geschäftsreise ist, bemängeln. Die Kenntnis dieser Daten ist nämlich – jedenfalls nach der Kurtaxesatzung dieser Gemeinde – nicht erforderlich, um die Kurtaxe festzusetzen. Außerdem haben wir moniert, dass auf diesem Vordruck neben den Rechtsgrundlagen für die Kurtaxeerhebung auch die melde-

rechtlichen Vorschriften angegeben waren. Letztere sind nur für den Hotelmeldeschein einschlägig; auf dem Kurtaxevordruck haben sie nichts verloren.

Ferner haben wir festgestellt, dass die nach dem Kommunalabgabengesetz grundsätzlich zulässige Beauftragung eines Dritten nicht wie im Gesetz vorgeschrieben in der gemeindlichen Kurtaxesatzung verankert war. Ohne eine solche Satzungsbestimmung hätte die Gemeinde die GmbH nicht beauftragen dürfen, bei der Erhebung der Kurtaxe mitzuwirken. In diesem Zusammenhang haben wir die Gemeinde auch auf die Vorschriften des Landesdatenschutzgesetzes über die Datenverarbeitung im Auftrag hingewiesen.

Von einer förmlichen Beanstandung der erwähnten Datenschutzverstöße habe ich abgesehen, weil die Gemeinde zugesagt hat, ihre Kurtaxesatzung unverzüglich anzupassen und den Kurtaxevordruck zu ändern.

Unberechtigt war der Vorwurf der Petenten, die GmbH verlange von den Vermietern, ihr auch die Hotelmeldescheine zuzuleiten. Auf dem Hotelmeldeschein wird im Gegenteil deutlich darauf hingewiesen, dass dieser Vordruck beim Zimmervermieter verbleibt. Dieser Hinweis entspricht der einschlägigen Vorschrift des Meldegesetzes, wonach die ausgefüllten Meldescheine von der Beherbergungsstätte aufzuwahren, vor unbefugter Einsichtnahme zu sichern und bestimmten Behörden, unter anderem dem Polizeivollzugsdienst, auf Verlangen zur Einsichtnahme vorzulegen sind; Letzterem sind sie auf Verlangen auch zu übermitteln. Es obliegt demnach den Vermietern selbst sicherzustellen, dass die Hotelmeldescheine nicht in die Hände von Unbefugten gelangen. Darauf haben wir die Petenten hingewiesen.

4.2 Umfrage bei den Zimmervermietern

Die Tourist-Information GmbH hatte den Vermietern von Fremdenzimmern und Ferienwohnungen einen umfangreichen Fragebogen zugeleitet mit der Bitte, diesen ausgefüllt bis zu einem bestimmten Termin zurückzugeben. Die Fragen bezogen sich auf die Lage, Art, Ausstattung, Preiskategorie usw. des Hauses und der Zimmer. Die Angaben sollten die GmbH in die Lage versetzen, die Zimmer und Ferienwohnungen an Gäste zu vermitteln. Als Rechtsgrundlage für die Datenerhebung nannte uns die GmbH die Kurtaxesatzung der Gemeinde. Letzteres hat sich zwar als unzutreffend herausgestellt, weil diese Satzung, wie im Kommunalabgabengesetz vorgeschrieben, sich auf Regelungen zur Erhebung der Kurtaxe beschränkt. Das Landesdatenschutzgesetz enthält allerdings eine ausreichende Rechtsgrundlage, um bei den Vermietern Daten über die von der GmbH zu vermittelnden Zimmer zu erheben. Nach diesem Gesetz ist nämlich das Erheben personenbezogener Daten zulässig, wenn deren Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Das Landesdatenschutzgesetz schreibt aber zusätzlich vor, dass den Betroffenen gegenüber die beabsichtigte Datenverarbeitung und der Zweck der Verarbeitung sowie bei einer beabsichtigten Übermittlung auch die Empfänger der Daten oder Gruppen von Empfängern anzugeben sind, soweit die Betroffenen nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen müssen. Ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen (wie hier für die Vermittlung von Zimmern durch die GmbH), sind die Betroffenen hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen. Die GmbH hat sich mit einer „Bitte“ an die Zimmervermieter gewandt, als sie diesen die Fragebögen zusandte. Sie hat damit den Empfängern gegenüber hinreichend deutlich gemacht, dass sie nicht verpflichtet sind, die Vordrucke auszufüllen. Dennoch haben wir die GmbH gebeten, die Betroffenen zur Vermeidung von Missverständnissen künftig in vergleichbaren Fällen umfassend im oben genannten Sinne zu informieren.

5. Behandlung von Bürgereingaben durch Behörden

Immer wieder werden uns Fälle bekannt, in denen Behörden Schreiben von Bürgern unzulässigerweise an Unternehmen, Privatpersonen oder an andere Behörden weitergeben, wie die beiden folgenden Beispiele zeigen:

5.1 Weitergabe an den Arbeitgeber

Ein Mitarbeiter eines weltbekannten schwäbischen Unternehmens nahm einen Zeitungsartikel zum Anlass, sich per E-Mail an den Bürgermeister einer baden-württembergischen Kleinstadt zu wenden. Mit nicht sehr schmeichelhaften Worten und viel Ironie kommentierte der Absender die von der Presse wiedergegebenen Sorgen des Bürgermeisters um die künftige Nutzung eines ehemaligen Militärgeländes. Darüber war der Bürgermeister naturgemäß nicht sehr erfreut. Kurzerhand schickte er die E-Mail an das Unternehmen mit der Frage, ob es bei dieser Firma üblich sei, Briefe solchen Inhalts unter dem Firmennamen zu versenden. Diese Reaktion des Bürgermeisters hatte offenbar nachteilige arbeitsrechtliche und sonstige Folgen für den Mitarbeiter. Er wollte von uns wissen, ob der Bürgermeister befugt war, seinen Arbeitgeber über die E-Mail zu informieren.

Der von uns zu einer Stellungnahme aufgeforderte Bürgermeister rechtfertigte die Weitergabe der E-Mail an das Unternehmen damit, dass er davon ausgegangen sei, der Absender habe ihn im Auftrag des Unternehmens angeschrieben.

Datenschutzrechtlich stellt sich der Sachverhalt wie folgt dar: Wäre die E-Mail, wovon der Bürgermeister ausgeht, dem Unternehmen zuzurechnen, wäre die Sache datenschutzrechtlich unproblematisch. In diesem Fall hätte der Bürgermeister nicht einen Dritten, sondern den Absender selbst über dessen eigene E-Mail informiert. Eine solche Handlungsweise könnte man zwar als unnötig, vielleicht sogar als unsinnig ansehen, sie wäre aber datenschutzrechtlich unbedenklich gewesen. Wir mussten dem Bürgermeister aber mitteilen, dass wir die Sache anders sehen als er. Die E-Mail-Adresse enthielt zwar neben dem Namen des Mitarbeiters auch den Namen des Unternehmens. Der Inhalt der E-Mail und vor allem die ausdrückliche Bitte des Absenders, der Bürgermeister möge eine etwaige Antwort an seine Tochter richten, sprachen aber eindeutig für eine private Eingabe. Diese Eingabe, die zahlreiche personenbezogene Daten des Petenten enthielt, hätte der Bürgermeister, nachdem der Betroffene nicht eingewilligt hatte, nach der einschlägigen Vorschrift des Landesdatenschutzgesetzes nur an das Unternehmen weitergeben dürfen, wenn es zur Erfüllung der Aufgaben der Stadt erforderlich gewesen wäre oder das Unternehmen (vorher) ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt hätte. Diese datenschutzrechtlichen Voraussetzungen für eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs lagen hier nicht vor. Wir brauchten deshalb nicht zu prüfen, ob der Mitarbeiter als Betroffener ein schutzwürdiges Interesse am Ausschluss der Datenübermittlung gehabt hätte.

Diese datenschutzrechtliche Beurteilung ist unabhängig davon, ob der Arbeitgeber seinen Beschäftigten den privaten E-Mail-Versand ausdrücklich erlaubt, diesen stillschweigend geduldet oder untersagt hatte.

Der Bürgermeister hat letztlich akzeptiert, dass in seinem Vorgehen ein Datenschutzverstoß zu sehen ist, und zugesagt, die datenschutzrechtlichen Vorschriften künftig zu beachten. Von einer förmlichen Beanstandung konnte ich deshalb absehen.

5.2 Datenaustausch zwischen Behörden

Ein Gemeinderatsmitglied hatte den Verlauf einer Gemeinderatssitzung zum Anlass genommen, zwei Rechtsfragen an das Landratsamt zu richten. Unter anderem hatte er dort angefragt, ob die Wiederholung einer Abstimmung zu einem bestimmten Tagesordnungspunkt rechtens ist. Nachdem das Landratsamt die Fragen des Petenten bereits beantwortet hatte, fiel ihm ein, dass es den Brief des Gemeinderatsmitglieds der Ge-

meinde überlassen und von dieser eine Stellungnahme anfordern könnte. Schließlich ließ der Bürgermeister den an das Landratsamt gerichteten Brief des Gemeinderatsmitglieds während einer Gemeinderatssitzung an die Wand projizieren und informierte das Gremium über die Rechtsauffassung des Landratsamts.

Der Petent wollte von uns wissen, ob das Landratsamt befugt war, seinen Brief an die Gemeinde weiterzugeben, und ob der Bürgermeister sein Schreiben im Rahmen einer Gemeinderatssitzung öffentlich machen durfte. Nach Anhörung der beteiligten Behörden beurteilten wir den Sachverhalt datenschutzrechtlich wie folgt:

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Sie dürfen nach dem Landesdatenschutzgesetz an andere Behörden nur übermittelt werden, wenn es zur Aufgabenerfüllung erforderlich ist. Allein die Tatsache, dass sich der Petent in einer bestimmten Angelegenheit an das Landratsamt gewandt hatte, stellt schon ein personenbezogenes Datum dar. Das Landratsamt hätte die von dem Petenten gestellten Rechtsfragen auch ohne Anhörung der Gemeinde beantworten können, was es zunächst auch getan hatte. Das Landratsamt hätte seine Antwort mit dem Hinweis verbinden können, dass es eine Stellungnahme der Gemeinde zu dem Sachverhalt nicht eingeholt hat. Datenschutzrechtlich unbedenklich wäre auch gewesen, wenn das Landratsamt der Gemeinde den Sachverhalt mit eigenen Worten ohne Personenbezug geschildert hätte. Schließlich hätte es den Petenten auch fragen können, ob er in die Weitergabe seines Schreibens an die Gemeinde einwilligt. Jedenfalls war es zur Aufgabenerfüllung weder des Landratsamts noch der Gemeinde erforderlich, der Gemeinde das vollständige Schreiben des Petenten zuzuleiten.

Der Bürgermeister durfte den Gemeinderat über die Rechtsauffassung des Landratsamts informieren, weil die strittigen Fragen in der Zukunft immer wieder auftreten könnten. Es war aber zur Aufgabenerfüllung des Gemeinderats nicht erforderlich, dass der Bürgermeister ihm den vollständigen Wortlaut des an das Landratsamt gerichteten Schreibens des Petenten offenbart hat.

Wir haben beide Behörden gebeten, die aufgezeigte Rechtslage künftig in vergleichbaren Fällen zu beachten.

6. Adressen von Grundstückskäufern

Durch eine Bürgereingabe wurden wir auf folgenden Fall aufmerksam gemacht: Der Petent und seine Ehefrau hatten in einer Großen Kreisstadt ein Baugrundstück erworben. Die Käufer wunderten sich darüber, als sie kurz darauf von einer Privatperson Post erhielten. Die Absenderin wollte nämlich wissen, ob das Ehepaar Kinder hat und ob es beabsichtigt, diese in dem Neubaugebiet den Kindergarten besuchen zu lassen. Als Hintergrund dieser Anfrage nannte uns der Petent städtische Überlegungen, den Kindergarten in jenem Gebiet zu schließen. Das Schreiben sollte offenbar dazu dienen, Mitstreiter für den Erhalt des Kindergartens zu finden. Nicht dass der Petent gegen diese Initiative in der Sache etwas einzuwenden hätte. Er fragte aber zuerst sich und dann auch uns, wie die Absenderin wohl an seine Adresse und an die Daten anderer Grundstückskäufer gekommen ist.

Wir wollten der Sache auf den Grund gehen und forderten eine Stellungnahme der Stadt an. Diese teilte uns zunächst mit, dass das Baurechts- und Bauverwaltungsamt eine Liste mit den Adressen von mehr als zehn Grundstückserwerbern an eine städtische Angestellte herausgegeben hatte. Die Angestellte hatte die Daten nicht in dienstlicher Eigenschaft, sondern als Privatperson, und zwar als ehrenamtliches Mitglied des Elternbeirats des erwähnten städtischen Kindergartens angefordert. Da uns im Gegensatz zur Stadt nicht das Ersuchen dieser Person, sondern die Herausgabe der personenbezogenen Daten durch das Baurechts- und Bauverwaltungsamt rechtlich fragwürdig erschien, hakten wir nach. Dabei stellte sich heraus, dass die künftigen „Häuslebauer“ ihre Bauplätze von der Stadt erworben hatten. Das Baurechts- und Bauverwaltungsamt hatte offenbar einfach die Daten

seiner Vertragspartner – neben deren Adressen auch die Flurstücksnummern – aus den Kaufverträgen entnommen und dem Elternbeiratsmitglied zur Verfügung gestellt.

Wir haben diese Handlungsweise der Stadt datenschutzrechtlich wie folgt beurteilt: Nach dem Landesdatenschutzgesetz hätte die Stadt die personenbezogenen Daten nur herausgeben dürfen, wenn es zur Erfüllung der städtischen Aufgaben erforderlich gewesen wäre oder das Elternbeiratsmitglied ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft dargelegt und die betroffenen Grundstückskäufer kein schutzwürdiges Interesse am Ausschluss der Datenübermittlung gehabt hätten. Die erste Alternative scheidet hier von vornherein aus, weil es auf der Hand liegt, dass die Datenübermittlung nicht zur Erfüllung von Aufgaben des Baurechts- und Bauverwaltungsamts erforderlich war. Die Datenempfängerin mag zwar in ihrer Eigenschaft als Elternbeiratsmitglied möglicherweise ein berechtigtes Interesse an der Kenntnis der Daten gehabt haben. Das Baurechts- und Bauverwaltungsamt hätte aber nicht unterstellen dürfen, dass die betroffenen Grundstückskäufer kein schutzwürdiges Interesse am Ausschluss der Datenübermittlung haben. Die Betroffenen konnten und mussten beim Vertragsabschluss mit der Stadt nämlich nicht damit rechnen, dass ihre Daten für private Zwecke verwendet werden. Das Amt, das nach dem Landesdatenschutzgesetz als übermittelnde Stelle die Verantwortung für die Zulässigkeit der Datenübermittlung trug, hätte demnach die Adressen ohne Einwilligung der Grundstückskäufer nicht herausgeben dürfen.

Der Vollständigkeit halber weisen wir darauf hin, dass auch entsprechende personenbezogene Auskünfte aus der Kaufpreissammlung, welche die bei den Gemeinden gebildeten Gutachterausschüsse nach dem Baugesetzbuch zu führen haben, unzulässig gewesen wären.

Ich habe den Datenschutzverstoß gegenüber dem Oberbürgermeister beanstandet und ihn gebeten, für die künftige Beachtung der datenschutzrechtlichen Vorschriften innerhalb der Stadtverwaltung zu sorgen.

7. Tücken bei der Postzustellung

Eine Bürgerin wandte sich mit folgendem Fall an uns: Ein Landratsamt habe ihr einen Bußgeldbescheid förmlich zugestellt. Die Postzustellungsurkunde, die dem Absender der Postsendung nach erfolgter Zustellung von der Post zugeschickt wird, ging jedoch nie beim Landratsamt ein. Da das Landratsamt ohne Postzustellungsurkunde nicht nachweisen kann, dass der Bußgeldbescheid formgerecht zugestellt worden ist, erkundigte sich das Landratsamt über den Verbleib der Postzustellungsurkunde. Im Betreff der an die Post gerichteten Anfrage gab das Landratsamt an, dass es in dem zugestellten Schreiben um ein Bußgeldverfahren gegen die Adressatin des Schreibens gegangen war. Eine Information, die die Post für die Nachforschungen nach dem Verbleib der Postzustellungsurkunde nicht benötigte.

Diese Mitteilung stellt eine Übermittlung personenbezogener Daten an eine öffentliche Stelle dar, denn die Deutsche Post AG gilt nach dem Bundesdatenschutzgesetz als öffentliche Stelle des Bundes. Eine solche Übermittlung ist jedoch nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Eine Einwilligung der Betroffenen lag nicht vor. Eine bereichsspezifische Übermittlungsbefugnis besteht ebenfalls nicht. Auch auf die Übermittlungsregelungen des Landesdatenschutzgesetzes kann die Information der Post über den Betreff des zugestellten Schreibens nicht gestützt werden. Denn diese Regelungen setzen voraus, dass die Übermittlung der Daten zur Aufgabenerfüllung der übermittelnden Stelle oder der Stelle, an die die Daten übermittelt werden, erforderlich ist. Im Anschreiben an die Post anzugeben, dass das zugestellte Schreiben ein Bußgeldverfahren gegen die Adressatin betraf, war daher unzulässig.

Wir forderten das Landratsamt auf, unsere Rechtsauffassung künftig zu beachten.

8. Videoüberwachung

An die zunehmende Überwachung von Gebäuden und öffentlichen Plätzen durch Videokameras hat man sich mittlerweile – leider – schon gewöhnt (s. auch die Ausführungen zur polizeilichen Videoüberwachung im 2. Teil, 1. Abschnitt, Nr. 2). Beklagenswerte Folge ist, dass man sich auf Seiten der Anwender solcher Techniken häufig kaum mehr Gedanken darüber macht, ob die rechtlichen Voraussetzungen für solche Videoeinsätze überhaupt vorliegen. Die Hemmschwelle sinkt, auch wenn die Gerichte immer wieder darauf hinweisen, dass die Überwachung mittels bildgebender Verfahren, bei der die äußere Erscheinung und das Verhalten der erfassten Personen in ihrer Gesamtheit registriert werden, in schwerwiegender Weise in das Grundrecht auf Datenschutz der Betroffenen eingreift und deshalb nur in engen Grenzen akzeptiert werden kann. Findet Videoüberwachung statt, können die Betroffenen diesen Eingriff in ihr Persönlichkeitsrecht oft nicht vermeiden, etwa wenn sie bestimmte Einrichtungen aufsuchen möchten oder sogar müssen, die sich innerhalb des überwachten Bereichs befinden. Die Videoüberwachung ist deshalb nur in engen Grenzen zulässig und setzt insbesondere voraus, dass Gründe des Allgemeinwohls die Videoüberwachung erfordern, die so gewichtig sind, dass sie die schutzwürdigen Interessen der Betroffenen überwiegen. Nur unter strengen Voraussetzungen können die mit der Videoüberwachung verbundenen Eingriffe in das Persönlichkeitsrecht einer Vielzahl von meist rechtstreuen Bürgern gerechtfertigt sein.

Ihr mit Steuermitteln finanziertes Eigentum vor Diebstahl oder mutwilliger Zerstörung zu schützen, gehört durchaus zu den Aufgaben jeder Behörde. Das Erheben personenbezogener Daten zu diesem Zweck ist deshalb nicht von vornherein unzulässig. Auch die Wahrung ihres Hausrechts kann Maßnahmen, die Datenverarbeitungen beinhalten, legitimieren. Werden begangene Straftaten als Grund für die künftige Überwachung von Dienstgebäuden mit Videoanlagen angegeben, muss deren Erforderlichkeit allerdings belegt werden können, etwa durch die Vielzahl oder die Schwere der begangenen Straftaten in dem zur Überwachung vorgesehenen Bereich. Außerdem muss dargetan werden, dass Alternativen zur Videoüberwachung (zum Beispiel Kontrollgänge durch Personal) nicht zum gleichen Ergebnis führen. Schließlich bedarf es einer besonderen Rechtfertigung, wenn statt der bloßen Beobachtung mittels Bildübertragung (so genanntes Kamera-Monitor-Prinzip) eine Videoüberwachung in der Form der Bildaufzeichnung erfolgen soll. Nur wenn die Behörde im Rahmen einer umfassenden Güter- und Interessenabwägung zum Ergebnis gelangt, dass die Videoüberwachung erforderlich ist, darf sie letztlich zu diesem Mittel greifen. Dabei muss sie auch regelmäßig prüfen, ob die Überwachung noch erforderlich ist.

Außer mit der polizeilichen Videoüberwachung haben wir uns im Berichtszeitraum mit drei weiteren Fällen einer Videoüberwachung befassen müssen. Wegen des Sachzusammenhangs schildern wir als dritten Fall einen Vorgang aus dem Universitätsbereich, der begrifflich natürlich nicht dem Abschnitt „Kommunales“ zuzurechnen ist.

8.1 Der Dieb im Umkleideraum

Anfang November, also erst kurz vor Drucklegung dieses Tätigkeitsberichts, haben wir durch die Presse erfahren, dass die Stadt Freiburg in einem ihrer Hallenbäder, und zwar in den Sammelumkleideräumen, Videokameras in Betrieb genommen hat. Weitere städtische Bäder sollten entsprechend ausgestattet werden. Vorausgegangen waren offenbar zahlreiche Aufbrüche von Kleiderschränken, die sich in den Umkleideräumen befinden. Die Überwachung soll dazu dienen, derartige Sachbeschädigungen an städtischem Eigentum und Diebstähle zulasten der Badbesucher künftig zu verhindern oder strafrechtlich zu verfolgen.

Vor allem die Tatsache, dass so sensible Bereiche wie Umkleideräume Gegenstand der Videoüberwachung sein sollen, veranlasste uns, der Sache unverzüglich auf den Grund zu gehen. Die behördliche Datenschutzbeauftragte der Stadt bestätigte bei einer ersten Kontaktaufnahme den von der Presse dargestellten Sachverhalt. Unsere Intervention führte

erfreulicherweise dazu, dass die Stadt die Kameras bis zur rechtlichen Klärung sofort abgeschaltet hat. Zu diesem Schritt dürfte unsere vorläufige Einschätzung beigetragen haben, dass die Videoüberwachung von Bereichen wie Umkleide-, Dusch- und Toilettenräumen, durch die die Intimsphäre der Betroffenen tangiert wird, grundsätzlich nicht als eine verhältnismäßige und datenschutzrechtlich zulässige Maßnahme angesehen werden kann.

Inzwischen liegt uns die Stellungnahme der behördlichen Datenschutzbeauftragten der Stadt Freiburg vor. Demnach ist es in den fünf Hallenbädern der Stadt in den letzten Jahren vermehrt zu Aufbrüchen von Kleiderschränken und zu Diebstählen zulasten der betroffenen Badbesucher gekommen. In Einzelfällen wurden sogar mit Hilfe entwendeter Schlüssel Kraftfahrzeuge der Badbesucher gestohlen. In einem der Hallenbäder entstand in den ersten zehn Monaten dieses Jahres durch die Beschädigung von über 100 Kleiderschränken allein der Stadt ein Schaden von 40.000 Euro. Das Schul- und Sportamt der Stadt sah keine andere Möglichkeit, als durch Videoüberwachung das städtische und private Eigentum zu schützen. Zunächst wurden in den acht Herren-Sammelumkleideräumen des am schlimmsten heimgesuchten Bades, in denen sich auch Kleiderschränke befinden, jeweils zwei Videokameras installiert und in Betrieb genommen. Die Kameras erfassten nicht nur den Schrank-, sondern auch den Umkleidebereich. Somit verblieben als „videofreie Zonen“ in jeder Sammelumkleide nur zwei abgetrennte und abschließbare Einzelkabinen. Die Besucher wurden auf die Video- bzw. auf die Nicht-Videoüberwachung durch entsprechende Schilder hingewiesen. Die Aufnahmen konnten durch das Badpersonal nicht laufend beobachtet werden. Vielmehr sollten die Bilder aufgezeichnet, drei Tage lang gespeichert und nur insoweit ausgewertet werden, als es zur Aufklärung eines festgestellten Schrankaufbruchs notwendig ist. Nur der Betriebsleiter des Bades wäre gemeinsam mit der Polizei hierzu befugt gewesen.

Die behördliche Datenschutzbeauftragte, die im Vorfeld stadtintern nicht eingeschaltet worden war, hat uns mitgeteilt, dass sie die Videoüberwachung im Umkleidebereich aus Rechtsgründen nicht für zulässig hält. Sie schlägt folgende Maßnahmen vor: Der Umkleidebereich einerseits und der Schrankbereich andererseits sollen räumlich strikt voneinander getrennt werden. In den Räumen, die künftig ausschließlich dem Umkleiden dienen, werden die Kameras abgebaut. In den anderen Räumen, in denen die Kleiderschränke untergebracht sind, werden nach Entfernung der Sitzbänke die Kameras wieder eingeschaltet, natürlich mit einem deutlichen Hinweis auf die Videoüberwachung.

Wir beurteilen die Sache, die auf ein erhebliches öffentliches Interesse gestoßen ist, datenschutzrechtlich wie folgt: Wie bereits im Vorspann dargelegt, kann es zwar durchaus zu den Aufgaben einer öffentlichen Stelle gehören, ihr Eigentum gegebenenfalls auch mit Hilfe der Videoüberwachung zu schützen. Grundvoraussetzung für eine solch einschneidende Maßnahme, die in die Persönlichkeitsrechte der Betroffenen eingreift, ist aber, dass im Rahmen einer nach dem Landesdatenschutzgesetz vorgeschriebenen Vorabkontrolle geprüft worden ist, ob mildere Mittel (hier zum Beispiel regelmäßige – oder noch besser: unregelmäßige – Kontrollgänge durch das Personal) zur Verfügung stehen, die zu demselben Erfolg führen. Im vorliegenden Fall ist diese Vorabkontrolle, bei der die behördliche Datenschutzbeauftragte und gegebenenfalls auch der Landesbeauftragte für den Datenschutz zu beteiligen gewesen wäre, vor dem Beginn der Überwachungsmaßnahmen unterblieben. In Übereinstimmung mit der städtischen Datenschutzbeauftragten sind wir der Auffassung, dass eine Vorabkontrolle zu einem negativen Ergebnis hätte führen müssen. Denn es liegt auf der Hand, dass durch die Videoüberwachung von Personen beim Umkleiden deren Intimsphäre in nicht hinnehmbarer Weise berührt wird. Die Stadt hätte deshalb im Rahmen der gebotenen Güter- und Interessenabwägung den schutzwürdigen Interessen der Badbesucher Vorrang einräumen und von der unverhältnismäßigen Maßnahme einer Videoüberwachung in den Umkleideräumen absehen müssen.

