

# 8. Tätigkeitsbericht

## des Thüringer Landesbeauftragten für den Datenschutz

Berichtszeitraum:	1. Januar 2008 bis 31. Dezember 2009
Drucksache:	5/1038
Veröffentlichungsdatum:	20. Mai 2010
Zitervorschlag:	8. TB LfD Thüringen

Der 8. Tätigkeitsbericht steht im Internet unter der Adresse [www.thueringen.de/datenschutz](http://www.thueringen.de/datenschutz) zum Abruf bereit.

Harald Stauch  
Der Thüringer Landesbeauftragte für den Datenschutz

---

## Inhaltsverzeichnis

<b>1.</b>	<b>Schwerpunkte im Berichtszeitraum</b> .....	9
<b>2.</b>	<b>Allgemeine Entwicklungen im Datenschutz</b> .....	12
<b>3.</b>	<b>Europäischer und Internationaler Datenschutz</b> ....	19
3.1	Keine Vorratsdatenspeicherung von Flugpassagierdaten .....	19
3.2	Austausch von Sicherheitsdaten D-USA ohne ausreichende Datenschutzgarantien.....	19
3.3	Polizeilicher Datenaustausch in der EU nicht immer auf höchstem Datenschutzniveau.....	20
3.4	Stockholmer Programm - Mehr Sicherheit und (auch mehr) Freiheit in Europa? .....	22
3.5	Kein Ausverkauf europäischer Finanzdaten an USA.....	23
<b>4.</b>	<b>Neue Medien - Rundfunk – Telekommunikation</b>	25
4.1	Bundesverfassungsgericht stoppt die Vorratsdaten- speicherung.....	25
4.2	Bürgerportalgesetz und De-Mail.....	27
<b>5.</b>	<b>Kommunales</b> .....	29
5.1	Kommunalkontrollen: Datenschutz - auch das noch! .....	29
5.2	Kommunal betriebene Videoanlagen und Webcams .....	33
5.3	Veröffentlichung von Ratssitzungen, Dokumenten und Mitarbeiterdaten im Internet .....	37
5.4	Veröffentlichung der Wortprotokolle von Niederschriften kommunaler Gremien .....	40
5.5	Auskunftsrecht des Gemeinderats bzw. eines seiner Mitglieder zu privatrechtlichen Verträgen.....	42
5.6	Unzulässige Übermittlung personenbezogener Daten von Kaufvertragsparteien an Erschließungsträger.....	42
5.7	Firmenumsatz und Fremdenverkehrsabgabe.....	43
5.8	Startschwierigkeiten mit der Online-Melderegisterauskunft .....	44
5.9	ePass und neuer Personalausweis (nPA).....	46
5.10	Unzulässige Datenübermittlung an die Presse zu einem akademischen Grad.....	49
5.11	Unzureichende Entsorgung personenbezogener Unterlagen durch Betreiber einer Asylbewerberunterkunft.....	51

5.12	Ausländerbehörde übermittelt zu freigiebig an Uni .....	52
5.13	Luftbildauswertung durch Zweckverband .....	53
5.14	Zustellung dienstlicher Schreiben in geöffneten Briefumschlägen in zwei Fällen .....	54
5.15	Auskunftsgewährung im Widerspruchsverfahren zu Straßenausbaubeiträgen .....	55
5.16	Datenhunger der Abfallwirtschaftsgesellschaft des Landkreises Gotha .....	56
5.17	Datenschutz im Rettungswesen - Einsichtnahme des TLfD in Notarztprotokolle .....	57
<b>6.</b>	<b>Personaldaten</b> .....	<b>59</b>
6.1	Beschäftigtendatenschutz - ein beschwerlicher (und hoffentlich bald erfolgreicher) Weg .....	59
6.2	Kreativität bei der Überführung von vermeintlich krank feiernden Mitarbeitern .....	59
6.3	Personalakten der Schulverwaltung enthalten teilweise unzulässige Daten .....	61
6.4	Nutzung von PC-Protokolldaten von Mitarbeitern .....	63
6.5	Kündigung wegen Beschwerde beim TLfD .....	64
<b>7.</b>	<b>Polizei</b> .....	<b>66</b>
7.1	Novellierung des Polizeiaufgabengesetzes (Teil II) .....	66
7.2	Kompetenzzuwachs des Bundeskriminalamts .....	68
7.3	Ermittlungen wegen Amok-Drohungen gegen eine Erfurter Schule .....	69
7.4	Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmern .....	73
7.5	Fehlende Rechtsgrundlage für INPOL-Dateien .....	74
7.6	Zugriffsprotokollierung und Kontrolle bei polizeilichen Dateien .....	74
7.7	Der oft schwierige Weg vom Blitzfoto zum Verantwortlichen .....	77
<b>8.</b>	<b>Verfassungsschutz</b> .....	<b>80</b>
8.1	Kontrolle der Anti-Terror-Datei bei Polizei und Verfassungsschutz .....	80
8.2	Auskunftsanspruch bei der Sicherheitsüberprüfung .....	81

<b>9.</b>	<b>Finanzwesen</b> .....	83
9.1	Steuerbürokratieabbaugesetz und Bürgerentlastungsgesetz Krankenversicherung.....	83
9.2	Haushaltsmanagementsystem (HAMASYS).....	85
9.3	Auskunftsanspruch im Steuerverfahren.....	86
9.4	Fragebogen Grunderwerb.....	86
9.5	Unzulässige Offenbarung von Steuerdaten des Finanzamtes Mühlhausen.....	87
9.6	Datenlöschung in gepfändeter IuK-Technik.....	88
9.7	Verwenden von Kundendaten der Sparkasse Mittelthüringen zu Werbezwecken.....	90
<b>10.</b>	<b>Justiz</b> .....	91
10.1	Einsatz von Videoüberwachung im Strafvollzug.....	91
10.2	Abfrage von Telekommunikations-Verkehrsdaten einschränken.....	92
10.3	Justizzahlstellenverfahren speichert längst erledigte Forderungen.....	93
<b>11.</b>	<b>Gesundheits- und Sozialdatenschutz</b> .....	95
11.1	Arbeitshilfe „Außendienst“ der Bundesagentur für Arbeit.....	95
11.2	DDR-Heimkinder.....	97
11.3	Thüringer Initiative zur Integration und Armutsbekämpfung - Nachhaltigkeit (TIZIAN).....	98
11.4	Gemeinsame Empfehlung zur Verbesserung der ressortüber- greifenden Kooperation beim Kinderschutz in Thüringen.....	98
11.5	Arge ARGEN?.....	99
11.6	Patientenarmbänder in Krankenhäusern.....	101
11.7	Krankenhausinformationssysteme.....	102
<b>12.</b>	<b>Wirtschaft, Arbeit, Bau und Verkehr</b> .....	103
12.1	Geodaten und Persönlichkeitsrecht.....	103
12.2	Deutschland-Online Kfz-Wesen.....	105
12.3	Falsche Adressaten für Gasliefervertrag.....	105
12.4	Intelligente Stromzähler.....	106
12.5	Videoüberwachung in Wohngebäuden.....	108

<b>13. Bildung, Wissenschaft, Forschung</b> .....	110
13.1 2. Europäischer Datenschutztag mit Folgen .....	110
13.2 Kooperationsvertrag TLF/D/ThILLM: Ein Erfolgsmodell .....	110
13.3 Der gläserne Schüler.....	111
13.4 Befragung von Kindern und Jugendlichen der Stadt Jena .....	112
13.5 Lebenslauf von Studienbewerbern?.....	115
<b>14. Entwicklungen der automatisierten Datenverarbeitung</b> .....	116
14.1 Datenschutzförderndes Identitätsmanagement.....	116
14.2 Biometrische Authentisierung .....	118
14.3 Kennzeichnung von Daten.....	119
14.4 Protokollierung .....	120
14.5 Datenschutz im Projekt- und Produktivbetrieb .....	122
14.6 Anschluss von Netzen der öffentlichen Verwaltung an das Internet.....	123
14.7 Cloud Computing.....	125
14.8 Viren .....	127
<b>15. Technische Entwicklung in der Thüringer Landesverwaltung</b> .....	128
15.1 Umsetzung EU-Dienstleistungsrichtlinie in Thüringen - ThEA .....	128
15.2 Einsatz EiCoNeD in Thüringen .....	129
15.3 Protokollierung von Zugriffen auf Internetangebote in der Thüringer Landesverwaltung.....	131
15.4 Einsatz BlackBerry in der Thüringer Landesverwaltung.....	133

## Anlagen

### Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin

Anlage 1	Berliner Erklärung: Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts.....	134
Anlage 2	Keine Vorratsspeicherung von Flugpassagierdaten.....	136

Anlage 3	Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen.....	138
Anlage 4	Unzureichender Datenschutz beim deutsch- amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden.....	141
Anlage 5	Mehr Augenmaß bei der Novellierung des BKA-Gesetzes .....	143
Anlage 6	Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern .....	145
Anlage 7	Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten.....	147
Anlage 8	Medienkompetenz und Datenschutzbewusstsein in der jungen „online-Generation“ .....	150

### **Entschliefungen zwischen den Konferenzen 2007/2008**

Anlage 9	Entschlossenes Handeln ist das Gebot der Stunde.....	152
----------	--	-----

### **Entschliefung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008 in Bonn**

Anlage 10	Mehr Transparenz durch Informationspflichten bei Datenschutzpannen .....	154
Anlage 11	Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich .....	156
Anlage 12	Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU- Mitgliedstaaten geboten.....	160
Anlage 13	Datenschutzgerechter Zugang zu Geoinformationen....	162
Anlage 14	Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren .....	164
Anlage 15	Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen.....	166
Anlage 16	Adress- und Datenhandel nur mit Einwilligung der Betroffenen .....	169

Anlage 17	Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten .....	170
Anlage 18	Elektronische Steuererklärung sicher und datenschutzgerecht gestalten .....	172
Anlage 19	Gegen Blankettbefugnisse für die..... Software-Industrie .....	174

### **Entschliefungen zwischen den Konferenzen 2009**

Anlage 20	Stärkung der IT-Sicherheit – aber nicht zu Lasten des Datenschutzes! (EntschlieÙung zum BSI-Gesetzesentwurf vom 18.02.2009) .....	176
-----------	---	-----

### **EntschlieÙung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. März 2009 in Berlin**

Anlage 21	Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz .....	178
Anlage 22	Defizite beim Datenschutz jetzt beseitigen.....	180
Anlage 23	Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage.....	181
Anlage 24	Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten!.....	182

### **EntschlieÙung zwischen den Konferenzen 2009**

Anlage 25	Datenschutz beim vorgesehenen Bürgerportal unzureichend.....	183
-----------	--	-----

### **EntschlieÙung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin**

Anlage 26	Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur .....	186
Anlage 27	Datenschutzdefizite in Europa auch nach Stockholmer Programm.....	188
Anlage 28	Krankenhausinformationssysteme datenschutzgerecht gestalten! .....	190
Anlage 29	Staatsvertrag zum IT-Planungsrat – Datenschutz darf nicht auf der Strecke bleiben.....	192

Anlage 30	"Reality-TV" – keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen .....	193
Anlage 31	Kein Ausverkauf von europäischen Finanzdaten an die USA! .....	195

### **Abkürzungsverzeichnis**

### **Sachregister**

### **Organigramm des TLfD**

## 1. Schwerpunkte im Berichtszeitraum

Erstmals führte der TLfD in den vergangenen zwei Jahren eine repräsentative Kontrolle in Thüringer Kommunen durch (5.1). Grund hierfür waren Ergebnisse einzelner Kontrollen im vorherigen Zeitraum, die auf technische und organisatorische Defizite beim Datenschutz schließen ließen. Dabei wurde in insgesamt 40 Kommunen unterschiedlichster Größe über Thüringen verteilt schwerpunktmäßig geprüft, ob grundlegende Datenschutzvorschriften umgesetzt sind, wie das Vorliegen eines Sicherheitskonzeptes, die Bestellung eines Datenschutzbeauftragten sowie das Vorhandensein von Verfahrensverzeichnis und Verfahrensfreigaben. Im Ergebnis haben sich die Befürchtungen leider bestätigt. So mussten 16 von 40 Stellen (40 %) formell beanstandet werden. Je kleiner die Kommunen – umso gravierender die Mängel. So wird in den kleinsten Kommunen ganz selbstverständlich modernste Technik zur Verarbeitung personenbezogener Daten eingesetzt, für einen angemessenen Datenschutzstandard fehlt aber häufig sowohl Geld, qualifiziertes Personal und nicht zuletzt auch das Problembewusstsein. Letzteres wurde sicherlich durch die Kontrollen bei den betreffenden Kommunen geschaffen. So ist im Nachgang ein enormer Bedarf an Beratung durch den TLfD entstanden und die Beseitigung der Mängel kommt nur langsam voran. Die Querschnittskontrolle hat aber auch gezeigt, dass der TLfD mit seiner sehr knapp bemessenen Personalausstattung an deutliche Grenzen gestoßen ist und andere ebenso wichtige Aufgaben nur unzureichend wahrnehmen konnte. In 15 Kommunen wurde zudem der Einsatz von Videoanlagen und Webcams überprüft (5.2). Vorangegangen war eine Umfrage bei 205 Kommunen über den Einsatz dieser Technik. Obwohl keine Stelle formell beanstandet werden musste, gab es zahlreiche Mängel bei den Rahmenbedingungen. Gerade die häufig anzutreffenden Unsicherheiten wegen fehlender konkreter gesetzlicher Regelungen zum Videoeinsatz müssen endlich zu einem gesetzgeberischen Gesamtkonzept für die Videoüberwachung durch öffentliche Stellen führen.

Bei der Kontrolltätigkeit gab es wiederum zahlreiche Beschwerden im Bereich der Ermittlungstätigkeit der Arbeitsgemeinschaften. So musste eine ARGE im Berichtszeitraum zweimal beanstandet werden, weil sie unverhältnismäßig in die Privatsphäre von Antragstellern bei der Sachverhaltsermittlung eingegriffen hat (11.5). Von den insgesamt 29 Beanstandungen betrafen zwei weitere die fehlende umfassende Aufklärung

und Einwilligung von Eltern und Schülern bei einer Befragung von Kindern und Jugendlichen (13.4), außerdem die unzulässige Veröffentlichung von Mitarbeiterdaten im Internet (5.3), die unzulässige Offenbarung von Daten aus einem Verwaltungsverfahren gegenüber der Presse (5.10) sowie die Weigerung eines Zweckverbandes zur Änderung seiner Satzungen hinsichtlich der Auswertung von Luftbildern (5.13). Auch im Verhältnis der öffentlichen Arbeitgeber zu ihren Bediensteten gab es in zwei extremen Fällen Anlass für eine Beanstandung. So hatte eine Gemeinde einem Bediensteten unter anderem deswegen gekündigt, weil er sich an den TLfD gewandt hat (6.5). In einem anderen Fall setzte eine Polizeidienststelle unzulässigerweise polizeiliche Mittel zur verdeckten Observation ein, um einen Kollegen des unberechtigten Krankfeierns zu überführen (6.2). Diese Fälle zeigen, dass der Beschäftigtendatenschutz endlich umfassend geregelt werden muss (6.1).

Für die Entwicklungen des Datenschutzes auch in Thüringen bedeutsam waren die grundlegenden Entscheidungen des Bundesverfassungsgerichts zur Vorratsdatenspeicherung (4.1) bzw. zur Online-Durchsuchung (2.), in der das sog. „IT-Grundrecht“ bzw. „Computer-Grundrecht“ entwickelt wurde. In beiden Urteilen ging es um die Herstellung der Balance zwischen Freiheit und Sicherheit. Die konkreten Auswirkungen auf Thüringen bestehen u. a. darin, dass das gerade erst novellierte Polizeiaufgabengesetz (7.1) in Bezug auf den Zugriff auf Telekommunikationsverkehrsdaten dieser Rechtsprechung angepasst werden muss.

Auch die Bürger gaben mit ihren Beschwerden im vergangenen Berichtszeitraum wichtige Hinweise auf datenschutzrechtliche Mängel. Neben dem Sozialbereich gab es auch einige Hinweise auf unzulässige Abfragen aus polizeilichen Datenbanken, die im Ergebnis zu gewissen Verbesserungen bei der Protokollierung und Auswertung der Abfragen führten (7.6). Gerade bei der unbefugten privaten Nutzung von dienstlich erlangten Informationen ist der TLfD zur Feststellung von Defiziten auf die Mithilfe der Bürger angewiesen, wie ein Fall aus dem Steuerbereich zeigt (9.7).

Einen ständig steigenden Stellenwert nimmt schließlich die Beratung sowohl der öffentlichen Stellen (z.B. 5.3, 5.4, 5.8, 11.4, 15.1) als auch des Gesetzgebers (z. B. 7.1 und 12.1) ein. Bei der Entwicklung der automatisierten Datenverarbeitung deutet sich insbesondere das sog. Cloud Computing (14.7) als eine Technik an, die zwar unter wirtschaftlichen

Gesichtspunkten positive Effekte versprechen könnte, allerdings durch den ggf. ständig wechselnden Verarbeitungsort vom Datenschutzrecht in seiner bisherigen Ausprägung kaum fassbar ist. Ebenso wird man sich in Zukunft innerhalb der Landesverwaltung verstärkt mit der (Nicht-)Protokollierung von Zugriffen der Bürger auf Internetangebote der Landesbehörden beschäftigen müssen (15.3).

Auch wenn sich bei vielen Behörden des Landes das Datenschutzbewusstsein verbessert hat, haben jedoch die vergangenen zwei Jahre gezeigt, dass es in der Fläche noch zum Teil gravierende Defizite gibt. Dies dürfte auch an der ständig fortschreitenden Digitalisierung sämtlicher Arbeitsbereiche der Verwaltung liegen. Um dies begleiten zu können, muss jedoch auch die Datenschutzkontrollbehörde angemessen ausgestattet sein.

## **2. Allgemeine Entwicklungen im Datenschutz**

Zunächst sollen hier einige allgemeine Entwicklungen im Datenschutz angesprochen werden, die sich vor allem im nicht-öffentlichen Bereich ergeben haben.

Von grundlegender Bedeutung sowohl für den öffentlichen wie auch für den nicht-öffentlichen Bereich war im Berichtszeitraum das Urteil des Bundesverfassungsgerichts zur sog. Online-Durchsuchung (Urteil vom 27. Februar 2008, 1 BvR 370/07), mit dem Teile des Verfassungsschutzgesetzes Nordrhein-Westfalen für nichtig erklärt wurden. Über den Einzelfall hinaus liegt dessen Bedeutung darin, dass die verfassungsrechtlichen Grundlagen des Datenschutzes an die technische Entwicklung angepasst und ein sog. „IT-Grundrecht“ bzw. „Computer-Grundrecht“ vom Bundesverfassungsgericht entwickelt worden ist. Dieses Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme ergänzt das bislang schon aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitete Recht auf informationelle Selbstbestimmung beim Einsatz informationstechnischer Systeme. Damit wird anerkannt, dass sich auf Personalcomputern und anderen IT-Systemen mit Wissen des Nutzers, aber vor allem auch unbemerkt, eine Vielzahl von persönlichen Informationen und Datenspuren befinden, die besonders zu schützen sind. Nicht nur der Staat wird vom BVerfG bei Eingriffen in dieses Grundrecht (wie bei der Online-Durchsuchung) engen Grenzen unterworfen, sondern auch der Gesetzgeber wird im Rahmen seiner Schutzpflichten im Datenschutzrecht Vorkehrungen treffen müssen, um im Verhältnis von Privaten den objektiven Gehalt des Grundrechts zur Wirkung zu verhelfen. Darauf haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung zu dem Urteil (Anlage 7) hingewiesen und den Gesetzgeber u. a. dazu aufgefordert, sich aktiv für die Vertraulichkeit und Integrität von IT-Systemen durch Verbesserung der Regelungen zum Schutz der Betroffenen vor einer elektronischen Ausforschung einzusetzen.