Das habe ich der Stadt Freiburg mitgeteilt. Von einer förmlichen Beanstandung habe ich nur deshalb Abstand genommen, weil die Überwachung, nachdem ich mich eingeschaltet hatte, sofort eingestellt worden ist. Ich habe die Stadt außerdem wissen lassen, dass die von der behördlichen Datenschutzbeauftragten vorgeschlagenen Maßnahmen (insbesondere räumliche Trennung zwischen Umkleide- und Schrankbereich, wobei nur noch Letzterer videoüberwacht werden soll) unter der Voraussetzung akzeptabel erscheinen, dass eine Vorabkontrolle zum Ergebnis kommt, auf die Videoüberwachung könne mangels geeigneter Alternativen nicht völlig verzichtet werden.

8.2 Der Dieb im Krankenhaus

Im Städtischen Krankenhaus Sindelfingen ist es in der Vergangenheit offenbar wiederholt zu Diebstählen aus Patientenzimmern gekommen. Die Krankenhausverwaltung wollte das Problem durch eine Videoüberwachung in den Griff bekommen: Jeder, der den Eingangsbereich des Krankenhauses durchquert, sollte vorsorglich erst einmal auf Band aufgenommen werden. Die Bänder sollten dann nach acht Tagen wieder gelöscht werden. Auf unsere Frage, wie man denn Diebstähle dadurch verhindern wolle, dass die Besucher beim Betreten und Verlassen des Krankenhauses gefilmt werden, räumte man ein, dass sich Diebstähle zwar nicht verhindern ließen. Man könne aber unter Umständen, wenn man eine Täterbeschreibung besitze, anhand der Videoaufnahmen prüfen, ob darauf eine Person festgehalten sei, auf die die Beschreibung zutreffe.

Nun ist es so, dass das Anfertigen von Videobildern, um mit deren Hilfe Straftäter zu ermitteln, Strafverfolgungszwecken dient. Die Strafverfolgung gehört aber zu den Aufgaben, die der Polizei, nicht aber dem Krankenhaus zugewiesen sind. Allein zu diesem Zweck darf das Krankenhaus deshalb die Videokameras nicht einsetzen. Allerdings beruft sich das Krankenhaus darauf, die Videoüberwachung solle auch potenzielle Diebe abschrecken. Dieser Zweck der Gefahrenvorsorge kann zwar gerade noch als eine Ausprägung des Hausrechts akzeptiert werden, sodass die Zulässigkeit der Videoüberwachung nicht schon daran scheitern muss, dass das Krankenhaus damit eine ihm generell nicht zustehende Aufgabe erfüllen will. Im konkreten Fall ist die Aufstellung von Videokameras im Eingangsbereich allerdings völlig ungeeignet, um diesen Zweck zu erreichen. Denn zum einen kann nach allgemeiner Lebenserfahrung jedenfalls nicht ausgeschlossen werden, dass ein Teil der Diebstähle im Krankenhaus auf Personal des Krankenhauses selbst zurückzuführen ist. Diese Personen benutzen aber in der Regel den Personaleingang. Zum anderen ist die Wahrscheinlichkeit, dass ein Dieb, der selbstverständlich darauf achtet, bei seiner Tat nicht beobachtet zu werden, dann doch auf dem Videoband entdeckt wird, so gering, dass er sich durch eine Videoüberwachung des Eingangs kaum von seiner Tat wird abhalten lassen. Schließlich kann man sich, bei entsprechendem Verhalten, ohnehin so an den Videokameras vorbeibewegen, dass eine nachträgliche Identifizierung ausgeschlossen ist. Mit anderen Worten: Dem Krankenhaus haben wir vorgehalten, dass die Videoüberwachung des Eingangsbereichs das selbst gesteckte Ziel niemals erreichen könnte und schon deshalb unzulässig wäre. Davon abgesehen wäre sie auch unverhältnismäßig. Denn durch die Videoüberwachung werden unterschiedslos alle Personen erfasst, die sich im Eingangsbereich des Krankenhauses aufhalten. Auf ein störendes Verhalten kommt es nicht an. Nach der Rechtsprechung ist unter diesen Voraussetzungen ein Eingriff in das Recht auf informationelle Selbstbestimmung nur zulässig, wenn ein „hinreichender Zurechnungszusammenhang zwischen der zu verhindernden Gefahr und den betroffenen Personen besteht“. Dies ist hier nicht der Fall. Denn die Diebstähle, die mit der Videoüberwachung verhindert werden sollen, finden gerade nicht im überwachten Bereich statt. Eine Videoüberwachung darf allenfalls an solchen Orten stattfinden, an denen Straftaten zu erwarten sind. Dies wären hier die Patientenzimmer. Deren Überwachung hat das Krankenhaus jedoch mit der zutreffenden Begründung ausgeschlossen, damit zu sehr in die Privatsphäre der Patienten einzugreifen.

Aufgrund unserer Einwendungen hat das Städtische Krankenhaus Sindelfingen mittlerweile davon abgesehen, Überwachungskameras zu installieren.

8.3 Der Dieb in der Universitätsbibliothek

Seit April 2002 werden in der Bibliothek der Universität Konstanz insgesamt drei Bereiche mit einer Videoanlage überwacht, nämlich der Hauptein- und -ausgang, der so genannte „PC-Pool Rechtswissenschaft“ und die Wessenberg-Bibliothek.

Die Universität Konstanz hält seit April 2001 ihre Bibliothek an fast allen Tagen im Jahr rund um die Uhr für Studierende und Mitarbeiter, darüber hinaus aber auch für jedermann geöffnet. Dieser Service einer 24-Stunden-Bibliothek hat wohl bislang bei den Professoren, Studierenden und der Öffentlichkeit eine durchweg positive Resonanz erzeugt. Die Schattenseite dieser Konzeption lag nach Mitteilung der Universität darin, dass während des Nachtbetriebs sowie an Sonn- und Feiertagen die Räume von einem einzigen Wachmann, der seinen Arbeitsplatz nicht verlassen kann, nicht hinlänglich überwacht werden können. Bereits im Tagesbetrieb soll es hin und wieder zu Störungen, Verstößen gegen die Benutzungsordnung bis hin zu strafbaren Vorfällen (z. B. Beschädigung oder Diebstahl von Büchern, Diebstahl von PCs oder von deren Komponenten, Missbrauch bei der Nutzung von Internet-Diensten und körperliche Übergriffe auf Bibliotheksbenutzer) gekommen sein.

Bei der von der Videoüberwachung ebenfalls erfassten Wessenberg-Bibliothek handelt es sich im Gegensatz zu den anderen videoüberwachten Bereichen um einen abgeschlossenen und für die Öffentlichkeit nicht zugänglichen Raum, in welchem sich ein antiquarischer Buchbestand von mehr als 30 000 Bänden befindet. Diesen Buchbestand hatte die Stadt Konstanz der Universität als Dauerleihgabe überlassen. Im Zuge der Übergabeverhandlungen zwischen der Stadt und der Universität war die Videoüberwachung vereinbart worden, um eine zusätzliche Sicherung des wertvollen antiquarischen Buchbestands zu erzielen.

Die Universität hatte uns – leider erst einige Monate nach Beginn der Videoüberwachung – im Rahmen einer so genannten Vorabkontrolle nach dem Landesdatenschutzgesetz um Prüfung und Zustimmung gebeten.

Die Prüfung führte zu dem Ergebnis, dass die Videoüberwachung der Wessenberg-Bibliothek dem Datenschutzrecht nicht entspricht. Denn diese Videoüberwachung ist zur Erreichung des angestrebten Sicherungszwecks nicht erforderlich. Der grundsätzlich verschlossene Raum kann ohnehin nur von Personen betreten werden, die den Zahlencode für die Tür kennen. Die Abholung der Bände zur Einsichtnahme oder zur Ausleihe erfolgt ausschließlich durch hierzu befugte Bibliotheksmitarbeiter. Welchen Schutz darüber hinaus die Videoüberwachung noch bringen kann oder soll, ist nicht nachvollziehbar. Daher hat die Universität mitgeteilt, dass sie im Rahmen anstehender Verhandlungen mit der Stadt Konstanz darauf hinwirken werde, dass eine andere (technische) zusätzliche Sicherung eingerichtet und auf die Videoüberwachung verzichtet wird.

Die Videoüberwachung der öffentlich zugänglichen Bereiche kann jedenfalls dann in Betracht kommen, wenn etwa in der Vergangenheit wiederholt körperliche Übergriffe auf Benutzerinnen und Benutzer der Bibliothek erfolgt sind. Aber auch dann ist noch zu prüfen, ob der erwünschte Schutz nicht durch andere Maßnahmen erreicht werden kann, welche die Privatsphäre der Betroffenen weniger beeinträchtigen. Die von der Universität ursprünglich überlassenen Unterlagen ließen nicht erkennen, ob und mit welchem Ergebnis Alternativen zur Videoüberwachung in Betracht gezogen worden waren. Mittlerweile hat die Universität hierzu weitere Informationen vorgelegt. Gleichwohl müssen noch einige nach wie vor offene Punkte ausgeräumt werden, bevor die

datenschutzrechtliche Zulässigkeit der Videoüberwachung abschließend beurteilt werden kann.

2. Abschnitt: Personalwesen

Das Spektrum der Fragen des Personaldatenschutzes, mit denen wir uns im Berichtszeitraum befassten, erstreckte sich erneut von der Verarbeitung personenbezogener Daten in herkömmlichen Akten bis zur elektronischen Datenverarbeitung und erfasste komplexe Fragestellungen wie auch Selbstverständlichkeiten. Dass Letztere keineswegs stets umgesetzt werden, mussten wir erneut feststellen. Während im vorangegangenen Tätigkeitsbericht etwa die „Entsorgung“ von Sozialakten in öffentlich zugänglichen Altpapiertonnen zu bemängeln war, geht es diesmal zum Beispiel um Probleme im Zusammenhang mit einem Stellenbesetzungsverfahren. Wieder einmal hat sich gezeigt, wie wichtig es ist, dass die Behörden stets auch das kleine Einmaleins des Datenschutzes im Blick behalten.

1. NSI und noch kein Ende

Im Berichtszeitraum befassten wir uns erneut mit datenschutzrechtlichen Fragen bei den Neuen Steuerungsinstrumenten (NSI).

Unter anderem nahmen wir gegenüber dem Finanzministerium zum Datenschutzkonzept Anwendungsdaten NSI, das bisher Sicherheitskonzept Anwendungsdaten NSI hieß, sowie zum Konzept zur kostenorientierten Zeit- und Mengenerfassung Stellung, die uns jeweils in mehreren Versionen vorgelegt wurden. Nachfolgend seien nur einzelne Punkte angesprochen:

– Nach dem Sicherheitskonzept Anwendungsdaten NSI sind für die Zeiterfassung unter anderem für die Identifikation der Erfassungsperson verschiedene Stammdaten erforderlich. Personenbezogene Daten sind nach dem Konzept der Name, der Vorname, das Geburtsdatum und die Soll-Arbeitszeit des Beschäftigten sowie eine „Ident.-Nummer“.

  Auf unsere Mitteilung, dass nicht ersichtlich sei, wozu zusätzlich zu der „Ident.-Nummer“ das Geburtsdatum benötigt werde, erklärte das Finanzministerium, das Geburtsdatum sei ein Pflichtfeld des eingesetzten Programms. Es könne ohne aufwändige Programmierung nicht geändert und insofern aus wirtschaftlichen Gründen nicht entfernt werden. Die datenschutzrechtlichen Aspekte (Datenvermeidung/Datensparsamkeit) seien bekannt. Aus diesem Grund könne das Feld mit einem „Dummy-Geburtsdatum“ versehen werden. Die Ressorts würden entsprechend unterrichtet. Sollte eine Dienststelle die Notwendigkeit des echten Geburtsdatums feststellen, könne jedoch auch dieses verwendet werden. Die Ausführungen im Konzept wurden dahin gehend ergänzt, dass das Geburtsdatum mit dem Zusatz „(anwendungsbedingter Dummy)“ versehen wurde.

  Dies erweckt den Eindruck, als wollte das Finanzministerium sich alle Optionen erhalten: Einerseits bemühte es das Pflichtfeld-Argument und fügte im Konzept dem Geburtsdatum den Zusatz „(anwendungsbedingter Dummy)“ bei, was letztlich bedeutet, dass in das Datenfeld Geburtsdatum ausschließlich ein „Dummy-Geburtsdatum“ einzufügen ist. Andererseits setzte es sich dazu in Widerspruch, wenn es erklärte, dass es auch möglich sein solle, das echte Geburtsdatum zu verwenden, wenn eine Dienststelle die Notwendigkeit dazu feststelle. Das Konzept und die Stellungnahme passten daher nicht zusammen.

  Vor diesem Hintergrund hätte es uns nicht mehr überraschen dürfen, dass wir bei einem Kontrollbesuch – von dem noch die Rede sein wird – feststellen mussten, dass eine Reihe von Dienststellen die tatsächlichen Geburtsdaten ihrer Beschäftigten in das Pflichtfeld eingegeben hatten, jedoch nicht dartun konnten, dass dies erforderlich war. Zur Begründung wurde beispielsweise erklärt, das tatsächliche Geburtsdatum sei entsprechend „der Bezeichnung des Feldes“ oder gemäß der der Dienststelle „eingeräumten Wahlmöglichkeit“ erfasst worden.

Ein solches (nicht erforderliches) Verarbeiten der tatsächlichen Geburtsdaten war rechtswidrig. In Anbetracht der datenschutzrechtlichen Verantwortung der Dienststellen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten hätten diese prüfen müssen, ob es auch vor dem Hintergrund des das Datenschutzrecht prägenden Erforderlichkeitsgrundsatzes zulässig war, die tatsächlichen Geburtsdaten der Beschäftigten zu verarbeiten. Der Verweis auf eine eingeräumte „Wahlmöglichkeit“ erweckt den Eindruck, die Dienststelle sei davon ausgegangen, sie dürfe beliebig wählen, ob sie das tatsächliche Geburtsdatum oder ein „Dummy-Geburtsdatum“ verwende, sie dürfe also personenbezogene Daten auch dann verarbeiten, wenn dies nicht notwendig ist. Die Annahme einer solchen Wahlmöglichkeit verkennt jedoch die Rechtslage.

– Das Konzept zur kostenorientierten Zeit- und Mengenerfassung (KZM) – mit deren Hilfe sollen im Rahmen der Kosten- und Leistungsrechnung bestimmten Produkten Personalkosten verursachungsgerecht zugeordnet werden, um die (Personal-)Kosten dieser Produkte zu ermitteln – sieht unter anderem eine „Vollständigkeitsprüfung“ vor. Diese soll erfolgen, wenn die Beschäftigten ihre den jeweiligen Produkten zugeordneten tatsächlichen Arbeitsstunden, die sie tagesgenau erfasst haben, am Monatsende freigegeben haben. Die mit der „Vollständigkeitsprüfung“ Beauftragten sollen prüfen, ob alle Beschäftigten, die an der Zeiterfassung teilnehmen, ihre Daten in das System eingegeben haben. Hierfür wird, so das Konzept, ein Bericht bereitgestellt, „aus dem ersichtlich ist, wenn einzelne Mitarbeiter/innen keine oder signifikant zu wenige/zu viele Stunden erfasst haben“. Signifikant soll eine Abweichung regelmäßig dann sein, wenn sie mindestens 25 vom Hundert der Soll-Arbeitszeit des Beschäftigten beträgt; dies soll jedoch behördenindividuell variiert werden können. Der bereitgestellte Bericht enthält die entsprechenden Daten (unter anderem Name sowie Soll- und Ist-Arbeitszeit) aller Beschäftigten, die an der Zeiterfassung teilnehmen, wobei die Daten der Beschäftigten mit signifikanten Abweichungen optisch hervorgehoben sind. Für den im Konzept genannten Zweck reicht es jedoch aus, ausschließlich die Daten derjenigen Beschäftigten anzuzeigen, die (keine oder) signifikant zu wenige/zu viele Stunden erfasst haben. Eine Anzeige der Daten der anderen Beschäftigten ist dazu nicht erforderlich.

  Das Finanzministerium führte dazu auf unsere Nachfrage aus, bei dem Bericht zur Vollständigkeitsprüfung handle es sich um einen Standardbericht des eingesetzten Programms. Dieser zeige dem für die Vollständigkeitsprüfung Zuständigen Soll- und Ist-Arbeitszeit der zu prüfenden Beschäftigten. Auf Vollständigkeit prüfen bedeute auch, alle Mitarbeiter auf schlichte Teilnahme an der KZM zu überprüfen.

  Welche Zielrichtung dem letztgenannten Vortrag zugedacht war, konnten wir nicht feststellen. Ein Grund dafür, die Daten aller Beschäftigten anzuzeigen, ist diesem jedenfalls nicht zu entnehmen, denn bei Beschäftigten, die zwar verpflichtet sind, an der KZM teilzunehmen, jedoch gleichwohl keine Arbeitsstunden eingeben, läge eine signifikante Abweichung vor, die ohnehin angezeigt würde. Das Finanzministerium brachte sein ursprüngliches Argument in einer weiteren Stellungnahme nicht mehr vor.

  Am Standardbericht-Argument hielt das Finanzministerium allerdings fest und führte dazu noch aus, eine Änderung dieses Berichts verursache einen erheblichen zusätzlichen Programmier- und Kostenaufwand und erfordere die Vergabe neuer Berechtigungsrollen.

  Dazu ist ebenso wie zum oben angesprochenen Pflichtfeld-Argument auf § 9 LDSG hinzuweisen: Die Gestaltung und Auswahl der technischen Einrichtungen und der Verfahren zur automatisierten Verarbeitung personenbezogener Daten hat sich an dem Grundsatz auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu verarbeiten. Es sind die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften des Landesdatenschutzgesetzes entsprechende Datenverarbeitung zu gewährleisten. Erforderlich in diesem Sinne sind Maßnahmen, wenn ihr Aufwand, insbesondere unter

Berücksichtigung der Art der zu schützenden personenbezogenen Daten, in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Auch wenn die Auswahl des Verfahrens zur Verarbeitung personenbezogener Daten im Rahmen des Projekts NSI bereits erfolgt ist, besteht (weiterhin) die Pflicht, die Gestaltung dieses Verfahrens an den Grundsätzen der Datenvermeidung und Datensparsamkeit auszurichten. Inwieweit dies hinsichtlich des Standardberichts oder des Pflichtfelds der Fall ist, lassen die bisherigen Angaben des Finanzministeriums, die weder den Aufwand der Programmierung beziffern noch etwaige sonstige Wirtschaftlichkeitserwägungen enthalten, nicht erkennen.

Soweit zu ausgewählten Punkten aus den Konzepten. Nachdem mit der kostenorientierten Zeit- und Mengenerfassung (KZM/CATS) die Stufe 2 des Projekts NSI gestartet wurde, wollten sich meine Mitarbeiter so bald wie möglich in einer Pilotdienststelle, die CATS einsetzt, ein Bild von der datenschutzrechtlichen Ausgestaltung der Anwendung machen. Bei der Kontrolle von CATS wurden unter anderem folgende datenschutzrechtliche Mängel des Systems festgestellt:

– Unzureichende Passwortlänge

  Wenn man das CATS-Programm aufruft, muss man eine Benutzerkennung und ein Passwort eingeben, um das Programm bedienen zu können. Schon beim Datenschutzkonzept der Anwendung IS-PS hatten wir darauf hingewiesen, dass die Länge eines Passworts, wie neuerdings vom Bundesamt für Sicherheit in der Informationstechnik empfohlen, acht Zeichen nicht unterschreiten sollte. Diese Empfehlung wäre uneingeschränkt auf das Teilsystem CATS übertragbar gewesen. Bedauerlicherweise mussten meine Mitarbeiter feststellen, dass die Einstellungen so vorgenommen wurden, dass vier Zeichen für ein Passwort ausreichten.

– Unberechtigter Zugriff auf alle Benutzer von CATS

  Ein Einstiegsdialog bei CATS erlaubte die Eingabe des Nachnamens, um auf das Arbeitszeitblatt des Benutzers zu gelangen. Allerdings ist es nicht notwendig, den ganzen Namen einzugeben. Es genügt, wenn man den Anfang eines Nachnamens gefolgt von einem „*“ eingibt. Das System zeigt dann in einem weiteren Fenster alle Benutzer an, deren Nachnamen mit dem Namensfragment beginnt. So ist es meinen Mitarbeitern in mehreren Stichproben gelungen, sich Vornamen, Nachnamen, Dienststelle, verfahrensspezifische Personalnummer und – worüber nachfolgend noch zu reden sein wird – bisweilen das tatsächliche Geburtsdatum von beliebigen Bediensteten eines Ministeriums, eines Regierungspräsidiums, eines Staatlichen Hochbauamts, mehrerer Finanzämter und weiterer Dienststellen anzeigen zu lassen. Theoretisch hätten wohl alle Bediensteten der Landesverwaltung, deren Arbeitszeit mit dem System erfasst wird, angezeigt werden können.

– Unberechtigter Zugriff auf Name und Vorname

  Innerhalb von CATS hat jeder Bedienstete eine verfahrensspezifische Personalnummer. Gibt man in einem Einstiegsdialog des Arbeitszeitblatts eine Nummer ein, dann sucht das System nach dem Benutzer, dem diese Personalnummer zugeordnet ist. Durch Probieren konnten meine Mitarbeiter Namen und Vornamen einer Reihe von Mitarbeitern über deren verfahrensspezifische Personalnummer selektieren.

– Unzulässige Eingabe und Anzeige des Geburtsdatums

  In der Stellungnahme zum Datenschutzkonzept KZM/CATS hatten wir darauf hingewiesen, dass für die eindeutige Identifikation eines Benutzers das Geburtsdatum nicht notwendigerweise abgespeichert werden muss, wenn ohnehin eine systemweit eindeutige Benutzeridentifikation in Form der verfahrensspezifischen Personalnummer berechnet wird. Es genügt bei der Initialisierung des Systems, aus den mitzuteilenden Angaben die eindeutige verfahrensspezifische Personalnummer zu generieren. Da das System ein Feld für das Geburtsdatum vorsieht, machten wir den Vor-

schlag, in das Feld ein Surrogat-Datum – beispielsweise 01. 01. 2000 – einzugeben. Bedauerlicherweise folgte eine Reihe von Dienststellen diesem Vorschlag nicht. So kam es, dass bei den Stammdaten von vielen Bediensteten ihr tatsächliches Geburtsdatum angezeigt wurde. Immerhin haben die betreffenden Dienststellen auf unsere Nachfrage hin veranlasst, dass die tatsächlichen Geburtsdaten durch ein für alle ihre Beschäftigten identisches fiktives Geburtsdatum (etwa 01. 01. 2001) ersetzt werden.

– Unzulässige Anzeige der letzten sechs bebuchten Kostenstellen

  Wenn man die verfahrensspezifische Personalnummer oder den Namen eines Bediensteten kennt, kann man versuchen, sich dessen Arbeitszeitblatt anzeigen zu lassen. Es gelingt zwar nicht, die Arbeitszeitbuchungen zu erfahren. Allerdings werden die Kostenstellen angezeigt, die der Bedienstete bei den letzten sechs Buchungen angegeben hat. So hätte jeder Bedienstete Einblick nehmen können, welche Kostenstellen andere Bedienstete der Dienststelle – beispielsweise Vorgesetzte – bebucht haben.

– Nicht beschriebenes Freitextfeld

  Auf dem Arbeitszeitblatt jedes Benutzers war ein Symbol enthalten, das beim Anklicken ein aus einem großen Freitextfeld bestehendes Dialogfenster öffnet. Freitextfelder sind datenschutzrechtlich sehr problematisch, weil damit beliebige Eingaben und folglich Speicherungen erfolgen können. Üblicherweise hätte man erwarten können, dass das Freitextfeld im Datenschutzkonzept von CATS erwähnt und dass festgelegt worden wäre, was als Eingabe zulässig ist. Dies ist hier aber nicht geschehen. Die Erklärung der Projektverantwortlichen, dass das Freitextfeld von NSI nicht unterstützt würde, ist schon deshalb nicht plausibel, weil eine Eingabe und Speicherung in dem Feld natürlich möglich war und weiterhin ist. Wenn schon nicht technisch unterbunden werden soll, dass in das Feld Daten eingegeben werden können, dann ist eine Regelung im Datenschutzkonzept darüber erforderlich, was in das Freitextfeld eingegeben werden darf und wann die Daten zu löschen sind.

In ihrer Stellungnahme erklären die Projektverantwortlichen, dass einige der Mängel im Produktivsystem nicht mehr nachvollzogen werden könnten. Wenn dem so ist, dann sind diese erfreulicherweise ohne unser Zutun behoben worden. Die verbleibenden Mängel will das Projekt beseitigen.

Die aufgeführten Punkte zeigen auch, worauf an dieser Stelle ausdrücklich hingewiesen sei, wie wichtig es ist, dass die Behörden, auch wenn sie personenbezogene Daten im Rahmen eines ressortübergreifend eingesetzten Verfahrens verarbeiten, sich ihrer eigenen Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen bewusst sind und entsprechend handeln.

2. Prüfmitteilung des Rechnungshofs: Lektüre für alle interessierten Beschäftigten?

Auch wenn Prüfmitteilungen des Rechnungshofs personenbezogene Daten enthalten, befasst mein Amt sich nicht mit der Frage, wie der Inhalt der Prüfmitteilung oder die Art und Weise ihres Versands einschließlich der Adressierung durch den Rechnungshof datenschutzrechtlich zu beurteilen sind, denn der Rechnungshof unterliegt der datenschutzrechtlichen Aufsicht meines Amts nur außerhalb seiner Prüfungstätigkeit. Dagegen beurteilt mein Amt, und darum geht es im Folgenden, wie andere Stellen mit personenbezogenen Daten in Prüfmitteilungen umgehen.

Eine vom Rechnungshof geprüfte Behörde gab die Prüfmitteilung ungekürzt an alle Abteilungsleiter weiter. Zudem machte sie eine gekürzte Fassung der Prüfmitteilung, aus der ein Teil der Ausführungen zum Personal entfernt war, allen Beschäftigten zugänglich. Auch wenn die Behörde die Prüfmitteilung nur eingeschränkt weitergegeben hatte, wurde sie damit den datenschutzrechtlichen Anforderungen nicht gerecht: Einerseits durften nicht alle Abteilungsleiter eine ungekürzte Fassung der Prüfmitteilung bekommen und andererseits enthielt die gekürzte Fassung immer noch per-

sonenbezogene Daten, die nicht für alle Beschäftigten bestimmt waren. Im Einzelnen:

Die gekürzte Fassung der Prüfmitteilung enthielt unter anderem Angaben zu den „Fahrleistungen der Fahrer im Jahr 2000“. Dabei war jedem der namentlich benannten Fahrer eine Kilometerzahl zugeordnet. Die Behörde leitete diese gekürzte Fassung an alle Abteilungsleiter und Referatsleiter elektronisch weiter mit der Bitte, ihre Mitarbeiter darüber zu informieren. Überwiegend wurden die Mitarbeiter mündlich informiert, jedoch wurden, so die Behörde unserem Amt gegenüber, auch Ausdrucke dieser gekürzten Mitteilung „interessierten Bediensteten zur Einsicht überlassen“.