Obwohl von den Datenschutzbeauftragten seit vielen Jahren immer wieder die Modernisierung des Datenschutzrechts gefordert wurde, haben erst die Datenskandale der letzten beiden Jahre auch einer breiten Öffentlichkeit vor Augen geführt, dass es unter den veränderten Bedingungen der allgegenwärtigen und vernetzten Verarbeitung ihrer digitalisierten Daten durch Staat und Private auch Veränderungen beim

Schutz ihrer Persönlichkeitsrechte geben muss. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb in mehreren Entschliefungen die neuen Gefahren für die Privatheit aufgezeigt und die notwendigen Maßnahmen u. a. bei der Gesetzgebung gefordert. In einer „Berliner Erklärung“ vom April 2008 (Anlage 1) wurden in einer Art Bestandsaufnahme die Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts zusammengefasst. Nach den Datenskandalen im Frühjahr und Sommer 2008, bei denen ein Missbrauch von personenbezogenen Daten von Millionen von Menschen durch Privatunternehmen bekannt geworden war, haben sich die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich am 4. September 2008 zu einem sog. Datenschutzgipfel beim Bundesinnenminister getroffen und einen Maßnahmenkatalog u. a. auch zur Änderung der gesetzlichen Grundlagen beschlossen. Dieser Katalog wurde durch eine Entschliebung der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008 (Anlage 9) „Entschlossenes Handeln ist das Gebot der Stunde“ nachdrücklich unterstützt. Eine bereits zur Verbesserung der Informations- und Auskunftsansprüche beim Scoringverfahren im Bundestag diskutierte Änderung des Bundesdatenschutzgesetzes sollte danach um wichtige Regelungen ergänzt werden. Dazu gehörte u. a. die Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren, die Stärkung der datenschutzrechtlichen Auskunftsrechte, die Gewinnabschöpfung aus unbefugtem Datenhandel, die Einführung eines gesetzlichen Datenschutzaudits sowie die Stärkung der Datenschutzbeauftragten. Aufgrund der damaligen Datenskandale hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zwei Forderungen zur Novellierung des BDSG in Entschliefungen im November 2008 nochmals gesondert hervorgehoben. So sollten Unternehmen und öffentliche Stellen in den Datenschutzgesetzen verpflichtet werden, die Betroffenen und die Datenschutzaufsichtsbehörden umfassend über Datenschutzpannen zu informieren (Anlage 10). Zusätzlich wurde die Bundesregierung bestärkt, künftig den Adress- und den Datenhandel nur noch auf der Grundlage einer Einwilligung zuzulassen (Anlage 16). Der im Januar 2009 vorgelegte Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften enthielt einige Verbesserungen bei der Verwendung von personenbezogenen Daten zum Adresshandel, zu Werbezwecken sowie zur Markt- und Meinungsforschung. Außerdem war für Unternehmen vorgesehen, sich einem Datenschutzaudit unterziehen zu können, um für Datenschutzkonzepte und technische Einrichtungen ein Datenschutzsie-

gel zu erhalten. Auch nach einem erneuten Appell der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2009, die ersten notwendigen Korrekturen im BDSG zügig zu verabschieden (Anlage 22) und vor allem den Adresshandel künftig nur noch mit Einwilligung der Betroffenen zu erlauben, konnte sich der Bundestag zu einer umfassenden Einwilligungslösung nicht durchringen. Neben dem grundsätzlichen Einwilligungserfordernis gibt es noch eine Vielzahl von Ausnahmen. So dürfen Unternehmen weiterhin ihre bisherigen Kunden bewerben. Berufsbezogene Werbung an die berufliche Anschrift bedarf ebenso wie Spendenwerbung gemeinnütziger Organisationen keiner Einwilligung, wenn lediglich Listendaten genutzt werden. Zudem darf Werbung weiterhin versandt werden, wenn der Betroffene aus dem Werbeschreiben erkennen kann, welches Unternehmen seine Adressdaten hierfür weiterverkauft hat. Das Datenschutzauditgesetz wurde in der letzten Legislaturperiode nicht mehr verabschiedet. Nach der Bundestagswahl hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 26) nochmals bekräftigt, dass zu Beginn der neuen Legislaturperiode des Deutschen Bundestages eine Generalrevision des Datenschutzrechts erforderlich ist. Hierzu muss es u. a. an die Herausforderungen neuer Technologien angepasst, die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet, ein praktikables Datenschutzaudit geschaffen sowie die Datenschutzaufsichtsbehörden so ausgestaltet werden, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können. Der Koalitionsvereinbarung ist zu entnehmen, dass „Grundsätze der Verhältnismäßigkeit, der Datensicherheit und -sparsamkeit, der Zweckbindung und der Transparenz im öffentlichen und privaten Bereich noch stärker zur Geltung“ gebracht werden sollen. Dazu „soll das Bundesdatenschutzgesetz unter Berücksichtigung der europäischen Rechtsentwicklung lesbarer und verständlicher gemacht sowie zukunftsfest und technikneutral ausgestaltet werden.“ Die Datenschutzbeauftragten wollen im Rahmen ihrer Möglichkeiten diese Modernisierung des Datenschutzes begleiten.

Modernisierungsbedarf gibt es aber nicht nur auf der Bundesebene. Ebenso muss auf Landesebene das Thüringer Datenschutzgesetz u. a. den veränderten technischen Anforderungen angepasst werden. Bereits bei der Novellierung im Jahr 2001 wurden einige Modernisierungsschritte noch nicht gegangen, deren Notwendigkeit sich heute umso stärker in der Praxis zeigt. Eines dieser Probleme sind die unzureichen-

den Regelungen zum Einsatz der Videoüberwachung, auf die bereits in den vergangenen Tätigkeitsberichten (7. TB, 5.2) hingewiesen wurde. Hierzu gehört auch das Problem von Gemeinsamen Verfahren bzw. Verbundverfahren. Bei der Einführung zentraler Verfahren (z. B. im Bereich des eGovernment) gibt es im Gegensatz zu anderen Ländern keine gesetzliche Möglichkeit, dass sich mehrere Stellen einen automatisierten Zugriff auf einen gemeinsamen Datenbestand einräumen, obwohl hierfür ein nachvollziehbares Interesse besteht. Deshalb müssen hier eine Vielzahl von Auftragsdatenverarbeitungen nach § 8 ThürDSG in Verbindung mit einer entsprechenden Anzahl von automatisierten Ab-rufverfahren nach § 7 ThürDSG eingerichtet werden, was ein sehr bürokratisches Verfahren darstellt. Zunehmende Probleme werfen auch die Veröffentlichungen personenbezogener Daten durch öffentliche Stellen im Internet auf. Wegen der fast unbegrenzten Speicherdauer und der sehr einfachen Recherchierbarkeit dieser Daten über Suchmaschinen im Vergleich zu den bislang üblichen Veröffentlichungsmethoden muss über die Zulässigkeit einer Internetveröffentlichung neu nachgedacht werden. Aber auch bei der Einrichtung von Foren oder Blogs, bei denen die öffentlichen Stellen die Plattform zur Veröffentlichung von Meinungen oder Anregungen der Bürger zur Verfügung stellen, müssen Regelungen getroffen werden, unter welchen Voraussetzungen und wie mit diesen Daten umgegangen werden darf. Diese und eine Reihe weiterer Punkte hat der TLfD zum Ende der Legislaturperiode der Landesregierung zur Einbeziehung in die bereits angekündigte Novellierung des ThürDSG übermittelt. Der Koalitionsvereinbarung ist zu entnehmen, dass „das Thüringer Datenschutzgesetz novelliert und den veränderten Anforderungen an die Verwendung personenbezogener Daten und an die aktuelle Rechtsprechung angepasst werden soll.“ Es bleibt zu hoffen, dass im Gleichklang mit den Modernisierungsschritten auf Bundesebene auch eine Modernisierung des Thüringer Datenschutzgesetzes gelingt.

Für die Frage, ob und wie die Datenschutzaufsichtsbehörden in ihrer Kontrollfunktion gestärkt werden können, ist auch das Urteil des Europäischen Gerichtshofs zu einer Vertragsverletzungsklage der Kommission von Bedeutung. Darin warf diese Deutschland vor, dass in allen 16 Bundesländern gegen das Gebot der völligen Unabhängigkeit der Datenschutzkontrollstellen aus Artikel 28 Abs. 1 Satz 2 der Richtlinie 95/46/EG verstoßen werde. Weil selbst in denjenigen Bundesländern, in denen die Aufsicht im nicht-öffentlichen Bereich von den Datenschutzbeauftragten wahrgenommen wird, eine Rechtsaufsicht durch ein Lan-

desministerium oder die Landesregierung bestehe, könne nach Ansicht der EU-Kommission die Verwaltung die Entscheidungen der Datenschutzaufsichtsbehörden beeinflussen. Das sei aber nicht mehr als völlige Unabhängigkeit anzusehen. Dem folgte der Europäische Gerichtshof in seiner Entscheidung vom 9. März 2010 (C-518/07) in vollem Umfang. Damit sind alle Länder nunmehr verpflichtet, die Aufsichtsbehörden außerhalb der Landesverwaltung ohne Fach- und Rechtsaufsicht zu organisieren. Es wird hinsichtlich der bereits beim Datenschutzgipfel vereinbarten Stärkung der Aufsichtsbehörden zu überlegen sein, ob diese noch schlagkräftiger werden könnten, wenn sie in allen Bundesländern unter dem Dach des jeweiligen Landesdatenschutzbeauftragten gebündelt werden. Der TLfD ist in dieser Hinsicht für Vorschläge offen, wenn dadurch seine Unabhängigkeit nicht beeinträchtigt wird.

Großen Raum in der datenschutzrechtlichen Diskussion der letzten Jahre nahm auch die Nutzung des Internets ein. Viele Fragen stellten sich bei den Anwendungen, die unter dem Begriff „Web 2.0“ zusammengefasst sind. Darunter versteht man vor allem sog. soziale Netzwerke wie MySpace, Facebook, StudiVZ und ähnliche Plattformen, die den Beteiligten die Möglichkeit bieten, Profile in das Netz zu stellen und die Zugriffsberechtigten selbst festzulegen. Sie gewähren u. a. die Kontaktaufnahme zu anderen Mitgliedern, die Versendung und den Empfang von Nachrichten sowie das Einstellen von Bildern und Blogs in das jeweilige Netzwerk. Man sollte vor dem Hintergrund, dass einmal im Internet gespeicherte Daten nur noch sehr schwer zu kontrollieren sind, genau überlegen, wem man was über sich und sein Leben offenbart. Richtig ist, dass hier jeder selbst entscheiden muss, wie viel er über sich selbst Preis geben möchte. Eine solche informationelle Selbstbestimmung kann aber nur dann wahrgenommen werden, wenn man die „Privatsphäre-Einstellungen“ auf seinem sozialen Netzwerk versteht. Deshalb sind auch die Anbieter gefordert, ihre Systeme verständlich und datenschutzfreundlich zu gestalten und dürfen sich nicht hinter dem Argument der Selbstbestimmung der Nutzer verstecken. Besonders Schüler und Jugendliche müssen einen verantwortungsvollen Umgang mit ihren persönlichen Daten gerade in solchen Netzwerken praktizieren (vgl. 13.1).

Die Möglichkeiten des Web 2.0 könnten künftig auch bei der Arbeit des Petitionsausschusses im Thüringer Landtag genutzt werden. So sah es jedenfalls ein von der Fraktion DIE LINKE in der vierten Legislaturpe-

riode eingebrachter Gesetzentwurf vor, mit dem nach dem Vorbild des Bundestages sog. Online-Petitionen ermöglicht werden sollten. Danach könnten öffentliche Petitionen auf einer vom Landtag betriebenen Internetseite veröffentlicht werden, die in einem öffentlichen Internetforum von weiteren Personen als Mitzeichner unterstützt oder auch kommentiert werden können. Obwohl die Datenverarbeitung im Landtag nicht in den Zuständigkeitsbereich des TLfD fällt, hat dieser im Rahmen einer schriftlichen Anhörung des Petitionsausschusses zu dem Gesetzentwurf Stellung genommen. Bei den Online-Petitionen sind im Grundsatz zwei Personengruppen mit unterschiedlichem Schutzbedürfnis vorhanden. Soweit es sich um Petenten oder deren Unterstützer handelt, machen diese ihre Unterstützung der Petition aus eigenem Antrieb freiwillig öffentlich und sind daher nicht besonders schutzwürdig. Allerdings müssen zur Wahrung der Freiwilligkeit ausreichende Datenschutzvorkehrungen getroffen werden. Dabei ist wichtig, dass die Betroffenen über die einzelnen Schritte der Datenverarbeitung aufgeklärt werden und nach den geltenden Bedingungen auch Herr über ihre personenbezogenen Daten bleiben. Das schließt z. B. auch ein, dass die Daten nicht auf unbefristete Zeit abrufbar gespeichert bleiben und der Betroffene die Löschung seiner Daten verlangen kann. Welche Daten und Ansichten er über sich dabei preisgibt, muss er sich ebenso wie bei sozialen Netzwerken selbst genau überlegen. Die Akzeptanz solcher Foren kann auch dadurch erhöht werden, dass die Beiträge und Kommentare durch Pseudonym erfolgen, wobei der Landtagsverwaltung die Identität der Betroffenen bekannt ist. Die andere Gruppe von Betroffenen bei Online-Petitionen sind die Personen, auf die sich die Online-Petition inhaltlich beziehen könnte. Da es für die Veröffentlichung von deren Daten grundsätzlich keine gesetzliche Befugnis gibt, muss der Schutz dieser Personen weitgehend gewährleistet werden. Zu einer Beschlussfassung über den Gesetzentwurf ist es aber wegen Ablauf der Legislaturperiode nicht gekommen.

Die Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über Volks- und Wohnungszählungen verpflichtet die Mitgliedstaaten der Europäischen Union, Daten anhand eines festgelegten Katalogs von Merkmalen (Zensusdaten) im Jahr 2011 zu erheben. Bereits in den letzten Tätigkeitsberichten wurde darauf hingewiesen, dass sich Deutschland an dieser Volkszählungsrunde der Europäischen Union 2011 mit einem registergestützten Zensus beteiligen wird. Aufbauend auf dem Zensusvorbereitungsgesetz 2007 wurde

im Juli 2009 mit dem Zensusanordnungsgesetz das eigentliche Zensusgesetz 2011 (ZensG 2011) beschlossen und verkündet (BGBl. I, S. 1781). Damit ist nun klar, dass die Statistischen Ämter des Bundes und der Länder zum Stichtag 9. Mai 2011 eine Bevölkerungs-, Gebäude- und Wohnungszählung durchführen werden, die erstmals nicht mehr im Wege einer traditionellen Volkszählung, einer Befragung aller Einwohner, sondern im wesentlichen registergestützt, d. h. durch Auswertung vorhandener Melde- und anderer Verwaltungsregister durchgeführt wird. Haushalte werden nur noch auf Stichprobenbasis befragt. Wird die Volkszählung gesetzeskonform durchgeführt, bestehen seitens der Datenschutzbeauftragten des Bundes und der Länder zwar keine grundsätzlichen datenschutzrechtlichen Bedenken, die Vorbereitung und Durchführung des Zensus muss aber weiterhin kritisch begleitet werden. Auf die Einhaltung der Vorgaben des Volkszählungsurteils des Bundesverfassungsgerichts von 1987, insbesondere auf die Einhaltung des entscheidenden Grundsatzes der Trennung der Statistik vom Verwaltungsvollzug, wird zu achten sein. Das ZensG 2011 überlässt den Landesgesetzgebern die Bestimmung von Erhebungsstellen und das Nähere zur Organisation der vorzunehmenden Erhebungen und Maßnahmen. Deshalb ist die Schaffung eines Thüringer Gesetzes zur Ausführung des Zensus 2011 erforderlich. Darin sollen die erforderlichen organisations- und verfahrensrechtlichen Bestimmungen für die Durchführung dieser Volks-, Gebäude- und Wohnungszählung im Jahr 2011 im Freistaat Thüringen normiert werden. Dem TLfD wurde vom Thüringer Innenministerium die Möglichkeit der datenschutzrechtlichen Stellungnahme zum Entwurf des o. g. Thüringer Gesetzes gegeben. Die datenschutzrechtlichen Forderungen des TLfD sind alle in den Gesetzentwurf übernommen worden.

### **3. Europäischer und Internationaler Datenschutz**

#### **3.1 Keine Vorratsdatenspeicherung von Flugpassagierdaten**

Der Bekämpfung des Terrorismus und der organisierten Kriminalität soll eine Initiative der EU-Kommission vom November 2007 dienen, mit der die Mitgliedsstaaten verpflichtet werden sollen, Flugpassagierdaten auf Vorrat zu speichern und zusätzlich ermächtigt werden, diese Daten mit Drittstaaten auszutauschen. Im Entwurf eines Rahmenbeschlusses ist die Erweiterung der bereits bislang zu speichernden Datensätze und die Verlängerung der Speicherfristen auf bis zu 13 Jahre vorgesehen. Gegen dieses Vorhaben haben sich Anfang 2008 sowohl der Bundesrat in einer Stellungnahme wie auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Anlage 2) ausgesprochen. Hauptkritikpunkt war, dass die Daten aller Flugreisenden, die in Nicht-EU-Staaten reisen, für bis zu 13 Jahre in Zentralstellen aufbewahrt und für Risikoanalysen benutzt werden sollen, ohne dass von diesen Menschen eine besondere Nähe zu einer Gefahr bestehen muss. Dies wäre aber der klassische Fall einer Vorratsdatenspeicherung, die weder mit europäischem Recht noch mit deutschem Verfassungsrecht vereinbar wäre. Die Konferenz hat daher gefordert, dass die Bundesregierung den Entwurf auf europäischer Ebene ablehnt. In den Ratsgremien ist bislang noch keine Entscheidung über den Rechtsakt gefallen.

Es bleibt zu hoffen, dass auch vor dem Hintergrund aktueller terroristischer Bedrohungen im internationalen Luftverkehr das von der Bundesregierung in der Bundestagsdebatte vom April 2008 vorgetragene Ziel, einen Beschluss zu erreichen, der das Gleichgewicht zwischen Sicherheits- und Datenschutzinteressen wahrt, erreicht wird.

#### **3.2 Austausch von Sicherheitsdaten D-USA ohne ausreichende Datenschutzgarantien**

Gibt es beim Datenaustausch der Strafverfolgungs- und Gefahrenabwehrbehörden bereits innerhalb der Europäischen Union das Problem noch fehlender einheitlich hoher Datenschutzstandards (s. u. 3.3), so verschärft sich dieses beim Austausch von Erkenntnissen zwischen deutschen und US-amerikanischen Sicherheitsbehörden noch weiter. Dass es angesichts weltweit agierender Straftäter insbesondere bei der Bekämpfung des Terrorismus aber auch der organisierten Kriminalität

einen zunehmenden Bedarf an Austausch von Informationen gibt, kann durchaus nachvollzogen werden. Allerdings dürfen dabei die bestehenden Grundrechtsstandards nicht abgesenkt werden. Gerade das muss aber bei dem im Jahr 2008 unterzeichneten deutsch-amerikanischen Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Bekämpfung schwerwiegender Kriminalität konstatiert werden. Nach dem Vorbild des Prümer Vertrages (7. TB, 3.1) wird mit dem Abkommen ein gegenseitiger Online-Zugriff auf DNA- und Fingerabdruck-Indexdateien eingeräumt sowie ein präventiver Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten ermöglicht. Allerdings wurden die im Prümer Vertrag enthaltenen Datenschutzregelungen zum größten Teil nicht in das Abkommen übernommen. Hauptkritikpunkt ist das nur unzureichende Datenschutzniveau in den USA, das vor allem keine unabhängige Datenschutzkontrolle kennt und deutschen Staatsbürgern keine selbst einklagbaren Datenschutzrechte (z. B. auf Auskunft, Berichtigung oder Löschung) einräumt. Trotz der von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 4) geäußerten deutlichen Kritik, wurde das Abkommen zwischenzeitlich ratifiziert. Auch mit dem ebenfalls verabschiedeten Gesetz zur Umsetzung des Abkommens sind diese datenschutzrechtlichen Mängel nicht beseitigt. Zwar kann sich danach ein deutscher Betroffener an das BKA wenden, damit dieses die nach dem Abkommen bestehenden völkerrechtlichen Ansprüche auf Auskunft, Berichtigung, Sperrung und Löschung gegenüber den USA geltend macht. Letztlich kann jedoch auch das BKA diese Ansprüche nicht durchsetzen. Sei es bei einem Auskunftsbegehren, wenn unvollständige oder unzutreffende Auskünfte gegeben werden oder bei Zweifeln, ob eine zugesicherte Datenlöschung, tatsächlich erfolgt ist, da keine unabhängige Kontrollinstanz angerufen werden kann.

Bei künftigen Abkommen muss bei einem mangelhaften Datenschutzniveau im Empfängerstaat ein ausreichendes Datenschutzregime in das Abkommen selbst mit einklagbaren Rechten der Betroffenen aufgenommen werden.

### **3.3 Polizeilicher Datenaustausch in der EU nicht immer auf höchstem Datenschutzniveau**

Wie sich bereits im letzten Berichtszeitraum abgezeichnet hat (7. TB, 3.1) konnte bei der polizeilichen und justiziellen Zusammenarbeit in der

EU bislang kein angemessenes Datenschutzniveau erreicht werden. Der über Jahre diskutierte Rahmenbeschluss 2008/977/JI vom 27. November 2008 über den Datenschutz in der sog. Dritten Säule stellt zwar eine gewisse Verbesserung der Datenschutzstandards beim Austausch von Daten zum Zweck der Gefahrenabwehr oder Strafverfolgung dar. Allerdings erfüllt er die nochmals von den Datenschutzbeauftragten des Bundes und der Länder in einer EntschlieÙung (Anlage 11) erhobene Forderung nach seiner Anwendbarkeit auf die gesamte nationale und grenzüberschreitende Informationsverarbeitung in diesem Bereich nicht. Vielmehr gelten die festgelegten Prinzipien zunächst nur für den Austausch, nicht aber generell für die nationale Datenverarbeitung durch Polizei- und Strafverfolgungsbehörden in den Mitgliedsstaaten. Es bleibt zu hoffen, dass mit dem Inkrafttreten des Vertrages von Lissabon, mit dem die Säulenstruktur in der Innen- und Justizpolitik aufgelöst wurde, nun bald von der in Art. 16 Abs. 2 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) eingeräumten Kompetenz zur Schaffung eines einheitlichen europäischen Datenschutzgesetzes Gebrauch gemacht wird. Das fehlende einheitliche Datenschutzniveau bei der polizeilichen und justiziellen Zusammenarbeit wirkt sich aktuell bei der Umsetzung der sog. „Schwedischen Initiative“ aus. Mit diesem Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 soll der Informationsaustausch zwischen den Strafverfolgungsbehörden der EU-Mitgliedsstaaten dahingehend vereinfacht werden, dass auf EU-Ebene keine strengeren Übermittlungsvoraussetzungen als auf nationaler Ebene gelten sollen. Hintergrund ist der Umstand, dass in den einzelnen Mitgliedstaaten in diesem Rechtsbereich bislang noch sehr unterschiedliche Voraussetzungen für die Datenübermittlung gelten. Häufig wird in diesen Vorschriften eine Datenübermittlung davon abhängig gemacht, ob beim Empfängerstaat ein bestimmter Mindeststandard an Datenschutzregelungen garantiert ist. Gerade das ist aber noch nicht ausreichend gewährleistet, vor allem für die weitere Verwendung der Daten bei den Empfängern. Da der Rahmenbeschluss nicht direkt anwendbar ist, sondern erst noch vom Gesetzgeber in nationales Recht umgesetzt werden muss, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer EntschlieÙung (Anlage 12) gefordert, den verbleibenden Umsetzungsspielraum zu nutzen und die Befugnisse normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit zu regeln. Im Polizeiaufgabengesetz war bereits vor der Verabschiedung des Rahmenbeschlusses im Sommer 2008 (7.1) eine sehr allgemeine und wenig konkrete Befugnis in § 41 Abs. 1 Satz 2 PAG aufgenommen

worden, wonach Daten zwischen Dienststellen der Polizei auch anderer Mitgliedsstaaten der Europäischen Union in Übereinstimmung mit datenschutzrechtlichen Regelungen übermittelt werden können, wenn sie zur polizeilichen Aufgabenerfüllung erforderlich sind. Ein Entwurf eines Bundesgesetzes zur Umsetzung des Rahmenbeschlusses lag bis zum Redaktionsschluss noch nicht vor.

Nach dem Erlass eines Bundesgesetzes zur Umsetzung der „Schwedischen Initiative“ sollte geprüft werden, inwieweit es weiteren Konkretisierungsbedarf bei der Übermittlungsnorm des Polizeiaufgabengesetzes gibt.

### **3.4 Stockholmer Programm - Mehr Sicherheit und (auch mehr) Freiheit in Europa?**

In der zweiten Jahreshälfte 2009 hat die Europäische Kommission den Entwurf für ein Programm vorgestellt, das die politischen Zielvorgaben zur Weiterentwicklung des Raums der Freiheit, der Sicherheit und des Rechts (Haager Programm) für die nächsten fünf Jahre festschreiben soll. Es wird den Titel „Stockholmer Programm“ erhalten und wie bei politischen Zielvorgaben häufig, sind die beabsichtigten Maßnahmen nur sehr allgemein beschrieben. Zwar wird an vielen Stellen des Entwurfs die Bedeutung der Freiheitsrechte und der Schutz der Privatsphäre hervorgehoben, indem z. B. der Beitritt der EU zur Europäischen Menschenrechtskonvention oder aber die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien angekündigt werden. Allerdings enthält der Entwurf auch wieder einen Katalog sehr eingriffsintensiver Maßnahmen, wie ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems. Wie auch bei anderen Maßnahmen auf EU-Ebene haben die Datenschutzbeauftragten des Bundes und der Länder in einer EntschlieÙung (Anlage 27) angemahnt, ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen, indem z. B. der Rahmenbeschluss 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht weiterentwickelt wird (vgl. auch 3.3) oder ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedsstaaten eingerichtet wird. Das Programm wurde in diesen Punkten in eher unverbindlicher Form verabschiedet. Allgemeinplätze

wie die Ankündigung einer „soliden Datenschutzregelung“ müssen wohl erst noch mit Leben erfüllt werden und so bleibt abzuwarten, welche konkreten Maßnahmen in den kommenden fünf Jahren aus dem Programm abgeleitet werden.

Bei den auf der Grundlage des Stockholmer Programms geplanten Eingriffen in die Bürgerrechte muss endlich auch dem Datenschutz durch konkrete Maßnahmen der ihm zukommende Stellenwert eingeräumt werden.

### **3.5 Kein Ausverkauf europäischer Finanzdaten an USA**

Ende 2009 wurde zwischen der Europäischen Union und den USA über ein Abkommen verhandelt, das US Behörden den Zugriff auf Finanztransaktionsdaten erlaubt, die auf Servern der belgischen Genossenschaft SWIFT in Europa gespeichert sind. Diese Zugriffe sollen der Bekämpfung der Terrorismusfinanzierung dienen. Kritisch daran ist vor allem, dass auch Zugriffe auf Transaktionsdaten erfolgen sollen, bei denen gegen die Betroffenen kein hinreichender Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Notwendig geworden war ein solches Abkommen, weil nach massiver Kritik im Jahr 2006 (7. TB, 3.1) die belgische Genossenschaft SWIFT, die den größten Teil des weltweiten bargeldlosen Zahlungsverkehrs abwickelt, sich veranlasst sah, einen Server, auf dem sämtliche Transaktionen als Sicherungskopie enthalten waren, von den USA nach Europa zu verlegen. Damit war jedoch der bis dahin ungehinderte Zugriff durch die US-Behörden nicht mehr möglich. Da aber auch europäische Sicherheitsbehörden bislang von den Erkenntnissen der US-Behörden bei der Terrorbekämpfung profitiert haben, sollten in einem Abkommen den US-Behörden weiterhin Zugriffsrechte eingeräumt werden. Wie bereits bei dem deutsch-amerikanischen Abkommen zum Datenaustausch (3.2) war auch hier ein Hauptproblem das in den USA fehlende ausreichende Datenschutzniveau. Zusätzlich gab es Zweifel, ob ein solch umfassender Zugriff überhaupt notwendig ist, da die Strafverfolgungsbehörden bereits im Einzelfall im Rahmen der Rechtshilfe Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln dürfen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung (Anlage 31) auf diese Defizite hingewiesen und die Bundesregierung aufgefordert, einem Abkommen nicht zuzustimmen, das eine Datenübermittlung weit unterhalb der Schwelle

des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt. Als Provokation wurde vom Europäischen Parlament die Beschlussfassung über das Abkommen durch die Innen- und Justizminister der EU-Staaten auf einer Sitzung einen Tag vor dem Inkrafttreten des Lissabonner Vertrages empfunden, da dieser dem Europäischen Parlament erweiterte Mitspracherechte für den Abschluss derartiger Abkommen einräumt. Letztlich konnte sich Deutschland nicht durchringen, gegen das Abkommen zu stimmen, sondern enthielt sich, was im Ergebnis als Zustimmung gewertet wurde. Es wurde allerdings nur eine sehr kurze Laufzeit vereinbart mit dem Ziel, so schnell wie möglich ein überarbeitetes Abkommen auszuhandeln, das die datenschutzrechtlichen Anforderungen erfüllt und unter Mitbestimmung des Europäischen Parlaments abgeschlossen werden soll. Schließlich konnte es doch nicht endgültig in Kraft treten, weil das Europäische Parlament am 11. Februar 2010 mit großer Mehrheit gegen das am 1. Februar 2010 vorläufig in Kraft getretene Abkommen votiert hat. Es war die erste Entscheidung des Europäischen Parlaments im erweiterten Mitentscheidungsverfahren im Bereich der Inneren Sicherheit nach dem Vertrag von Lissabon überhaupt. Dass dabei ein deutliches Zeichen zur Stärkung der Grundrechte auf europäischer Ebene gesetzt wurde, ist sehr erfreulich.

Das Verfahren zum Abschluss des Abkommens war kein Ruhmesblatt für die Verteidigung der Grundrechte der EU-Bürger durch die EU. Es bleibt zu hoffen, dass dies im zweiten Anlauf besser gelingt.

## **4. Neue Medien - Rundfunk - Telekommunikation**

### **4.1 Bundesverfassungsgericht stoppt die Vorratsdatenspeicherung**

In einer viel beachteten Grundsatzentscheidung vom 2. März 2010 (Az.: 1 BvR 256/08) hat das Bundesverfassungsgericht die Vorschriften zur Vorratsdatenspeicherung von Telekommunikationsdaten (7. TB, 4.1) für nichtig erklärt und die Löschung aller bislang auf dieser Grundlage gespeicherten Daten angeordnet. Die vorsorgliche anlasslose Speicherung der Daten stellt nach Ansicht des Gerichts einen besonders schweren Eingriff in das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG mit einer Streubreite dar, wie sie die Rechtsordnung bislang nicht kennt. Dennoch kann ein solcher Eingriff nach Auffassung des Gerichts noch verhältnismäßig sein, wenn angemessene gesetzliche Regelungen zur Datensicherheit, zur Begrenzung der Verwendungszwecke der Daten, zur Transparenz der Datenübermittlung sowie zum Rechtsschutz getroffen werden. All diese Anforderungen fanden bei der geltenden Regelung keine ausreichende Beachtung, weshalb § 113a und § 113b TKG für nichtig erklärt wurden; ebenso § 100g Abs. 1 Satz 1 StPO, soweit danach Verkehrsdaten nach § 113a Telekommunikationsgesetz (TKG) erhoben werden dürfen.

Es gab bereits in den letzten zwei Jahren seit dem Inkrafttreten der Regelungen eine ganze Reihe vorläufiger Entscheidungen und Verfahrensschritte von Gerichten auf europäischer und nationaler Ebene, die sich mit der auf der Grundlage der Richtlinie 2006/24/EG angeordneten Maßnahme befassten. Die vom Europäischen Gerichtshof ergangene Entscheidung vom 10. Februar 2009 (C-301/06) hat hinsichtlich der Vereinbarkeit der Richtlinie mit den Grundrechten keine Klarheit gebracht, weil in dem von Irland ausgelösten Verfahren nur über die Frage der einschlägigen Kompetenznorm und damit über die Art der Rechtsnorm und das bei deren Erlass einzuhaltende Verfahren entschieden wurde. Der EuGH bestätigte die gewählte Kompetenznorm aus der sog. ersten Säule zur Rechtsangleichung im Binnenmarkt, weil die Richtlinie überwiegend das Funktionieren des Binnenmarkts betreffe.

Das Bundesverfassungsgericht hat am 11. März 2008 (1 BvR 256/08) eine einstweilige Anordnung erlassen, in der festgelegt wurde, dass Anbieter von Telekommunikationsdiensten die verlangten Daten zwar

zu erheben und zu speichern haben. Die Daten durften jedoch nur dann an die Strafverfolgungsbehörden übermittelt werden, wenn Gegenstand des Ermittlungsverfahrens eine schwere Straftat im Sinne des § 100a Abs. 2 StPO ist, die auch im Einzelfall schwer wiegt, der Verdacht durch bestimmte Tatsachen begründet war und die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert oder aussichtslos wäre. In den übrigen Fällen des § 100g Abs. 1 StPO war von einer Übermittlung der Daten einstweilen abzusehen. Eigentlich hätte man erwarten können, dass vom Bundesverfassungsgericht nicht nur Anordnungen zur Verwendung der auf Vorrat gespeicherten Daten für die Strafverfolgung ergehen, sondern auch zu der verdachtslosen Vorratsdatenspeicherung selbst. Daran sah sich das Bundesverfassungsgericht aber bislang gehindert, weil die Speicherpflicht auf der Grundlage einer zwingend umzusetzenden EU-Vorschrift erfolgt und das Bundesverfassungsgericht hierzu seine Gerichtsbarkeit solange nicht ausübt, als die Europäischen Gemeinschaften einen wirksamen Grundrechtsschutz generell gewährleisten. Mit der Entscheidung des EuGH, dass die Richtlinie 2006/24/EG rechtmäßig zustande gekommen ist, wurde auch kein erweiterter Spielraum zur Prüfung des Gesetzes am Maßstab deutscher Grundrechte geschaffen. Dadurch, dass das Bundesverfassungsgericht in seiner Hauptsacheentscheidung eine Vorratsdatenspeicherung unter engen Voraussetzungen für verfassungsrechtlich zulässig ansieht, ist es der Bundesrepublik Deutschland weiterhin möglich, die Richtlinie auch nach der Nichtigkeit von § 113a und § 113b TKG mit einem neuen Gesetz umzusetzen.

Die einstweiligen Anordnungen wurden jeweils um 6 Monate verlängert und mit Beschluss vom 28. Oktober 2008 nochmals inhaltlich erweitert. Der Grund dafür lag darin, dass nach der ersten Anordnung vom 11. März 2008 in den Polizeiaufgabengesetzen der Freistaaten Bayern und Thüringen sowie im Bayerischen Verfassungsschutzgesetz unter ausdrücklicher Bezugnahme auf § 113a TKG der Zugriff auf Telekommunikationsverbindungsdaten erlaubt wurde. Hier hat das Bundesverfassungsgericht einen Abruf auf die Abwehr von dringenden Gefahren für Leib, Leben, Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder auf die Abwehr einer gemeinen Gefahr beschränkt. Dies wurde in der Hauptsacheentscheidung bestätigt und gleichzeitig festgestellt, dass für die Gefahrenabwehr eine wirksame Begrenzung des Datenzugriffs durch Bezugnahme auf Kataloge von Straftaten, deren Verhinderung die Datenverwendung dienen soll, eine

ungeeignete Regelungstechnik ist. Damit sind die in § 34a Abs. 3 Nr. 2 und 3 PAG Thüringen vorgesehenen Befugnisse zur Verhütung von dort aufgeführten Straftaten für einen möglichen künftigen Zugriff auf Vorratsdaten nicht mehr verfassungsgemäß und müssen geändert werden.

Die Auswertung des Urteils zur Vorratsdatenspeicherung muss auch im Polizeiaufgabengesetz zu einer Anpassung bei den Voraussetzungen zum Zugriff auf Verkehrsdaten führen.

## 4.2 Bürgerportalgesetz und De-Mail

In der heutigen Kommunikation ist mittlerweile die E-Mail nicht mehr wegzudenken. Ein großer Teil der Menschen nutzt sie für private aber auch zunehmend für geschäftliche Mitteilungen. Die Hauptvorteile der E-Mail gegenüber der Briefpost sind die hohe Geschwindigkeit, die einfache Handhabung, die geringen Kosten und die Ortsunabhängigkeit. Allerdings gibt es auch neben der lästigen SPAM-Flut noch weitere gewichtige Nachteile. So kann nach wie vor der E-Mail eine nur unzureichende Vertraulichkeit zugesprochen werden, da sie unverschlüsselt über die Datennetze ggf. der halben Welt unterwegs ist. Dabei kann sie sich in diesen Datenwelten verirren, verfälscht oder von Filtern unterschiedlichster Art abgefangen werden bzw. der Empfänger selbst löscht sie versehentlich ungelesen. Es gibt also bislang kein verlässliches Verfahren, um Absender und Empfänger die erfolgreiche unveränderte Übermittlung zu quittieren. Hier soll ein von der Bundesregierung geplantes Projekt mit dem Namen De-Mail Abhilfe schaffen. Es wurde noch zum Ende der letzten Legislaturperiode der Entwurf eines Bürgerportalgesetzes vorgelegt, mit dem eine Infrastruktur für eine sichere E-Mail-Kommunikation durch Einrichtung von Bürgerportalen erreicht werden soll. Die Bürgerportale sollen von privaten Diensteanbietern betrieben werden, die standardisierte Adressformate (vorname.name@provider.de-mail.de) bereitstellen, die sich eindeutig von normalen E-Mail-Adressen unterscheiden. An diese Bürgerportale muss sich der Nutzer mit seiner Kennung und ggf. mit einem elektronischen Ausweis (Chipkarte, Token oder neuer elektronischer Personalausweis) sowie einem Passwort anmelden. Die Kommunikation erfolgt dann zwischen den zertifizierten Diensteanbietern über verschlüsselte Kanäle. Damit soll die Vertraulichkeit, Integrität und Authentizität der Kommunikation hergestellt werden. Technisch und auch rechtlich ist dies schon seit vielen Jahren durch den Einsatz der elektronischen Signatur und

eine Ende-zu-Ende-Verschlüsselung möglich. Da die Verfahren bislang jedoch noch relativ kompliziert und kostenträchtig sind, haben sie noch keine ausreichende Verbreitung gefunden. Deshalb ist eine solche Initiative, die breit angelegt zu einer Verbesserung der Vertraulichkeit der elektronischen Kommunikation führen soll, grundsätzlich zu begrüßen. Sicherlich ist hier der Spatz (die Kommunikation über verschlüsselte Kanäle und zertifizierte Anbieter) in der Hand besser als die Taube (die ausschließliche Ende-zu-Ende-Verschlüsselung) auf dem Dach. Allerdings haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 25) noch Verbesserungen zu dem Gesetzentwurf gefordert. In jedem Fall muss das System es zulassen und auch fördern, dass die Kommunikationspartner bei sensiblen Informationen auf einfachem Weg eine qualifizierte Signatur einsetzen können. Außerdem sind elektronische Sende- und Empfangsbestätigungen vorgesehen, die mit einer hohen Beweiskraft ausgestattet sind und so Verlässlichkeit über das Absenden und den Empfang wichtiger Mitteilungen schaffen sollen. Das Gesetz konnte in der letzten Legislaturperiode nicht mehr verabschiedet werden und ist bislang noch nicht wieder in den Bundestag eingebracht worden. Praxiserfahrungen sollen in einem in Friedrichshafen im Oktober 2009 gestarteten Pilotprojekt gesammelt werden.