Die genannten Kilometerzahlen seien doch gar keine personenbezogenen Daten, weil sie, anders als dies aus der Prüfmitteilung hervorgehe, nicht die Kilometerleistungen der Fahrer wiedergeben würden, sondern diejenigen bestimmter Fahrzeuge. Dieser Argumentation der Behörde war nicht zu folgen, denn Kilometerzahlen sind dann personenbezogene Daten der Fahrer, wenn sie ihnen als ihre Jahresfahrleistungen zugeordnet sind. Genau das war hier der Fall: Die Kilometerzahlen wurden ausdrücklich jeweils bestimmten Fahrern zugeordnet; Anhaltspunkte dafür, dass es sich dabei um die Kilometerleistungen bestimmter Fahrzeuge handelt, waren der Prüfmitteilung auch nicht andeutungsweise zu entnehmen. Ob die bestimmten Fahrern als Jahresfahrleistungen zugeordneten Kilometerzahlen auch tatsächlich deren Jahresfahrleistungen entsprachen, ist für die Frage, ob sie personenbezogene Daten sind, ohne Bedeutung, denn es handelte sich jedenfalls um (gegebenenfalls unrichtige) Angaben über die Fahrer.

Bei der Weitergabe dieser (wenn auch unrichtigen) personenbezogenen Daten der Fahrer musste die Behörde unter anderem den Grundsatz der Erforderlichkeit beachten. Dass sie das getan hat, war nicht festzustellen. Insbesondere hat die Behörde nicht dargelegt, wozu jeder Abteilungsleiter und jeder Referatsleiter die Jahresfahrleistungen jedes Fahrers kennen musste. Erst recht war nicht ersichtlich, wozu jeder einzelne Beschäftigte diese Daten kennen musste. Auch wenn, wie die Behörde vortrug, der Rechnungshof jeden einzelnen Beschäftigten befragt hatte und so jeder einzelne Beschäftigte in die Prüfung der Haushalts- und Wirtschaftsführung der Behörde durch den Rechnungshof eingebunden war, rechtfertigte dies nicht, allen „interessierten“ Beschäftigten personenbezogene Daten anderer Beschäftigter zugänglich zu machen. Die Weitergabe der personenbezogenen Daten der Fahrer war daher rechtswidrig.

Die ungekürzte Prüfmitteilung enthielt im personalwirtschaftlichen Teil unter anderem Ausführungen zur Eingruppierung namentlich benannter Beschäftigter. Wozu jeder Abteilungsleiter einen Ausdruck der ungekürzten Prüfmitteilung benötigte, der auch personenbezogene Daten derjenigen Betroffenen enthielt, die nicht in seiner Abteilung beschäftigt waren, konnte die Behörde nicht dartun. Dass eine Prüfmitteilung, so die Behörde, eine wichtige, die Behördenleitung betreffende Angelegenheit ist, rechtfertigte die Weitergabe der personenbezogenen Daten nicht.

Ich habe diese datenschutzrechtlichen Verstöße beanstandet und das zuständige Ministerium um Stellungnahme dazu bis Mitte Januar nächsten Jahres aufgefordert.

3. System „Fortbildung 21“

Auf Wunsch der Führungsakademie Baden-Württemberg berieten wir diese im Rahmen mehrerer Besprechungen und Schreiben zum System „Fortbildung 21“. Dieses umfasst zunächst ein Bildungsmanagementsystem, das von Landesbehörden und deren Beschäftigten über das Landesverwaltungsnetz genutzt werden soll: Unter anderem sollen sich alle an Bildungsmaßnahmen Interessierten elektronisch über die Bildungsangebote informieren und anmelden können. Die administrative Abwicklung der Fortbildung (etwa die Anmeldung zu Veranstaltungen sowie der Versand von Einladungen und Teilnahmebestätigungen) soll möglichst weitgehend elektronisch erfolgen. Gegenstand unserer Beratung, die sich im Wesentlichen auf die datenschutzrechtlichen Beziehungen zwischen der Führungsakademie und (künftigen) Teilnehmern an Bildungsmaßnahmen bezog, war unter anderem Folgendes:

– Generell wiesen wir auf den Grundsatz der Erforderlichkeit hin. Dieser besagt im Wesentlichen, dass eine Verarbeitung (also etwa das Erheben, die Weitergabe und das Speichern) personenbezogener Daten nur zulässig ist, soweit sie notwendig ist, um den damit verfolgten Zweck zu erreichen. Die Zulässigkeit der Verarbeitung personenbezogener Daten hängt daher mit von dem Zweck ab, den die Daten verarbeitende Stelle jeweils verfolgen möchte.

  • Im Konzept war beispielsweise ursprünglich vorgesehen, dass das Landesamt für Besoldung und Versorgung Baden-Württemberg der Führungsakademie allmonatlich bestimmte personenbezogene Daten aller Beschäftigten des Landes (unter anderem Personalnummer, Name und Vorname, Geburtsdatum, Laufbahn und Status) übermittelt. Dabei war nicht ersichtlich, wozu die Führungsakademie die Daten auch derjenigen Beschäftigten benötigt, die weder gegenwärtig noch in absehbarer Zeit an einer Maßnahme teilnehmen. Vielmehr dürften für die Durchführung der Fortbildung die von den Teilnehmern bei ihrer Anmeldung angegebenen Daten genügen. Die Führungsakademie erklärte daraufhin, von einem solchen Datenabgleich abzusehen.

  • Mit Blick darauf, dass die Personalnummer sowie Vor- und Nachname wegen Namensgleichheiten der eindeutigen Identifizierung des Betroffenen dienen, haben wir keine Bedenken dagegen geltend gemacht, dass die Angabe dieser Daten zur Voraussetzung der elektronischen Anmeldung gemacht wird und diese Daten zur Identifizierung der Teilnehmer bei der Anmeldung verarbeitet werden. Davon zu unterscheiden ist ein Einsatz der Personalnummer im Anschluss daran zur Durchführung der Fortbildung, etwa als Kundennummer oder zur Prüfung der Zugangsberechtigung bei einer Anmeldung am System. Ein solches weitergehendes Verarbeiten der Personalnummer ist aus Sicht des Datenschutzes kritisch zu betrachten, weil die Personalnummer objektiv die Funktion eines einheitlichen Personenkennzeichens hat, das einen automatisierten Datenabgleich sowie eine automatisierte Zusammenführung personenbezogener Daten jedenfalls erleichtern kann; dessen Einsatz ist daher möglichst zu vermeiden.

  • Weiter sollen von künftigen Teilnehmern Amts- und Dienstbezeichnung, Laufbahnbezeichnung sowie Statusbezeichnung erfragt werden. Als Zweck, zu dem die Daten verarbeitet werden sollen, waren unter anderem Zielgruppenzusammenstellung und Teilnehmerzusammensetzung genannt. Bei der Frage nach der Zulässigkeit dieser Datenverarbeitung kommt es auch darauf an, inwieweit anstelle der konkreten Amts- und Dienstbezeichnung etwa die Laufbahnbezeichnung – soweit diese sich als erforderlich erweisen sollte – genügt, um den angestrebten Zweck zu erreichen.

– Ein weiterer Diskussionspunkt war, an welche (elektronische) Anschrift Mitteilungen zu einer Maßnahme zu senden sind, etwa Einladungen der Teilnehmer zu Veranstaltungen oder Mitteilungen an deren Dienststellen, ob die Maßnahme tatsächlich stattfindet, zu der ein Beschäftigter angemeldet ist. Da die (vorgesehene oder erfolgte) Teilnahme an einer bestimmten Maßnahme regelmäßig vertraulich zu behandeln ist, dürfen entsprechende Unterlagen nicht an eine allgemeine (E-Mail-)Adresse der Dienststelle (etwa poststelle@...) gesandt werden. Vielmehr ist sicherzustellen, dass nur die bei den zuständigen Stellen jeweils zuständigen Personen oder die Teilnehmer persönlich von diesen Nachrichten (per E-Mail oder in Papierform) Kenntnis nehmen können.

– Wir wiesen die Führungsakademie darauf hin, dass die bei ihr gespeicherten personenbezogenen Daten über Fortbildungen zu löschen sind, sobald sie diese nicht mehr zur Erfüllung ihrer Aufgaben benötigt, also sobald die konkrete Maßnahme hinsichtlich des Teilnehmers abgeschlossen und abgewickelt ist, d. h. insbesondere die Teilnahmebescheinigungen versandt und die Fortbildungskosten abgerechnet sind.

4. Die zurückgenommene Bewerbung

Weil er es sich anders überlegt hatte, zog ein Lehrer seine Bewerbung um eine Schulleiterstelle zurück. Seine schriftliche Rücknahmeerklärung ging bei der Schulverwaltung an einem Montag ein. Vier Arbeitstage später, am darauf folgenden Freitag, versandte die Schulverwaltung unter anderem an die Gemeinde als Schulträger und an die Schulkonferenz der betreffenden Schule Bewerberübersichten. Diese enthielten unter anderem das Geburtsdatum, den Familienstand, die Zahl der Kinder, die Privatanschrift, die bisherigen Dienststellen, Ausführungen zu besonderen Tätigkeiten im schulischen Bereich sowie Eignungsbewertungen mit aussagekräftigen Begründungen (Anlassbeurteilungen) der Bewerber – doch nicht nur dieser, sondern auch des ehemaligen Bewerbers. Warum die Schulverwaltung die personenbezogenen Daten des Lehrers, der seine Bewerbung bereits vor Tagen zurückgezogen hatte, in die Bewerberübersicht aufnahm und an die genannten Stellen versandte, konnten wir nicht nachvollziehen. Der Verweis der Schulverwaltung auf einen „engen“ Zeitablauf liefert dafür keine Erklärung. So wie sich die Angelegenheit uns darstellt, fand die Rücknahme der Bewerbung bei der Schulverwaltung einfach zu spät ihren Weg in die Akte zum Bewerbungsverfahren. Ich habe diesen datenschutzrechtlichen Verstoß beanstandet und die Schulverwaltung aufgefordert, bis Ende Januar nächsten Jahres dazu Stellung zu nehmen und dabei auch darauf einzugehen, durch welche Maßnahmen solche datenschutzrechtlichen Verstöße künftig verhindert werden sollen.

3. Abschnitt: Schul- und Hochschulwesen

1. Einladung zur Selbstbedienung: Schlecht konfigurierte Mailinglisten

Längst ist die Nutzung von E-Mails zur Kommunikation aus dem wissenschaftlichen Bereich nicht mehr wegzudenken. Um die Hochschulangehörigen zielgerichtet informieren zu können, haben zahlreiche Hochschulen Mailinglisten zu verschiedensten Themen eingerichtet. Jede dieser Listen enthält die E-Mail-Adressen sämtlicher Personen, die sich für das jeweilige Thema interessieren und sich daher als Teilnehmer der Mailingliste angemeldet haben. Wer sich zu einem solchen Thema äußern möchte, muss nur eine Mail an die entsprechende Mailingliste senden. Der Listenserver sorgt dann dafür, dass die Nachricht umgehend an alle in der Liste genannten E-Mail-Adressen weitergeleitet wird.

Die Eingabe eines Bürgers machte uns darauf aufmerksam, dass sich jeder Internet-Nutzer eine Liste mit mehr als 2 600 E-Mail-Adressen von einer von der Fachhochschule betriebenen Mailingliste mit dem Titel „Parties“ abrufen konnte. Daraufhin durchgeführte stichprobenweise Überprüfungen machten deutlich, dass diese Problematik keineswegs nur auf diese eine Fachhochschule beschränkt war. Vielmehr war es auch an zwei Universitäten möglich, die Teilnehmer einer Reihe von Mailinglisten abzurufen. In einem Fall konnte jeder Internet-Nutzer die E-Mail-Adressen sämtlicher Teilnehmer der Mailinglisten für Bewohner verschiedener Studentenwohnheime, für VWL-Studenten, für Mitarbeiter der Universitätsbibliothek, für Hilfskräfte des Rechenzentrums, für Fragen zum Thema „Jobticket“ sowie die Teilnehmer einer Reihe weiterer Mailinglisten in Erfahrung bringen. Im anderen Fall ließen sich beispielsweise Teilnehmer von Mailinglisten wie „ersties“, „fechten“, „photo-ak“ oder „windows-ag“ abrufen.

Bei der datenschutzrechtlichen Beurteilung dieser Abrufmöglichkeiten ist zu berücksichtigen, dass E-Mail-Adressen vielfach den vollen Vor- und Zunamen der Mailinglisten-Nutzer offenbaren. Hinzu kommt, dass sich aus der Zuordnung der Teilnehmer zu den Listen sowie den in den Einträgen zum Teil enthaltenen zusätzlichen personenbezogenen Anmerkungen weitere Erkenntnisse über diese Personen ergeben. Ist eine personenbezogene E-Mail-Adresse mehreren Mailinglisten zugeordnet, so ergibt sich dadurch ein noch deutlicheres Interessenprofil dieser Person. Ferner ist zu bedenken, dass die genannten Daten ohne weiteres auch von Adresshändlern oder sonstigen Internet-Nutzern abgerufen werden können, die diese Daten möglicherweise zur Vervollständigung ihrer Datenbestände oder zur Übersen-

dung unverlangter E-Mail-Werbung (SPAM) verwenden können, die viele Internet-Nutzer belästigt.

In keinem der Fälle hatten die Betroffenen ihre Einwilligung zu der Abrufmöglichkeit erteilt. Da zudem eine solche Abrufmöglichkeit zum sachgerechten Betrieb der Mailinglisten nicht notwendig ist, ist es datenschutzrechtlich nicht zulässig, sämtlichen Nutzern des Internets derart umfassende Möglichkeiten zum Abruf personenbezogener Daten zu bieten. Um diesen datenschutzrechtlichen Mangel abzustellen, habe ich die Hochschulen aufgefordert, die bestehenden Abrufmöglichkeiten umgehend zu unterbinden und sicherzustellen, dass diese oder ähnliche Abrufmöglichkeiten weder bei den übrigen bereits vorhandenen Mailinglisten noch bei künftig neu eingerichteten Mailinglisten genutzt werden können. Alle betroffenen Hochschulen sagten daraufhin zu, ihre Mailinglisten künftig so zu betreiben, dass ein solcher Abruf nicht mehr möglich ist.

Einige Monate später stellten wir jedoch fest, dass die Hochschulen diese Zusagen nur zum Teil eingehalten hatten:

– Die erwähnte Fachhochschule ließ zwar nun keinen Abruf der Teilnehmer der Liste „Parties“ zu, sie hatte jedoch mittlerweile eine neue Mailingliste eingerichtet, über die erneut mehr als 2 600 E-Mail-Adressen abgerufen werden konnten. Als Begründung gab sie dazu an, dass sie die Teilnehmer der Liste „Parties“ vor deren Konfigurationsänderung in eine andere Liste kopiert habe, es dann aber versäumte, diese Liste nach erfolgter Änderung wieder zu löschen oder zumindest auch für diese Liste die Abrufmöglichkeit sämtlicher E-Mail-Adressen in gleicher Weise zu sperren.

– Bei beiden erwähnten Universitäten bestanden die zunächst festgestellten Abrufmöglichkeiten zwar nicht mehr, gleichwohl war es auch dort möglich, erneut eine Vielzahl von E-Mail-Adressen aus Mailinglisten-Servern in Erfahrung zu bringen:

  • Im einen Fall war auf die von uns zunächst verwendete Weise keine Auskunft über E-Mail-Adressen mehr zu erhalten. Mit Hilfe einer anderen Abfrageart gelang es jedoch, mehr als 30 000 E-Mail-Adressen sowie deren Zuordnung zu den jeweils gewünschten Mailinglisten abzurufen.

  • Die andere Universität hatte den ursprünglich betroffenen Mailinglisten-Server durch ein anderes Produkt ersetzt, das nicht mehr auf die genannte Weise Auskunft über E-Mail-Adressen gab. Daneben gab es jedoch noch weitere Mailinglisten-Server der Universität, die einen Abruf von E-Mail-Adressen zuließen.

Aufgrund des wiederholten Auftretens sprach ich in diesen Fällen eine Beanstandung aus. Daneben stellten wir bei ergänzenden stichprobenweisen Überprüfungen fest, dass noch zwei weitere Universitäten und eine Fachhochschule Mailinglisten betrieben, die ohne weiteres jedem Internet-Nutzer die E-Mail-Adressen der Listenteilnehmer mitteilten. In einigen Fällen waren dabei neben der E-Mail-Adresse noch weitere Kommentare abrufbar wie z. B. „Amnesty“, „Frieden“, „RCDS“, „Frauenreferat“ oder „JuSo“. Den zuständigen Administratoren war dabei durchweg die Abrufmöglichkeit nicht bewusst. Nachdem wir sie darauf hingewiesen hatten, sagten sie zu, die Abrufmöglichkeiten umgehend zu unterbinden.

Da es sich dabei nicht nur um ein örtliches Problem handelt, habe ich auch das Wissenschaftsministerium hierüber informiert und es aufgefordert, sämtliche Hochschulen auf die Problematik hinzuweisen und dafür Sorge zu tragen, dass derartige unzulässige Abrufmöglichkeiten künftig nicht mehr eingerichtet werden.

2. Private E-Mails an einen Universitätsprofessor sind im Internet fehl am Platze

In einem weiteren an uns herangetragenen Fall hatte ein Universitätsprofessor von einer ehemaligen Studentin einige E-Mails erhalten. Diese E-Mails waren im Wesentlichen privater Natur. Daneben hatte eine der E-Mails darüber hinaus einen konkreten Bezug zur Lehrtätigkeit der Universität: Die ehemalige Studentin wies auf ein Praktikumsgesuch eines ihrer Kollegen hin, welches für Studenten der Universität geeignet sein könnte. Das Praktikumsgesuch war der E-Mail in Gestalt eines abtrennbaren Textes beigefügt. Die Universität setzte dieses Praktikumsgesuch auf ihre Mailingliste, um durch diese Veröffentlichung im Internet das Angebot mit großer Streubreite publik zu machen.

Datenschutzrechtliche Probleme ergaben sich dadurch, dass von Seiten der Universität neben dem Praktikumsgesuch auch die E-Mails mit persönlichem Inhalt in die Mailingliste aufgenommen wurden. Denn diese E-Mails waren nicht für die Universität, sondern allein für den angeschriebenen Professor bestimmt. Deren Veröffentlichung im Internet war auch in keiner Weise geeignet, die Tätigkeit der Universität in Forschung, Lehre, Studium und Weiterbildung zu fördern. Eine gesetzliche Ermächtigung für eine solche Veröffentlichung privater E-Mails besteht nicht. Die Veröffentlichung in der Mailingliste hätte allenfalls auf der Grundlage einer ausdrücklichen Einwilligung der ehemaligen Studentin erfolgen können. Eine solche lag aber nicht vor. Auch eine nach geltendem Datenschutzrecht ohnehin von vornherein grundsätzlich ausgeschlossene stillschweigende Einwilligung war den privaten E-Mails nicht zu entnehmen. In diesem Zusammenhang wurde deutlich, dass bei der Universität ein grundlegendes Missverständnis bestanden hatte. Allein aus der Tatsache, dass sich die ehemalige Studentin durch Übersendung von E-Mails eines automatisierten Datenverarbeitungssystems bedient hatte, wurde geschlossen, dass sie schon deshalb die Öffentlichkeit bzw. Veröffentlichung ihrer Mitteilungen in Kauf genommen und damit akzeptiert hatte. Wir haben gegenüber der Universität klargestellt, dass diese Deutung absolut unzutreffend ist.

Damit aber nicht genug. Weitere Probleme zeigten sich bei dem Versuch, die privaten E-Mails zu löschen. Denn die Universität bediente sich für den Betrieb der Mailingliste eines privaten, in den USA ansässigen Providers. Nach dessen Nutzungsbedingungen war die vollständige Löschung von Nachrichten (auch aus dem angebotenen Archiv) nur für solche Nachrichten möglich, die im laufenden Monat erstellt wurden. Erst nach einiger Zeit hat dieser Provider die Löschung der E-Mails aus dem Archiv dann doch vorgenommen. Daher haben wir die Universität auch darauf aufmerksam gemacht, dass sie beim Betrieb einer Mailingliste dafür Sorge zu tragen hat, dass sich einzelne Nachrichten bei Bedarf jederzeit ohne weiteres löschen lassen.

3. Eine fehlgeschlagene Aktenaussonderung

Spaziergänger staunten nicht schlecht, als sie auf einem Acker im Raum Tübingen klein gerissene, aber noch lesbare Bewerbungsunterlagen einer jungen Wissenschaftlerin, Reisekostenabrechungen sowie weitere vertrauliche Papiere eines Sonderforschungsbereichs der Universität Tübingen fanden. Folgendes war geschehen:

Mitarbeiter des Sonderforschungsbereichs hatten diese Unterlagen in einem Papiersack an die Straße gestellt, wo sie von einem Fahrer der Universität abgeholt und in zentralen Aktenvernichtern zerkleinert werden sollten. Bevor dieser Fahrer kam, nahm jedoch bereits die städtische Grüngutabfuhr den Papiersack mit. Die Unterlagen wurden daher wie das Grüngut nur grob gehäckselt und danach an Landwirte abgegeben. So kam es, dass ein Landwirt die nach wie vor gut lesbaren Unterlagen auf seinem Acker verstreute.

Unser Kontrollbesuch ergab, dass es die Universität nicht nur in diesem Einzelfall an der notwendigen Sorgfalt bei der Entsorgung schutzbedürftiger Papierunterlagen hatte fehlen lassen, sondern dass sie diesem Thema generell zu wenig Aufmerksamkeit schenkte:

– Unzulänglichkeiten beim Sammeln des zur Vernichtung vorgesehenen Papiers

  Die Zentrale Verwaltung der Universität stellt den Instituten braune Papiersäcke mit der Aufschrift „Papierabfälle“ zur Verfügung. In diesen Säcken sammeln die Institute sowohl Altpapier als auch schutzbedürftige Unterlagen mit personenbezogenen Daten, die später in den zentralen Aktenvernichtern zerkleinert werden sollen. Im letzteren Fall beschriften die anliefernden Institute die Säcke vielfach mit einem Hinweis wie z. B. „Reißwolf“. Gelegentlich finden Hausmeister in den Fluren abgestellte und mit „Papier“ beschriftete Plastiksäcke, die sie einsammeln; sie entscheiden nach Sichtung des Inhalts, ob sie die betreffenden Unterlagen im Aktenvernichter zerkleinern. Die vielen tagtäglich zentral angelieferten Papiersäcke, die keinen handschriftlichen Hinweis tragen, werden unbesehen zum Altpapier gegeben. Dass sich in solchen Papiersäcken nicht nur Altpapier, sondern auch Unterlagen mit personenbezogenen Daten befinden, zeigte sich indes beim Kontrollbesuch. In dem über mannshoch mit solchen Papiersäcken gefüllten Altpapierkeller fanden sich auch personenbezogene Unterlagen, wie z. B. eine größere Zahl von Anmeldebescheinigungen, aus denen ersichtlich war, dass sich im Rahmen der internationalen Sprachprogramme der Universität Tübingen beispielsweise eine namentlich genannte Studentin für einen Konversationskurs, ein Student für den Kurs „Diskutieren, Argumentieren, Referieren“ und wiederum eine andere Studentin für den Kurs „Kunst etc. des deutschen Expressionismus“ angemeldet hat und wie viel Euro sie jeweils für den Kurs bezahlt haben. Wir forderten die Universität daher auf, ihre bisherige Praxis zu ändern, die wegen der Verwendung von ein und denselben Papiersäcken zum Sammeln von Altpapier und zum Sammeln von Unterlagen mit personenbezogenen Daten geradezu darauf angelegt ist, dass es bei der Vernichtung von Unterlagen mit personenbezogenen Daten zu Verstößen gegen das Datengeheimnis kommt.

– Unzureichende organisatorische Vorgaben für die Aktenvernichtung

  In dem von der Universitätsverwaltung geführten „Handbuch der Verwaltung“ wird die Vernichtung von Papierunterlagen lediglich im Zusammenhang mit der Abgabe von Unterlagen nach Ablauf der jeweiligen Aufbewahrungsfristen an das Archiv der Universität angesprochen. Darüber hinaus gibt es keine schriftlichen Regelungen der Universitätsverwaltung über die Vernichtung von Unterlagen, die personenbezogene Daten enthalten. Es sei vielmehr, so sieht es die Universitätsverwaltung, Sache eines jeden Bediensteten, sich selbst um eine datenschutzgerechte Vernichtung der tagtäglich im laufenden Betrieb anfallenden Unterlagen mit personenbezogenen Daten zu kümmern. Das Fehlen schriftlicher Regelungen über die Aussonderung und Vernichtung von Unterlagen mit personenbezogenen Daten dürfte jedoch ganz erheblich dazu beigetragen haben, dass es überhaupt zu dem Vorfall kam. Es war daher zu begrüßen, dass die Vertreter der Zentralen Verwaltung noch beim Kontrollbesuch angekündigt haben, die Institute und Einrichtungen der Universität per Rundschreiben an die Einhaltung des Datenschutzes bei der Vernichtung von Unterlagen mit personenbezogenen Daten zu erinnern.

– DIN-Norm für Vernichtung beachten

  Unterlagen mit personenbezogenen Daten fallen nach dem Sprachgebrauch der DIN 32757 in die Klasse der vertraulichen Unterlagen, für die in der Regel eine Vernichtung zumindest nach Sicherheitsstufe 3 vorzunehmen ist. Für einen Streifenschnitt bedeutet dies, dass die Streifenbreite nicht mehr als 2 Millimeter betragen darf. Sonstige Partikel dürfen nicht größer als 800 Quadratmillimeter groß sein. Diesen Anforderungen wurde der größere der beiden zentralen Aktenvernichter nicht gerecht. Wir forderten die Universität daher auf, dieses Gerät sowie eventuelle weitere, die den Anforderungen der DIN 32757 nicht gerecht werden, durch entsprechend leistungsfähigere Geräte zu ersetzen oder dafür Sorge zu tragen, dass zerschnittene Unterlagen durch weitere Arbeitsschritte (z. B. Verbrennung) so behandelt werden, dass die Kenntnis-

nahme der ursprünglich darauf enthaltenen personenbezogenen Daten zuverlässig verhindert werden kann.