Mit einem Bürgerportalgesetz und der Einführung der De-Mail könnte ein Anfang bei der flächendeckenden Verbesserung der Vertraulichkeit von elektronischer Kommunikation gemacht werden.

## **5. Kommunales**

### **5.1 Kommunalkontrollen: Datenschutz - auch das noch!**

Aufgrund der bereits zu Beginn des Jahres 2007 gewonnenen und noch immer nicht enden wollenden Erfahrungen mit der Stadtverwaltung Stadroda (7. TB, 5.6) hat der TLfD hinsichtlich des allgemeinen Datenschutzstandards in einigen Kommunen stichprobenhaft kontrolliert. Veranlasst durch den wenig ermutigenden Befund reifte der Entschluss, eine repräsentative flächendeckende datenschutzrechtliche Kommunalkontrolle anzuberaumen. Gleichmäßig über Thüringen verteilt wurden zwischen Juni 2008 und August 2009 überprüft: 5 Landkreise, 2 kreisfreie Städte, 3 große kreisangehörige Gemeinden, 6 Gemeinden mit mehr als 10.000 Einwohnern, 8 Gemeinden mit 3.000 – 10.000 Einwohnern, 6 Gemeinden mit weniger als 3.000 Einwohnern sowie 9 Verwaltungsgemeinschaften. Eine Kontrolle (Gemeinde mit 3.000 – 10.000 Einwohnern) fand im Vorberichtszeitraum statt.

Prüfungsgegenstand war der sogenannte Grunddatenschutz, also grundlegender datenschutzrechtlicher Standard:

➤ Existiert ein behördeninterner Datenschutzbeauftragter?

Gemäß § 10a ThürDSG haben Daten verarbeitende Stellen, die personenbezogene Daten mit Hilfe automatisierter Verfahren verarbeiten oder nutzen, einen ihrer Beschäftigten zum Beauftragten für den Datenschutz schriftlich zu bestellen. Gemäß Absatz 1 dieser Vorschrift darf nur bestellt werden, wer die notwendige Fachkenntnis in Fragen des Datenschutzes und der Datensicherheit hat und durch diese Tätigkeit keinem unüberwindbaren Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird. Der behördliche Datenschutzbeauftragte hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung des ThürDSG und anderer Rechtsvorschriften über den Datenschutz zu unterstützen und auf deren Einhaltung hinzuwirken. Zu seinen Aufgaben gehört insbesondere auch die im § 10a Abs. 2 Nummer 3 ThürDSG geforderte ordnungsgemäße Anwendung und Überwachung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden. Analog gilt dies auch für seinen Stellvertreter.

➤ Wird ein Verzeichnisseverzeichnis geführt?

Das gemäß § 10 ThürDSG zu führende Verzeichnisseverzeichnis, in dem jedes automatisierte Verfahren, mit dem personenbezogene Daten verarbeitet werden, zu erfassen und zu dokumentieren ist, dient der Transparenz und Nachvollziehbarkeit der Datenverarbeitung öffentlicher Stellen und damit der Eigenkontrolle. Es ist von den Fachabteilungen in Zusammenarbeit mit den behördlichen Datenschutzbeauftragten zu erstellen und vom behördlichen Datenschutzbeauftragten zu führen.

➤ Liegen Verfahrensfreigaben vor?

Zweck der datenschutzrechtlichen Freigabe ist die Vorabkontrolle der Zulässigkeit der automatisierten Verarbeitung personenbezogener Daten. So ist durch geeignete organisatorische Regelungen sicherzustellen, dass automatisierte Verfahren erst nach der vorherigen schriftlichen Freigabe zum Einsatz gelangen (§ 34 Abs. 2 ThürDSG). Damit werden letztlich auch Ausgaben vermieden, die durch den Einsatz von IT-Verfahren entstehen, die infolge eines Verstoßes gegen datenschutzrechtliche Bestimmungen nicht einsetzbar sind.

➤ Werden personenbezogene Daten von externen Stellen im Auftrag verarbeitet und bestehen datenschutzrechtskonforme Vertragsvereinbarungen?

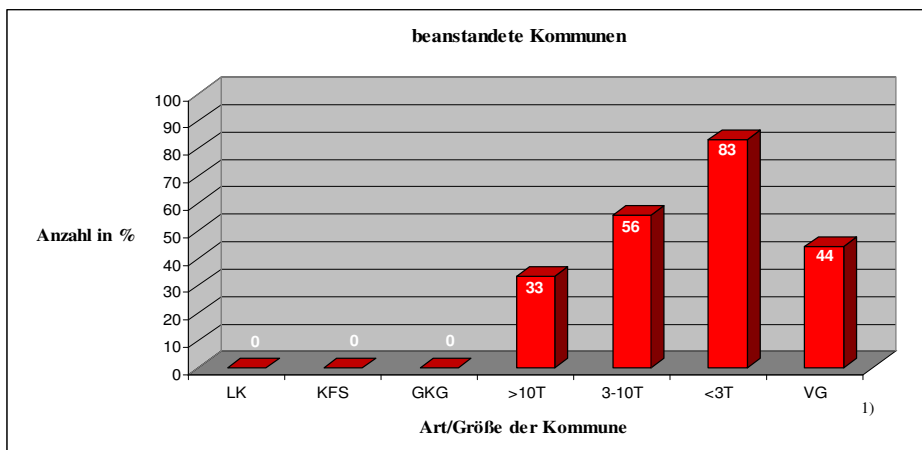
Werden personenbezogene Daten im Auftrag öffentlicher Stellen durch andere Personen oder Stellen verarbeitet oder genutzt, bleibt gemäß § 8 ThürDSG der Auftraggeber für die Einhaltung der Bestimmungen des ThürDSG oder anderer Vorschriften über den Datenschutz verantwortlich. Daher muss sich der Auftraggeber entsprechende Kontrollrechte bei dem Auftragnehmer einräumen lassen. Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Entsprechendes gilt auch für die Wartung oder Fernwartung automatisierter Datenverarbeitungsanlagen, soweit ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Auf den in Anlage 23 des 5. TB veröffentlichten Mustervertrag wird hingewiesen.

- Liegt ein Sicherheitskonzept vor, existieren entsprechende Dienst-anweisungen und sind diese Vorgaben auch umgesetzt?

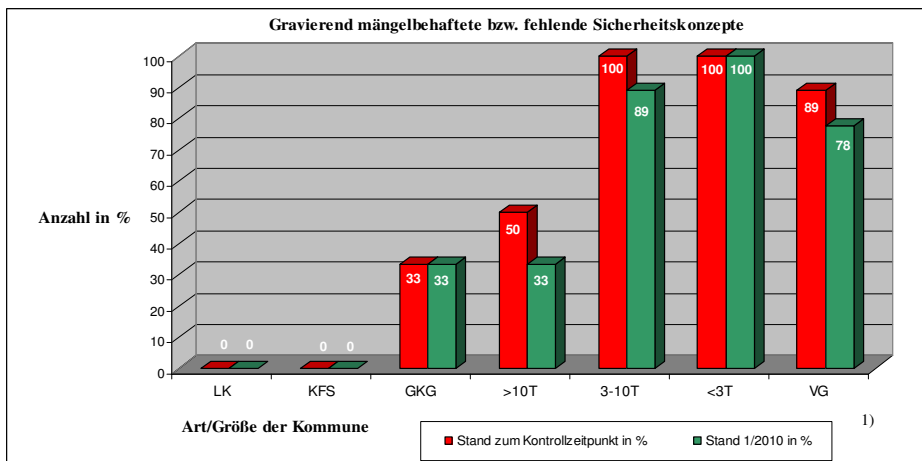
Nach § 9 Abs. 1 und 2 ThürDSG haben öffentliche Stellen auf der Grundlage eines Sicherheitskonzepts technische und organisatorische Maßnahmen zur Datensicherheit zu ermitteln und umzusetzen. Unter anderem sind die Maßnahmen Zugangs- und Zugriffskontrolle einschließlich Passwortregelung und Log-In-Funktionalität sowie Schutzmaßnahmen zur Absicherung des internen lokalen Netzes (wie der Einsatz einer Firewall, Schutzsoftware vor Schaden stiftenden Programmen, sicherheitstechnische Einstellungen der Browser, etc.) darzulegen. Des Weiteren sind Aussagen zu Protokollierungen wie auch zu notwendigen Datensicherungen erforderlich. Ebenso sind Angaben zur Wartung bzw. zu möglicher Fernwartung durch Fremdfirmen in das Sicherheitskonzept aufzunehmen. Musterhafte Hinweise finden sich unter [www.datenschutz.de](http://www.datenschutz.de); zudem stellt das TLRZ entsprechende Muster zur Verfügung.

Kontrolliert haben jeweils ein Mitarbeiter aus dem Rechts- und Technikreferat. Überprüft wurden neben den entsprechenden Unterlagen auch die tatsächlichen technischen und örtlichen Gegebenheiten in den Kommunalbehörden. Schließlich fanden in diesem Zusammenhang spezielle punktuelle Kontrollen statt, etwa zum ePass-Verfahren, zum Postlauf innerhalb der Behörde, im Sozialamt sowie in den sogenannten Bürgerbüros. An Mängelfreiheit litt keine der Kommunen, allerdings wurden bei den 5 Landkreisen, 2 kreisfreien Städten und 3 großen kreisangehörigen Gemeinden keine derart gravierenden Missstände vorgefunden, dass Beanstandungen auszusprechen waren. Von den 6 Gemeinden mit mehr als 10.000 Einwohnern waren aber immerhin 2 zu beanstanden also 33 %. 56 % bzw. 5 der 9 Gemeinden mit 3.000 bis 10.000 Einwohnern mussten beanstandet werden und 83 % bzw. 5 der 6 Gemeinden mit weniger als 3.000 Einwohnern. Nachdem auch 4 der 9 Verwaltungsgemeinschaften einer Beanstandung nicht entgehen konnten, ergab sich eine Beanstandungsquote von 40% der kontrollierten Kommunen.

Beanstandet wurden die Kommunen bzw. Verwaltungsgemeinschaften (VG): Greiz, Leinefelde-Worbis, Schleiz, Stadtilm, Kahla, Bad Frankenhausen, Stadtroda, Stadtlengsfeld, Schkölen, Elxleben (LK Söm.), Helbedündorf, Uder, VG Mittleres Schwarzatal, VG Oberes Feldatal, VG Straußfurt, VG Creuzburg.



Ein wesentlicher datenschutzrechtlicher Mangel stellt sich folgendermaßen dar:



<sup>1)</sup> LK: Landkreise; KFS: Kreisfreie Städte; GKG: Große kreisangehörige Gemeinden; >10T: Kommunen mit mehr als 10.000 Einwohnern; 3-10T: Kommunen mit 3.000 bis 10.000 Einwohnern; <3T: Kommunen mit weniger als 3.000 Einwohnern; VG: Verwaltungsgemeinschaften

Die Quantität und Qualität der Datenschutzmängel hat im negativen Sinne überrascht. Ersichtlich nehmen im Grundsatz die Datenschutzverstöße mit abnehmender Größe der kommunalen Kontrolleinheit zu. Die Beseitigung dieser Mängel gestaltet sich bisweilen zäh, was sich insbesondere auf fehlende Sachkunde in den Kommunen bzw. auf die kosten- und zeitintensive Inanspruchnahme externen Sachverständigen zurückführen lässt, seltener auf den fehlenden Willen zur datenschutzrechtskonformen Ausrichtung der Kommunalverwaltung. Die Gründe für den schlechten Datenschutzstandard vor allem in den kleineren Kommunen sind den gewonnenen Erkenntnissen zu folge vielfältig: Mangelnde Aktivitäten der Kommunalaufsichtsbehörden im Bereich des Datenschutzrechts, fehlender Blick der kommunalen Leitungsebene für den Datenschutz, relativ schwache rechtliche Stellung des behördlichen Datenschutzbeauftragten und Überlastung mit anderen Aufgaben, für die Belange des Datenschutzes unzureichende Personal- und Finanzausstattung der Kommunen, mangelndes datenschutzrechtliches Problembewusstsein, fehlende (Rechts-) Kenntnisse und wenig ausgeprägte Motivation, (Wissens-) Lücken zu schließen. Die Zahl der noch unkontrollierten Kommunen und damit die Dunkelziffer datenschutzrechtlicher Verstöße ist mit Sicherheit hoch. Entsprechend intensiv sollten daher die Bemühungen der Verantwortlichen ausfallen, das Feld des Datenschutzes gründlicher zu bestellen.

Die rasant zunehmende Bedeutung des Datenschutzes macht vor den Kommunen nicht halt. Alle Verantwortlichen müssen daher rasch ein Bewusstsein für den Datenschutz entwickeln, um die datenschutzrechtlich prekäre Situation in den Kommunen zu retten. Erst dann wird die zarte Pflanze „Kommunaler Datenschutz“ derart gedeihen und sich verwurzeln, wie es sich nicht nur die Datenschützer wünschen, sondern wie es der Gesetzgeber gewollt hat und wie es der Bürger erwarten kann.

## **5.2 Kommunal betriebene Videoanlagen und Webcams**

Im Rahmen einer Umfrage des TLfD bei 205 Thüringer Kommunen zu den in ihrer Zuständigkeit betriebenen Videokameras und Webcams gaben 157 an, weder Webcams noch Videokameras zu betreiben. Im Einzelnen wurden bis Anfang 2008 273 Videokameras gemeldet, deren

Einsatz in 22 Fällen mit der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung im Sinne von § 26 Thüringer Ordnungsbehördengesetz (ThürOBG) und in den übrigen 251 Fällen mit dem Hausrecht des Betreibers begründet wurde. Die gemeldeten 40 Webcams wurden ausschließlich zu touristischen Werbezwecken eingesetzt. Insgesamt wurden die Videotechnik und - soweit vorhanden – Webcams in 15 Kommunen überprüft, darunter in neun Fällen aufgrund der Umfrageergebnisse, drei mal hatten die Kontrollen Beschwerden von Bürgern zum Anlass und in weiteren drei Fällen baten Stadtverwaltungen den TLfD um Beratung zu geplanten Überwachungsvorhaben. In der Mehrzahl der Fälle betraf die Videoüberwachung öffentlich zugängliche Flächen wie städtische Plätze, einschließlich Marktplätze, Parkplätze, Bushaltestellen sowie einen Spielplatz, ein Schwimmbad und einen Fahrradstellplatz. Je einmal wurden die Fassaden eines Rathauses und die eines Museums überwacht. In einem Fall zielte die Überwachung mittels einer mobilen Videokamera auf die Verhinderung von illegaler Müllablagerung. Die Überwachungen wurden mit Sachbeschädigung bzw. Vandalismus, mit Diebstahl sowie mit Körperverletzung und Beleidigung begründet. Seltener wurden die Verhinderung von Ordnungswidrigkeiten oder die Sicherung von Beweisen im Falle eines Unfalls als Überwachungszweck genannt. Aus fünf Kontrollen resultierte die Forderung, die Anzahl und Größe der Hinweisschilder zu erhöhen und nur noch schwer erkennbare Hinweise auf die Überwachungsmaßnahme zu erneuern. Die Kameraaufnahmen überschritten in drei Fällen den erforderlichen räumlichen Umfang. So wurden in zwei Fällen die Fassaden von Wohnhäusern und bei einem Schwimmbad, abweichend von der Projektplanung, auch die Liegewiese und ein angrenzendes Wohngrundstück mit erfasst.

Eine unzureichende Dokumentation und das Fehlen organisatorischer Regelungen zum datenschutzgerechten Umgang mit der Videotechnik wurden in fast allen geprüften Kommunen bemängelt. Nur in einem Fall war das Verfahren ordnungsgemäß freigegeben, die Formblätter zum Verfahrensverzeichnis ausgefüllt und eine – allerdings ergänzungsbedürftige - Dienstanweisung zum Umgang mit der Videotechnik erstellt worden.

Da Videoaufnahmen tief in das Grundrecht auf informationelle Selbstbestimmung eingreifen, steht im Fokus der Prüfungen zunächst die rechtliche Zulässigkeit einer derartigen Überwachung. An der Bewertung der Videoüberwachung durch die Kommunen hat sich seit dem letzten Tätigkeitsbericht (7. TB, 5.2) nichts geändert. Vielmehr hat der

zahlreiche Einsatz dieser Überwachungstechnik ohne eine ausreichend normenklare gesetzliche Regelung die Auffassung des TLfD bestärkt, dass die Videoüberwachung durch Thüringer Ordnungsbehörden nach § 26 Satz 1 Nr. 1 ThürOBG einer Angleichung an die Regelungen des § 33 PAG bedarf, sowie im ThürDSG eine Bestimmung über den Einsatz von Videoüberwachung für die Durchsetzung des öffentlich-rechtlichen Hausrechts aufgenommen werden sollte. Unabhängig von dieser grundlegenden Forderung wurde daher in der Kontroll- und Beratungspraxis darauf geachtet, bei der Auslegung der vorhandenen sehr allgemeinen Regelungen auf eine möglichst datenschutzgerechte Verfahrensweise hinzuwirken.

Unterschiedliche Folgen ergeben sich z. B. daraus, ob die Überwachung den öffentlichen Raum, wie Straßen, Plätze und Denkmale oder aber die nur einem eingeschränkten Personenkreis zugänglichen Bereiche des Betreibers der Überwachungsanlage selbst betrifft. Einen schwerer wiegenden Grundrechtseingriff stellt eine Überwachung des öffentlichen Raumes dar, da die Betroffenen hier darauf vertrauen dürfen, sich unbeobachtet bewegen zu können. Daher müssen im öffentlichen Bereich höhere Zulässigkeitsvoraussetzungen erfüllt sein. So setzt eine ordnungsbehördliche Videoüberwachung der Kommunen im öffentlichen Raum im Sinne von § 26 ThürOBG voraus, dass tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit oder Ordnung entstehen. Ein Nachweis dieser Sachlage kann im Falle von Sachbeschädigung durch Bildaufnahmen der betroffenen Objekte und den Unterlagen zu den hierzu erstatteten Strafanzeigen erfolgen. Bis die notwendige legislative Harmonisierung zwischen § 33 ThürPAG und § 26 ThürOBG erfolgt, ist § 26 ThürOBG verfassungskonform dahingehend auszulegen, dass von dieser Befugnisnorm lediglich in Fällen drohender grober Rechtsverstöße Gebrauch gemacht wird. Es ist außerdem zu prüfen, ob der Zweck der Überwachung auch ohne Aufzeichnung (sog. Kamera-Monitor-Prinzip) erreicht werden kann. Zu beachten ist weiterhin, dass angesichts des nicht unerheblichen Grundrechtseingriffs - etwa halbjährlich - zu prüfen ist, ob eine Fortsetzung der Videoüberwachung weiterhin erforderlich ist oder diese gegebenenfalls eingestellt werden muss. Auch diese Prüfung ist zu dokumentieren.