Um künftig besser vor solchen Vorkommnissen geschützt zu sein, forderten wir die Universitätsverwaltung auf, für ihren eigenen Bereich sowie auch für die Institute und sonstigen Einrichtungen der Universität schriftliche Regelungen über die Vernichtung von Unterlagen mit personenbezogenen Daten zu treffen und allen Bediensteten bekannt zu geben. Neben den bereits erwähnten sollten darin insbesondere folgende Punkte angesprochen werden:

- Vor dem Abholen dürfen schutzbedürftige Papierabfälle nicht in Papiersäcken oder anderen offenen Behältern gesammelt werden. Stattdessen sind Behälter zu verwenden, die verhindern, dass einmal eingeworfene Unterlagen vor ihrer Vernichtung ohne weiteres wieder herausgeholt werden können.
- Schutzbedürftige Unterlagen dürfen auch zum Abholen nicht für jedermann frei zugänglich abgestellt werden, sondern sind dem Abholer entweder persönlich zu übergeben oder in einem verschlossenen Raum zum Abholen bereitzustellen.
- Die von den Gebäudereinigungsunternehmen eingesetzten Reinigungskräfte müssen auf das Datengeheimnis verpflichtet werden. Dies gilt auch dann, wenn Zweifel daran bestehen, ob die Reinigungskräfte der deutschen Sprache ausreichend mächtig sind. In solchen Fällen bietet sich die Verwendung mehrsprachiger Hinweisblätter und Vordrucke an.

Die Universität hat sich bislang noch nicht abschließend dazu geäußert, wie sie dem Datenschutz bei der Vernichtung schutzbedürftiger Papierunterlagen künftig Rechnung tragen will.

4. Handlungsfähigkeit minderjähriger Schülerinnen und Schüler

Das Kultusministerium hat im Jahr 2003 die fast zehn Jahre alte Verwaltungsvorschrift über die Verarbeitung von Schüler- und Elterndaten durch öffentliche Schulen umfassend überarbeitet und die Neufassung zum 1. November 2003 in Kraft gesetzt. Aufgrund unserer frühzeitigen Beteiligung durch das Ministerium konnten wir im Rahmen der Erarbeitung der neuen Verwaltungsvorschrift verschiedene datenschutzrechtliche Belange zur Geltung bringen. Ein wichtiges Thema war dabei die Frage, ob und in welchem Umfang minderjährige Schülerinnen und Schüler in datenschutzrechtlicher Hinsicht selbstständig handlungsfähig sind. Diese Frage hat insoweit ganz erhebliche praktische und rechtliche Bedeutung, als beim Vorliegen einer solchen Handlungsfähigkeit die Eltern bzw. Erziehungsberechtigten der minderjährigen Schüler nicht gehalten sind, stellvertretend für diese aufzutreten und z. B. gegenüber der Schule Rechte geltend zu machen oder rechtswirksame Erklärungen abzugeben. In datenschutzrechtlicher Hinsicht ist dabei von folgenden Überlegungen auszugehen:

Nach einer der Kernvorschriften des Landesdatenschutzgesetzes ist eine Datenverarbeitung unter anderem dann zulässig, wenn der Betroffene darin eingewilligt hat. Für die Fähigkeit, eine solche Einwilligung selbstständig zu erklären, kommt es – anders als etwa bei den Vorschriften des Bürgerlichen Gesetzbuchs über die Geschäftsfähigkeit mit dem „Stichtag“ der Vollendung des 18. Lebensjahres – allein auf die Einsichtsfähigkeit eines Minderjährigen an. Diese datenschutzrechtliche Einsichtsfähigkeit liegt vor, wenn ein Minderjähriger nach seinem ganz individuellen Reifegrad in der Lage ist, die Bedeutung und Tragweite der ebenfalls individuell zu betrachtenden konkreten Datenverarbeitung zu beurteilen. Vor diesem Hintergrund kommt eine „starre“ Altersgrenze dafür nicht in Betracht.

Das Kultusministerium hat diese Überlegungen bei der Neufassung der Verwaltungsvorschrift nur teilweise umgesetzt. Die Verwaltungsvorschrift sieht nun vor, dass alle Rechte von minderjährigen Schülern, mit Ausnahme der Einwilligung in die Datenverarbeitung personenbezogener Daten, allein durch deren Erziehungsberechtigte ausgeübt werden. Dagegen ist die Frage der Handlungsfähigkeit minderjähriger Schüler hinsichtlich der Einwilligung in die Datenverarbeitung nun erstmals deutlich und detailliert geregelt.

Danach ist festzuhalten: Die nötige Einsichtsfähigkeit minderjähriger Schüler ist nach dem jeweiligen Reifegrad des Schülers und dem Verwendungszusammenhang der Daten zu beurteilen. Sie liegt nicht vor, wenn der Schüler die Folgen einer Verarbeitung der jeweiligen Daten nicht erkennen und sachgerecht einschätzen kann. Mit Vollendung des 16. Lebensjahres ist – im Sinne einer Regelannahme – grundsätzlich vom Vorliegen der Einsichtsfähigkeit auszugehen. Diese Altersgrenze ist nach oben und nach unten flexibel: In einfach gelagerten Fällen kann z. B. bereits ein 14 Jahre alter Schüler die erforderliche Einsichts- und Handlungsfähigkeit besitzen; in schwierigen Fällen von großer Bedeutung und Tragweite kann es auch einem 17 Jahre alten Schüler an der erforderlichen Einsichts- und Handlungsfähigkeit mangeln. Bei der Einwilligung in die Veröffentlichung von personenbezogenen Daten im Internet, insbesondere wenn es sich um Bilder von Schülerinnen bzw. Schülern handelt, sind besonders hohe Anforderungen an das Vorliegen der Einsichts- und Handlungsfähigkeit zu stellen.

5. Teil: Technik und Organisation

1. Schwierigkeiten auf dem Weg zur anonymen Nutzung elektronischer Dienstleistungen

Als in den 90er-Jahren die rechtlichen Rahmenbedingungen für die Nutzung des Internets sowie anderer elektronischer Dienste gesetzt wurden, wurde unter anderem auch darauf Wert gelegt, dass bei der Abwicklung elektronischer Vorgänge nicht automatisch mehr personenbezogene Daten erfasst werden, als dies bei herkömmlicher Erledigung des Vorgangs, also etwa bei einem Einkauf oder bei der Nutzung einer Bibliothek, geschieht. Datenschutz und Datenvermeidung wurden dabei als Qualitätsmerkmale dieser Dienste angesehen. Vor diesem Hintergrund wurden Anbieter von Tele- und Mediendiensten verpflichtet, auch eine anonyme oder pseudonyme Nutzung und Bezahlung ihrer Dienstleistungen zu ermöglichen, sofern dies realisierbar ist. Doch selbst wenn alle Anbieter elektronischer Dienste diesen Anforderungen Rechnung tragen, läuft die Dienstenutzung insgesamt noch nicht zwangsläufig anonym ab. Beispielsweise kann es dann trotzdem noch sein, dass der Internet-Provider, auf dessen Dienstleistungen man angewiesen ist, um die Tele- und Mediendienste zu nutzen, personenbezogen registrieren kann, welcher seiner Kunden wann welche Angebote nutzt. Neben den Schwierigkeiten, die einer anonymen Nutzung durch system- und netztechnische Hürden erwachsen, sehen sich anonym nutzbare Angebote nicht selten auch mit grundlegenden Bedenken von Seiten staatlicher Sicherheitsbehörden konfrontiert.

1.1 Technische Hürden für die anonyme Nutzung

Selbst wenn jemand einen an sich anonym nutzbaren Tele- oder Mediendienst nutzt, können die auf anderen Kommunikationsebenen anfallenden Verbindungsdaten Rückschlüsse auf den Nutzer zulassen. Zudem übertragen manche Hard- oder Softwareprodukte weitere, zur Identifizierung verwendbare Daten. Diese können so spezifisch sein, dass der Nutzer später wiedererkannt werden kann und Informationen über sein Nutzungsverhalten Schritt für Schritt in einem Persönlichkeitsprofil zusammengeführt werden können.

Folgende Datenspuren ziehen die Nutzung des Internets sowie des World Wide Web (WWW) nach sich:

– IP-Adresse

IP-Adressen bestehen aus vier durch Punkte voneinander getrennten Zahlen (z. B. 129.69.2.171) und bezeichnen die im Internet erreichbaren Computer. Jedes im Internet transportierte Datenpaket weist seine Herkunft und sein Ziel anhand solcher IP-Adressen nach. Man unterscheidet dabei statische und dynamische IP-Adressen. Statische IP-Adressen sind einzelnen Computern dauerhaft zugeordnet. Über diese Zuordnung ist vielfach auch ein Rückschluss auf den oder die Nutzer möglich. Dynamische IP-Adressen erhalten Internet-Nutzer von ihrem Zugangsprovider nur für die Dauer der Nutzung. Dabei kann der Personenbezug aufgedeckt werden, wenn man neben den bei der Internet-Nutzung anfallenden Benutzerspuren (z. B. in Log-Dateien von Web-Servern) auch Kenntnis darüber hat, welche IP-Adresse wann welchem Nutzer zugeordnet war. Nicht auszuschließen ist etwa, dass einzelne Personen als freie Mitarbeiter sowohl für den Internet-Provider wie auch für den Anbieter des genutzten Tele- oder Mediendienstes tätig sind und zumindest technisch die Möglichkeit haben, mit Hilfe der gespeicherten IP-Adressen nachzuvollziehen, wer wann welches Internet-Angebot genutzt hat.

– Cookies

Betreiber von Web-Servern können Informationen über den Nutzer und dessen Interessen in einem Cookie auf dem PC des Nutzers speichern. Bei einem späteren Besuch der Web-Seite wird dieses wieder an den Web-Server übertragen. Firmen, die Werbeeinblen-

dungen für zahlreiche Web-Angebote vornehmen, können mit Hilfe von Cookies feststellen, welche unterschiedlichen Web-Angebote ein Nutzer besucht (vgl. 21. Tätigkeitsbericht, LT-Drs. 12/5740, S. 12 f.).

– Beim Surfen im WWW vom Browser automatisch übertragene Informationen

  Browser übertragen in der Regel Angaben über das auf dem PC eingesetzte Betriebssystem, dessen Versionsstand, den benutzten Browsertyp und dessen Sprachversion an jeden Web-Server, mit dem sie in Verbindung treten. Wechselt man durch Anklicken eines Links von einem Web-Angebot zu einem anderen, so wird dem Server des neu aufgerufenen Angebots mit Hilfe des Referrers zudem mitgeteilt, von welcher zuvor besuchten Seite aus der Wechsel erfolgte.

– Nutzer- sowie installationsbezogene Informationen in Office-Dokumenten

  Wer beispielsweise ein mit Microsoft Word erstelltes Dokument elektronisch überträgt, kann, wenn er die unter Nummer 6 beschriebenen Schutzmaßnahmen außer Acht lässt, bei der elektronischen Übertragung solcher Dokumente unbeabsichtigt auch eine Reihe personenbezogener Daten übermitteln.

– Eindeutige Produktkennzeichen

  Manche Hard- und Softwareprodukte versuchen, über Internet mit ihrem Hersteller Verbindung aufzunehmen. Teilweise dient dies dazu zu ermitteln, ob es mittlerweile Updates oder aktuellere Softwareversionen gibt. Eindeutige Produktkennzeichen, wie z. B. die in den Pentium-III-Prozessoren des Herstellers Intel enthaltenen eindeutigen Nummern, Seriennummern von Druckern oder auch die in Office-Produkten enthaltenen Kennungen, können dabei zur Identifizierung des Systems sowie unter Umständen auch seines Nutzers dienen (vgl. dazu auch: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999 zum Thema „Transparente Hard- und Software“).

1.2 Möglichkeiten für anonyme Kommunikation

Um anonyme Nutzungen zu ermöglichen, muss auf allen an der Kommunikation beteiligten Ebenen sichergestellt sein, dass dort keine identifizierenden Daten ausgetauscht werden. Geht man davon aus, dass die Anbieter von Tele- und Mediendiensten auf der von ihnen gestalteten Diensteebene anonyme Nutzungsformen ermöglichen, sind auch auf Anwendungs- wie auf der Telekommunikationsebene die Weichen für eine anonyme Nutzung richtig zu stellen. Einiges davon können die Anwender sowie die Behörden oder sonstigen Stellen, die die Computer betreiben, selbst leisten:

– Konfiguration der eingesetzten Produkte

  Einige der identifizierenden Funktionen lassen sich durch entsprechende Konfiguration der eingesetzten Software abschalten. So lässt sich etwa die Speicherung von Cookies durch entsprechende Browserkonfiguration verhindern. Zum Teil lässt sich zudem verhindern, dass beim Surfen die Referrer übertragen werden.

– Anpassung der internen Arbeitsabläufe

  Wie am Beispiel der versteckten Informationen in Office-Dokumenten erläutert, kann die Weitergabe identifizierender Angaben zum Teil auch durch darauf abgestimmte Arbeitsabläufe vermieden werden.

– Informationen über identifizierende Merkmale

  Wesentliche Voraussetzung für das Ergreifen wirksamer Maßnahmen ist, dass die Anwender sich um Informationen über die in

den eingesetzten Produkten enthaltenen identifizierenden Funktionen und Kennzeichen bemühen und dass entsprechende Kenntnisse in Behörden an die Nutzer weitergegeben und die Bediensteten auf diese Weise für die Problematik sensibilisiert werden.

Diese Maßnahmen eignen sich vor allem, um auf Anwendungsebene vorhandene Hindernisse für eine anonyme Kommunikation zu beseitigen. Die Möglichkeit, anhand der benutzten IP-Adressen Benutzerprofile zu erstellen, lässt sich allerdings durch Maßnahmen allein auf Seiten der Anwender nicht verhindern. Dazu ist es vielmehr nötig, spezielle Anonymisierungsdienste zu nutzen, die auf der Datentransportebene (Netzwerkebene) wirken. Dazu gibt eine Reihe von Konzepten, die zum Teil auch in der Praxis angeboten werden. Sie unterscheiden sich in dem Ausmaß, in dem sie Anonymität bieten können:

– Anonymisierungsproxy

  Im einfachsten Fall funktioniert ein solcher Anonymisierungsdienst wie eine in die Kommunikation eingeschaltete Zwischenstation, über die alle Internet-Zugriffe des Nutzers abgewickelt werden. Der Internet-Nutzer teilt dem Proxy jeweils mit, auf welche Internet-Seite er zugreifen möchte. Der Proxy greift dann unter seiner eigenen IP-Adresse auf das gewünschte Angebot zu und leitet die abgerufenen Daten an den Internet-Nutzer weiter. Zum Teil entfernt der Proxybetreiber außerdem weitere Daten, die auf persönliche oder systemtechnische Verhältnisse beim Internet-Nutzer schließen lassen. Ein Internet-Nutzer kann so gegenüber seinen Kommunikationspartnern sowie gegenüber den Anbietern der von ihm genutzten Informationsdienste anonym bleiben, nicht jedoch gegenüber dem Betreiber des Anonymisierungsdienstes. Dieser kann nachvollziehen, wann und unter welchen IP-Adressen welche Informationen abgerufen wurden. Die Verwendung eines solchen Modells setzt voraus, dass sich der Nutzer auf die Vertrauenswürdigkeit des Proxybetreibers verlassen kann.

– Anonymisierung im Zwiebelschalen-Modell: das Onion-Routing

  Demgegenüber ist das Onion-Routing so konzipiert, dass die Kommunikation stets über mehrere, von unterschiedlichen Personen oder Einrichtungen betriebene Anonymisierungsstationen abgewickelt wird. Dies geschieht so, dass der Betreiber einer einzelnen Anonymisierungsstation nicht mehr nachvollziehen kann, wer wann welches Angebot genutzt hat. Durch Verschlüsselung der übertragenen Daten lässt sich dabei erreichen, dass die Betreiber der meisten Anonymisierungsstationen nicht einmal mehr erkennen können, auf welche Inhalte zugegriffen wird. Die Anonymität der Nutzer bleibt in diesem System gewahrt, sofern nicht die Betreiber sämtlicher genutzter Anonymisierungsstationen die ihnen zugänglichen Informationen miteinander abgleichen.

– Mix-Technologie

  Beim Einsatz dieser Technologie bieten die Anonymisierungsstationen nicht nur die vom Onion-Routing bekannte Funktionalität, sondern sorgen zudem dafür, dass die bei ihnen eintreffenden Anfragen nicht in der gleichen Reihenfolge weitergeleitet werden. Damit kann die Anonymität der Nutzer sogar dann noch gewahrt werden, wenn man unterstellt, dass ein omnipräsenter Dritter in die Rolle eines „Big Brother“ schlüpft und nicht nur Zugriff auf fast alle verwendeten Anonymisierungsstationen hat, sondern auch auf die genutzten Netzwerkverbindungen, und daher registrieren kann, wann über welche Datenverbindungen Daten zwischen welchen Computern oder Anonymisierungsstationen ausgetauscht werden. Ein solches Mix-Modell liegt beispielsweise dem von der TU Dresden in Zusammenarbeit mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein betriebenen und für die WWW-Nutzung vorgesehenen AN.ON-Anonymisierungsdienst zugrunde (vgl. http://www.anon-online.de).

Gegenwärtig ist dabei allerdings noch nicht die volle Mix-Funktionalität realisiert.

1.3 Vorbehalte staatlicher Sicherheitsbehörden

Staatliche Sicherheitsbehörden betrachten anonyme Nutzungsformen vielfach vor allem unter dem Aspekt, dass diese auch von Straftätern genutzt werden könnten und diese Nutzung nachträglich, etwa im Rahmen staatsanwaltschaftlicher Ermittlungsverfahren, nicht mehr anhand individueller Benutzerspuren nachvollzogen werden könne. Im Rahmen einer Tagung fasste der baden-württembergische Polizeipräsident diese Bedenken Anfang Juli in folgende Worte:

> „Gerade die Möglichkeit des anonymen Agierens (‚fake-accounts', Internetcafes, Gratis-Zugänge über Werbe-CDs u. a.) machen dabei das Netz zum willkommenen Freiraum für Straftäter, die sich dieses neuen Tatmittels bedienen und dabei immer ausgefeiltere Tatbegehungsformen entwickeln. Aber auch ansonsten unbescholtene Bürger nutzen die Anonymität des Internets und lassen sich zu Straftaten wie dem Download teurer kommerzieller Software verleiten. Auch hier gilt, wie im ‚richtigen Leben', dass Gelegenheit bekanntlich Diebe macht!"

Im Sinne solcher Überlegungen unternahm der Bundesrat bereits mehrfach den Versuch, Anbieter von Kommunikationsdiensten zu verpflichten, die bei ihnen anfallenden Verbindungsdaten in jedem Fall für eine bestimmte Mindestdauer aufzubewahren, also auch dann, wenn diese Daten für Betrieb und Abrechnung der Dienstleistungen nicht mehr benötigt werden. Zuletzt geschah dies im November anlässlich der Bundesratsberatungen zur Novellierung des Telekommunikationsgesetzes. In dem dazu vom Bundeskabinett vorgelegten Gesetzentwurf zur Novellierung des Telekommunikationsgesetzes ist zudem ausdrücklich vorgesehen, eine anonyme Nutzung so genannter Prepaid-Handys zu untersagen. Telekommunikationsunternehmen sollen dazu auch dann zur Erhebung und Speicherung personenbezogener Kundendaten verpflichtet werden, wenn sie diese für eigene Zwecke gar nicht benötigen. In ihrer Entschließung vom 21. November 2003 unter dem Titel „Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes" wenden sich die Datenschutzbeauftragten des Bundes und der Länder unter anderem gegen diese beiden Anliegen (s. Anhang 8).

Wie auch auf Grundlage der bestehenden Rechtslage ein datenschutzgerechter Ausgleich der Interessen der Anbieter von Anonymisierungsdiensten sowie der Strafverfolgungsbehörden zu erzielen ist, lässt sich aus der gerichtlichen Behandlung eines Falles ableiten, in dem zu klären war, unter welchen Voraussetzungen die Betreiber des oben bereits erwähnten Anonymisierungsdienstes AN.ON den Strafverfolgungsbehörden welche Informationen zur Verfügung stellen müssen. Dabei ergab sich Folgendes:

– Das Bundeskriminalamt wollte erreichen, dass der Anonymisierungsdienst Informationen darüber aufzeichnet, welche ursprünglichen IP-Adressen dessen Nutzer verwenden, die mit Hilfe dieses Dienstes auf einen bestimmten strafbaren Inhalt zugreifen. Es hatte dazu eine richterliche Anordnung erwirkt, die die Betreiber des Anonymisierungsdienstes verpflichtete, Auskunft über die näheren Umstände der von ihnen erbrachten Telekommunikationsdienstleistung zu geben. Derartige Anordnungen werden ansonsten beispielsweise benötigt, wenn Strafverfolgungsbehörden von einem Telekommunikationsunternehmen Auskunft darüber erhalten wollen, welche Rufnummern wann und von welchem Anschluss aus angerufen wurden. Obwohl die Anordnung den Anbieter lediglich zur Herausgabe von Daten verpflichtet, vertrat das Bundeskriminalamt die Auffassung, dass die Anordnung den Anbieter für den Fall, dass er über keine Daten verfügt, die er herausgeben könnte, dazu verpflichte, diese Daten künftig überhaupt erst aufzuzeichnen. Das mit der gerichtlichen Überprüfung befasste Landgericht Frankfurt/M. schloss sich

jedoch der Auffassung der Betreiber des Anonymisierungsdienstes an, nach der die Verpflichtung zur Herausgabe von Daten nicht zugleich auch eine Verpflichtung zur Aufzeichnung der Daten umfasst.

– Will eine Strafverfolgungsbehörde die Aufzeichnung solcher Daten durch einen Anonymisierungsdienst erreichen, muss sie dazu eine Anordnung erwirken, wie sie ansonsten zur Telefonüberwachung benötigt wird. Eine solche, nur unter engeren rechtlichen Voraussetzungen zulässige Anordnung, umfasst auch die Verpflichtung, die darin näher zu bezeichnenden Kommunikationsvorgänge aufzuzeichnen.

– Für den Betrieb eines Anonymisierungsdienstes nach diesen Maßgaben ist allerdings noch zu klären, wie dessen Nutzer auf eine zeitweise vorhandene Einschränkung der gebotenen Anonymität hingewiesen werden können.

Diese Vorgehensweise stellt aus unserer Sicht einen auch aus datenschutzrechtlicher Sicht akzeptablen Weg dar, um die von Anonymisierungsdiensten gebotene Anonymität in bestimmten, gesetzlich eindeutig geregelten Einzelfällen gegenüber den Sicherheitsbehörden aufzuheben.

Demgegenüber hätte eine Verpflichtung zur Vorratsdatenspeicherung für einen Anonymisierungsdienst zur Folge, dass dieser die Kommunikationsvorgänge sämtlicher Teilnehmer zu erfassen und zur Mitteilung an Sicherheitsbehörden bereitzuhalten hätte, ohne dass dabei im Einzelfall die Voraussetzungen der angesprochenen richterlichen Anordnung vorliegen. In der Abwägung zwischen dem Recht der Nutzer auf unbeobachtete Kommunikation und den berechtigten Interessen der Sicherheitsbehörden ist eine solche Vorratsdatenspeicherung daher als unverhältnismäßig anzusehen. (Vgl. dazu auch die Entschließung vom 21. November 2003 „Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes“ – Anhang 8 – sowie die im vergangenen Jahr gefassten Entschließungen zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet, zum geplanten Identifikationszwang in der Telekommunikation sowie zum Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten.)

2. Aktuelle Entwicklungen im Bereich elektronischer Signaturen

Mit dem 1997 verabschiedeten Signaturgesetz schuf der Bundesgesetzgeber rechtliche Grundlagen für die Verwendung elektronischer Signaturen, die heute in Form einfacher, fortgeschrittener sowie qualifizierter Signaturen verwendet werden können. Das Signaturgesetz enthält eine Vielzahl technischer und organisatorischer Anforderungen für den Umgang mit qualifizierten Signaturen. Sie richten sich insbesondere an Trust-Center, die Chipkarten mit den zur Signatur erforderlichen Signaturschlüsseln ausgeben und elektronische Zertifikate ausstellen, die darüber Auskunft geben, welche Signaturschlüssel welchen Personen zugeordnet sind. Demgegenüber verzichtet das Gesetz auf entsprechende Anforderungen an den Umgang mit fortgeschrittenen und einfachen elektronischen Signaturen. Diese müssen lediglich zur Identifizierung von Personen dienen. Besondere Bedeutung kommt den qualifizierten Signaturen auch deshalb zu, weil geänderte Formvorschriften des Zivil- und des Öffentlichen Rechts es mittlerweile zulassen, zahlreiche Vorgänge, die bislang die eigenhändige Unterschrift tragen mussten, künftig elektronisch abzuwickeln.

Gleichwohl blieb der Einsatz qualifizierter elektronischer Signaturen bislang nur auf relativ kleine Anwenderkreise beschränkt. Mittlerweile sind jedoch Projekte beschlossen, die die Ausgabe signaturfähiger Chipkarten an alle Mitglieder der gesetzlichen Krankenversicherungen sowie an alle Beschäftigen vorsehen:

– Bis zum Jahr 2006 sollen die gesetzlichen Krankenversicherungen an Stelle der bisherigen Krankenversichertenkarte funktional wesentlich erweiterte elektronische Gesundheitskarten an ihre Versicherten ausgeben,

die unter anderem auch für Authentifizierung, Verschlüsselung und elektronische Signaturen nutzbar sein sollen.

– Der für Leistungserbringer vorgesehene elektronische Heilberufsausweis (Health Professional Card) soll qualifizierte Signaturen enthalten. Deren Verwendung soll künftig notwendig sein, wenn beispielsweise ein Arzt auf die in den elektronischen Gesundheitskarten gespeicherten Daten eines Patienten zugreifen will.

– Rund 40 Millionen Arbeitnehmer sollen ebenfalls bis zum Jahr 2006 eine Job-Card erhalten. Darin sollen nicht nur Daten zu Beschäftigungszeiten, zur Höhe von Entgeltzahlungen sowie weitere Angaben über Beschäftigungsverhältnisse gespeichert werden, sondern sie sollen ebenfalls über eine Signaturfunktion verfügen. In einem gegenwärtig durchgeführten Modellprojekt werden dafür qualifizierte Signaturen eingesetzt.

Wie sich der Einsatz qualifizierter, aber auch fortgeschrittener Signaturen darüber hinaus weiter fördern lässt, erörtern öffentliche Stellen und interessierte Unternehmen im Rahmen des von der Bundesregierung ins Leben gerufenen Signaturbündnisses. Um weitere Anreize für die Verwendung qualifizierter Signaturen zu geben, wurde dort vorgeschlagen, die Anforderungen an die qualifizierten Signaturen generell auf das im Bereich der Steuerverwaltung definierte Niveau der „qualifizierten Signatur mit Einschränkungen“ abzusenken. In diesem Fall müssten bei einer Reihe sicherheitsrelevanter Anforderungen Abstriche von dem für qualifizierte Signaturen geltenden Niveau hingenommen werden. Bei der Diskussion über eine mögliche Absenkung des Sicherheitsniveaus ist allerdings zu berücksichtigen, dass aus unternehmerischer Sicht unter Umständen ein gewisses Maß fehlerhafter Identifizierungen in Kauf genommen werden kann, sofern der dadurch verursachte Schaden geringer ist als der zur Beseitigung der Sicherheitslücken notwendige Aufwand. Demgegenüber können öffentliche Stellen, die sich etwa vor der Ausgabe eines Waffenscheins Klarheit über die Identität des Antragstellers verschaffen müssen, dabei nicht ohne weiteres Abstriche an der Zuverlässigkeit der Identifizierung in Kauf nehmen. Die Überlegungen zu einer entsprechenden Absenkung des Anforderungsniveaus sind zudem auch deshalb kritisch zu beurteilen, weil diese „qualifizierte Signatur mit Einschränkungen“ von der Steuerverwaltung ausdrücklich nur für eine bis Ende 2005 befristete Übergangsphase zugelassen wird, während danach uneingeschränkte qualifizierte Signaturen zu verwenden sind. In ihrer Entschließung vom 27./28. März 2003 zur elektronischen Signatur im Finanzbereich (s. Anhang 11) wiesen die Datenschutzbeauftragten des Bundes und der Länder auf weitere datenschutzrechtliche Probleme hin, die sich aus einer möglichen Absenkung des Niveaus qualifizierter Signaturen ergeben können. In jedem Fall sollte bei einer Fortschreibung der Anforderungen an qualifizierte Signaturen verhindert werden, dass dadurch die angestrebte zuverlässige Identifizierbarkeit beeinträchtigt und damit eine Grundlage für den sicheren und verlässlichen elektronischen Rechts- und Geschäftsverkehr in Frage gestellt wird.

3. Chancen und Risiken von Trusted Computing

Beinahe täglich erscheinende Meldungen über neue Computerviren, über die Ausbreitung so genannter Dialer-Programme oder andere Schadenssoftware und die durch sie verursachten Schäden verdeutlichen, dass bei herkömmlichen Computersystemen erhebliche Sicherheitsdefizite bestehen. Diese Systeme sind vielfach unzureichend vor unberechtigten und unerwünschten Systemänderungen geschützt. Um Abhilfe zu schaffen, bedarf es auch entsprechender Hard- und Software, die von Haus aus bessere Voraussetzungen für einen sicheren Systembetrieb mit sich bringen. Besonderes Augenmerk ist daher auf die von der Trusted Computing Group (TCG) erarbeiteten Konzeptionen zu richten, die eine solche zuverlässige Systemplattform zum Ziel haben. Deren öffentliche Diskussion konzentrierte sich rasch auf die Frage, inwieweit diese Techniken Benutzer einschränken und beispielsweise eine technische Grundlage für das Digital Rights Management bieten sollen, etwa indem sich auf den entsprechenden Computern nur noch solche urheberrechtlich geschützten Texte, Bilder, Filme oder Musikstücke

wiedergeben lassen, die zuvor ausdrücklich für die Nutzung auf diesem Computer freigegeben wurden. Zu weiterer Verunsicherung über Sinn und Zweck dieser Konzeptionen trug zudem bei, dass die auch in der TCG mitwirkende Firma Microsoft zunächst unter dem Namen Palladium und später unter der Bezeichnung NGSCB (Next Generation Secure Computing Base) eigene Vorstellungen zu sicheren Systemplattformen präsentierte.

Demgegenüber rückte die Frage, inwieweit die von der TCG präsentierten Konzepte auch im Sinne des Datenschutzes und der Datensicherheit wünschenswerte Elemente enthalten, in den Hintergrund. Dabei lohnt es sich, auch aus dieser Perspektive einen näheren Blick auf die vorgeschlagenen Lösungen zu werfen:

Die im Frühjahr 2003 gegründete und unter anderem von den Firmen HP, IBM, Intel und Microsoft getragene Trusted Computing Group führt die ursprünglich von der Trusted Computing Platform Alliance (TCPA) begonnenen Arbeiten fort. Das Modell sieht vor, Personal Computer und andere zu sichernde Geräte um ein Trusted Platform Module (TPM) zu erweitern. Darin kann zum einen ein als sicher erkannter Systemzustand hinterlegt werden. Zum anderen lässt sich mit Hilfe der darin enthaltenen Mechanismen jederzeit nachweisen, dass sich das System noch in diesem Zustand befindet. Ähnlich wie bei Signaturchipkarten sollen im TPM ein oder mehrere Schlüssel hinterlegt werden, die zur Identifikation des Computers und damit unter Umständen auch seiner Nutzer dienen. Neben einem in jedem Fall vorhandenen Schlüssel, der dem PC eindeutig zugeordnet ist („Endorsement Key“), können auch weitere von Trust-Centern vergebene Schlüssel („Attestation Identity Keys“, AIK) gespeichert und verwendet werden.

Verwendet man solche mit einem TPM ausgestattete Systeme in einem Computernetzwerk, so kann dies zu einer höheren Sicherheit beitragen. Ein Bürger, der eine elektronische Dienstleistung einer Behörde, oder der Kunde einer Bank, der ein POS-Zahlungssystem nutzen will, könnte sich, bevor er sich gegenüber der Behörde oder der Bank persönlich identifiziert und dabei schutzbedürftige Daten, etwa ein Passwort oder eine PIN, in das System eingibt, zunächst nachweisen lassen, dass sich diese Systeme in einem ordnungsgemäßen Systemzustand befinden und außer der ausdrücklich dafür vorgesehenen und freigegebenen Software keine anderen Programme darauf installiert sind. Auch wenn noch eine Reihe von Umsetzungsfragen zu klären ist, wird zugleich deutlich, dass die von der TCG vorgestellte Konzeption zu einer Erhöhung der Systemsicherheit beizutragen vermag. Damit entsprechende Systeme auch datenschutzgerecht verwendet werden können, ist bei deren weiterer Ausgestaltung noch eine Reihe von Anforderungen zu berücksichtigen:

- Damit die erwünschte Sicherheit erreicht werden kann, muss auch ein geeignetes organisatorisches Umfeld vorhanden sein: Im obigen Bank-Beispiel muss etwa gewährleistet sein, dass in der durch das TPM als unverändert nachgewiesenen Systemkonfiguration des genutzten POS-Zahlungssystems selbst keine sicherheitsrelevanten Programmfehler oder bewusst eingefügte Hintertüren enthalten sind.
- Sichergestellt sein sollte auch, dass sämtliche Standards von Dritten, wie dem Bundesamt für Sicherheit in der Informationstechnik, überprüft werden können.
- Die benötigten Schlüssel sollten auch von Trust Centern erstellt werden können, die von der TCG und ihren Mitgliedern unabhängig sind. Daneben sollte es auch möglich sein, dass der für einen PC verantwortliche Administrator die notwendigen Schlüssel selbst erzeugt.
- Der für einen PC verantwortliche Administrator sollte auf Wunsch Programme auch außerhalb der geschützten Umgebung ablaufen lassen können.
- Die korrekte Funktion der sicheren Systemplattform darf nicht davon abhängen, dass die einzelnen Computer regelmäßig Online-Verbindungen zu zentralen Servern aufbauen müssen.
- Die Verwendung des TPM darf eine anonyme Kommunikation etwa im Internet nicht verhindern. Dies ist bislang nicht sichergestellt. Denn für

die Vergabe der AIK müssen die Nutzer dem Trust Center etliche Angaben über ihren PC inklusive ihres gerätespezifischen Schlüssels offenbaren. Bedenkt man, dass Online-Diensteanbieter, bei denen sich jemand mit einem solchen Key identifiziert, diesen Schlüssel dem Trust-Center zur Überprüfung der Gültigkeit vorlegen können, so bedeutet dies, dass das Trust-Center dadurch zugleich erfährt, welche Dienste wann von welchem PC aus genutzt werden.

– Weitere datenschutzrechtliche Anforderungen ergeben sich aus der Entschließung „TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden“, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Rahmen ihrer Sitzung am 27./28. März 2003 gefasst hat (s. Anhang 13).

4. Internet und eGovernment

4.1 e-Bürgerdienste-Portal Baden-Württemberg

In diesem Jahr wurden die ersten beiden Ausbaustufen des e-Bürgerdienste-Portals des Landes für die Nutzung über Internet freigeschaltet. Damit ist es möglich, sich über Behörden und die von ihnen angebotenen Dienstleistungen zu informieren, anhand bestimmter Lebenslagen Hinweise zu den damit verbundenen Behördengängen zu erhalten und per Mausklick etliche kommunale und staatliche Bürgerdienste aufzurufen. Die zu diesem Projekt erarbeiteten Rahmen- und Strukturkonzeptionen zum Datenschutz wiesen noch zu Beginn des Jahres grundlegende Unzulänglichkeiten auf (vgl. dazu auch 23. Tätigkeitsbericht, LT-Drs. 13/1500, S. 83 ff.). Im Rahmen unserer Beratungstätigkeit konnten wir jedoch in der Folge noch eine Reihe konzeptioneller Verbesserungen erreichen:

– Präzisierung des Funktionsumfangs

  Während die erwähnten Datenschutzkonzeptionen in ihrer ursprünglichen Fassung nicht einmal genau erkennen ließen, von welchen künftigen Dienstleistungen überhaupt die Rede ist, werden diese nun im Einzelnen genannt. Dies ist keineswegs nur eine Formalie. Denn erst, wenn man weiß, welche Dienstleistungen für welchen Zweck angeboten werden, lässt sich ermitteln, welche Rechtsgrundlagen dabei zu berücksichtigen sind, und klären, welche personenbezogenen Daten dafür verarbeitet werden dürfen.

– Präzisierung der Rechtsgrundlagen

  Die Datenschutzkonzeptionen gingen in ihrer ursprünglichen Fassung nicht durchgängig von den gleichen rechtlichen Grundlagen für die Datenverarbeitung aus, sondern erwähnten mal diese, mal andere Gesetze und Verordnungen. Auch in dieser Hinsicht trat mittlerweile eine wesentliche Verbesserung ein.

– Verzicht auf Cookies und aktive Inhalte

  Anders als ursprünglich geplant, verzichtet das e-Bürgerdienste-Portal nun vollständig auf Cookies sowie auf so genannte aktive Inhalte wie JavaScript, Java-Applets sowie ActiveX-Controls. Wenn nun vielfältige interaktive Dienstleistungen angeboten werden, ohne auf diese datenschutzrechtlich problematischen Hilfsmittel zurückzugreifen, wird das Projekt eher dem Anspruch gerecht, auch datenschutzrechtlich beispielhafte Lösungen zu präsentieren.

Auch wenn sich dadurch bereits deutliche Verbesserungen für den Datenschutz ergeben haben, steht die datenschutzgerechte Lösung einiger Punkte noch aus:

– Protokollierung der Zugriffe auf das Portal

  Das Betriebskonzept für das e-Bürgerdienste-Portal sieht bislang vor, dass jeder Zugriff auf das Portal protokolliert wird. Jedes Mal also,

wenn ein Bürger die im Portal enthaltenen Inhalte liest oder per Mausklick einen Bürgerdienst aufruft, wird registriert, welche IP-Adresse der PC des Bürgers hat, wann der Zugriff erfolgt, auf welchen Inhalt zugegriffen wurde oder ob sich beim Zugriff ein Fehler ereignet hat und wenn ja welcher. Wenn der Nutzer überhaupt erst durch Anklicken eines auf einer anderen Web-Seite angebrachten Links zum e-Bürgerdienste-Portal kam, wird auch registriert, von welchem zuvor besuchten Angebot aus dieser Wechsel erfolgte. Als Grund für diese Protokollierung gab das Innenministerium an, diese Angaben seien für die Aufrechterhaltung der Systemsicherheit nötig.

Zwar darf eine Stelle auch personenbezogene Daten speichern, wenn dies erforderlich ist, um die Sicherheit von Systemen zu gewährleisten, mit denen personenbezogene Daten verarbeitet werden. Das Innenministerium legte bislang jedoch noch nicht dar, weshalb sämtliche von der Protokollierung erfassten Daten tatsächlich zur Abwehr sicherheitsrelevanter Vorkommnisse benötigt werden. Insbesondere sehen wir keinen Grund, auch solche Abrufe zu protokollieren, bei denen Bürger – so wie vom Innenministerium vorgesehen – auf die im Portal enthaltenen Informationen zugreifen und diese Zugriffe auch fehlerlos abgewickelt werden. Wir forderten das Innenministerium daher nochmals auf, den Umfang der Protokollierung auf das Maß zurückzuführen, das zur Identifikation und zur Bearbeitung sicherheitsrelevanter Ereignisse notwendig ist.

– Verschlüsselung der übertragenen Daten

Gerade weil im Rahmen des e-Bürgerdienste-Portals auch interaktive Bürgerdienste nutzbar sein sollen, bei denen personenbezogene Daten ausgetauscht werden können, ist sicherzustellen, dass diese Daten durch Verschlüsselung vor unberechtigter Kenntnisnahme oder gezielter Verfälschung geschützt werden. Im e-Bürgerdienste-Portal wird dementsprechend zwar eine Verschlüsselungsfunktion integriert, diese wird aber nur dann wirksam, nachdem sie der Benutzer durch Mausklick eingeschaltet hat. Um zu vermeiden, dass schutzbedürftige Daten nur deshalb ungeschützt über das Internet übertragen werden, weil der Nutzer die Aktivierung der Verschlüsselung versäumt, baten wir das Innenministerium, die Verschlüsselung als Standard zu realisieren.

4.2 Entschließung zum automatischen Software-Update

Die Herstellung von Software ist ein fehlerträchtiges Geschäft. Diese leidvolle Erfahrung mussten die Benutzer machen, die im Berichtszeitraum von einer Flut neuer Viren heimgesucht wurden. Machten sich doch die Virenprogrammierer verstärkt die Softwarefehler in Betriebs- und Anwendungssystemen zu Nutze, um ihren Viren und sonstiger schadenstiftender Software zu einer hohen Verbreitung auf PCs zu verhelfen.

Um den Angriffen der Virenprogrammierer nicht hilflos ausgeliefert zu sein, stellen die Softwarehersteller unentgeltlich so genannte Software-Updates zur Verfügung. Andererseits versteht man unter einem Software-Update auch die nachträgliche Installation von Programmen und Softwarebibliotheken zur Beseitigung von Fehlern in einem installierten Programm, die vom Softwarehersteller zur Verfügung gestellt werden.

Bei der Durchführung eines Software-Updates, die auch über das Internet erfolgen kann, ist festzustellen, dass den Softwareherstellern weitreichende Zugriffsrechte auf den Rechnern ihrer Kunden eingeräumt werden müssen. Ob und welche personenbezogenen Daten von den Rechnern der Kunden an die Softwarehersteller übertragen werden, wird, wenn überhaupt, in kurzen Erklärungen mitgeteilt. Nachprüfbar sind diese Aussagen für die meisten Benutzer im Allgemeinen nicht.

Deshalb hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Berichtszeitraum eine Entschließung gefasst, die die datenschutzrechtlich zulässige Durchführung von Software-Updates zum Inhalt hat (s. Anhang 15).

Beim Software-Update haben sich im Wesentlichen zwei Vorgehensweisen herausgebildet: Eine Methode besteht darin, dass die Client-Rechner, auf denen die fehlerhafte Software installiert ist, automatisch nach dem Start oder wenn eine Verbindung in das Internet hergestellt wird mit einem Rechner des Softwareherstellers – dem so genannten Verteilserver – in Verbindung treten und anfragen, ob ein Software-Update für die installierte Software vorliegt, es gegebenenfalls übertragen und installieren. Die zweite Methode unterscheidet sich von der ersten darin, dass die Software-Updates von einem Verteilserver des Softwareherstellers auf einen zweiten Verteilserver, der der Sphäre des Kunden zugeordnet ist, übertragen und gespeichert werden. Die Clients treten beim Start mit diesem lokalen Verteilserver in Verbindung und installieren gegebenenfalls die auf diesem Verteilserver vorgehaltenen Software-Updates. Bei dieser Variante kann ein Administrator im Allgemeinen Einfluss darauf nehmen, ob ein Software-Update auf den Clients installiert werden soll.

Eine datenschutzrechtliche Prüfung hat ergeben, dass folgende Bedingungen hinsichtlich des technischen Datenschutzes an die Softwaresysteme, die automatische Software-Updates installieren, zu stellen sind:

– Zustimmung

  Die Installation eines Software-Updates darf nur nach vorheriger Zustimmung durchgeführt werden. Die Zustimmung kann nur von Personen erteilt werden, die für die Sicherheit des Systems verantwortlich sind. Für die Erteilung der Zustimmung ist es dann nicht erforderlich, dass sich ein Administrator zu jedem Arbeitsplatzrechner begibt, wenn ein lokaler Verteilserver eingesetzt wird. Das Einstellen des Software-Updates auf dem Verteilserver oder die Freigabe eines Software-Updates zur Installation auf den Clients ist der Zustimmung gleichzusetzen. Steht kein lokaler Verteilserver zur Verfügung, muss zwangsläufig bei jedem PC die Zustimmung direkt erteilt werden.

– Grundsatz der Datensparsamkeit

  Software-Updates sind nicht auf einzelne Personen zugeschnitten, sondern nur spezifisch auf ein Softwareprodukt. Daher kann es auch nicht erforderlich sein, dass personenbezogene Daten über die Benutzer, die mit einem entsprechenden Rechnersystem arbeiten, zu Zwecken der Durchführung eines Software-Updates an den Softwarehersteller übermittelt werden. Ein Lizenzschlüssel, der bei einer Installation eines Programms einzugeben ist, ist im Allgemeinen kein personenbezogenes Datum und darf vom Softwarehersteller zu Zwecken des Software-Updates abgerufen werden. Für die personenbezogenen Daten, die ein Benutzer in seinen Dateien speichert oder verarbeitet, gilt gleichfalls, dass eine Übermittlung der Dateien an die Softwarehersteller nicht zulässig ist. Die Daten, die im Rahmen des Software-Update-Prozesses vom Client an den Verteilserver übertragen werden, sollten sich also auf technische Daten, die den Zustand des Systems beschreiben und für die Durchführung eines Software-Updates notwendig sind, beschränken.

– Grundsatz der Datenvermeidung

  Ein Software-Update sollte nur die tatsächlich aufgetretenen Fehler der installierten Software beheben. Die Installation weiterer Software, die nicht der Fehlerbehebung dient und deren Funktionalität nicht benötigt wird, sollte nicht durchgeführt werden. Die Hersteller sollten zusätzliche Funktionalität in gesonderten Upgrades oder so genannten Optionpacks zur Verfügung stellen.

– Revisionssicherheit

  Zur Gewährleistung eines sicheren Betriebs gehört, dass man sich über den Sicherheitszustand des Systems im Klaren ist. Daher sollten die Softwarehersteller erklären, dass sie Software-Updates nicht nachträglich verändern. Sind Änderungen eines Software-Updates

notwendig, weil sich beispielsweise herausstellt, dass die Fehlerbehebung nur unzureichend ist, dann sollte hierfür ein weiteres Software-Update verwendet werden. Dann ist nachvollziehbar, welchen Sicherheitsstand ein Rechnersystem tatsächlich hat. Bedauerlicherweise war im Berichtszeitraum aufgrund gleicher Benennung unterschiedlicher Updates zu beobachten, dass nicht nur bei den Benutzern und Administratoren bisweilen eine große Verunsicherung darüber herrschte, welches Software-Update welchen Fehler behebt und auf welchen Systemen installiert werden muss.

– Übermittlungskontrolle

Da schon ein Fall bekannt geworden ist, wonach ein als Software-Update getarnter Computervirus über den Verteilmechanismus installiert werden sollte, ist es erforderlich, dass die Herkunft eines Software-Updates nachvollziehbar ist. Um dies zu gewährleisten, sollten von den Softwareherstellern Authentifikationsverfahren eingesetzt werden, die es ermöglichen, dass Software-Updates eindeutig auf Hersteller zurückgeführt werden können. Umgekehrt sollten Benutzer und Administratoren nur Software-Updates installieren, deren Herkunft zweifelsfrei festgestellt werden kann.

– Transportkontrolle

Der Transport der Software-Updates findet fast immer über das Internet statt. Die Integrität der Software-Updates muss daher durch einen Prüfmechanismus gewährleistet werden, der sicherstellt, dass die übertragenen Daten nicht während des Transports verändert wurden. Die Integritätsprüfung kann beispielsweise durch Verwendung so genannter Hashwert-Verfahren durchgeführt werden. Da es sich bei Software-Updates nicht um personenbezogene Daten handelt, ist eine Verschlüsselung bei der Übertragung nicht zwingend erforderlich.

– Verfügbarkeitskontrolle

Die Verträglichkeit eines Software-Updates mit der laufenden Produktionsumgebung sollte geprüft werden. Schließlich darf die Installation eines Updates nicht die ganze IT-Infrastruktur einer Behörde lahm legen. Zur Gewährleistung der Verfügbarkeitskontrolle sollte daher in einer Testumgebung nach Installation eines Software-Updates der Client hinsichtlich seiner Funktionalität geprüft werden. Das Ergebnis der Prüfung sollte Aufschluss darüber geben, welche Daten vom Client zum Verteilserver übertragen, welche Dateien auf dem Client ersetzt beziehungsweise gelöscht und welche Konfigurationsänderungen auf dem Client durchgeführt wurden. Wenn neben dem den Fehler behebenden Software-Update zusätzlich noch weitere Software aufgespielt oder die Konfiguration des Systems geändert wird, dann ist zu prüfen, welche zusätzlichen Komponenten installiert wurden und wie sie sich auf die Systemsicherheit auswirken. Gegebenenfalls müssen diese Komponenten nachträglich wieder entfernt werden. Bei Update-Systemen, die es erfordern, dass ein Client direkt mit einem Software-Verteilserver des Herstellers kommuniziert, kann ein einmaliger Test, der die datenschutzrechtliche Unbedenklichkeit zum Ergebnis hat, keine Gewähr dafür bieten, dass jede weitere Installation die gleichen Änderungen durchführt, steht es doch dem Softwarehersteller frei, das Software-Update nach seinem Gutdünken zu ändern.

Bei den zu installierenden Komponenten kann zwischen reinen Anwendungsdaten, wie beispielsweise Virensignaturen von Virenschutzprogrammen, und Programmen, die auf den Rechnern ausgeführt werden können, unterschieden werden. Beim Update von Virensignaturen kann eine vereinfachte Prüfung vorgenommen werden. Aber auch in diesem Fall sollte die Verteilung einer authentifizierbaren Virensignaturdatei auf die Clients von einem lokalen Verteilserver ausgehen.

– Datenverarbeitung im Auftrag

Wenn die beschriebenen Bedingungen nicht erfüllt sind, dann handelt es sich bei der Durchführung eines Software-Updates im Allgemeinen um eine Tätigkeit im Rahmen von Wartungsarbeiten, die der Softwarehersteller vornimmt. Bei einer Wartungstätigkeit, bei der auch personenbezogene Daten mit im Spiel sein können, handelt es sich nach allgemeiner Auffassung um eine Datenverarbeitung im Auftrag. Es wäre dann im öffentlichen Bereich in Baden-Württemberg § 7 LDSG anzuwenden, der unter anderem einen schriftlich abzufassenden datenschutzrechtlichen Vertrag zwischen Auftraggeber und Auftragnehmer erfordert.

Nur mit sicheren Systemen ist eine datenschutzrechtlich zulässige Verarbeitung personenbezogener Daten möglich. Die zeitnahe Installation von Software-Updates ist daher zu begrüßen, weil dadurch die Systemsicherheit eines Rechners oder Rechnernetzwerks insgesamt erhöht und damit dem Datenschutz in verstärktem Maße Genüge getan wird.

Allerdings muss auch die Durchführung des Software-Updates datenschutzrechtlich unbedenklich gestaltet sein.

5. Neue Technologien

Trotz des schlechten wirtschaftlichen Umfelds wird die IT-Branche nach wie vor von einem hohen Innovationspotenzial beherrscht. Neue Technologien der Hardware und Software werden weiterhin nahezu monatlich vorgestellt und am Markt eingeführt. Für den technischen Datenschutz in der Landesverwaltung bedeutet dies, dass die neuen Technologien darauf geprüft werden müssen, wie mit ihnen ein Höchstmaß an datenschutzrechtlich zulässigem Einsatz realisiert werden kann und welche Randbedingungen hierfür erfüllt werden müssen. In diesem Abschnitt stellen wir Auszüge der Tätigkeiten in diesem Bereich dar.

5.1 Datensicherheit beim Einsatz von Funknetzwerken (WLANs)

Nicht nur wenn es darum geht, Notebooks, Pocket-PCs oder andere mobile Geräte mit lokalen Computernetzen zu verbinden, kommt der Einsatz eines Funknetzwerks (Wireless Local Area Network, WLAN) in Frage. Auch bei der Vernetzung stationärer Computer fällt die Wahl immer öfter auf ein WLAN, das sich oft preiswert und schnell realisieren lässt. Die Technik ermöglicht zum einen die unmittelbare Kommunikation zwischen mehreren Geräten. Zum anderen gestattet sie die Integration mehrerer PCs, Notebooks oder anderer Geräte in ein stationäres, kabelgebundenes LAN. Dabei wird die Kommunikation über einen an das stationäre Netz angeschlossenen so genannten „Access-Point“ abgewickelt.

Auch öffentliche Stellen interessieren sich für den WLAN-Einsatz. Dabei geht es auch um Bereiche, in denen sensible Daten verarbeitet werden, wie z. B. Krankenhäuser. Diese erwarten Kosteneinsparungen, wenn sie zur Patientenbetreuung am Krankenbett Notebooks einsetzen können, die über WLAN mit dem Klinikinformationssystem verbunden sind. Aus Sicht des Datenschutzes ist bei der WLAN-Nutzung vorerst noch Zurückhaltung angebracht: Deren Technik umfasst zwar auch eine Reihe von Sicherheitsmaßnahmen, diese bieten bislang jedoch nur unzureichenden Schutz vor dem Abhören der übertragenen Daten sowie einem Eindringen fremder Nutzer in das lokale Netzwerk. Die WLAN-Technik ermöglicht standardmäßig folgende Schutzmaßnahmen:

– Örtliche Begrenzung des Sendebereichs

Die Sendeleistung der Komponenten und die Anordnung der Antennen ist so zu wählen, dass der Sendebereich möglichst wenig über den mit dem WLAN zu versorgenden räumlichen Bereich hinausreicht.