Hinsichtlich der technisch-organisatorischen Bedingungen einer Videoüberwachung sind Regelungen u. a. zu folgenden Gesichtspunkten erforderlich:

- Der Überwachungsumfang ist zeitlich, bspw. nur nachts, und räumlich auf den erforderlichen Umfang zu beschränken; so ist die Aufnahme u. a. von privaten Hauseingängen, Geschäftshäusern und sensiblen Bereichen wie Pressenhäusern, Rechtsanwaltskanzleien und Arztpraxen unzulässig.
- Es ist am Einsatzort erkennbar auf die Überwachungsmaßnahme hinzuweisen.
- Die Videoüberwachungstechnik sollte nicht an das zentrale Computernetz der Kommune angeschlossen werden.
- Der Personenkreis der Zugriffsberechtigten auf die Videoaufnahmen ist zu beschränken. Die Befugnisse der Zugriffsberechtigten sind zu benennen.
- Regelungen zum Verfahren und der Dauer der Aufbewahrung der Aufzeichnungen sowie deren Löschung sind erforderlich. Die Dauer der Speicherung von aufgenommenen Daten, die keine Ordnungswidrigkeiten und Straftaten betreffen, sollte grundsätzlich 72 Stunden nicht überschreiten. Im Falle von Ordnungswidrigkeiten sind die Aufnahmen in der Regel zwei Monate nach Abschluss des Verfahrens zu löschen.

Dass diese Anforderungen nicht in jedem Fall beachtet werden, zeigen folgende Fälle:

Die Stadt Heiligenstadt hat wegen früherer Sachbeschädigungen einen Teil des öffentlich zugänglichen Parks mittels einer verdeckten Kamera monatelang videografiert. Auf Hinweisschilder zur Überwachung sei nach Ansicht der Verantwortlichen deshalb verzichtet worden, da sich die Täter ansonsten maskieren könnten. Zu der Angelegenheit stellte der TLfD fest, dass die beabsichtigte Verfolgung von Straftaten nicht in der Zuständigkeit der Ordnungsbehörden liegt, sondern ausschließlich in der Zuständigkeit der Polizei. Das für die kommunalen Ordnungsbehörden maßgebliche ThürOBG enthält keine Befugniszuweisung zur Verfolgung von Straftaten. Einen erheblichen datenschutzrechtlichen Verstoß - insbesondere gegen das Gebot der Transparenz - stellte der Betrieb der Videoaufnahme ohne Hinweisschilder dar. Diese heimlich gemachten Aufnahmen betrafen auch unbeteiligte Parkbesucher. Im Ergebnis war der Betrieb der Videoanlage ohne Hinweisschilder zum Zwecke der Strafverfolgung als Verstoß gegen die Befugniszuweisung des ThürOBG anzusehen. Der Forderung, die fragliche Videoüberwachung unverzüglich einzustellen, ist die Stadtverwaltung nachgekommen.

Bei der Vor-Ort-Kontrolle der Videoüberwachung des Marktplatzes Bad Salzungen, die die Stadt wegen Sachbeschädigungen und Beleidigung von Kurgästen betreibt, wurde bemängelt, dass auch Fassaden von Wohnhäusern von der Videokamera aufgenommen wurden. Dem Vorschlag des TLfD, dem Grundsatz der Erforderlichkeit entsprechend die betreffenden Aufnahmebereiche mittels geeigneter Software auszublenden, wurde gefolgt.

Abgesehen von zwei neueren und noch nicht abgeschlossenen Fällen werden zwischenzeitlich die überprüften Videoanlagen bzw. Webcams datenschutzrechtskonform betrieben, soweit der Betrieb - wie in zwei Fällen - nicht eingestellt wurde.

Eine auf § 26 ThürOBG gestützte kommunale Videoüberwachung des öffentlichen Raumes ist nur unter sehr engen Voraussetzungen zulässig. Der Gesetzgeber ist aufgefordert, ein Gesamtkonzept zur Zulässigkeit der Videoüberwachung durch öffentliche Stellen in Thüringen zu erlassen, das die Grundrechte der Betroffenen angemessen berücksichtigt.

### **5.3 Veröffentlichung von Ratssitzungen, Dokumenten und Mitarbeiterdaten im Internet**

Die Stadt Erfurt bat den TLfD zu prüfen, ob Stadtratssitzungen zeitversetzt in das Internet übertragen werden dürfen, nachdem die bislang von einem lokalen Fernsehsender durchgeführten Übertragungen eingestellt worden waren. Auch die Anfrage der Gemeindeverwaltung Saalfelder Höhe nach der Zulässigkeit der Bereitstellung von digitalen Mitschnitten öffentlicher Gemeinderatssitzungen in Form von Audiodateien im Internet zum Zwecke des Downloads betraf eine ähnliche Problematik. Nach Klärung einiger vorgreiflicher kommunalrechtlicher Fragestellungen mit dem Thüringer Innenministerium wurden derartige Vorhaben wie folgt bewertet:

Ausgangspunkt für die Zulässigkeit der Übertragung von Gemeinderatssitzungen über das Internet ist das in § 40 Abs. 1 Thüringer Kommunalordnung (ThürKO) festgeschriebene Gebot, Sitzungen des Gemeinderats grundsätzlich öffentlich durchzuführen. Dieses Gebot ist jedoch schon dann gewahrt, wenn ein ausreichend großer Sitzungsraum für den Normalbürger zumutbar erreichbar ist, zu dem jedermann im Rahmen des hierfür zur Verfügung stehenden Platzes in der Reihenfolge des Eintreffens freien Zugang hat. Daher besteht keine Verpflichtung für eine Übertragung des Sitzungsverlaufs mit elektronischen Medien (sowohl

im Rundfunk als auch über das Internet). Vom Thüringer Innenministerium wird die Auffassung vertreten, dass der Gemeinderat über diesen Mindeststandard auch eine weitergehende Öffentlichkeit herstellen kann. Allerdings können aus § 40 Abs. 1 ThürKO keine weitergehenden Eingriffe in das informationelle Selbstbestimmungsrecht der anwesenden Personen (Gemeinderatsmitglieder, sonstige teilnehmende Personen oder Bürger, deren Angelegenheiten dort behandelt werden) abgeleitet werden, als dass die anwesenden Zuhörer sich ggf. Notizen machen und im Anschluss an die Sitzung in der Presse berichtet wird. Aus kommunalrechtlicher Sicht ist zu beachten, dass nach der Rechtsprechung des Bundesverwaltungsgerichts (Urteil vom 03.08.1990, 7 C 14/90) es im öffentlichen Interesse liegt, dass die Willensbildung im Rat ungezwungen, freimütig und in aller Offenheit erfolgt. Nach dieser Entscheidung kann durch die Tonbandaufzeichnung diese Willensbildung dadurch beeinträchtigt werden, dass „insbesondere in kleineren und ländlichen Gemeinden weniger redegewandte Ratsmitglieder durch das Bewusstsein des Tonmitschnitts ihre Spontanität verlieren, ihre Meinung nicht mehr ‚geradeheraus‘ vertreten oder schweigen, wo sie sonst gesprochen hätten“. Deshalb liegt es trotz etwaiger zustimmender Ratsbeschlüsse sowie der Einwilligung aller Ratsmitglieder in der Sitzungs- und Hausordnungsbefugnis des Vorsitzenden, im Einzelfall zu entscheiden, ob durch die beabsichtigte Aufzeichnung dieses öffentliche Interesse an einer unbeeinträchtigten Willensbildung verletzt würde und daher zu untersagen ist. Diese Grundsätze kommen erst Recht bei Bildaufnahmen zum Tragen, die mittels elektronischer Medien wie dem Internet einer weltweiten Öffentlichkeit zugänglich gemacht werden. Mangels einer bereichsspezifischen Vorschrift kann eine Veröffentlichung der personenbezogenen Daten der Sitzungsteilnehmer daher nur nach allgemeinem Datenschutzrecht erfolgen. Hier kommt einzig eine Einwilligung aller Betroffenen in Frage. Eine solche Einwilligung ist auch deshalb erforderlich, weil es sich bei einer Internetveröffentlichung um eine Datenübermittlung immer auch an Drittstaaten nach § 23 Abs. 2 ThürDSG handelt, in denen kein angemessenes Datenschutzniveau gewährleistet ist. Die einzig einschlägige Zulässigkeitsvoraussetzung ist hier die zweifelsfreie Einwilligung des Betroffenen nach § 23 Abs. 2 Nr. 1 ThürDSG.

Durch flankierende technische und organisatorische Maßnahmen ist bei dieser Einwilligungslösung anzustreben, dass der Wille der Betroffenen so weit wie möglich umgesetzt und die Verbreitung dieser personenbezogenen Daten über das Internet nicht umfangreicher erfolgt, als es zur

Herstellung der Sitzungsöffentlichkeit notwendig ist. Hierzu gehören insbesondere:

- ausdrückliche vorherige Information aller Sitzungsteilnehmer und Besucher über die Art und den Umfang der Aufzeichnung, die Abrufbarkeit im Internet sowie die Speicherung und Löschfrist der Aufnahmen,
- vorherige ausdrückliche Einwilligung jedes von der Übertragung erfassten Sitzungsteilnehmers, ohne dass dabei psychischer Druck (z. B. vor laufender Kamera) ausgeübt wird,
- Nichtaufnahme in bzw. Herausnahme aus der Übertragung von solchen Redebeiträgen, bei denen der Redner nicht eingewilligt oder nachträglich seine Einwilligung widerrufen hat,
- Einrichtung der Kamerapositionen in der Weise, dass nur der jeweilige Redner, die übrigen Ratsmitglieder nur in einer Übersichtsposition sowie die sonstigen Zuhörer gar nicht zu sehen sind,
- Bereitstellung der Videoclips bzw. Audiodateien grundsätzlich in einem Format, das nicht ohne weiteres eine Speicherung durch die Internetnutzer erlaubt,
- zeitliche Begrenzung der Abrufbarkeit der Videoclips bzw. Audiodateien höchstens bis zur nächsten Sitzung.

Eine Live-Übertragung ist demgegenüber als problematisch anzusehen, da hier die Gefahr besteht, dass der betroffene Redner vor laufender Kamera zu einer Einwilligung genötigt wird, die dann nicht mehr als freiwillig anzusehen wäre. Zudem wäre ihm die Möglichkeit genommen, nach seinem Redebeitrag nochmals zu entscheiden, ob dieser einer derart breiten Öffentlichkeit in Wort und Bild zugänglich gemacht werden soll. Im Allgemeinen dürfte jedoch eine zeitversetzte Übertragung um einige Minuten oder Stunden ausreichen, um die interessierte Öffentlichkeit über den Inhalt der Sitzungen zu informieren.

Eine Internetpräsentation von Kommunen wird vielfach genutzt, ohne die datenschutzrechtlichen Vorgaben ausreichend zu berücksichtigen. So wies ein Bürger darauf hin, dass die Stadtverwaltung Jena im Rahmen ihrer Internetpräsentation ihr Telefonverzeichnis veröffentlicht. Mittels einer Suchfunktion kann eine Übersicht über die Namen und Arbeitsaufgaben aller Mitarbeiter abgerufen werden, einschließlich der Schreibkräfte, der Auszubildenden und der Kraftfahrer.

Der TLfD hat diese Veröffentlichung der Stadtverwaltung Jena gemäß § 39 ThürDSG beanstandet. Nach einem Beschluss des Bundesverwaltungsgerichts vom 12.03.2008 (2 B 131/07) ist eine Veröffentlichung

von Mitarbeiterdaten im Internet – auch ohne Einwilligung – dann zulässig, soweit der betreffende Mitarbeiter dem außen stehenden Publikum zur Verfügung stehen soll. Diese Voraussetzung ist im Falle der Schreibkräfte, der Auszubildenden und der Kraftfahrer nicht ersichtlich. Der Kommune wurde daher aufgegeben, die Veröffentlichung auf das erforderliche und sachlich gebotene Maß zu beschränken. Um dies auch zeitnah durchsetzen zu können, wurde die Kommunalaufsicht eingeschaltet. Die Angelegenheit ist noch immer nicht abgeschlossen.

Aufgrund einer Beschwerde wurde die Zulässigkeit der Veröffentlichung des Namens, der Adresse von Bauantragstellern und von Einzelangaben zu einem Bauantrag in den Gemeindeblättern im Rahmen der Internetpräsentation der Gemeinde Förritz geprüft. Ziel der Veröffentlichung im Internet war es, auswärts wohnende Eigentümer von Grundstücken in Förritz über das Gemeindeleben zu informieren.

Nachdem der TLfD die Gemeindeverwaltung gebeten hatte, aufgrund fehlender Rechtsgrundlage umgehend dafür Sorge zu tragen, dass ein Zugriff auf die o. g. Daten ausgeschlossen ist, hat die Gemeindeverwaltung den Internetzugang zu den Gemeindeblättern unterbunden. Um auch zukünftig die auswärts wohnenden Eigentümer informieren zu können, wurde auf die Möglichkeit hingewiesen, nur einer geschlossenen Nutzergruppe mittels entsprechender Passwörter den Zugang auf Antrag zu gewähren. Dies setzt u. a. voraus, dass datenschutzkonforme Regelungen zur Prüfung der Berechtigung der Antragsteller auf Zuteilung eines Passwortes und zur Gestaltung und Änderungsfrequenz der Passwörter fixiert werden.

Eine Übermittlung von kommunalen Ratssitzungen im Internet ist nur zulässig, wenn zuvor jeder erfasste Sitzungsteilnehmer hierin eingewilligt hat.

Eine Veröffentlichung von Mitarbeiterdaten im Internet – auch ohne deren Einwilligung – ist nur dann zulässig, soweit der betreffende Mitarbeiter dem außen stehenden Publikum zur Verfügung stehen soll.

#### **5.4 Veröffentlichung der Wortprotokolle von Niederschriften kommunaler Gremien**

Die Stadtverwaltung Erfurt bat um Prüfung eines Änderungsvorschlags zur Geschäftsordnung eines städtischen Gremiums, wonach künftig auf

Wunsch eines seiner Mitglieder der Wortlaut jeder Äußerung im Gremium im Sitzungsprotokoll dokumentiert werden sollte.

Nach § 42 Abs. 1 Satz 2 ThürKO sollen im öffentlichen Interesse neben dem gesetzlich bestimmten Mindestinhalt alle Vorgänge dokumentiert werden, die den Ablauf der Sitzung erklären und deutlich machen, wobei jedoch das Persönlichkeitsrecht der Ausschussmitglieder an ihrem gesprochenen Wort zu berücksichtigen ist. Hierbei ist zu bedenken, dass sich insbesondere Ausschussmitglieder mit wenig Praxis in der öffentlichen Darstellung durch die von ihnen nicht erwünschte Dokumentation ihrer Äußerungen an einer freien und ungezwungenen Rede gehindert sehen könnten. Auch ist kein zwingendes Erfordernis für die Protokollierung aller Wortbeiträge festzustellen. Da die ThürKO keine ausdrückliche Regelung zur Zulässigkeit der Dokumentation persönlicher Wortbeiträge (auf Antrag eines Dritten) enthält, ist diese Problematik an § 4 Abs. 1 ThürDSG zu messen. Danach ist eine Niederschrift persönlicher Wortbeiträge – als Form des Verarbeitens (Erhebens) personenbezogener Daten - nur dann zulässig, wenn es ein Gesetz oder eine Rechtsvorschrift erlaubt oder der Betroffene einwilligt, was jedoch gerade infolge der beantragten Neuregelung nicht der Fall wäre.

Daher hat der TLfD empfohlen, von der beabsichtigten Änderung der Geschäftsordnung Abstand zu nehmen. Diese Einschätzung deckt sich auch mit der allgemein vertretenen Auffassung zur Dokumentation des Abstimmungsverhaltens, wonach ein anderes Mitglied nicht verlangen kann, dass das Stimmverhalten eines Kollegen dokumentiert wird. Umso mehr muss dieser Grundsatz bei der Frage der Dokumentation von verbalen Äußerungen gelten, da diese in einem stärkeren Maße das Verhalten einer Person gegenüber Dritten offenbaren.

Eine Regelung, wonach jegliche Äußerungen auf Wunsch eines Mitgliedes eines kommunalen Gremiums im Sitzungsprotokoll festzuhalten sind, begegnet erheblichen datenschutzrechtlichen Bedenken.

### **5.5 Auskunftsrecht des Gemeinderats bzw. eines seiner Mitglieder zu privatrechtlichen Verträgen**

Aufgrund einer abstrakten Anfrage des Landratsamtes Weimarer Land zum Auskunftsrecht eines Gemeinderatsmitgliedes zu einem Mietvertrag, welchen eine Gemeinde mit einem privaten Mieter abgeschlossen hatte, wurde der TLfD um eine rechtliche Bewertung gebeten. Hierbei wurde folgendes festgestellt:

Nach § 22 Abs. 3 Satz 4 ThürKO ist der Gemeinderat berechtigt und auf Verlangen eines Viertels seiner Mitglieder verpflichtet, vom Bürgermeister in den Angelegenheiten, die die Überwachung seiner Beschlüsse betreffen, Auskunft zu fordern bzw. durch die von ihm beauftragten Ausschüsse oder bestimmten Gemeinderatsmitglieder Akteneinsicht zu nehmen. Das Überwachungsrecht des Gemeinderats erstreckt sich jedoch nicht allgemein auf die Tätigkeit der Gemeindeverwaltung, insbesondere nicht auf die Angelegenheiten, die der Bürgermeister in eigener Zuständigkeit erledigt.

Da der fragliche Mietvertrag ohne Gemeinderatsbeschluss zustande gekommen ist, war das Auskunftsbegehren als unbegründet anzusehen. Abgesehen davon, ist ein individueller Auskunftsanspruch von Gemeinderatsmitgliedern im Gesetz nicht vorgesehen. Vorsorglich wurde zudem darauf hingewiesen, dass eine gleichwohl erfolgende Auskunft bzw. Einsicht in den Mietvertrag eine unzulässige Offenbarung personenbezogener Daten gegenüber unbefugten Dritten darstellen würde.

Eine Offenbarung des Inhalts privatrechtlicher Verträge auch gegenüber einem Gemeinderatsmitglied erfolgt unzulässig, wenn dieses Begehren nicht der Überwachung der Ausführung der Beschlüsse des Gemeinderats dienen sollte.

### **5.6 Unzulässige Übermittlung personenbezogener Daten von Kaufvertragsparteien an Erschließungsträger**

Ein Betroffener beschwerte sich über die Übermittlung von personenbezogenen Daten der Parteien eines Grundstückskaufvertrags von der Stadtverwaltung Rudolstadt an den Erschließungsträger im Zusammenhang mit der Prüfung des gemeindlichen Vorkaufsrechts. Festgestellt wurde, dass die fraglichen personenbezogenen Daten zeitlich vor dem Stadtratsbeschluss zur Ausübung des gemeindlichen Vorkaufsrechts übermittelt wurden. Da die Entscheidung zum Vorkaufsrecht lediglich

die Kenntnis grundstücksbezogener Daten wie Lage, Größe und Kaufpreis erforderte, erfolgte die Übermittlung der personenbezogenen Daten wegen Verstoßes gegen das Prinzip der Erforderlichkeit ohne Rechtsgrund. Ebenso stellt § 27a Abs. 1 Satz 1 Nr. 2 Baugesetzbuch (BauGB), wonach das gemeindliche Vorkaufsrecht auch zugunsten des Erschließungsträgers ausgeübt werden kann, keine Rechtfertigung dar, da diese Daten nicht für eine Einbeziehung des Erschließungsträgers in die Verwaltungsentscheidung erforderlich waren. Die Stadtverwaltung teilte mit, künftig nur die für die Aufgabenerfüllung erforderlichen Daten zu übermitteln und legte eine entsprechende Dienstanweisung vor.

Vor der Entscheidung über das gemeindliche Vorkaufsrecht darf die Kommune nur die hierfür erforderlichen Daten wie Lage, Größe und Kaufpreis des Grundstücks an einen öffentlichen Bedarfs- und Erschließungsträger übermitteln.

## **5.7 Firmenumsatz und Fremdenverkehrsabgabe**

Eine Beschwerde hatte die Frage zum Gegenstand, ob ein Firmeninhaber von seiner Gemeindeverwaltung zur Berechnung der Fremdenverkehrsabgabe verpflichtet werden kann, den Jahresumsatz seiner Firma anzugeben. Die Gemeinde Schmiedefeld am Rennsteig begründete das Auskunftersuchen mit Normen ihrer Fremdenverkehrsbeitragssatzung, die Unternehmen zu einer umsatzabhängigen Fremdenverkehrsabgabe verpflichtete, wenn diesen „... durch den Fremdenverkehr im Gemeindegebiet unmittelbare oder mittelbare wirtschaftliche Vorteile erwachsen“. Gem. § 4 Abs. 1 ThürDSG darf der Umsatz des betroffenen Einzelunternehmens nur dann erhoben werden, wenn es das ThürDSG oder eine andere Rechtsvorschrift erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Da der Betroffene in eine Datenerhebung nicht eingewilligt hatte, war die Zulässigkeit der Datenerhebung an Hand der o. g. Satzung zu prüfen. Im Ergebnis der Prüfung war nicht ersichtlich, dass der Firma durch den Fremdenverkehr unmittelbare oder mittelbare wirtschaftliche Vorteile erwachsen. Dies zeigte sich insbesondere daran, dass die Firma ein reiner Produktionsbetrieb für ein Messgerät ist, also nicht z. B. im Einzelhandel der Gemeinde tätig wird. Der Vortrag der Gemeinde, dass dem Unternehmen zumindest ein mittelbarer Vorteil aus dem Fremdenverkehr unterstellt werden müsse, da der Fremdenverkehr auch zu einer Erhöhung des Auftragsvolumens eines solchen Unternehmens führen könne, entbehrt einer substanziellen Grundlage. Auf Grund

einer solchen Argumentation könnte jedermann abgabepflichtig werden. Derartige Regelungen bzw. Auslegungen genügen den verfassungsrechtlichen Vorgaben der Klarheit und Bestimmtheit nicht.

Nachdem das zuständige Landratsamt gebeten wurde, zur Zulässigkeit einer künftigen Erhebung von Umsatzdaten Stellung zu nehmen, wurde mitgeteilt, dass die Gemeindeverwaltung nunmehr beabsichtige, die Satzung derart zu ändern, dass künftig die Veranlagung der ortsansässigen Gewerbetreibenden eindeutig geregelt wird. Da die geänderte Satzung bisher noch nicht in Kraft getreten ist, konnte noch keine abschließende datenschutzrechtliche Bewertung erfolgen.

Eine kommunale Datenerhebung darf nur auf gesetzlicher Grundlage erfolgen. Auch Satzungen sind an verfassungsrechtlichen Vorgaben der Klarheit und Bestimmtheit zu messen.

## **5.8 Startschwierigkeiten mit der Online-Melderegisterauskunft**

Im Berichtszeitraum wurde der TLfD informiert, dass die Stadt Erfurt beabsichtigt, ein Online-Verfahren im Rahmen der E-Government-Anwendungen in Betrieb zu nehmen, welches einfache Online-Auskünfte aus dem Melderegister ermöglicht. Rechtsgrundlage für diese einfache Online-Melderegisterauskunft über das Internet ist § 31 Abs. 3 Thüringer Meldegesetz (ThürMeldeG) i. V. m. mit den §§ 29 ff Thüringer Meldeverordnung (ThürMeldeVO). Eine einfache Melderegisterauskunft nach § 31 ThürMeldeG kann grundsätzlich jeder erhalten, ohne dass man dies begründen muss. Diese Auskunft umfasst Vor- und Familiennamen, Doktorgrad und Anschriften einzelner bestimmter Einwohner, also keine Listenauskünfte. Bei einer Online-Melderegisterauskunft über das Internet kommt einschränkend hinzu, dass der Antragssteller den Gesuchten genauer bezeichnen muss. Neben Vor- und Familiennamen sowie Wohnort müssen mindestens zwei weitere Merkmale angegeben werden, die sich auch im Melderegister befinden (alles außer Geschlecht oder Staatsangehörigkeit). Dabei liegt es im Ermessen der Meldebehörde, welche dieser Merkmale in der elektronischen Antragsmaske nach § 29 ThürMeldeVO genannt werden müssen. In der Stadt Erfurt sind es das Geburtsdatum, der frühere Name und die (frühere) Anschrift, wobei zwei der drei Angaben ausreichen. Die Abfrage der Merkmale soll dazu dienen, dass die Identität des Gesuchten im Melderegister eindeutig festgestellt werden kann. Die Online-Auskunft wird ebenso wie die sonstige Auskunft dann nicht erteilt, wenn eine Aus-

kunftssperre vorliegt oder die Auskunft zum Schutz des Adoptionsgeheimnisses unzulässig ist. Ein automatisierter Abruf über das Internet ist generell nicht zulässig, wenn der Betroffene gemäß § 31 Abs. 3 Satz 3 ThürMeldeG dieser Form der Auskunftserteilung widersprochen hat. Widersprüche gegen den automatisierten Internetabruf von Auskünften aus dem Melderegister können beim jeweils zuständigen Meldeamt abgegeben oder an dieses geschickt werden. Diese Widersprüche können formlos eingelegt werden, darüber hinaus ist auf der Internetseite des TLfD ein entsprechendes Formular eingestellt ([www.thueringen.de/imperia/md/content/datenschutz/vordruck-widerspruch.pdf](http://www.thueringen.de/imperia/md/content/datenschutz/vordruck-widerspruch.pdf)). Zwar kann mit diesem Widerspruch nichts gegen die schriftliche oder persönliche Meldeauskunft unternommen werden, aber dafür sind die persönlichen Daten in diesem Bereich vor einem evtl. Internetmissbrauch sicher. Spätestens einen Monat vor der Eröffnung des Zugangs zur automatisierten Erteilung von Melderegisterauskünften sowie einmal jährlich muss zudem die Meldebehörde gemäß § 31 Abs. 3 Satz 4 ThürMeldeG durch öffentliche Bekanntmachung auf das Widerspruchsrecht hinweisen. Der TLfD hat der Stadt Erfurt mitgeteilt, dass keine Bedenken gegen die vorgesehene Verfahrensweise bei der Online-Melderegisterauskunft bestehen. Bereits im 7. TB (5.3) hat der TLfD aber gefordert, im Zuge der Modernisierung des Melderechts die bisherige Widerspruchsregelung auf den Prüfstand zu stellen und durch Einwilligungslösungen zu ersetzen.

Das Fernseh-Magazin „Report aus München“ erregte am 23.06.2008 die Aufmerksamkeit der Datenschützer: In mehreren Gemeinden Deutschlands waren die Einwohnermeldedaten sämtlicher Bürger für Online-User abrufbar. Viele Einwohnermeldeämter verwenden die Software „MESO“ und das dazugehörige Modul „OLMERA“ der Software-Firma HSH für Online-Melderegisterauskünfte. Bei der Installation des Programms versäumten es bundesweit 15 Meldeämter, das mitgelieferte und für alle Kunden gleiche Installationspasswort in ein eigenes Passwort abzuändern. Anfang 2008 veröffentlichte HSH aufgrund einer internen „Panne“ das Installationspasswort auf seiner Firmen-Homepage. Laut HSH war es daher seit März 2008 möglich, mithilfe dieses Passworts auf die bei den Meldeämtern gespeicherten Daten zuzugreifen. In der Folge seien in zwei Gemeinden tatsächlich unberechtigte Zugriffe auf Einwohnerdaten erfolgt. Der TLfD musste feststellen, dass auch im Meldeamt der Stadt Jena das Passwort nicht verändert worden war. Bei einer kurzfristig veranlassten Kontrolle vor Ort war zu

klären, ob auch dort unberechtigt über das Internet Einwohnermeldedaten abgerufen wurden. Da sich die Anwendung der Software noch im Testlauf befand, konnte Entwarnung gegeben werden. Auf Anregung des TLfD hat das Thüringer Innenministerium Hinweise an die Kommunen zur Überprüfung der Sicherheitseinstellungen veranlasst. Für das Melderegisterverfahren selbst wurde darüber hinaus festgestellt, dass weder eine datenschutzrechtliche Freigabe nach § 34 Abs. 2 ThürDSG noch eine Aufnahme in das Verzeichnissverzeichnis gemäß § 10 Abs. 2 ThürDSG erfolgt war und darüber hinaus auch keine Vereinbarung über die Fernwartung des Systems im Auftrag durch eine private Firma nach § 8 Abs. 7 ThürDSG nachgewiesen werden konnte. Inzwischen wurden alle datenschutzrechtlichen Forderungen von der Stadt Jena erfüllt.

Zum Redaktionsschluss war nach Kenntnis des TLfD wegen Fortdauer der technischen Erprobungsphasen des Online-Melderegisterauskunftsverfahrens in den o. g. Meldeämtern nach wie vor kein automatisierter Abruf von Meldedaten möglich.

Gegen das Verfahren des automatisierten Internetabrufs von Auskünften aus dem Melderegister bestehen grundsätzlich keine datenschutzrechtlichen Bedenken. Ob der Bürger aber eine Online-Melderegisterauskunft zu seinen Daten überhaupt zulassen will, kann er selbst bestimmen, indem er ggf. bei der für ihn zuständigen Meldebehörde widerspricht.

## **5.9 ePass und neuer Personalausweis (nPA)**

Derzeit befinden sich ca. 62 Millionen Personalausweise in Umlauf. Am 1. November 2010 tritt das Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PAuswG) in Kraft, welches die Einführung des neuen Personalausweises regelt. Die Daten, die heute auf dem Dokument ablesbar sind, sollen zukünftig zusätzlich in einem Ausweis-Chip gespeichert werden. Mit Hilfe dieses neuen Personalausweises soll der Bürger dann auch optional seine Identität elektronisch eindeutig gegenüber der Wirtschaft und der Verwaltung nachweisen, bei Bedarf mit seiner qualifizierten Signatur elektronisch rechtskräftig unterschreiben oder für Reisezwecke freiwillig seinen Fingerabdruck speichern lassen können. Der neue Personalausweis (nPA) soll künftig auch der Erstregistrierung und der Anmeldung am De-Mail-Konto dienen (4.2). Die Personalausweisbehörde hat gemäß § 13 PAuswG den Ausweisinhaber bei Antragstellung auf die Risiken dieses Verfahrens hinzuweisen.

Die antragstellende Person hat bei der Aushändigung des Personalausweises schriftlich gegenüber der Personalausweisbehörde zu erklären, ob sie den elektronischen Identitätsnachweis nutzen will. Dies kann jederzeit während der Gültigkeitsdauer des Personalausweises schriftlich gegenüber der Personalausweisbehörde abgeändert werden (§ 10 PAuswG). Vom Ausweishersteller werden den antragstellenden Personen zum Zweck der Verwendung, Sperrung und Entsperrung des elektronischen Identitätsnachweises die Geheimnummer, die Entsperrnummer und das Sperrkennwort des Personalausweises übersendet (§ 13 PAuswG). Störungen der Funktionsfähigkeit des elektronischen Speicher- und Verarbeitungsmediums berühren nicht die Gültigkeit des Personalausweises (§ 28 PAuswG).

Dienstleister aus Wirtschaft und Verwaltung können ihre Identität dem Bürger gegenüber nachweisen und auch nur auf personenbezogene Daten des Personalausweises zugreifen, wenn sie zuvor ein Berechtigungszertifikat vom Staat erhalten haben. Für Verfahren, bei denen der Nachweis nur für bestimmte Eigenschaften (wie z. B. Volljährigkeit) erbracht werden muss, wird ein speziell dafür erforderliches Berechtigungszertifikat erteilt werden, so dass der Bürger diesen Dienst pseudonym oder anonym nutzen kann. Die Datenschutzbeauftragten des Bundes und der Länder waren es, die diese pseudonyme Nutzungsmöglichkeit des nPA einforderten. Denn nicht jede Anwendung bedarf gleich der Offenlegung aller gespeicherten personenbezogenen Daten. Des Weiteren wird es eine Vergabe „hoheitlicher“ Berechtigungszertifikate geben, mit denen der Zugriff auf biometrische Daten des Personalausweises ermöglicht wird. Gemäß § 2 Abs. 2 i. V. m. Abs. 4 PAuswG ist dies nur zur Identitätsfeststellung berechtigten Behörden vorbehalten. Diese für den hoheitlichen Gebrauch gespeicherten Daten werden nach Aussagen der Bundesregierung durch eine elektronische Signatur zur Wahrung der Identität und Authentizität gesichert.

Doch wie sieht es mit der Datensicherheit in den Pass- und Personalausweisbehörden selbst aus? Kontrollen zum Antragsverfahren des elektronischen Reisepasses (ePass), der 2007 eingeführt wurde, ergaben bereits, dass die Fingerabdruckdaten bis zur Passübergabe an den Antragsteller mehrere Wochen unverschlüsselt in den Kommunen und im Rechenzentrum vorliegen. Das Passgesetz hat lediglich die verschlüsselte Datenübertragung der Passdaten von den Passbehörden zur Bundesdruckerei gesetzlich vorgeschrieben, leider nicht verpflichtend eine

Verschlüsselung der Fingerabdruckdaten vor Ort. Für Thüringen fehlen hierfür weiterhin verbindliche Vorgaben. Das Innenministerium des Landes Schleswig-Holstein hat bspw. reagiert und zumindest für die gespeicherten Daten außerhalb der Daten verarbeitenden Stelle die Verschlüsselung gefordert. Der TLfD, der nicht nur die derzeit vom Bund eingesetzten Lesegeräte für Pässe kritisierte (7. TB 5.5, DuD 5/2009), sieht auch hier Handlungsbedarf durch den Bund. Will man deutschlandweit ein gleiches Sicherheitsniveau für die Speicherung der Fingerabdrücke sicherstellen, erscheint die Bereitstellung von getesteter IT-Sicherheitssoftware durch den Bund für die Kommunen unabdingbar. Wird im Handlungsleitfaden zum ePass noch vom BSI empfohlen, die Vertraulichkeit durch Verschlüsselungsverfahren sicherzustellen, fehlt dies für den nPA gänzlich. Und dies obwohl das BSI einschätzt, dass für die sensiblen personenbezogenen Daten Sicherheitsvorkehrungen getroffen werden müssen, um diese vor Bedrohungen wie Missbrauch, Diebstahl und Manipulation zu schützen.

Bei einigen Kontrollen wurde auch festgestellt, dass die Vorgaben des vom BSI versandten Handlungsleitfadens zum ePass nicht konsequent umgesetzt wurden. So die Forderung, für das ePass-Verfahren ein gesondertes Sicherheitskonzept zu erstellen, oft konnte nicht einmal das nach § 9 ThürDSG geforderte Sicherheitskonzept vorgelegt werden. Ab November 2010 werden die Kommunen schon mit dem nächsten Verfahren konfrontiert. Gemäß ThürDSG ist auch für dieses Verfahren explizit eine datenschutzrechtliche Freigabe, die Aufnahme in das Verzeichnissesverzeichnis und die Erstellung eines Sicherheitskonzeptes sicherzustellen. Die Frage, welche technisch organisatorischen Maßnahmen im Antragsverfahren für den nPA notwendig sind, ist ohne Fachwissen eines IT-Spezialisten, welcher vor Ort oft fehlt, kaum zu beantworten. Die Behörden sind also auch hier auf zentrale Vorgaben angewiesen.

Im § 27 PAuswG werden die Pflichten des Ausweisinhabers geregelt. So hat u. a. der Bürger (Personalausweisinhaber) durch technische und organisatorische Maßnahmen zu gewährleisten, dass der elektronische Identitätsnachweis nur in einer Umgebung eingesetzt wird, die nach dem jeweiligen Stand der Technik als sicher anzusehen ist. Dabei soll er insbesondere solche technischen Systeme und Bestandteile einsetzen, die vom BSI als für diesen Einsatzzweck als sicher bewertet werden. Ist dies tatsächlich von jedem Bürger zu leisten? Kann der Bürger in jedem Fall eine Information oder Warnung des BSI zeitnah erfassen und auch

umsetzen? Das BVerfG hat in seinem Urteil zur Online-Durchsuchung (2.) bereits darauf hingewiesen, dass informationstechnische Systeme mittlerweile einen derart hohen Komplexitätsgrad erreicht haben, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwirft und zumindest den durchschnittlichen Nutzer überfordern kann. Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat berechnete Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet.

Mit dem neuen Personalausweis soll zukünftig eine sichere elektronische Nutzungsmöglichkeit von E-Government und E-Business geschaffen werden. Dies setzt eine durchgängige Sicherstellung der Vertraulichkeit und der Integrität der Daten voraus.

### **5.10 Unzulässige Datenübermittlung an die Presse zu einem akademischen Grad**

Bei der Prüfung des Melderegisters anlässlich der Anmeldung eines Bürgers wurde die Richtigkeit des eingetragenen Doktorgrads bezweifelt. Daraufhin leitete die Stadtverwaltung Nordhausen ein Verwaltungsverfahren zur Korrektur von Melderegister, Personalausweisregister und Personalausweis ein und erstattete Strafanzeige wegen des Verdachts des Missbrauchs von Titeln und mittelbarer Falschbeurkundung. Während der laufenden Verfahren wurde die zuständige Aufsichtsbehörde beim Landratsamt Nordhausen vom Bürgermeister der Stadt aufgefordert über den konkreten Fall, die Identität und die berufs- bzw. ehrenamtliche Tätigkeit des Betroffenen informiert, um vor ähnlich gelagerten Fällen zu warnen. Nachfolgend wurde vom Verantwortlichen des Landratsamtes für das Meldewesen die Mitteilung des Bürgermeisters, einschließlich der darin enthaltenen personenbezogenen Daten des Betroffenen, vor dem Kreisausschuss verlesen. Im gleichen Zeitraum wurden in der Presse Äußerungen des Bürgermeisters und weitere Details zum Sachverhalt veröffentlicht. Da die personenbezogenen Daten aus dem Verwaltungsverfahren rechtswidrig gegenüber der Presse offenbart wurden, hat der TLfD die Stadtverwaltung gem. § 39 Abs. 1 ThürDSG beanstandet. Es wurde gefordert, den Vorgang dahingehend auszuwerten, dass künftig bei Presseanfragen die datenschutzrechtlichen

Bestimmungen beachtet werden. Ebenso wurde darauf hingewiesen, dass personenbezogene Daten nur dann an andere Stellen übermittelt werden dürfen, wenn eine Übermittlungsbefugnis vorliegt. Die Beanstandung beruht darauf, dass nach § 22 Abs. 1 Nr. 2 ThürDSG und § 30 ThürVwVfG derartige Auskünfte im Hinblick auf schutzwürdige Interessen des Betroffenen rechtswidrig sind. Diese Datenübermittlungen waren auch nicht damit zu rechtfertigen, dass sie zur Aufgabenerfüllung der Kommune erforderlich oder die erteilten Auskünfte offenkundig und Jedermann zugänglich waren. Auch wenn die Presse bereits vor den Äußerungen des Bürgermeisters über entsprechende Informationen verfügt haben sollte, die möglicherweise unter Verstoß gegen das Datengeheimnis erlangt wurden, berechtigt dies eine Behörde nicht, derartige Berichte zu bestätigen bzw. zu ergänzen. Gemäß § 4 Abs. 2 Thüringer Pressegesetz sind die Behörden verpflichtet, Auskünfte gegenüber der Presse zu verweigern, soweit Vorschriften über die Geheimhaltung und den Datenschutz entgegenstehen. Dies war im vorliegenden Fall im besonderen Maße gegeben, da weder das Verwaltungsverfahren noch die staatsanwaltschaftlichen Ermittlungen abgeschlossen waren. Ebenso erfolgte die Datenübermittlung des Bürgermeisters an den Landkreis ohne Rechtsgrund, da zu Warnungszwecken die anonyme Sachverhaltsdarstellung ausreichend, mithin die Übermittlung personenbezogener Daten nicht erforderlich gewesen wäre. Eine Datenübermittlung, etwa im Rahmen einer einfachen Melderegisterauskunft, hätte nur die gesetzlich vorgegebenen Daten umfassen dürfen. Darüber hinausgehende Auskünfte, z. B. ob und wann ein Doktor-Titel eingetragen oder gelöscht wurde, sind somit unzulässig. Auch gehören Auskunftserteilungen aus dem Melderegister nicht zu den Aufgaben eines Bürgermeisters, Rechtsamtes oder eines Pressesprechers. Zuständig für die kostenpflichtigen Auskünfte aus dem Melderegister ist im Rahmen eines Aktes der laufenden Verwaltung ausschließlich die Meldebehörde.