– Vergabe eines Netzwerknamens

  Für jedes WLAN kann ein Netzwerkname (SSID) vergeben werden. Um Zugang zu einem solchen Netz zu erhalten, muss man den Netzwerknamen kennen. Da der Netzwerkname jedoch im Klartext übertragen wird, lässt er sich durch Abhören des Funkverkehrs ermitteln. Zudem wird dieser Name von einigen Access-Points auf Anfrage mitgeteilt.

– MAC-Adress-Filterung

  Jede Netzwerkkarte, die einem PC, einem Notebook oder einem sonstigen Gerät die Teilnahme an der Netzwerkkommunikation ermöglicht, verfügt über eine weltweit eindeutige MAC-Adresse (MAC: Media Access Control). In Filterlisten des WLAN kann man darauf zurückgreifen und festlegen, welche Geräte mit welchen MAC-Adressen Zugang zum lokalen Netz erhalten dürfen.

  Die Sicherheit dieses Mechanismus ist jedoch dadurch begrenzt, dass sich MAC-Adressen ebenso wie die Netzwerknamen abhören lassen. Ein Angreifer kann dann die in seiner Hardware fest hinterlegte MAC-Adresse softwaretechnisch durch die abgehörte ersetzen. Darüber hinaus ist zu berücksichtigen, dass die manuelle Pflege derartiger Filterlisten, zumindest in größeren Netzwerken, vielfach als unpraktikabel angesehen wird.

– WEP-Verschlüsselung und Authentisierung (Wired Equivalent Protocol)

  Ein zentrales Sicherheitselement im WLAN ist die Verschlüsselung der übertragenen Daten. Das dafür standardmäßig eingesetzte WEP verwendet Schlüssel mit 40 oder 104 Bit Schlüssellänge. Daneben verwendet es weitere 24 Bit als so genannten Initialisierungsvektor (IV), der vor jedem Datenpaket unverschlüsselt übertragen wird. Diese WEP-Verschlüsselung weist eine Reihe von Unzulänglichkeiten auf:

  • In manchen Systemen werden die verwendeten Schlüssel im Klartext abgespeichert.
  • Eine Schlüssellänge von 40 Bit ist zu niedrig.
  • Die Länge des Initialisierungsvektors (24 Bit) ist zu niedrig.
  • Der verwendete RC4-Algorithmus weist konzeptionelle Lücken auf und ist dadurch angreifbar.

  Insgesamt bedeutet dies, dass die WEP-Verschlüsselung nicht ausgereift ist und noch vielfältige Angriffspunkte bietet.

Um diese Sicherheitslücken zu schließen, sollen im WLAN kommender Generationen statt des RC4-Algorithmus eine Verschlüsselung mit Hilfe des AES (Advanced Encryption Standard) vorgenommen und höhere Schlüssellängen verwendet werden. Zudem sind weitere Veränderungen geplant, um auch unberechtigtes Anmelden an vorhandenen Funknetzwerken zu erschweren. Es ist gegenwärtig noch zu früh, um darüber zu urteilen, ob diese Techniken einen ausreichenden Schutz der übertragenen Daten bieten können. Nach den bisherigen Erfahrungen erscheint es jedoch in jedem Fall angebracht abzuwarten, ob sich die künftigen Produkte im Praxisbetrieb als sicher erweisen. Solange das nicht der Fall ist, kommt der Einsatz von WLAN, soweit nur die o. g. Standardsicherungsmaßnahmen ergriffen worden sind, zumindest in solchen Umgebungen nicht in Betracht, in denen personenbezogene oder andere schutzbedürftige Daten verarbeitet werden.

Wer trotz der gegenwärtig bestehenden sicherheitstechnischen Unzulänglichkeiten ein WLAN einrichten und damit auch personenbezogene oder andere schutzbedürftige Daten verarbeiten will, muss zusätzliche Maßnahmen ergreifen, die die bestehenden Sicherheitslücken schließen. An Folgendes ist dabei zu denken:

– Verschlüsselung

Zum Schutz der übertragenen Daten vor unberechtigter Kenntnisnahme und Veränderung ist eine als sicher angesehene Verschlüsselung, etwa durch ein auf IPSec beruhendes virtuelles privates Netzwerk (VPN), zu realisieren.

– Identifikation der zugelassenen Geräte und Nutzer

Zusätzliche Sicherheitsmaßnahmen sind auch zu ergreifen, um eine zuverlässige Identifikation der zugelassenen Geräte und Nutzer vornehmen zu können. Dazu kommt etwa die Verwendung eines so genannten RADIUS-Servers (Remote Authentication Dial-In User Service) in Betracht.

– Kontrollierte Datenflüsse zwischen Fest- und Funknetz

Ähnlich wie beim Anschluss eines lokalen Netzwerks an das Internet ist der Übergang zwischen dem stationären Teil eines LAN und den über Funk eingebundenen Komponenten durch eine Firewall so zu sichern, dass an dieser Schnittstelle nur solche Datenströme gestattet werden, die zuvor ausdrücklich zugelassen wurden. Alle anderen Kommunikationswünsche werden abgewiesen.

– Administration des Access-Point

Es sind sichere Wege für die Administration der Funknetzkomponenten vorzusehen. Diese sollten nicht über Funk administriert werden können. Die Administration sollte nicht mit Hilfe von Diensten wie Telnet erfolgen, die die zur Anmeldung erforderlichen Passwörter im Klartext übertragen. Sofern jemand versucht, sich als Administrator anzumelden, sollte dies eine Alarmmeldung auslösen.

5.2 Bluetooth – datenschutzrechtlich auf den Zahn gefühlt

Neben WLAN für die Funkvernetzung gibt es für mobile Geräte wie Handy oder Notebook sowie für Peripheriegeräte wie Maus, Tastatur oder Headset einen weiteren, sich rasch verbreitenden Standard namens Bluetooth, der die drahtlose Übertragung von Daten und Sprache bis zu einer Entfernung von zehn Metern ermöglicht. Bei Funkverbindungen besteht die Gefahr, dass Unberechtigte diese Daten abhören können, natürlich auch dann, wenn personenbezogene Daten mit im Spiel sind. Deshalb müssen bei Verwendung von Bluetooth Maßnahmen zur Übermittlungskontrolle und Transportkontrolle ergriffen werden. Folgendes muss beim Einsatz von Bluetooth bedacht werden:

– Entdeckung

Ein Bluetooth-fähiges Gerät nimmt andere Geräte in seinem Sendebereich wahr, indem es betriebsbereite Geräte in seiner Umgebung abfragt. Das Gerät kennt dann die weltweit eindeutigen, 48 Bit langen Adressen aller Geräte in seinem Sendebereich. Damit unbefugte Geräte nicht Kenntnis von der Geräteadresse erlangen, sollte bei sicherheitskritischen Geräten der Betriebszustand auf „non discoverable“ (nicht entdeckbar) eingestellt werden. Dann ist das Gerät „unsichtbar“ und kann nur auf eigene Initiative hin eine Verbindung mit einem anderen Gerät aufbauen. Ist dies nicht möglich und handelt es sich um ein mobiles Gerät, dann besteht die Gefahr, dass ein Bewegungsprofil des Geräts und damit seines Benutzers erstellt werden kann.

– „Paarung“

Damit zwei Bluetooth-Geräte miteinander kommunizieren können, müssen sie auf logischer Ebene gekoppelt werden. Dies geschieht durch eine so genannte Paarung. Für die Koppelung verwendet Bluetooth eine PIN. Sie ist entweder fest in das Gerät eingebaut (Funkmaus, Headset) oder muss vom Benutzer eingegeben werden. Zur Koppelung ist auf beiden Geräten die gleiche PIN einzugeben. Für die Gewährleistung der Sicherheit der Verbindung ist die Länge und

Komplexität der PIN wichtig, da aus ihr eine Reihe von Schlüsseln, die die Verbindung absichern, generiert wird. Die PIN muss mindestens ein Zeichen und kann höchstens 16 Zeichen lang sein. Es sollte eine PIN gewählt werden, die nicht leicht „erratbar“ ist (Beispiel: 1234) und mindestens acht Zeichen umfasst. Wenn möglich, sollten von Herstellern getroffene Voreinstellungen der PIN geändert werden. Wurde die beabsichtigte Koppelung zwischen zwei Geräten durchgeführt und sollen keine weiteren Verbindungen mit anderen Geräten aufgebaut werden, dann sollten die Geräte in einen Betriebszustand gesetzt werden, bei dem keine weiteren Koppelungen mehr durchgeführt werden können („non-pairable“).

Damit zwei Geräte miteinander kommunizieren können, ist die Berechnung eines Verbindungsschlüssels notwendig. Laut Spezifikation kann hierfür auch der Geräteschlüssel verwendet werden. Dieser wird durch die Paarung mit anderen Geräten auch diesen bekannt. Dadurch können andere Geräte die Kommunikation abhören. Geht ein mobiles Gerät verloren oder wird außer Betrieb genommen, dann ist weiterhin auf allen Geräten, mit denen es gekoppelt wurde, der Verbindungsschlüssel gespeichert. Wenn der Verbindungsschlüssel ein Geräteschlüssel ist, dann kann man mit Kenntnis der Geräteadresse und gewissem technischen Aufwand ein nicht gekoppeltes Gerät so programmieren, dass es an Stelle des ursprünglichen Geräts eingesetzt werden kann und dadurch unberechtigte Zugriffe ermöglicht werden. Dem kann dadurch begegnet werden, dass man die Verbindungsschlüssel auf den verbleibenden Geräten löscht.

– Authentifizierung

Damit ihre Geräte mit möglichst vielen anderen Geräten problemlos kommunizieren können, wählen die Hersteller der Sicherheit nicht dienliche Standardeinstellungen, wie beispielsweise deaktivierte Authentifizierung und Verschlüsselung. Authentifizierung und Verschlüsselung sind aber bei der Verarbeitung personenbezogener Daten erforderlich.

Weiter ist zu bedenken, dass die Authentifizierung bei Bluetooth auf der Ebene der Geräte stattfindet. Eine Benutzerauthentifizierung kennt Bluetooth derzeit nicht. Das bedeutet, dass auch der unbefugte Besitzer alle mit einem Gerät möglichen Verbindungen nutzen kann. Wenn personenbezogene Daten verarbeitet werden, sollte deshalb eine Benutzerauthentifizierung in der Anwendung durchgeführt werden.

– Verschlüsselung

Der Bluetooth-Standard bietet die Möglichkeit, die Daten bei der Übertragung zu verschlüsseln. Es wird ein Stromverschlüsselungsverfahren namens E0 eingesetzt. Bei Geräten einfacher Funktionsart ist eine Verschlüsselung beim Aufbau einer Verbindung nicht erforderlich; vielmehr muss die Verbindungsverschlüsselung optional angefordert werden. Bevor Daten verschlüsselt übertragen werden, muss sich mindestens eines der Geräte gegenüber dem anderen authentifizieren. Aus dem dabei gewonnenen Authentifizierungsschlüssel wird der Schlüssel für die Verschlüsselung gewonnen. Dies bedeutet, dass eine Verschlüsselung bei der Datenübertragung von zwei Geräten, die beide nicht die Fähigkeit zur Authentifizierung haben, nicht möglich ist.

Wenn eine Verschlüsselung gewünscht wird, tauschen im Fall einer Punkt-zu-Punkt-Verschlüsselung die beteiligten Geräte einen Verschlüsselungsschlüssel aus. Dabei einigen sich die Geräte auf einen kleinsten Nenner. Sind einfache Geräte beteiligt, dann kann dieser Schlüssel der Geräteschlüssel sein. Während diese Einschränkung bei einer Funkmaus oder einer Fernsteuerung nicht problematisch ist, ist es beispielsweise bei einer Funktastatur bedenklich, wenn der Verbindungsschlüssel des Geräts mit dem Geräteschlüssel identisch ist. Denn dann besteht die Gefahr, dass der Geräteschlüssel nicht die

erforderliche Schlüssellänge hat oder dass der Geräteschlüssel anderen Geräten möglicherweise durch andere Kommunikationsbeziehungen bekannt ist (Beispiel: zwei PCs und eine Funktastatur).

Zur Stromverschlüsselung von Bluetooth ist zu sagen, dass die Qualität der Verschlüsselung vermutlich erst nach einer gewissen Zeit verlässlich eingeschätzt werden kann. Mathematisch bewiesen wurde beispielsweise schon, dass das Verschlüsselungsverfahren nicht so stark ist, wie die Schlüssellänge von 128 Bit vermuten lässt.

– Unsichere Einstellungen

Wie schon dargestellt, enthalten Bluetooth-Geräte eine Konfiguration ab Werk, die aus dem Namen des Geräts und einer PIN besteht. Weiterhin können Bluetooth-Geräte so konfiguriert sein, dass festgelegt werden kann, ob das Gerät für andere Geräte sichtbar, mit anderen Geräten koppelbar ist und ob es den Aufbau einer Verbindung zulässt. Vor Inbetriebnahme sollten diese Einstellungen geprüft und gegebenenfalls rekonfiguriert werden. Wird ein Gerät nicht gebraucht, dann empfiehlt es sich, dass der Arbeitsmodus auf „non connectable“ (nicht verbindbar) eingestellt wird.

– Sicherheitsbetriebsarten

Bluetooth kennt beim Betrieb drei verschiedene Sicherheitsmodi. Nur der Sicherheitsmodus 3 gewährleistet, dass sich die Kommunikationspartner beim Aufbau einer Verbindung gegenseitig authentifizieren müssen. Dieser Modus sollte daher bei der Übertragung und Verarbeitung von personenbezogenen Daten gewählt werden.

Ersatzweise kann der Modus 2, der die Authentifizierung beim Verbindungsaufbau abhängig von der Charakteristik der beteiligten Geräte erfordert, gewählt werden, wenn an der Kommunikation Geräte beteiligt sind, mit denen schon eine Koppelung durchgeführt wurde.

Da das Innovationstempo bei Bluetooth, bedingt durch die Marktdynamik mit laut Presseberichten ca. 1 200 Geräten und durch die Fortschreibung des Standards, weiterhin hoch ist, können diese Hinweise nicht abschließend sein. Erfahrungsgemäß kommt es durch Implementierungen, die aus unterschiedlicher Interpretation des Standards resultieren, immer wieder zu Situationen, die die Sicherheit beeinträchtigen. Hier gilt es, die Entwicklung weiterhin zu beobachten.

5.3 Nutzung von DSL-Technik

Die Preisentwicklung bei Kommunikationsverbindungen über das Internet veranlasst Gemeinden auf der Suche nach Einsparpotenzialen, die Kommunikation zwischen den Standorten der Gemeindeverwaltung oder gemeindenahen Institutionen darüber abzuwickeln. Dagegen ist nichts einzuwenden, wenn die Anforderungen an die Sicherheit erfüllt werden. Eine Gemeinde ist nämlich in der Regel auch Teilnehmer an weiteren Rechnernetzen wie beispielsweise das Kommunale Verwaltungsnetz (KVN). Daher ist eine unsichere Anbindung an das Internet auch eine Bedrohung für die Sicherheit weiterer, nicht zur Gemeinde gehörender Rechner und Rechnernetze.

Konkret ging es im Berichtszeitraum um eine Gemeinde, die eine DSL-Verbindung zwischen zwei Standorten der Gemeindeverwaltung über das Internet schalten wollte. Ein Mitarbeiter der Gemeinde schilderte telefonisch, dass eine digitale Hochgeschwindigkeitsverbindung (DSL) für die Kommunikation zwischen zwei Standorten hergestellt werden sollte. Mit der DSL-Technik ist es aber im Gegensatz zu ISDN nicht möglich, mit einem bestimmten Kommunikationspartner in Verbindung zu treten, sondern es wird nur eine Verbindung zu einem Telekommunikationsprovider aufgebaut, über die Daten in das Internet geschickt werden können. Meine Mitarbeiter gingen daher davon aus, dass es sich um eine so genannte DSL-flat-rate-Verbindung handeln würde, die über

fest zugewiesene IP-Adressen permanent eine Verbindung zwischen den zwei Standorten über das Internet ermöglicht, und baten um eine schriftliche Darstellung insbesondere der Maßnahmen zur Gewährleistung der Sicherheit der Rechner und Rechnernetze. In der äußerst kurz gefassten Antwort tauchte der Begriff DSL überhaupt nicht auf. Statt dessen war die Rede von ISDN-Ports und festen IP-Adressen, die den Routern zugewiesen wären und dass die Verbindung abgebaut würde, wenn keine Daten mehr zu übertragen wären. Von dieser unerwarteten technischen Erklärung überrascht und auch aufgrund der fehlenden Beschreibung von Sicherheitsmaßnahmen baten meine Mitarbeiter um Klärung, wie sich die Dinge denn jetzt verhielten: ISDN oder DSL?

Als Antwort erhielten wir, dass beides verwendet würde. Die ISDN-Verbindung solle als Punkt-zu-Punkt-Verbindung eingesetzt werden; eine nicht permanente Verbindung über das Internet, die es ermöglicht, private Netzwerke über ein öffentliches Netz zu verbinden (VPN), solle als DSL-Verbindung aufgebaut werden. Wir vermuteten, dass aus Gründen der Redundanz diese Vorgehensweise gewählt wurde, konnten uns aber nicht erklären, wie eine VPN-Verbindung über eine beidseitig nicht permanente DSL-Verbindung aufgebaut wird. Woher weiß die Datenquelle von der bei jedem Verbindungsaufbau dynamisch zugewiesenen IP-Adresse des Kommunikationspartners? Daher wurde die Gemeinde erneut gebeten, die Lösung für dieses Problem zu beschreiben. Die Antwort war, dass die ISDN-Verbindung nicht zur Datenübertragung benutzt würde, sondern nur zum Aufbau einer VPN-Verbindung über die jeweils aufzubauende DSL-Verbindung. Damit waren im vierten Anlauf die Dinge wenigstens formal geklärt. Der Verbindungsaufbau soll dabei wohl so laufen, dass dann, wenn Daten zwischen den zwei Standorten ausgetauscht werden sollen, jeweils die Datenquelle eine DSL-Verbindung eröffnet und ihr dabei eine IP-Adresse zugewiesen wird. Die Datenquelle baut daraufhin ihrerseits eine ISDN-Punkt-zu-Punkt-Verbindung zum Kommunikationspartner auf und teilt diesem ihre IP-Adresse mit, worauf der Kommunikationspartner eine DSL-Verbindung zum Internet herstellt und die dabei zugewiesene IP-Adresse über die ISDN-Verbindung der Datenquelle rückmeldet. Nachdem beide Kommunikationspartner in Kenntnis der IP-Adresse des anderen gelangt sind, kann eine abgesicherte IP-Verbindung (IPSec) aufgebaut werden. Fraglich war, über welches Protokoll die IP-Adressen der DSL-Verbindung über die ISDN-Verbindung übertragen werden. Hierfür gibt es zwei Möglichkeiten. Die eine besteht in der Übertragung mit dem ISDN-Protokoll. Die zweite Alternative besteht im Aufbau einer TCP/IP-Verbindung über die ISDN-Strecke. Ein gängiges Standardprotokoll von TCP/IP, das die gewünschte Kommunikation realisiert, ist meinen Mitarbeitern nicht bekannt. Da der Verbindungsaufbau vollständig von den Routern durchgeführt wird, handelt es sich vermutlich um ein firmenspezifisches Protokoll des Herstellers der Router. Weil die Sicherheit dieses Protokolls für eine Abschätzung der Sicherheit der Lösung nicht unerheblich ist und dem WWW-Angebot des Herstellers keine Erkenntnisse darüber zu entnehmen waren, setzten sich meine Mitarbeiter erneut mit der Gemeinde in Verbindung und baten um eine detailliertere Beschreibung, wie der Verbindungsaufbau einer IPSec-DSL-Verbindung unter Vermittlung einer ISDN-Verbindung tatsächlich funktioniert. Eine derartige Beschreibung muss es gegeben haben, wie sonst hätte die skizzierte Lösung entwickelt werden können. Die Gemeinde teilte daraufhin mit, dass man in Anbetracht des Termindrucks die Schaltung einer Standleitung in Auftrag gegeben habe.

Fazit aus dieser Geschichte:

In der schnelllebigen Welt der Informations- und Kommunikationsbranche ist das Innovationstempo nach wie vor sehr hoch. Hier den Überblick zu behalten ist kaum möglich. Daher ist es für die Erstellung einer datenschutzrechtlichen Stellungnahme erforderlich, das Sicherheitskonzept, insbesondere wenn neue Technologien eingesetzt werden, nachvollziehen zu können. Eingaben an den Landesbeauftragten für den

Datenschutz müssen daher so detailliert sein, dass meine Mitarbeiter aus dem Sicherheitskonzept die datenschutzrechtlich relevanten Zusammenhänge nachvollziehen können.

5.4 Zugriffskontrolle bei USB

Eine große Vielfalt von externen Geräten wie Drucker, Modem, Scanner, Chipkartenlesegerät, PDA-Synchronisationsstation usw. können an PCs angeschlossen werden. Bisher verfügten die meisten PCs nicht über genügend Anschlüsse, um die von den Benutzern benötigten Geräte an einem PC gleichzeitig betreiben zu können. Ein Gerät im laufenden Betrieb auszustecken und ein anderes Gerät anzuschließen, war in der Vergangenheit nicht möglich, da beim Start des PCs fest vorgegeben war, an welcher Schnittstelle welches Gerät angeschlossen werden musste. Die Aufrüstung mit weiteren Schnittstellen konnte meist deshalb keine Abhilfe schaffen, weil es beispielsweise dadurch zu Konflikten kam, dass zwei unterschiedliche Geräte anwendungsbedingt den gleichen Anschluss hätten belegen müssen. Und angesichts von Prozessortaktraten im Gigahertzbereich ist die Übertragungsgeschwindigkeit der in die Jahre gekommenen seriellen und parallelen Schnittstellen alles andere als hoch.

Um aus dieser Misere herauszukommen, haben sich die Rechnerhersteller in nicht ganz uneigennütziger Art der Angelegenheit angenommen und uns schon vor geraumer Zeit mit einer neuen Schnittstelle namens USB (Universal Serial Bus) bedacht, die schneller arbeitet, mehr Anschlüsse bietet und im laufenden Betrieb auswechselbare Geräte unterstützt, die beim Ein- und Ausstecken automatisch konfiguriert werden. Nunmehr wird die Schnittstelle in der wesentlich schnelleren Version 2.0 in nahezu jeden PC gleich mehrfach eingebaut und von den Herstellern externer Zusatzgeräte, so genannter Peripherie, reichlich mit neuer Hardware in Form von einsteckbaren Halbleiterspeichern, externen Festplatten, CD-RW/DVD-RW-Laufwerken, Netzwerkanschlüssen und diversen anderen Geräten bedacht.

Eine Untersuchung der neuen Schnittstelle unter dem Gesichtspunkt des technischen Datenschutzes zeigt, dass bei Rechnern, die über eine oder mehrere USB-Schnittstellen verfügen, Maßnahmen ergriffen werden müssen, um mit diesen Rechnern weiterhin einen datenschutzrechtlich zulässigen Betrieb zu gewährleisten. Folgenden Gefährdungen muss beim Betrieb von Rechnern mit USB-Schnittstelle begegnet werden:

– Booten

  Vermehrt werden Rechner angeboten, mit denen es möglich ist, über ein an einem USB-Port angeschlossenes Speichergerät den Rechner statt mit dem auf der Festplatte gespeicherten Betriebssystem mit einem auf dem Speichergerät vorgehaltenen alternativen Betriebssystem zu starten. Nach einem derartigen Startvorgang kann man auf die lokale Festplatte, die das alternative Betriebssystem meist ohne zusätzliche Aktivitäten einbindet, lesend und schreibend zugreifen, da die Zugriffsrechte für die Dateien der lokalen Festplatte, die vom ursprünglichen Betriebssystem vorgegeben werden, nicht für das alternative Betriebssystem gelten. Ein Benutzer, der sich am alternativen Betriebssystem anmeldet, kann so auf personenbezogene Daten zugreifen, für deren Zugriff er nicht berechtigt ist.

– Speicher

  Es werden mehrere Arten von Geräten angeboten, die an eine USB-Schnittstelle angeschlossen werden können, um Daten auf ihnen zu speichern. Angefangen bei Halbleiterspeichern mit 16 bis 1 000 Megabyte Kapazität über CD/DVD-Brenner mit Kapazitäten von 600 bis 4 300 Megabyte bis hin zu Festplatten mit Kapazitäten im dreistelligen Gigabytebereich. Aber auch Kartenlesegeräte für Halbleiterspeicher, wie sie in digitalen Kameras eingesetzt werden, zählen dazu. Durch den Anschluss von derartigen Speichern ist es möglich, Kopien von Dateien, in denen personenbezogene Daten gespeichert

sind, zu erstellen. Es müssen daher Maßnahmen ergriffen werden, die sicherstellen, dass Unbefugte kein Gerät an eine USB-Schnittstelle anschließen und nutzen können, das zur Speicherung von Dateien, die personenbezogene Daten enthalten, verwendet werden kann.

– Netzwerk

Des Weiteren sind Geräte problematisch, die es ermöglichen, über die USB-Schnittstelle eine Netzwerkverbindung aufzubauen. Hier werden Geräte angeboten, mit denen ein PC in Funknetze (WLAN, Bluetooth) oder konventionelle Netze (Ethernet) eingebunden werden kann. Ebenfalls werden Modems angeboten, mit denen über das Festnetz eine Verbindung zu anderen Rechnern hergestellt werden kann. Dadurch wird nicht nur eine Speicherung von personenbezogenen Daten auf einem anderen Rechner möglich, sondern es ist über diesen Weg auch möglich, von anderen Rechnern aus auf das Betriebssystem zuzugreifen und den Rechner aus der Ferne zu steuern.