Gegenüber dem Landkreis wurde festgestellt, dass das Verlesen der von der Stadtverwaltung unrechtmäßig übermittelten personenbezogenen Daten vor dem Kreisausschuss durch den Verantwortlichen des Landratsamtes für das Meldewesen rechtswidrig erfolgte. Dies stellte eine Weitergabe personenbezogener Daten innerhalb der Daten verarbeitenden Stelle oder an Teile derselben Stelle mit anderen Aufgaben im Sinne des § 3 Abs. 4 ThürDSG dar. Ein Erfordernis hierfür war nicht ersichtlich, da diese Frage bereits Gegenstand eines laufenden Verwaltungsverfahrens bzw. einer Strafanzeige war.

Nachfolgend wurde sowohl von der Stadtverwaltung als auch vom Landratsamt mitgeteilt, dass die datenschutzrechtlichen Bestimmungen nach der erfolgten Auswertung der Angelegenheit künftig beachtet werden.

Behörden sind gesetzlich verpflichtet, Auskünfte gegenüber der Presse zu verweigern, soweit Vorschriften über die Geheimhaltung und den Datenschutz entgegenstehen. Auch wenn die Presse bereits über Informationen verfügen sollte, die datenschutzrechtlich relevant sind, berechtigt dies eine Behörde nicht, derartige Berichte zu bestätigen bzw. zu ergänzen.

Eine Weitergabe personenbezogener Daten innerhalb der Daten verarbeitenden Stelle oder an Teile derselben Stelle mit anderen Aufgaben ist insbesondere dann unzulässig, wenn dies zur Aufgabenerfüllung nicht erforderlich ist.

### **5.11 Unzureichende Entsorgung personenbezogener Unterlagen durch Betreiber einer Asylbewerberunterkunft**

Am 30. Juli 2009 erhielt der TLfD die Information, auf dem Gelände der ehemaligen Asylbewerberunterkunft Gehlberg stünden mehrere Kartons mit Unterlagen von Asylbewerbern. Der Leiter des Sozialamtes des Ilm-Kreises stellte zwischenzeitlich die Kartons sicher, um sie vor dem Zugriff Unbefugter zu sichern. Eine Durchsicht der Unterlagen ergab, dass es sich überwiegend um personenbezogene Daten von Asylbewerbern, aber auch von Mitarbeitern des Betreibers handelte. Gegenüber der privaten Betreibergesellschaft der Asylbewerberunterkunft schritt das Landesverwaltungsamt als zuständige Datenschutzaufsichtsbehörde ein; gegenüber dem Landratsamt Ilm-Kreis nahm der TLfD unter anderem auch das Rechtsverhältnis zwischen dem Landratsamt und der Betreibergesellschaft unter die Lupe. Die Datenverarbeitung zwischen beiden Beteiligten ist als Auftragsdatenverarbeitung im Sinne von § 8 ThürDSG zu qualifizieren. Danach sind seitens des Landratsamtes die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten in einer entsprechenden Vereinbarung festzulegen. Das betrifft auch die Datenentsorgung. Hieran mangelte es bisher – allerdings sind diese Vertragsbeziehungen zwischenzeitlich auf datenschutzrechtskonforme Beine gestellt worden, sodass künftig derartige Vorfälle unterbleiben werden.

Stellt sich die Datenverarbeitung zwischen Landratsamt und privatem Betreiber einer Asylbewerberunterkunft als Auftragsdatenverarbeitung dar, sind die Vorgaben des § 8 ThürDSG einzuhalten.

### **5.12 Ausländerbehörde übermittelt zu freigiebig an Uni**

Ein ausländischer Student hatte seine Akte bei der TU Ilmenau eingesehen und dort ein Schreiben der Ausländerbehörde des Landratsamts des Ilm-Kreises entdeckt, in dem diese ungefragt der Universität mitteilte, dass sein Antrag auf Verlängerung der Aufenthaltserlaubnis abgelehnt worden ist. Er war der Auffassung, dass es für eine solche Übermittlung keine Rechtsgrundlage gibt und wandte sich an den TLfD mit der Bitte um Überprüfung. Eine Nachfrage beim Landratsamt des Ilm-Kreises hat ergeben, dass nach § 16 Abs. 1 i. V. m. § 4 AufenthaltsgG ein Ausländer für ein Studium zwar einen Aufenthaltstitel benötigt, im Ausländerrecht jedoch keine ausdrückliche Übermittlungsbefugnis der Ausländerbehörde an die Universitäten enthalten ist. Den Anwendungshinweisen zum Aufenthaltsgesetz sei nur zu entnehmen, dass sich eine Datenübermittlung an andere als in § 90 AufenthaltsgG genannte Stellen nach spezifischen Bundes- und Landesregelungen richtet. Das vom TLfD hierzu befragte TIM war der Ansicht, dass eine solche Übermittlung nach § 21 Abs. 1 Nr. 1 ThürDSG zulässig ist, wenn die Immatrikulationsordnung der jeweiligen Hochschule den Nachweis des Ausländers gegenüber der Hochschule über den rechtmäßigen Aufenthaltsort im Bundesgebiet vorschreibt. Diese differenzierende Auffassung ist auch sachgerecht, da bei den Universitäten nur in diesem Fall eine Erforderlichkeit für eine Übermittlung des Aufenthaltsstatus gegeben ist. Daraufhin wurde die Ausländerbehörde aufgefordert, die TU-Ilmenau auf die fehlende Rechtsgrundlage der Mitteilungen hinzuweisen und diese aufzufordern, die Mitteilungen nicht zu den Studentenakten zu nehmen, was dann auch erfolgt ist. Das TIM hat über das Thüringer Landesverwaltungsamt die Ausländerbehörden über seine Rechtsauffassung informiert und die Behörden wegen der unterschiedlichen Immatrikulationsordnungen aufgefordert, mit der jeweiligen Hochschule abzustimmen, ob derartige Mitteilungen erfolgen können.

Eine unaufgeforderte Übermittlung des Aufenthaltsstatus von Ausländern durch die Ausländerbehörden an Hochschulen darf nur in denjenigen Fällen erfolgen, in denen diese Informationen nach den jeweiligen Immatrikulationsordnungen der Hochschulen vorgeschrieben sind.

### 5.13 Luftbildauswertung durch Zweckverband

Über die datenschutzrechtliche Problematik bei der Erstellung von Luftbildaufnahmen für verschiedene Zwecke der Verwaltung hat der TLfD bereits ausführlich berichtet (7.TB, 12.1). Auch im aktuellen Berichtszeitraum beschäftigt den TLfD das Erstellen von Luftbildern im Zusammenhang mit der Einführung von Niederschlagswassergebühren durch Abwasserzweckverbände. So hat der Wasserversorgungs- und Abwasserzweckverband Sonneberg Luftbildaufnahmen im Verbandsgebiet erstellt, diese ausgewertet und die Ergebnisse den Grundstückseigentümern zum Zweck der Datenerhebung in einem Niederschlags-/Schmutzwasserabgabeverfahren zur Kenntnis gegeben. Daraufhin fragte ein hiervon betroffener Grundstückseigentümer an, ob eine solche Verfahrensweise aus datenschutzrechtlicher Sicht erlaubt sei. Der TLfD stellte bei der Durchsicht der Entwässerungssatzung sowie der Beitrags- und Gebührensatzung des Zweckverbandes fest, dass weder eine Regelung über die Einführung einer gesonderten Gebühr für Niederschlagswasser enthalten war, noch das Erhebungsverfahren auf der Grundlage ohne Wissen der Betroffenen erstellt und personenbezogen ausgewerteter Luftbildaufnahmen darin erwähnt wurde. Existiert keine normenklare Regelung darüber, welche personenbezogenen Daten zu welcher konkreten Aufgabenerfüllung mit den Luftbildaufnahmen auf welche Weise verarbeitet und genutzt werden, findet eine rechtsgrundlose und damit datenschutzrechtswidrige Vorratsdatenspeicherung statt. Darüber hinaus stellt das Erheben von personenbezogenen Grundstücksdaten mittels einer Luftbildaufnahme einen Eingriff in das Recht auf informationelle Selbstbestimmung des Grundstückseigentümers dar, der ebenfalls einer dem Bestimmtheitsgrundsatz genügenden Rechtsgrundlage bedarf. Dabei darf die Auflösung der Aufnahme nach Auffassung des TLfD nur so hoch sein, wie dies für die Aufgabenerfüllung als unbedingt erforderlich anzusehen ist. Der TLfD forderte den Zweckverband auf, seine Satzungen entsprechend anzupassen und empfahl die Übernahme einer vom TLfD vorgeschlagenen Musterformulierung, die vor dem erwähnten datenschutzrechtlichen Hintergrund bereits von anderen Zweckverbänden und Aufsichtsbehörden zu erforderlichen Satzungsänderungen aufgegriffen worden war. Nachdem der Zweckverband trotz mehrmaliger Aufforderung keine den vorgenannten datenschutzrechtlichen Forderungen entsprechende Satzungsänderung vornahm, wurde diese Verletzung von Vorschriften über den Datenschutz gemäß § 39 ThürDSG beanstandet und das Landratsamt Sonneberg als zustän-

dige Kommunalaufsicht von dem Vorgang verständigt. Der Prozess, das Landratsamt Sonneberg von der Notwendigkeit der datenschutzkonformen Ausrichtung der Zweckverbandssatzung zu überzeugen, gestaltete sich zunächst wider Erwarten schleppend. Zwischenzeitliche Änderungen der Entwässerungssatzung sowie die Aktualisierung der Abwassergebührensatzung des Abwasserzweckverbandes konnten den datenschutzrechtlichen Mängeln indes abhelfen.

Luftbildaufnahmen verstoßen gegen das Grundrecht auf informationelle Selbstbestimmung, wenn ein Grundstückseigentümer anhand von Satzungsregelungen nicht erkennen kann, zu welchem konkreten Zweck und auf welche Weise die gewonnenen personenbezogenen Daten von einem Abwasserzweckverband verarbeitet werden.

#### **5.14 Zustellung dienstlicher Schreiben in geöffneten Briefumschlägen in zwei Fällen**

Ein Petent gab an, dass ihm eine Anordnung des Landratsamts Saalfeld-Rudolstadt durch einen Mitarbeiter der Deutschen Post AG persönlich in einem unverschlossenen Briefumschlag gegen Unterschrift auf einem Rücklaufbogen zur Postzustellungsurkunde übersandt worden sei. Dadurch sei eine Kenntnisnahme des vertraulichen Schreibens durch Unbefugte möglich gewesen. Da die Klebep perforierung des Briefumschlages völlig unversehrt gewesen sei, sei anzunehmen, dass das Couvert mit dem fraglichen Schreiben im Landratsamt vor der Aufgabe zur Post nicht ordnungsgemäß verschlossen worden sei. Das Landratsamt teilte mit, es könne nicht geklärt werden, wie eine nicht ordnungsgemäß verschlossene Postsendung im zuständigen Amt unbemerkt bleiben konnte. In Auswertung der Angelegenheit hat das Landratsamt veranlasst, dass die Umschläge dieser Postzustellungsaufträge zusätzlich verklebt werden. Außerdem wurden die Mitarbeiter auf die erforderliche Sorgfalt bei der Behandlung dienstlicher Schreiben hingewiesen.

Einige Zeit später teilte der Petent mit, dass nunmehr ein Schreiben des TLfD durch die Deutsche Post AG - wiederum in einem geöffneten Briefcouvert - zugestellt worden sei. Da das Couvert des betreffenden Schreibens vor dem Postversand in der Behörde des TLfD korrekt verschlossen worden war, wurde der BfDI in seiner Zuständigkeit für die Deutsche Post AG um Sachverhaltsaufklärung gebeten. Wie sich herausstellte, wurde vor dem Vorfall die Wohnanschrift des Petenten infolge einer Eingemeindung und einer Umbenennung des Straßennamens

verändert. Da der TLfD ebenso wie der Petent dessen „alte“ Anschrift verwendet hatte, konnte das Schreiben nicht regulär zugestellt werden. Um den Brief mit einer korrekten Adresse zu versehen, wurde er dem Service Adress Management im zuständigen Briefzentrum zugeleitet. Wer die Sendung geöffnet hatte, konnte nicht ermittelt werden. Nachfolgend hat das Briefzentrum alle Mitarbeiter ausdrücklich belehrt und sich für den Vorfall entschuldigt. Die Möglichkeit, dass die Selbstklebperforation durch Alterung nicht mehr ausreichend klebte und später aufgegangen ist, konnte nicht ausgeschlossen werden

Die Übermittlung vertraulicher Daten in Postsendungen erfordert die Einhaltung geeigneter technischer und organisatorischer Maßnahmen im Sinne von § 9 ThürDSG.

### **5.15 Auskunftsgewährung im Widerspruchsverfahren zu Straßenausbaubeiträgen**

Im Rahmen eines Widerspruchsverfahrens stellte sich die Frage, ob die Verwaltungsgemeinschaft „An der Schmücke“ einem Verein privater Grundeigentümer Daten Dritter übermitteln darf. Konkret handelte es sich darum, dass der Verein Einsicht in personenbezogene bzw. personenbeziehbare Daten zu einzelnen Grundstücken aller betroffenen Anlieger – einschließlich der nicht in dem Verein vertretenen Eigentümer – beehrte, um damit die Beitragskalkulation dieser Grundstücke durch die Verwaltungsgemeinschaft nachvollziehen zu können. Festgestellt wurde, dass diese Daten für sich genommen nicht geeignet sind, um fehlerhafte Straßenausbaubeiträge zu belegen. Hierzu wäre darüber hinaus ein Vergleich der den Straßenausbaubeitragsbescheiden zugrunde liegenden Daten wie Geschossanzahl, bebaute Fläche, Grundstücksgröße und Nutzungsart mit den Gegebenheiten vor Ort erforderlich.

Der TLfD stellte fest, dass die beehrte Einsichtnahme unzulässig erfolgen würde. Diese Beurteilung beruht darauf, dass die Einsichtnahme personenbezogene bzw. personenbeziehbare Daten Dritter betrifft. Es war davon auszugehen, dass das schutzwürdige Interesse der nicht im Verein vertretenen Anlieger gegenüber dem Interesse der Widerspruchsführer, durch Einsichtnahme in die Unterlagen Dritter der Verwaltungsgemeinschaft Fehler beim Umlageverfahren nachzuweisen, überwog. Gemäß § 29 Abs. 2 ThürVwVfG muss Akteneinsicht nicht gewährt werden, soweit die Vorgänge wegen der berechtigten Interessen der Beteiligten oder Dritter geheim zu halten sind. Gegen eine Einsichtnah-

me in Akten mit geschwärzten bzw. anonymisiert personenbezogenen Daten bestehen keine Bedenken.

Gem. § 29 Abs. 2 ThürVwVfG muss Akteneinsicht nicht gewährt werden, wenn berechtigte Interessen Beteiligter oder Dritter überwiegen.

### **5.16 Datenhunger der Abfallwirtschaftsgesellschaft des Landkreises Gotha**

Ein Vermieter beschwerte sich über die Abfallwirtschaftsgesellschaft, einem Geschäftsbesorger des Landkreises Gotha, im Zusammenhang mit der Mülltonnennutzung. Dem Betroffenen wurde von der Abfallwirtschaftsgesellschaft ein mit „Änderungsmitteilung des anschluss- und erklärungspflichtigen Grundstückseigentümers“ benannter Fragebogen - unter Verwendung des Briefkopfs des Landratsamtes - übersandt. Der Erhebungsbogen enthielt eine Reihe von Fragen zu Name und Adresse des vorherigen Grundstückseigentümers und zu dem Ein- und Auszug von Mietern, dem eigenen Hausstand, dem Verzug aus dem Landkreis, dem Todesdatum, dem Trennungsdatum, dem „Geburtsdatum Kind“ und den „Vor- und Zunamen aller bisherigen/zukünftigen Haushaltsmitglieder“. Zur Prüfung der Zulässigkeit der Datenerhebung und zur Verwendung des Briefkopfs wurde das Landratsamt um eine Stellungnahme gebeten. Wie mitgeteilt wurde, sei bei einem Abgleich der Meldedaten festgestellt worden, dass nicht alle Bewohner des Grundstücks an die öffentliche Abfallentsorgung angeschlossen waren. Darauf hin sei zunächst der Vermieter befragt worden, wobei der Inhalt der Fragen mit der Abfallsatzung des Landkreises begründet wurde. Weiterhin wurde ausgeführt, dass Angaben zu den in einem Haushalt zusammenwohnenden Lebenspartnern, den in verschiedenen Haushalten wohnenden Familienmitgliedern und dem tatsächlichen Ein- oder Auszug von Mietern nur durch Befragung des Grundstückseigentümers aufgeklärt werden könnten. Die Verwendung des Briefkopfs des Landratsamtes durch dessen Geschäftsbesorger wurde damit begründet, dass dies einer bürger- und zeitnahen Verarbeitung diene. Die Erforderlichkeit der konkreten Datenerhebung zur Kontrolle des Anschlusses an die öffentliche Abfallentsorgung ist an der Abfallsatzung zu messen. Danach darf „die Anzahl der zu ihrem Haushalt gehörigen Personen“ bei den Grundstückseigentümern erhoben werden, „soweit diese selbst Bewohner der Grundstücke sind“. Somit durfte der Vermieter – vorausgesetzt er bewohnte das betroffene Grundstück – nur zur Anzahl der zu seinem

Haushalt gehörigen Personen, jedoch nicht zu den Haushalten seiner Mieter befragt werden. Eine weitere Norm der Satzung rechtfertigt eine Datenerhebung beim Eigentümer lediglich zu Namen und Anschriften der Mieter, nicht indes hinsichtlich weiterer Daten. Somit stellt die Erhebung von darüber hinausgehenden Daten, die Lebenspartner, die Haushalte und den Ein- oder Auszug von Mietern betreffen, einen Verstoß gegen § 4 Abs. 1 ThürDSG dar. Ebenso mangelt es an einer rechtlichen Befugnis für ein Tätigwerden des Grundstückseigentümers im Sinne eines „Erhebungsbeauftragten“ des Landkreises. Für die geforderten Auskünfte zu dem Beginn eines eigenen Hausstands, dem Datum einer Trennung, dem Vor- und Zunamen aller zukünftigen Haushaltsmitglieder und der bisherigen bzw. zukünftigen Adresse des Mieters ist eine Rechtsgrundlage für die Datenerhebung nicht ersichtlich. Daher wurde das Landratsamt Gotha aufgefordert, den Fragebogen an den für die Aufgabenerledigung erforderlichen Datenumfang anzupassen. Zur Verwendung des Briefkopfs des Landratsamtes durch die Abfallwirtschaftsgesellschaft wurde empfohlen, aus Gründen der datenschutzrechtlich gebotenen Transparenz in ähnlichen Fällen künftig schriftlich auf den bestehenden Geschäftsbesorgungsvertrag mit der Abfallwirtschaftsgesellschaft des Landkreises hinzuweisen. Der Fragebogen wurde zwischenzeitlich geändert.