Zur Abwehr der dargestellten Gefährdungen müssen folgende Maßnahmen ergriffen werden:

– Booten

Einfache Betriebssysteme können auf den schon jetzt erhältlichen Speichersteckern mit einer Kapazität bis ein Gigabyte installiert werden. Mit der nächsten Generation der Speicherstecker wird es möglich sein, darauf ein Client- oder Serverbetriebssystem, wie es in der Landesverwaltung überwiegend eingesetzt wird, zu installieren und damit einen anderen Rechner zu starten. Daher muss zur Gewährleistung einer effektiven Speicherkontrolle ausgeschlossen werden, dass alternative Betriebssysteme von USB-Geräten gestartet werden können. Ob ein Betriebssystem von einem USB-Gerät gebootet werden kann, entscheidet sich durch die Einstellungen im so genannten BIOS. Zu berücksichtigen ist ferner, dass Speicherstecker jedes beliebige Speichermedium wie Diskette, Festplatte, CD-ROM etc. nachbilden können. Es muss daher bei der Konfiguration des Systems darauf geachtet werden, dass im BIOS die Einstellungen so vorgenommen werden, dass Geräte des BIOS mit Namen usb-hdd, usb-cdrom, usb-fdd, usb-zip und möglicherweise weitere Geräte nicht als bootfähig gekennzeichnet sind. Wenn durch Konfiguration nicht verhindert werden kann, dass von einem externen USB-Gerät gebootet werden kann, dann sollten die Inhalte der lokalen Festplatte verschlüsselt werden. Dadurch wird der ungehinderte Zugriff durch ein alternatives Betriebssystem auf die lokale Festplatte unterbunden, da nur nach Eingabe eines Schlüssels ein unchiffrierter Zugriff möglich wird.

– Speicherung

Ob ein Benutzer auf ein an einer USB-Schnittstelle angeschlossenes Speichermedium zugreifen darf, wird auf der Ebene des Betriebssystems festgelegt. Das Betriebssystem muss zur effektiven Speicherkontrolle über Mechanismen verfügen, die es ermöglichen, den Zugriff lesend und schreibend für einzelne Benutzer festlegen zu können.

Externe Speichergeräte, die an einen USB-Anschluss angeschlossen werden können, sind den mobilen Speichermedien zuzurechnen. Werden auf mobilen Datenträgern personenbezogene Daten gespeichert, dann müssen im Rahmen der Datenträgerkontrolle die gleichen Schutzmaßnahmen wie bei sonstigen mobilen Datenträgern (Bänder, Disketten, etc.) ergriffen werden, etwa Verschlüsselung und gesicherte Aufbewahrung.

– Netzwerk

Eine effektive Übermittlungskontrolle erfordert, dass Netzwerkverbindungen nur mit Kommunikationspartnern aufgebaut werden kön-

nen, mit denen eine Verbindung eingegangen werden soll. Das bedeutet, dass das Betriebssystem so konfiguriert werden muss, dass bei Anschluss eines Vermittlungsgeräts an eine USB-Schnittstelle dieses nur dann in das Betriebssystem eingebunden werden darf, wenn der jeweilige Benutzer eine Verbindung über dieses Gerät aufbauen darf. Ist das Gerät als Betriebsmittel eingebunden, dann müssen zur Gewährleistung der Übermittlungskontrolle die gleichen Maßnahmen wie beispielsweise bei einem herkömmlichen Ethernet- oder Modemanschluss ergriffen werden.

Wenn zulässige Verbindungen aufgebaut werden dürfen, ist es im Sinne einer effektiven Transportkontrolle notwendig, dass personenbezogene Daten bei der Übertragung nicht von Dritten gelesen oder verändert werden können.

Die zur technischen Realisierung der Maßnahmen notwendigen Vorkehrungen sind bei dem in der Landesverwaltung überwiegend eingesetzten Betriebssystem auf der Ebene der administrativen Berechtigungsverwaltung nicht vorhanden. Zwar gibt es eine Reihe von Behelfslösungen, wie durch entsprechende Einträge in der Systemkonfiguration oder durch Löschen bestimmter Treiberdateien der Zugriff ganz unterbunden werden kann. Wenn auf einem PC mehrere Benutzer arbeiten, von denen einer auf ein USB-Gerät zugreifen muss, während den anderen Benutzern ein Zugriff nicht gewährt werden soll, sind diese Lösungen nicht praktikabel, da sie auf alle Benutzer wirken. Eine Beschränkung des Zugriffs mit so genannten access control lists (ACL) kann benutzerspezifisch durch Verwendung zusätzlicher kommerziell erhältlicher Produkte erreicht werden.

Bei Betriebssystemen, die Geräte auf das Dateisystem abbilden, können Systemmanager über Dateiberechtigungen und ACL lesenden oder schreibenden Zugriff benutzerspezifisch regeln.

6. Datenspuren bei der Bürokommunikation – Was Word und andere Standardprogramme erkennen lassen

Programme zur Textverarbeitung sind aus vielen Computern nicht mehr wegzudenken. Die Ministerien des Landes haben für sich und die ihnen nachgeordneten Dienststellen festgelegt, dass dort in der Regel die Office-Produkte der Firma Microsoft eingesetzt werden. Bereits in unserem 20. Tätigkeitsbericht (LT-Drs. 12/4600, S. 27 f.) informierten wir darüber, dass das Textverarbeitungsprogramm Word 97 einige Funktionen enthält, deren unbedachte Nutzung mitunter auch Datenschutzverstöße nach sich ziehen kann. Als besonders problematisch hat sich dabei die Eigenschaft erwiesen, in jedem Dokument automatisch eine Reihe von Informationen zu speichern, die auf den ersten und manchmal auch auf den zweiten Blick nicht zu erkennen sind. Wird ein solches Dokument per E-Mail versandt oder im Internet veröffentlicht, kann jeder, der das Dokument elektronisch erhält, diese Informationen lesen und so möglicherweise auch personenbezogene Angelegenheiten erfahren, die nicht für ihn bestimmt sind. Obwohl die Problematik als solche nicht neu ist, stellen wir doch immer wieder fest, dass sie auch heute noch vielen Nutzern unbekannt ist, die tagtäglich mit diesen Produkten arbeiten.

– Automatische Erfassung einiger Dateieigenschaften:

Die von uns verwendeten Versionen von Word 97, Word 2000, Word 2002 sowie Word 2003 speichern für jedes damit bearbeitete Dokument eine Reihe so genannter Dateieigenschaften, die im Programm durch Auswahl von „Eigenschaften“ im Menü „Datei“ sichtbar gemacht werden können. Folgende darin enthaltene Angaben können datenschutzrechtlich problematisch sein:

• Titel

Im Feld „Titel“ der Maske „Eigenschaften“ erfasst Word automatisch den ersten Satz des Dokuments, der sich darin beim ersten Speichern nach der Neuanlage des Dokuments befindet. Sofern es sich dabei um einen längeren Satz handelt, werden davon mehr als zwei Zeilen (max.

254 Zeichen) erfasst. Entsprechendes gilt auch, wenn man nach Neuanlage eines Dokuments gleich einen längeren Text dort hineinkopiert. Sofern dieser Eintrag nicht durch den Benutzer geändert wird, bleibt er so lang unverändert stehen wie das Dokument besteht. Datenschutzrechtlich problematisch ist daran, dass dieser Satz auch dann noch als „Titel“ gespeichert bleibt, wenn er längst aus dem Text des Dokuments wieder entfernt wurde.

- Autor und letzter Bearbeiter

  Im Feld „Autor“ registriert Word automatisch den Benutzernamen des Anwenders, der das Dokument angelegt hat. Dafür greift Word auf die Bezeichnung zurück, die es vom Benutzer beim erstmaligen Starten des Programms erfragt hat. In der Registerkarte „Statistik“ weist Word außerdem stets noch nach, wer das Dokument zuletzt gespeichert hat.

- Version und Bearbeitungsdauer

  Unter Version gibt Word auf der Registerkarte Statistik an, wie oft das Dokument seit seiner Neuanlage nach Veränderungen erneut gespeichert wurde. Dieser Wert gibt Auskunft darüber, wie oft ein Dokument verändert wurde. Ergänzt werden diese Informationen durch Angabe der Zeiten für die Neuanlage des Dokuments und dessen letztmalige Speicherung.

– Verborgene Erfassung weiterer Zusatzinformationen zum Dokument

  Im Gegensatz zu den unter „Eigenschaften“ angesprochenen Meta-Informationen erfasst Word daneben auch eine Reihe weiterer Informationen über ein Dokument, die nur dann sichtbar werden, wenn man das Dokument mit einem einfachen Texteditor wie Notepad öffnet.

  - Speicherort

    Wird eine Datei gespeichert, registrierten die von uns genutzten Versionen von Word 97 sowie Word 2000 in den im .doc-Format bearbeiteten Dokumenten nicht allein die Anzahl der Speicherungen, sondern sie erfassen dazu jeweils den vollständigen Dateipfad, unter dem das Dokument abgespeichert wird. Wird eine Datei mehrmals unter verschiedenen Dateipfaden gespeichert, so werden alle Dateipfade registriert. Auch auf diese Weise können unbeabsichtigt vielfältige Informationen, die nicht im Dokument als solchem enthalten sind, elektronisch an Dritte weitergegeben werden:

    Im Dateipfad können, etwa als Teil der Bezeichnungen persönlicher Ablagen, die Namen der Mitarbeiter erkennbar sein, die das Dokument bearbeitet haben.

    Enthält der Dateiname beispielsweise den Namen des Empfängers, so wird dies spätestens dann problematisch, wenn ein solches Dokument als Vorlage für ein Schreiben an einen anderen Empfänger verwendet wird. Dieser kann dann erkennen, an wen ein ähnliches oder sogar gleichlautendes Schreiben zuvor bereits versandt wurde.

  - Drucker

    Word 97 sowie Word 2000 registrieren in den im .doc-Format bearbeiteten Dokumenten zudem die Typenbezeichnung der Drucker, auf denen das Dokument ausgedruckt wurde. Da für jeden Ausdruck ein erneuter Eintrag erfolgt, lässt sich anhand dessen auch nachvollziehen, wie oft das Dokument überhaupt ausgedruckt wurde. Dies kann dem Empfänger einen weiteren Anhaltspunkt dafür liefern, wie intensiv an dem Schreiben vor dessen Versand gearbeitet wurde.

  - Mittlerweile gelöschte Textpassagen

    Ist bei den Einstellungen unter „Extras“ – „Optionen“ auf der Registerkarte „Speichern“ die Option „Schnellspeicherung zulassen“ ausge-

wählt, so bleiben in den von uns mit Word 97, Word 2000, Word 2002 sowie Word 2003 im .doc-Format bearbeiteten Dokumenten auch solche Textabschnitte enthalten, die früher einmal im Text der Dokumente enthalten waren, aber mittlerweile aus dem Dokument entfernt wurden und folglich von Word beim Öffnen des Dokuments auch nicht mehr angezeigt werden. Es liegt auf der Hand, dass es sich dabei um eine höchst problematische Eigenschaft handelt. Umso mehr überrascht es, dass diese Eigenschaft auch in den folgenden Versionen wieder aufgetreten ist.

Welche Konsequenzen sind aus diesen Feststellungen zu ziehen?

Jede Dienststelle und auch jeder einzelne Nutzer, der tagtäglich mit diesen Produkten arbeitet, sollte die erwähnten Eigenschaften kennen und entsprechende Vorsichts- und Schutzmaßnahmen ergreifen. Die oben angesprochenen Datenspuren lassen sich zwar nicht vollständig unterbinden, deren datenschutzrechtliche Brisanz lässt sich jedoch entschärfen:

– Um zu verhindern, dass Word den Namen oder ein charakteristisches Kürzel eines Bearbeiters im Dokument speichert, kann man für alle Benutzer einer Einrichtung einheitlich als Benutzernamen eine neutrale Bezeichnung wie z. B. „user“ verwenden.

– Um zu verhindern, dass jemand die Speicherorte, die Druckernamen sowie eventuell vorhandene versteckte Informationen erkennen kann, kommt die Speicherung des Dokuments im RTF- oder dem von Word 2003 unterstützten XML-Format in Frage, in denen die versteckten Informationen nicht enthalten sind. Zu bedenken ist aber, dass auch in RTF- oder XML-Dokumenten die o. g. Dateieigenschaften wie Titel und Bearbeiter weitergegeben werden. Zudem sollte sichergestellt sein, dass die Option „Schnellspeicherung zulassen“ nicht aktiviert wurde.

– Dass jemand durch Auswertung der „Dateieigenschaften“ aus der Titelangabe frühere Formulierungen des Schreibens oder die tatsächliche Zahl der Speicherungen eines Dokuments entnehmen kann, lässt sich verhindern, indem der Inhalt des Dokuments vor dem elektronischen Versand in ein neu angelegtes Dokument kopiert wird. Dann erscheint der erste Satz dieses kopierten Dokuments als Titel und auch der Versionszähler, der die Zahl der Speicherungen registriert, wird zurückgesetzt.

Ähnliche Probleme können grundsätzlich auch in anderen Produkten auftreten. Daher empfiehlt es sich, die individuell verwendeten Dokumentenformate darauf zu überprüfen, ob darin Dateieigenschaften transportiert werden und, wenn ja, wie diese (automatisch) mit Inhalten gefüllt werden. Zum anderen kann man die Dokumente, nachdem die Datei-Namensendung auf .txt abgeändert wurde, mit Hilfe eines einfachen Texteditors darauf überprüfen, ob darin Daten enthalten sind, die dort nicht hingehören.

Inhaltsverzeichnis des Anhangs

Anhang 1

Der Landesbeauftragte für den Datenschutz Baden-Württemberg

Innenministerium Baden-Württemberg
Stabsstelle für Verwaltungsreform (Bereich IuK-Technik, IuK-Recht)

Hinweise zum datenschutzgerechten IuK-Einsatz bei der Verwaltungsreform

29. Oktober 2003

1. Im Rahmen der Migrationskonzepte muss die verantwortliche Stelle i. S. des § 3 LDSG für jedes von der Verwaltungsreform betroffene IuK-Verfahren die vollständige Erfüllung aller Anforderungen des Datenschutzes sicherstellen. Sofern ein IuK-Verfahren inhaltlich, technisch oder bezüglich seiner Nutzung (organisatorisch) verändert wird, ist eine spezielle Konzeption zum Datenschutz und zur Datensicherheit zu erstellen. Dies gilt auch, wenn ein Verfahren unverändert in einem anderen IuK-technischen Umfeld, also etwa auf einem anderen Server oder in anderer netztechnischer Umgebung betrieben wird. Wird eine Aufgabe an eine andere Behörde übertragen, dürfen ihr nur diejenigen personenbezogenen Daten zugänglich gemacht werden, die sie zur Erfüllung der übertragenen Aufgabe benötigt.

2. Bei der fachlichen Konzeption bzw. Überprüfung der von der Verwaltungsreform betroffenen IuK-Verfahren muss die verantwortliche Stelle folgende Aspekte besonders berücksichtigen:

   - Sind alle rechtlichen Voraussetzungen zum Einsatz des IuK-Verfahrens (z. B. Rechtsvorschrift oder Einwilligung vorhanden, Richtigkeit der Daten im neuen Kontext sichergestellt, Übermittlung oder Datenverarbeitung im Auftrag? Richtigkeit und Vollständigkeit der Dokumentation, usw.) in der geplanten Weise gegeben?
   - Werden die Grundsätze des Datenschutzes (Datensparsamkeit, Beschränkung der Zugriffsrechte auf das notwendige Maß, Schriftlichkeit des Auftrags bei Datenverarbeitung im Auftrag, Schulung der Nutzer, usw.) beachtet?
   - Liegt ein vollständiges und systematisches Sicherheitskonzept mit einer Schwachstellenanalyse vor, das organisatorisch lückenlos umgesetzt werden kann?

3. Bezüglich der Datensicherheit muss die verantwortliche Stelle alle erforderlichen Sicherheitsmaßnahmen ergreifen. Zu den Sicherheitsmaßnahmen, die bei einer Nutzung innerhalb der Landesverwaltung ergriffen worden sind, sind je nach Fallgestaltung zusätzliche (Anpassungs-)Maßnahmen zu ergreifen. Dazu müssen die abgebenden und aufnehmenden Dienststellen in gebotenem Umfang zusammenwirken. Dabei ist die aufnehmende Behörde verantwortlich für die Konzeption und Umsetzung der zum weiteren Betrieb des Verfahrens notwendigen technischen und organisatorischen Maßnahmen. Die abgebende Behörde muss prüfen, ob sie ihrerseits ihr Datenschutz- und Sicherheitskonzept in Folge der Abgabe fortschreiben muss.

   Beispiele sind:

   - Übergabe eines staatlichen IuK-Verfahrens an Landkreise und/oder Stadtkreise:

     a. Für die Integration ist i. d. R. ein Datenschutzkonzept erforderlich, das insb. die Abschottung, die Verfügbarkeit und die Betriebssicherheit regelt.

     b. Die Integration in die neue IuK-Umgebung muss datenschutzrechtlich geprüft werden. Kritisch ist z. B., wenn über das lokale Netz der neuen Behörde Daten Unbefugten bekannt werden können.

     c. Die IuK-Verfahren müssen mit vollständiger Dokumentation übergeben werden.

d. Schulung der neuen Administratoren des IuK-Verfahrens ist notwendig.

e. Vor einer Integration muss das IuK-Verfahren getestet werden.

- Nutzung eines vom Land betriebenen IuK-Verfahrens durch Landkreise und/oder Stadtkreise:

  f. Da es sich um Datenverarbeitung im Auftrag i. S. von § 7 LDSG handeln dürfte, sind die entsprechenden schriftlichen Aufträge zu formulieren und zu erteilen.

  g. Für die Integration ist i. d. R. ein Datenschutzkonzept erforderlich, das insb. die Abschottung, die Verfügbarkeit und die Betriebssicherheit regelt.

  h. Die Integration in die neue IuK-Umgebung muss datenschutzrechtlich geprüft werden. Kritisch ist z. B., wenn über das lokale Netz der neuen Behörde Daten Unbefugten bekannt werden können.

  i. Schulung der neuen Administratoren des IuK-Verfahrens ist notwendig.

  j. Vor einer Integration muss das IuK-Verfahren getestet werden.

  k. Wo innerhalb des LVN unverschlüsselt kommuniziert worden ist, muss auf verschlüsselte Kommunikation umgestellt werden, sofern unsichere Netze mit benutzt werden. Aus Sicherheitsgründen sollte jeweils so früh wie möglich auf SSL-gesicherte oder BW-Card-gesicherte Transaktionen und/oder entsprechende andere kryptografisch gesicherte Datenübertragungsverfahren umgestellt werden.

- Gemeinsame Nutzung eines IuK-Verfahrens durch das Land sowie durch Landkreise und/oder Stadtkreise:

  Gemäß § 8 LDSG sind besondere datenschutzrechtliche Anforderungen zu beachten, wenn eine öffentliche Stelle online auf die von einer anderen Stelle gespeicherten Daten zugreifen kann. Im Zuge der Verwaltungsreform können derartige Konstellationen neu entstehen. Wird beispielsweise ein IuK-Verfahren von einer Landesbehörde für eigene Aufgaben genutzt und erhalten Landratsämter zur Wahrnehmung der ihnen übertragenen Aufgaben ein Zugriffsrecht auf dieses Verfahren, so greift das Landratsamt im Rahmen eines automatisierten Abrufverfahrens auf Daten der Landesbehörde zu. Vor der Einrichtung eines solchen Verfahrens ist eine Vorabkontrolle gem. § 12 LDSG durchzuführen (vgl. Nr. 4). Sofern danach sowie nach § 8 Abs. 1 LDSG die Einrichtung des Abrufverfahrens zulässig ist, haben die beteiligten Stellen schriftlich festzulegen:

  – Anlass und Zweck des Abrufverfahrens,

  – Dritte, an die übermittelt wird,

  – Art der abzurufenden Daten,

  – die nach § 9 LDSG erforderlichen technischen und organisatorischen Maßnahmen.

  Die speichernde Stelle hat dabei ferner zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

4. Gemäß § 12 LDSG ist eine datenschutzrechtliche Vorabkontrolle nicht nur dann durchzuführen, wenn ein automatisiertes Abrufverfahren gemäß § 8 LDSG eingerichtet wird, sondern auch, wenn besonders schutzbedürftige Daten gemäß § 33 LDSG verarbeitet („Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben hervorgehen“) oder wenn Datenträger gemäß § 5 Abs. 2 LDSG (z. B. Chipkarten) herausgegeben werden.

   Darüber hinaus ist eine Vorabkontrolle durchzuführen, wenn die wesentliche Änderung eines automatisierten Verfahrens geplant ist. Die Verwaltungsreform wird nicht nur eines, sondern eine Vielzahl IuK-Verfahren berühren und insgesamt zu einer nicht nur unwesentlichen Änderung der staatlichen und

kommunalen IT-Struktur führen. Gerade da sich aufgrund des Zusammenspiels vieler Einzelmaßnahmen Auswirkungen ergeben können, die zuvor nicht offensichtlich erkennbar waren, sollte, auch wenn sich die Vorschriften des § 12 LDSG nicht unmittelbar auf das Vorhaben „Verwaltungsreform“ als Ganzes anwenden lassen, die in § 12 LDSG beschriebene Vorgehensweise auch bei der Umsetzung der Verwaltungsreform berücksichtigt werden:

- Alle Stellen, deren IuK-Ausstattung, -Betrieb oder -Nutzung durch die Verwaltungsreform verändert wird, müssen eine Übersicht aller sie betreffenden Aspekte erstellen. Aus Sicht eines Landratsamtes sollte daraus z. B. erkennbar sein, welche IuK-Verfahren das Landratsamt künftig zusätzlich nutzen und wie sich die IuK-Struktur im Zuge der Aufnahme verschiedener staatlicher Behörden weiterentwickeln wird.
- Die Stellen müssen auf der Grundlage dieser Übersicht prüfen, welche sicherheitstechnischen Risiken die Änderungen mit sich bringen. Dabei ist der Blick nicht nur auf jedes einzelne von der Änderung betroffene Verfahren, sondern auch auf die Gesamtheit der künftig zu betreibenden und nutzenden IuK-Verfahren zu richten.
- In einem weiteren Schritt ist darzustellen, ob und, wenn ja, wie die Risiken durch technische und organisatorische Maßnahmen beherrscht werden können.
- Das Ergebnis dieser Untersuchungen, an denen der behördliche Datenschutzbeauftragte zu beteiligen ist, ist schriftlich festzuhalten.
- Alle diese konzeptionellen Schritte sind abzuschließen, bevor die entsprechenden Schritte der Verwaltungsreform umgesetzt werden.

5. Nach den vom Innenministerium und vom Finanzministerium vorgelegten Eckpunkten zur IuK-Migration ist zudem vorgesehen, dass die aus Gründen des Datenschutzes vorzunehmenden Anpassungsarbeiten im Einvernehmen mit Innenministerium und Finanzministerium vorzunehmen sind. Ferner ist vorgesehen, dass die Migrationskosten vom Land getragen werden. Unabhängig davon sind stets diejenigen Dienststellen für die Einhaltung der zur datenschutzgerechten Flankierung der Verwaltungsreform erforderlichen technischen und organisatorischen Maßnahmen verantwortlich, deren IuK-Ausstattung, -Betrieb oder -Nutzung sich durch die Verwaltungsreform ändert. Dies betrifft insbesondere die Landratsämter und die Regierungspräsidien in ihrer Rolle als „aufnehmende Behörden“.

6. Durch den im Rahmen der gemeinsamen Sitzung der AG zur Abstimmung der IuK zwischen Land und Kommunen und des AK-IT am 16. Oktober 2003 gefassten Beschluss 1 zu TOP 2 werden die Ressorts gebeten, die Migrationskosten unverzüglich abzuschätzen und an das Meldesystem des IM und dem FM zu melden. Die Kosten der migrationsbedingten technischen und organisatorischen Datenschutzmaßnahmen hängen maßgeblich von den technischen und organisatorischen Gegebenheiten bei den aufnehmenden Behörden ab. Soweit IuK-Verfahren an Landkreise und/oder Stadtkreise abgegeben werden, ist es zur korrekten Ermittlung der Migrationskosten notwendig, dass die betroffenen Landkreise und Stadtkreise den Ressorts mitteilen, in welcher Höhe ihnen migrationsbedingte Kosten zur Wahrung der Datensicherheit entstehen. Die Ressorts müssen die Landkreise und die Stadtkreise bei der Ermittlung der Migrationskosten entsprechend beteiligen.

7. Bevor eine öffentliche Stelle personenbezogene Daten auf der Basis von Einwilligungen verarbeiten darf, sind die betroffenen Bürger gemäß § 4 Abs. 2 LDSG unter anderem über die beabsichtigte Datenverarbeitung zu informieren. Dazu gehört, dass den Bürgern auch mitgeteilt wird, welche Stelle diese Datenverarbeitung vornimmt. Soll nun, beispielsweise in Folge einer Aufgabenübertragung, eine andere öffentliche Stelle die Datenverarbeitung übernehmen und fortführen, so sind die Bürger darüber rechtzeitig vor der geplanten Änderung zu informieren. Dabei ist ihnen Gelegenheit zu geben, der Verarbeitung ihrer Daten durch diese andere Stelle zu widersprechen.

Anhang 2

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 27./28. März 2003

Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger, sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.

Sie sehen dabei folgende essenzielle Punkte:

- Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes
  - Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.
  - Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.
  - Die Freiwilligkeit der Einwilligung muss gewährleistet sein.
  - Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in“ statt „opt out“).

- Technischer Datenschutz

  Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

- Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

  Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen.

Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

- Förderung von datenschutzgerechter Technik

  Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind.

  Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.

  Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

- Anonyme Internetnutzung

  Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von e-mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z. B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht.

  Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

- Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

  Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten:

  Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.

  Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

  Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in ande-

ren gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen – wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung – für geboten.

Die Evaluierung muss durch unabhängige Stellen und an Hand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z. B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des Richtervorbehalts – und zwar nicht nur im Bereich der Telefonüberwachung – als grundrechtssicherndes Verfahrenselement ergreifen muss.

- Stärkung des Schutzes von Gesundheitsdaten

  Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z. B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung“ einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

  Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung so weit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten, und zwar auch für deren Verwendung im Einzelfall.

  Der Bundesgesetzgeber wird auch aufgefordert gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis.

  Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, z. B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

- Datenschutz und Gentechnik

  Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen – dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto

größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.

Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes“ vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt.

- Datenschutz im Steuerrecht

  Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

  Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und -speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit.

  Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

- Arbeitnehmerdatenschutz

  Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

  – die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
  – die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,
  – die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,
  – die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

  Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.

  Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

- Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

  Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbe-

fugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet.

Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

- Stellung des Bundesdatenschutzbeauftragten

  Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

- Verbesserung der Informationsrechte

  Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

Anhang 3

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 27./28. März 2003

Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungs- und Abrechnungsdaten sollen eine stärkere Kontrolle der Patientinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen.

So sehen Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens u. a. vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungs- und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die

- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,
- das Prinzip der Stichprobe zugrunde legen,
- eine strikte Einhaltung der Zweckbindung gewährleisten und
- die Auswertung der Daten einer unabhängigen Stelle übertragen.

1.

Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungs- und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnose- und Behandlungsangaben z. B. zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und

organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2.

Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der – von den Betroffenen nicht beeinflussbar – Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden.

Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grundsätzlich selbst zu entscheiden,

– ob sie überhaupt verwendet wird,

– welche Daten darauf gespeichert werden oder über sie abgerufen werden können,

– welche Daten zu löschen sind und wann das zu geschehen hat,

– ob sie im Einzelfall vorgelegt wird und

– welche Daten im Einzelfall ausgelesen werden sollen.

Sicherzustellen ist weiterhin

– ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht, in Bezug auf die Daten, die auf der Karte gespeichert sind,

– die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und

– die Strafbarkeit des Datenmissbrauchs.

Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 24./25. Oktober 2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen“ vom 3. Mai 2002, wonach „der Patient Herr seiner Daten“ sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

3.

Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten („fährt Ski“, „raucht“, „trinkt zwei Biere pro Tag“), diese überwachen und so zur „Gesundheitspolizei“ werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

4.

Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.

Anhang 4

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. September 2003

Entschließung zum Gesundheitsmodernisierungsgesetz

Die Datenschutzkonferenz begrüßt, dass mit den gesetzlichen Regelungen zur Gesundheitskarte und zu dem bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildeten zentralen Datenpool datenschutzfreundliche Lösungen erreicht werden konnten. Die Gesundheitskarte unterliegt auch künftig der Verfügungsgewalt der Patientinnen und Patienten. Für den quartals- und sektorenübergreifenden Datenpool dürfen nur pseudonymisierte Daten gespeichert werden.

Die Datenschutzkonferenz wendet sich nicht grundsätzlich gegen zusätzliche Kontrollmechanismen der Krankenkassen.

Die Datenschutzbeauftragten kritisieren, dass sie zu wesentlichen, erst in letzter Minute eingeführten und im Schnellverfahren realisierten Änderungen nicht rechtzeitig und ausreichend beteiligt wurden. Diese Änderungen bedingen erhebliche Risiken für die Versicherten:

- Für das neue Vergütungssystem werden künftig auch die Abrechnungen der ambulanten Behandlungen mit versichertenbezogener Diagnose an die Krankenkassen übermittelt. Mit der vorgesehenen Neuregelung könnten die Krankenkassen rein tatsächlich umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Diese datenschutzrechtlichen Risiken hätten durch die Verwendung moderner und datenschutzfreundlicher Technologien einschließlich der Pseudonymisierung vermieden werden können. Leider sind diese Möglichkeiten überhaupt nicht berücksichtigt worden.
- Ohne strenge Zweckbindungsregelungen könnten die Krankenkassen diese Daten nach den verschiedensten Gesichtspunkten auswerten (z. B. mit datawarehouse-systemen).

Die Datenschutzkonferenz nimmt anerkennend zur Kenntnis, dass vor diesem Hintergrund durch Beschlussfassung des Ausschusses für Gesundheit und Soziale Sicherheit eine Klarstellung dahin gehend erfolgt ist, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen

- eine sektorenübergreifende Zusammenführung der Abrechnungs- und Leistungsdaten unzulässig ist, und dass
- die Krankenkassen die Daten nur für Abrechnungs- und Prüfzwecke nutzen dürfen.

Darüber hinaus trägt eine Entschließung des Deutschen Bundestages der Forderung der Datenschutzkonferenz Rechnung, durch eine Evaluierung der Neuregelung in Bezug auf den Grundsatz der Datenvermeidung und Datensparsamkeit unter Einbeziehung der Möglichkeit von Pseudonymisierungsverfahren sicherzustellen, dass Fehlentwicklungen vermieden werden.

Die Datenschutzkonferenz hält eine frühestmögliche Pseudonymisierung der Abrechnungsdaten für notwendig, auch damit verhindert wird, dass eine Vielzahl von Bediensteten personenbezogene Gesundheitsdaten zur Kenntnis nehmen kann.

Anhang 5

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 27./28. März 2003

Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes festgestellt, dass sich die Zweckbindung der bei dieser Maßnahme erlangten personenbezogenen Daten nur gewährleisten lässt, wenn auch nach ihrer Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassungs wegen geboten. Dementsprechend wurde die Kennzeichnungspflicht in der Novellierung des G 10-Gesetzes auch allgemein für jede Datenerhebung des Bundesnachrichtendienstes und des Verfassungsschutzes im Schutzbereich des Art. 10 GG angeordnet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Pflicht zur Kennzeichnung aufgrund der Ausführungen des Bundesverfassungsgerichts nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist. Sie gilt auch für vergleichbare Methoden der Datenerhebung, bei denen die Daten durch besonders eingriffsintensive Maßnahmen gewonnen werden und deswegen einer strikten Zweckbindung unterliegen müssen.

Deshalb müssen zumindest solche personenbezogenen Daten, die aus einer Telefon-, Wohnraum- oder Postüberwachung erlangt wurden, besonders gekennzeichnet werden.

Anhang 6

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 27./28. März 2003

Transparenz bei der Telefonüberwachung

Nach derzeitigem Recht haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen zu erstellen. Diese Zahlen werden von der Regulierungsbehörde für Telekommunikation und Post veröffentlicht. Auf diese Weise wird die Allgemeinheit über Ausmaß und Entwicklung der Telekommunikationsüberwachung in Deutschland informiert.

Nach aktuellen Plänen der Bundesregierung soll diese Statistik abgeschafft werden. Begründet wird dies mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. Dabei wird verkannt, das die beiden Statistiken unterschiedliches Zahlenmaterial berücksichtigen. So zählen die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen, während von den Landesjustizverwaltungen nur die Anzahl der Strafverfahren erfasst wird.

In den vergangenen Jahren ist die Zahl der überwachten Anschlüsse um jährlich etwa 25 Prozent gestiegen. Gab es im Jahr 1998 noch 9 802 Anordnungen, waren es im Jahr 2001 bereits 19 896. Diese stetige Zunahme von Eingriffen in das Fernmeldegeheimnis sehen die Datenschutzbeauftragten des Bundes und der Länder mit großer Sorge. Eine fundierte und objektive Diskussion in Politik und Öffentlichkeit ist nur möglich, wenn die tatsächliche Anzahl von Telefonüberwachungsmaßnahmen bekannt ist. Allein eine Aussage über die Anzahl der Strafverfahren, in denen eine Überwachungsmaßnahme stattgefunden hat, reicht nicht aus. Nur die detaillierten Zahlen, die derzeit von den Telekommunikationsunternehmen erhoben werden, sind aussagekräftig genug.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine Beibehaltung der Unternehmensstatistik nach § 88 Absatz 5 Telekommunikationsgesetz sowie ihre Erstreckung auf die Zahl der Auskünfte über Telekommunikationsverbindungen, um auf diesem Wege bessere Transparenz bei der Telefonüberwachung zu schaffen.

Anhang 7

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 25./26. September 2003

Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai diesen Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen“ vorgelegt. Darin hat es festgestellt, dass

- die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 % erhöht (1996: 2 149; 2001; 3 868) hat,
- die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2 494 um das Sechsfache auf 15 741 gestiegen ist,
- sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3 730 auf 9 122 fast verdreifacht hat,
- in 21 % der Anordnungen zwischen 1 000 und 5 000 Gespräche, in 8 % der Anordnungen mehr als 5 000 Gespräche abgehört worden sind,
- der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 % auf ca. 14 % angestiegen ist,
- die Beschlüsse in ca. ¾ aller Fälle das gesetzliche Maximum von 3 Monaten umfassen, ¾ aller Maßnahmen tatsächlich aber nur bis zu 2 Monaten andauern,
- lediglich 24 % der Beschlüsse substanziell begründet werden,
- es nur in 17 % der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,
- 73 % der betroffenen Anschlussinhaberinnen und -inhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden. Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann – entgegen häufig gegebener Deutung – nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen ultima ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

- Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.
- Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100 b StPO dahin gehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (z. B. Beweisverwertungsverbote).
- Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und -richter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.

- Der Umfang des – seit Einführung der Vorschrift regelmäßig erweiterten – Straftatenkataloges des § 100 a StPO muss reduziert werden.
- Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschaffen werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.
- Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte, zumindest aller bekannten Gesprächsteilnehmerinnen und -teilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.
- Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.
- Zur Sicherung der Zweckbindung nach § 100 b Abs. 5 StPO und § 477 Abs. 2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.
- Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.
- Auch aufgrund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (z. B. IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

Anhang 8

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 21. November 2003

Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes

Die Bundesregierung hat am 15. Oktober 2003 den Entwurf für ein neues Telekommunikationsgesetz (TKG) beschlossen. Dieser Entwurf sieht jetzt zwar – entsprechend der Forderung der Datenschutzbeauftragten – die vorläufige Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen vor; im Übrigen enthält er aber gravierende Verschlechterungen des Datenschutzniveaus.

Insbesondere berechtigt der Gesetzentwurf die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern. Damit wird ohne Not und ohne überzeugende Begründung eine Regelung aufgegeben, die bisher die Speicherung von verkürzten Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden. Die bisherige Regelung berücksichtigt in ausgewogener Weise sowohl die Datenschutz- als auch die Verbraucherschutzinteressen der beteiligten Personen und hat sich in der Praxis bewährt. Vollends inakzeptabel ist die inzwischen vom Rechtsausschuss des Bundesrates vorgeschlagene Pflicht zur Vorratsdatenspeicherung für sechs Monate. Gegen eine solche Regelung bestehen erhebliche verfassungsrechtliche Bedenken.

Schon die von der Bundesregierung vorgeschlagene Regelung würde dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für ihre Abrechnungszwecke nicht mehr benötigen. Das im Entwurf weiterhin vorgesehene Recht der Kundinnen und Kunden, die Speicherung gekürzter Zielrufnummern oder ihre vollständige Löschung nach Rechnungsversand zu verlangen, wird daran wenig ändern, weil nur eine Minderheit es wahrnehmen wird. Die Beibehaltung des bisherigen angemessenen Datenschutzstandards sollte nicht von der Initiative der Betroffenen abhängig gemacht werden, sondern allen zugute kommen, die nicht ausdrücklich einer weitergehenden Speicherung zustimmen. Zudem sind die Rechte der angerufenen Teilnehmerinnen und Teilnehmer zu berücksichtigen, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird.

Die Datenschutzbeauftragten haben zudem stets die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys als gesetzwidrig kritisiert und sehen sich jetzt in dieser Auffassung durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 23.02) bestätigt. Zugleich wenden sie sich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht, die zu einer verdachtslosen Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Schließlich soll den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten ohne Bindung an einen Straftatenkatalog oder einen Richtervorbehalt der Zugriff auf Passwörter, PINs, PUKs usw. eröffnet werden, mit denen die Inhalte oder nähere Umstände einer Telekommunikation geschützt werden. Dies würde die Möglichkeit eröffnen, von dieser Befugnis unkontrolliert Gebrauch zu machen. Die Befugnis dürfte zudem häufig ins Leere laufen, da die Anbieter diese Daten aus Gründen der Datensicherheit für sie selbst unlesbar verschlüsselt speichern.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, den Entwurf bei den bevorstehenden Beratungen in diesen sensiblen Punkten zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

Anhang 9

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 16. Juli 2003

Bei der Erweiterung der DNA-Analyse Augenmaß bewahren

Derzeit gibt es mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken in § 81 g StPO für die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster (sog. genetischer Fingerabdruck) in der zentralen DNA-Analyse-Datei des BKA abzusenken.

Die Vorschläge gehen dahin,

- zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr – wie vom geltenden Recht gefordert – in jedem Fall eine Straftat von erheblicher Bedeutung oder – wie jüngst vom Bundestag beschlossen – eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,
- zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tiefgreifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt; dies hat auch das Bundesverfassungsgericht in seinen Beschlüssen vom Dezember 2000 und März 2001 bestätigt.

Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nichtcodierenden Teile untersucht werden: Schon daraus können Zusatzinformationen gewonnen werden (Geschlecht, Altersabschätzung, Zuordnung zu bestimmten Ethnien, möglicherweise einzelne Krankheiten wie Diabetes, Klinefelter-Syndrom). Auch deshalb lässt sich ein genetischer Fingerabdruck mit einem herkömmlichen Fingerabdruck nicht vergleichen. Zudem ist immerhin technisch auch eine Untersuchung des codierenden Materials denkbar, sodass zumindest die abstrakte Eignung für viel tiefer gehende Erkenntnisse gegeben ist. Dies bedingt unabhängig von den gesetzlichen Einschränkungen ein höheres abstraktes Gefährdungspotenzial.

Ferner ist zu bedenken, dass das Ausstreuen von Referenzmaterial (z. B. kleinste Hautpartikel oder Haare), das mit dem gespeicherten Identifizierungsmuster abgeglichen werden kann, letztlich nicht zu steuern ist, sodass in höherem Maß als bei Fingerabdrücken die Gefahr besteht, dass genetisches Material einer Nichttäterin oder eines Nichttäters an Tatorten auch zufällig, durch nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation platziert wird. Dies kann für Betroffene im Ergebnis zu einer Art Umkehr der Beweislast führen.

Angesichts dieser Wirkungen und Gefahrenpotenziale sehen die Datenschutzbeauftragten Erweiterungen des Einsatzes der DNA-Analyse kritisch und appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Auf das Erfordernis der Prognose erheblicher Straftaten als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.

Im Hinblick auf die Eingriffsschwere ist auch der Richtervorbehalt für die Anordnung der DNA-Analyse unverzichtbar. Es ist deshalb auch zu begrüßen, dass zur Stärkung dieser grundrechtssichernden Verfahrensvorgabe für die Anordnungsentscheidung die Anforderungen an die Begründung des Gerichts gesetzlich prä-

zisiert wurden. Zudem sollte die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage der Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden.

Anhang 10

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 30. April 2003

Neuordnung der Rundfunkfinanzierung

Die Länder bereiten gegenwärtig eine Neuordnung der Rundfunkfinanzierung vor, die im neuen Rundfunkgebührenstaatsvertrag geregelt werden soll. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten lassen befürchten, dass bei ihrer Umsetzung die bestehenden datenschutzrechtlichen Defizite nicht nur beibehalten werden, sondern dass mit zum Teil gravierenden Verschlechterungen des Datenschutzes gerechnet werden muss:

- Insbesondere ist geplant, alle Meldebehörden zu verpflichten, der GEZ zum Inkrafttreten des neuen Staatsvertrages die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind. Dadurch entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen), obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.
- Auch wenn in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden, sollen alle dort gemeldeten erwachsenen Bewohner von vornherein zur Auskunft verpflichtet sein, selbst wenn keine Anhaltspunkte für eine Gebührenpflicht bestehen. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst – wie bei den amtlichen Statistiken erfolgreich praktiziert – nur die Meldedaten für eine Person übermittelt werden, die dazu befragt wird.
- Zudem soll die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten will die GEZ künftig auch online zugreifen.
- Gleichzeitig soll die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten – wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern – zu erheben, ausdrücklich erlaubt werden.
- Schließlich sollen die bisher bestehenden Möglichkeiten der Aufsicht durch die Landesbeauftragten für den Datenschutz ausgeschlossen werden, sodass für die Rundfunkanstalten und die GEZ insoweit nur noch eine interne Datenschutzkontrolle beim Rundfunkgebühreneinzug bestünde.

Diese Vorstellungen der Rundfunkanstalten widersprechen dem Verhältnismäßigkeitsprinzip und sind daher nicht akzeptabel.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der datenschutzfreundliche Modelle zu bevorzugen sind. Sie haben hierzu bereits praktikable Vorschläge vorgelegt.

Anhang 11

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 27./28. März 2003

Elektronische Signatur im Finanzbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3 000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die „qualifizierte elektronische Signatur“ der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als zwanzig freiwillig akkreditierte Zertifizierungsdiensteanbieter nach dem Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die „qualifizierte elektronische Signatur“ gesetzlich vorgeschrieben. Die Finanzverwaltung will eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung vom 28. Januar 2003 nutzen, nach der bis Ende 2005 eine lediglich fortgeschrittene, die so genannte „qualifizierte elektronische Signatur mit Einschränkungen“ eingesetzt werden kann. Aus folgenden Gründen lehnen die Datenschutzbeauftragten dieses Vorgehen ab:

- Die „qualifizierte elektronische Signatur mit Einschränkungen“ bietet im Gegensatz zur „qualifizierten elektronischen Signatur“ und der „qualifizierten elektronischen Signatur mit Anbieterakkreditierung“ keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unterzeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die „qualifizierte elektronische Signatur mit Einschränkungen“ hat geringeren Beweiswert als die eigenhändige Unterschrift.
- Die technische Infrastruktur, die die Finanzverwaltung für die „qualifizierte elektronische Signatur mit Einschränkungen“ vorgesehen hat, kann sie verwenden, um elektronische, fortgeschritten oder qualifiziert signierte Dokumente von Bürgerinnen und Bürgern und Steuerberaterinnen und Steuerberatern zu prüfen und selbst fortgeschrittene Signaturen zu erzeugen.

  Damit die Finanzverwaltung selbst qualifiziert signieren kann, reicht eine Ergänzung mit einem qualifizierten Zertifikat aus.
- Für die elektronische Steuererklärung ELSTER sollen Zertifizierungsdienste im außereuropäischen Ausland zugelassen werden, für die weder eine freiwillige Akkreditierung noch eine Kontrolle durch deutsche Datenschutzbehörden möglich ist, anstatt Zertifizierungsdienste einzuschalten, die der Europäischen Datenschutzrichtlinie entsprechen. Damit sind erhebliche Gefahren verbunden, die vermeidbar sind.
- Die elektronische Signatur soll auch zur Authentisierung der Steuerpflichtigen und Steuerberater gegenüber ELSTER genutzt werden, obwohl die Trennung der Schlüsselpaare für Signatur und Authentisierung unerlässlich und bereits Stand der Technik ist.

Die Datenschutzbeauftragten des Bundes und der Länder befürchten, dass bei Schaffung weiterer Signaturverfahren mit geringerer Sicherheit die Transparenz für die Anwenderinnen und Anwender verloren geht und der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr in Frage gestellt werden könnte.

Abweichend vom Vorgehen der Finanzverwaltung hat sich die Bundesregierung sowohl im Rahmen der Initiative „Bund Online 2005“ als auch im so genannten Signaturbündnis für sichere Signaturverfahren eingesetzt. Das Verfahren ELSTER sollte genutzt werden, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Vor diesem Hintergrund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung,

- dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,
- den Bürgerinnen und Bürgern *eine* sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,
- unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,
- die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und ggf. Signaturanwendungskomponenten für „qualifizierte elektronische Signaturen mit Anbieterakkreditierung“ staatlich zu fördern,
- die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,
- e-Government- und e-Commerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,
- die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern,
- die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

Anhang 12

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 28. April 2003

Verbesserung statt Absenkung des Datenschutzniveaus
in der Telekommunikation

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vgl. dazu Entschließung der 65. Konferenz vom 28. März 2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.

Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (z. B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weiter gehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss – wie bisher – die informierte Einwilligung des Betroffenen voraussetzen.

Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie z. B. PINs und PUKs – Personal Unblocking Keys –), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeordnet werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmäßig gebotenen Schutzschwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12. März 2003.

Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass z. B. der Erwerb eines „vertragslosen“ Handys, das mit einer entsprechenden – im Prepaid-Verfahren mit Guthaben aufladbaren – SIM-Karte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs der Sicherheitsbehörden auf Vorrat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose routinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen. So sind erfahrungsgemäß z. B. die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.

Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunikation zu verbessern, statt es weiter abzusenken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammengeführt werden könnte.

Anhang 13

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 27./28. März 2003

TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden

Mit großer Skepsis sehen die Datenschutzbeauftragten des Bundes und der Länder die Pläne zur Entwicklung zentraler Kontrollmechanismen und -infrastrukturen auf der Basis der Spezifikationen der Industrie-Allianz „Trusted Computing Platform Alliance“ (TCPA).

Die TCPA hat sich zum Ziel gesetzt, vertrauenswürdige Personalcomputer zu entwickeln. Dazu bedarf es spezieller Hard- und Software. In den bisher bekannt gewordenen Szenarien soll die Vertrauenswürdigkeit dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten des PCs überprüft, ob die installierte Hardware und das Betriebssystem mit den von der TCPA zertifizierten und auf zentralen Servern hinterlegten Konfigurationsangaben übereinstimmen. Danach übergibt der Prozessor die Steuerung an ein TCPA-konformes Betriebssystem. Beim Start einer beliebigen Anwendersoftware prüft das Betriebssystem dann deren TCPA-Konformität, beispielsweise durch Kontrolle der Lizenz oder der Seriennummer, und kontrolliert weiterhin, ob Dokumente in zulässiger Form genutzt werden. Sollte eine der Prüfungen Abweichungen zur hinterlegten, zertifizierten Konfiguration ergeben, lässt sich der PC nicht booten bzw. das entsprechende Programm wird gelöscht oder lässt sich nicht starten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennen auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf.

Wenn aber zentrale Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen Prüf- und Kontrollfunktionen zu steuern, müssten sich Anwenderinnen und Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit der externen Instanz verlassen können. Die Datenschutzbeauftragten erachten es für unzumutbar, wenn

- Anwenderinnen und Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,
- die Verfügbarkeit aller TCPA-konformen Personalcomputer und der darauf verarbeiteten Daten gefährdet wäre, da sowohl Fehler in der Kontrollinfrastruktur als auch Angriffe auf die zentralen TCPA-Server die Funktionsfähigkeit einzelner Rechner sofort massiv einschränken würden,
- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,
- die Nutzung von Servern oder PCs davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,
- der Zugang zum Internet und E-Mail-Verkehr durch Softwarerestriktionen behindert würde,
- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein würde und somit eine sehr weitgehende Zensur ermöglicht wird,
- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und
- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,
- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und
- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden.

Anhang 14

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 27./28. März 2003

Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik

Anwenderinnen und Anwender von komplexen IT-Produkten müssen unbedingt darauf vertrauen können, dass Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden, damit die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten gewährleistet sind. Dieses Vertrauen kann insbesondere durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Ausbleibende Erfolge bei eCommerce und eGovernment werden mit fehlendem Vertrauen in einen angemessenen Schutz der personenbezogenen Daten und mangelnder Akzeptanz der Nutzerinnen und Nutzer erklärt. Anwenderinnen und Anwender sollten ihre Sicherheitsanforderungen präzise definieren und Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Die Datenschutzbeauftragten des Bundes und der Länder wollen Herstellerinnen und Hersteller und Anwenderinnen und Anwender von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen.

So bietet der Bundesbeauftragte für den Datenschutz seit dem 11. November 2002 mit zwei so genannten Schutzprofilen (Protection Profiles) Werkzeuge an, mit deren Hilfe Anwenderinnen und Anwender bereits vor der Produktentwicklung ihre datenschutzspezifischen Anforderungen für bestimmte Produkttypen beispielsweise im Gesundheitswesen oder im eGovernment detailliert beschreiben können. Kerngedanke der in diesen Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Die Schutzprofile sind international anerkannt, da sie auf der Basis der „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)“ entwickelt wurden. Herstellerinnen und Hersteller können datenschutzfreundliche Produkte somit nach international prüffähigen Vorgaben der Anwenderinnen und Anwender entwickeln. Unabhängige Prüfinstitutionen können diese Produkte dann nach Abschluss der Entwicklung nach international gültigen Kriterien prüfen.[1)]

In Schleswig-Holstein bietet das Unabhängige Landeszentrum für Datenschutz ein Verfahren mit vergleichbarer Zielsetzung an, das ebenfalls zu überprüfbarer Sicherheit von IT-Produkten führt. Für nachweislich datenschutzgerechte IT-Produkte können Hersteller ein so genanntes Datenschutz-Gütesiegel erhalten. Das Landeszentrum hat auf der Grundlage landesspezifischer Rechtsvorschriften bereits im Jahr 2002 einen entsprechenden Anforderungskatalog veröffentlicht und zur CeBIT 2003 eine an die Common Criteria angepasste Version vorgestellt.[2)]

Die Datenschutzbeauftragten des Bundes und der Länder empfehlen die Anwendung von Schutzprofilen und Auditierungsprozeduren, damit auch der Nutzer oder die Nutzerin beurteilen kann, ob IT-Systeme und -Produkte vertrauenswürdig und datenschutzfreundlich sind. Sie appellieren an die Hersteller, entsprechende Produkte zu entwickeln bzw. vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

[1)] Die Schutzprofile mit dem Titel „BISS – Benutzerbestimmbare Informationsflusskontrolle“ haben die Registrierungskennzeichen BSI-PP-0007-2002 und BSI-PTT-008-2002 und sind beim Bundesbeauftragten für den Datenschutz unter http://www.bfd.bund.de/technik/protection_profile.html abrufbar.

[2)] Die Ergebnisse der bisherigen Auditierungen durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sind unter http://www.datenschutzzentrum.de/guetesiegel veröffentlicht.

Anhang 15

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 7. August 2003

zum automatischen Software-Update

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen.

Zur Gewährleistung der Sicherheit und der Aktualität von System- und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Weltweit agierende Softwarehersteller bieten in zunehmendem Maße an, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf die Rechner ihrer Kunden zu laden und automatisch zu installieren. Diese Verfahren bergen erhebliche Datenschutzrisiken in sich:

- Immer öfter werden dabei – oftmals vom Nutzer unbemerkt oder zumindest nicht transparent – Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt, ohne dass dies im derzeit praktizierten Umfang aus technischen Gründen erforderlich ist.
- Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann in der Regel ohne die erforderlichen Tests und Freigabeverfahren genutzt werden.
- Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das – unbemerkte – Update wird dann nicht als Fehlerursache erkannt.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Sollen im Zusammenhang mit derartigen Wartungstätigkeiten personenbezogene Daten von Nutzerinnen und Nutzern übermittelt und verarbeitet werden, ist die ausdrückliche Zustimmung der für die Daten verantwortlichen Stelle erforderlich.

Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die Daten verarbeitenden Stellen dürfen daher derartige Online-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Den Erfordernissen des Datenschutzes kann nicht ausreichend Rechnung getragen werden, wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nutzerinnen und Nutzer gefährdet wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher die Software-Hersteller auf, überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern. Auch weiterhin sollten datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden. Automatisierte Online-Update-Verfahren sollten nur wahlweise angeboten werden. Sie sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind. Software-Updates dürfen in keinem Fall davon abhängig gemacht werden, dass den Anbietern ein praktisch nicht kontrollierbarer Zugriff auf den eigenen Rechner gewährt werden muss. Personenbezogene Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrück-

lich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.