Eine Erhebung personenbezogener Daten im Zusammenhang mit kommunalen Aufgaben, die weder durch eine Einwilligung noch durch Satzung oder andere Rechtsgrundlagen gedeckt ist, erfolgt rechtswidrig.

### **5.17 Datenschutz im Rettungswesen - Einsichtnahme des TLfD in Notarztprotokolle**

Bereits im 5.TB (5.2.9) und im 6.TB (5.3.9) wurde darüber berichtet, dass im Rahmen einer Kontrolle von Notarztprotokollen dem TLfD seitens der Stadt Suhl die Einsichtnahme in sämtliche Unterlagen verweigert wurde. Das Landesverwaltungsamt hat als Aufsichtsbehörde das daraufhin vom TLfD eingeleitete Beanstandungsverfahren unterstützt und die Stadt Suhl angewiesen, ihrer Verpflichtung zur Gestattung der Einsichtnahme nachzukommen. Nach erfolglosem Widerspruchsverfahren klagte die Stadt Suhl gegen diese Weisung. Am 28.10.2008 wies das Verwaltungsgericht Meiningen (2 K 95/04.Me) die Klage ab und bestätigte die Auffassung von TLfD und Landesverwaltungsamt, dass die Stadt Suhl die Einsichtnahme in die Notarztprotokolle gewähren muss.

Die hier streitige Norm des § 37 Abs. 2 Satz 3 ThürDSG lautet: „Unbeschadet des Kontrollrechts des Landesbeauftragten unterrichtet die Daten verarbeitende Stelle die Betroffenen in allgemeiner Form über das ihnen zustehende Widerspruchsrecht.“ Hieraus lasse sich, so das Verwaltungsgericht, entgegen der Auffassung der Stadt Suhl, erkennen, dass das Kontrollrecht des Landesbeauftragten und die Unterrichtungspflicht der öffentlichen Stelle gleichrangig nebeneinander stehen, ohne dass es auf eine zeitliche Reihenfolge ankomme. Auch durch die Verwendung des abstrakten Begriffs „Kontrollrecht“ werde zum Ausdruck gebracht, dass es sich um ein allgemeines und uneingeschränktes Recht handle, das unabhängig von einer vorherigen konkreten oder allgemeinen Belehrung bestehe. Eine öffentliche Stelle dürfe eine Kontrolle durch den TLfD nicht boykottieren.

§ 37 Abs. 2 ThürDSG berechtigt den TLfD zur Einsicht in Daten, die dem Arztgeheimnis unterliegen auch dann, wenn der Betroffene über sein Widerspruchsrecht nicht belehrt wurde.

## **6. Personaldaten**

### **6.1 Beschäftigtendatenschutz - ein beschwerlicher (und hoffentlich bald erfolgreicher) Weg**

Seit vielen Jahren fordern die Datenschutzbeauftragten des Bundes und der Länder klare Regelungen zum Umgang mit personenbezogenen Daten, die im Rahmen eines Arbeitsverhältnisses erhoben und gespeichert werden. Schon im Frühjahr 1992 wurde hierzu eine Entschließung gefasst, in der die Grundsätze für ein Arbeitnehmerdatenschutzgesetz aufgeführt waren. Trotz der Unterstützung der Forderungen u. a. durch den Bundestag kamen die damaligen Bundesregierungen über vielfache Absichtserklärungen nicht hinaus. Offenbar haben jedoch die Daten-skandale der letzten beiden Jahre, bei denen es immer wieder zu Bespitzelungen der Beschäftigten durch ihre Arbeitgeber gekommen ist, zu einem Umdenken geführt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Anfang 2009 in einer Entschließung (Anlage 21) die Eckpunkte für einen Beschäftigtendatenschutz anlässlich der Daten-skandale aktualisiert und die Bundesregierung aufgefordert, jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen. Nach der Bundestagswahl 2009 haben nun die Koalitionspartner vereinbart, dass der Arbeitnehmerdatenschutz in einem eigenen Kapitel im Bundesdatenschutzgesetz ausgestaltet werden soll.

Eine zügige Umsetzung der Koalitionsvereinbarung sollte nun endlich Rechtssicherheit und Transparenz für Arbeitnehmer und Arbeitgeber bringen.

### **6.2 Kreativität bei der Überführung von vermeintlich krank feiernden Mitarbeitern**

Wie bereits im letzten Tätigkeitsbericht (7. TB, 6.2) gab es auch im aktuellen Berichtszeitraum wieder einige Fälle, in denen mit unkonventionellen Mitteln überprüft werden sollte, ob krank geschriebene Mitarbeiter tatsächlich arbeitsunfähig waren oder dies nur vortäuschten. Eine besondere Kreativität bei der Wahl der (unzulässigen) Mittel konnte dabei bei der Polizei beobachtet werden. So sollte laut Presseberichten ein Polizeibeamter der Polizeidirektion Nordhausen mittels Hubschrauber überwacht worden sein, weil es Gerüchte bzw. Hinweise darüber gab, dass er trotz Krankschreibung an seinem Pool gebaut hatte. Dieser

Verdacht hatte sich nach einer Überprüfung jedoch nicht bestätigt. Vielmehr wurden während eines Hubschrauberflugs und damit mit polizeilichen Mitteln Aufnahmen vom Hausgrundstück des Beamten und mindestens eines weiteren Kollegen gefertigt. Diese Aufnahmen sollten angeblich den Beamten zum Geschenk gemacht werden. Ein Zusammenhang der Anfertigung der Luftaufnahmen mit den krankheitsbedingten Fehlzeiten des Betroffenen oder deren Nutzung zur Überprüfung der Krankschreibungen war jedenfalls nicht feststellbar. Es ließ sich bei einer Kontrolle auch die in der Presse geäußerte Vermutung, dass dem für die Begutachtung der Arbeitsfähigkeit zuständigen Polizeiarztlichen Dienst die Beweisfotos übermittelt wurden, nicht bestätigen. Allerdings hat die Polizeidirektion Nordhausen dem Polizeiarztlichen Dienst mit dem Untersuchungsauftrag Einzelheiten über wiederholte Krankschreibungen des Betroffenen während Wochenendeinsätzen mitgeteilt und daraus die Vermutung abgeleitet, dass diese Krankschreibungen nicht immer notwendig waren. Zur Bekräftigung wurde dann noch mitgeteilt, dass der Beamte während einer Krankschreibung einen Swimmingpool errichtet haben soll. Diese Informationen haben jedoch mit der zu prüfenden Frage, ob der Beamte zu einem anstehenden Einsatzwochenende noch arbeitsunfähig ist nichts zu tun und waren daher als unzulässige Datenübermittlungen anzusehen. Das wurde dann auch von der Polizeidirektion Nordhausen sofort eingesehen und Besserung versprochen, indem künftig dem Polizeiarztlichen Dienst nur noch die für die anstehende Untersuchung erforderlichen Umstände mitgeteilt werden sollen.

Noch gravierender waren die Methoden, die von der Polizeidirektion Erfurt ergriffen worden sind, um einen angeblich krank feiernden Polizisten zu überführen. Hier wurde zum Mittel der heimlichen polizeilichen Observation gegriffen, um die angebliche Beteiligung des Beamten an der Renovierung einer Wohnung nachzuweisen. Allerdings blieb es nicht bei der heimlichen Beobachtung, sondern es wurden die Observationen zu Beweis Zwecken auf Video festgehalten. Als wäre dies nicht schon schlimm genug, wurde auch noch bei der Akteneinsicht durch den Anwalt des Polizeibeamten geschlampt. Statt der Videoaufnahmen seines Mandanten bekam dieser auch noch Aufnahmen aus früheren Observationsmaßnahmen mitgeliefert, die sich gegen mutmaßliche Straftäter richteten und nichts mit dem Fall zu tun hatten. Grund hierfür war, dass vor der neuen Videoaufnahme das alte Band nicht vollständig gelöscht wurde und auch beim Überspielen auf eine DVD keine Kontrolle erfolgte. Unter völliger Verkenntnis der Rechtslage hatte der Leiter der

Polizeidirektion Erfurt eine Anordnung zum Einsatz besonderer Mittel der Datenerhebung nach § 34 Abs. 1 PAG unterschrieben. Offenbar hatte er angenommen, bei disziplinarischen Vorermittlungen gegen einen Beamten durch die Personal verwaltende Stelle dürften auch Befugnisse eingesetzt werden, die nur zur Gefahrenabwehr erlaubt sind. Der Einsatz von polizeilichen Mitteln zu Zwecken der Personalverwaltung war jedoch unzulässig. Aber auch zur Aufklärung der hier allenfalls in Frage kommenden Straftat der Schwarzarbeit durch den Beamten war eine solche heimliche Ermittlungsmaßnahme nicht zulässig, da die gesetzlichen Voraussetzungen nicht vorlagen. Vor allem lag hier keine Gefahr für ein hochrangiges Rechtsgut vor. Diese gravierenden Verstöße gegen datenschutzrechtliche Vorschriften wurden formell beanstandet und die Polizeidirektion Erfurt aufgefordert, die aufgenommenen Videos zu löschen, Kopien von anderen Stellen zurückzufordern sowie organisatorische Maßnahmen zu treffen, um sicherzustellen, dass bei Videobändern gewährleistet ist, dass keine früheren Aufnahmen ungelöscht auf den Datenträgern verbleiben. Festzustellen war zudem, dass die Ergebnisse der Observierung völlig ungeeignet gewesen wären, um einen Nachweis der Arbeitsfähigkeit zu führen. Selbst wer bei Renovierungsarbeiten tätig sein kann, muss nicht zwingend auch dienstfähig sein, was z. B. für psychische Erkrankungen gilt.

Die beiden Fälle zeigen erneut, dass Zweifel an der Dienst(un)fähigkeit letztlich nur durch eine ärztliche Untersuchung unter Einbeziehung des Betroffenen beseitigt werden können.

### **6.3 Personalakten der Schulverwaltung enthalten teilweise unzulässige Daten**

Aufgrund von Beschwerden von Bediensteten erfolgten im Geschäftsbereich des Thüringer Kultusministeriums mehrere Kontrollen, bei denen es um den Umfang der zulässigerweise zu speichernden Daten in den Personalakten ging. Im Schulamt Erfurt enthielt die geprüfte Akte eines Beschwerdeführers entgegen den Vorgaben von § 89 Abs. 1 ThürBG i. V. m. § 50 BeamStG auch solche Unterlagen, die nicht im unmittelbaren inneren Zusammenhang mit dessen Dienstverhältnis stehen, wie z. B. Beschwerden des Betroffenen, aus denen sich keine Auswirkungen auf das Dienstverhältnis ergaben, Bewerbungen um Versetzung oder Abordnung an eine andere Dienststelle sowie eine Dienstaufsichtsbeschwerde gegen einen Dritten. All dieser Schriftverkehr steht mögli-

cherweise in einem gewissen Zusammenhang mit dem Dienstverhältnis, jedoch nicht in der vom Gesetz geforderten Unmittelbarkeit, so dass derartige Unterlagen nicht in die Personalakte, sondern allenfalls zeitlich befristet in eine Sachakte aufgenommen werden dürfen. Das Schulamt kam daraufhin der Forderung nach einer Überarbeitung der Personalakte mit Beschränkung auf die gesetzlich zulässigen Inhalte nach. Bei einer Kontrolle im Schulamt Bad Langensalza wurde festgestellt, dass entgegen der Auffassung des Beschwerdeführers, dem wegen einer Straftat gekündigt worden war, die Hinweise zum Strafverfahren nicht aus der Akte entfernt werden müssen, auch wenn die Tilgungsfristen des BZRG schon abgelaufen sind. Der Grund hierfür liegt darin, dass aus der Personalakte erkennbar bleiben muss, was zur Kündigung geführt hat. Festgestellt wurde aber, dass andere Unterlagen, z. B. nicht mehr erforderliche Arbeitszeitnachweise nach Ablauf der Aufbewahrungsvorschriften aus den Personalakten noch nicht entfernt worden waren. Vom Schulamt Bad Langensalza konnte wegen der vorrangigen Arbeitsbelastung für die laufende Personalverwaltung keine sofortige Überarbeitung aller Personalakten zugesichert werden. Es sollen aber nicht mehr benötigte Unterlagen jedenfalls im Einzelfall entfernt werden, bevor die Akten berechtigten Dritten zugänglich gemacht werden.

Die Kontrolle einer Akte im Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) hat ebenfalls ergeben, dass es eine Reihe von Mängeln in der Aktenführung gab. So waren häufig zusätzlich Kopien von Unterlagen in der Akte abgeheftet, deren Originale schon in der Akte enthalten waren. Zudem war auch hier die Trennung von Personalakten und Sachakten nicht sauber durchgeführt. Als besonders problematisch erwiesen sich Unterlagen über den Gesundheitszustand des Betroffenen. So waren Krankmeldungen seit dem Jahr 1997 in der Akte enthalten, obwohl diese nach § 95 Abs. 2 ThürBG nach 5 Jahren hätten gelöscht werden müssen. Teilweise aus DDR-Zeiten stammende ärztliche Untersuchungsergebnisse waren unverschlossen abgeheftet. In das abgeheftete Formular einer Stellungnahme zu einem Dienstunfall wurde eingetragen, dass der Betroffene wegen einer Erkrankung desselben nunmehr verletzten Körperteils bereits vorher 2 Monate krankgeschrieben worden war. Zwar wurde nicht auch noch unzulässiger Weise über die Krankheitsursachen „Buch“ geführt, jedoch hatte der Sachbearbeiter außerdienstliche Kenntnis von der Krankheitsursache. Da vom ThILLM zugesagt wurde, neben der geprüften Akte den gesamten Personalaktenbestand zu überarbeiten, konnte von einer

Beanstandung der Verletzungen datenschutzrechtlicher Vorschriften abgesehen werden.

Die laufenden Personalakten müssen von Zeit zu Zeit überprüft werden, ob sie nicht Angaben enthalten, deren Aufbewahrungszeit zwischenzeitlich abgelaufen ist und die zu entfernen sind.

#### **6.4 Nutzung von PC-Protokolldaten von Mitarbeitern**

Ein Mitarbeiter des Landratsamts Nordhausen wurde aufgrund der protokollierten Internetnutzungsdaten eine Abmahnung erteilt, weil er nach Auswertung der protokollierten IP-Adressen über einen längeren Zeitraum hinweg dienstlich verbotene Seiten auf seinem Dienst-PC während der Arbeitszeit aufgerufen haben soll. Er wandte sich daraufhin an den Personalrat, der den TLfD um eine Prüfung gebeten hat, ob bei der erfolgten Datenverarbeitung die rechtlichen Vorgaben eingehalten wurden. Eine datenschutzrechtliche Kontrolle hat dann tatsächlich einige Defizite in organisatorischer Hinsicht ergeben. In der vorgefundenen Dienstanweisung war zwar festgelegt, dass Zugriffe auf das Internet nur für dienstliche Zwecke gestattet sind, die Zugriffe rechnerbezogen protokolliert werden sowie Verstöße mit einer Sperre des Internetzugangs und einer Abmahnung geahndet werden können. Allerdings enthielt diese keine Regelungen, unter welchen Voraussetzungen und durch wen die protokollierten Daten zur Missbrauchskontrolle ausgewertet werden dürfen. Zudem war die Dienstanweisung ohne Beteiligung des Personalrats erlassen worden. Im konkreten Fall war die Feststellung der unzulässigen Nutzung durch den Mitarbeiter ein Zufallsfund bei der Protokollauswertung zur Feststellung der Ursachen für eine Netzüberlastung. Diese zunächst zum Zweck der Sicherstellung eines ordnungsgemäßen Betriebs genutzten Protokolldaten unterliegen nach § 20 Abs. 4 ThürDSG einer strengen Zweckbindung. Das bedeutet, dass eine Verwendung zur Missbrauchskontrolle nur dann zulässig ist, wenn es dafür eine Rechtsgrundlage gibt. Eine solche Rechtsgrundlage kann eine nach § 74 Abs. 2 ThürPersVG erforderliche Dienstvereinbarung (bzw. Dienstanweisung mit Zustimmung des Personalrats) sein, da die personenbezogenen Protokolldaten geeignet sind das Verhalten oder die Leistung der Beschäftigten zu überwachen oder zu erfassen. Allerdings muss dabei der Grundsatz der Verhältnismäßigkeit gewahrt bleiben. Wie in der Orientierungshilfe „Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ (7. TB, 4.3) dargestellt, hat

sich die Kontrolle der dienstlichen Nutzung auf Stichproben zu beschränken. Eine automatische Vollkontrolle durch den Arbeitgeber wäre als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Im vorliegenden Fall fehlte es bereits an einer Dienstvereinbarung und zudem waren die erforderlichen Regelungen zum Umfang der Protokollierung und dem Verfahren der Auswertung überhaupt nicht festgelegt. Im Ergebnis der Prüfung wurde dem Landratsamt Nordhausen mitgeteilt, dass die Erhebung und Verwendung der Protokolldaten für arbeitsrechtliche Zwecke unzulässig war. Zwischenzeitlich hat das Landratsamt Nordhausen eine Dienstanweisung zum Zugang und zur Nutzung des Internet erlassen, die den datenschutzrechtlichen Anforderungen entspricht. Allerdings hat sich bislang der Personalrat geweigert, der Dienstanweisung zuzustimmen.

Auch wenn die Nutzung des dienstlich zur Verfügung gestellten Internetzugangs nur auf dienstliche Zwecke beschränkt wird, darf eine Kontrolle dieser Nutzungsart nur im Rahmen der Verhältnismäßigkeit erfolgen, wobei das Verfahren transparent unter Beteiligung der Personalvertretung geregelt werden muss. Landratsamt und Personalrat sind aufgefordert, sich im Interesse des Mitarbeiterdatenschutzes zeitnah über dieses Verfahren zu einigen.

## **6.5 Kündigung wegen Beschwerde beim TLfD**

Einen bislang einmaligen Vorgang stellte eine Beschwerde beim TLfD dar, bei der dem Beschwerdeführer von der Stadtverwaltung Leinefelde-Worbis gekündigt wurde und das unter anderem mit der Begründung, dass er sich in der Vergangenheit bei verschiedenen Behörden u. a. auch beim TLfD über seinen Dienstherrn beschwert hatte. Obwohl im Zusammenhang mit früheren Beschwerden des Betroffenen die Stadtverwaltung Leinefelde-Worbis vom TLfD auf das Benachteiligungsverbot des § 11 Abs. 2 ThürDSG hingewiesen wurde, hatte sie ihre verhaltensbedingte Kündigung damit begründet, dass der Betroffene sich mit unwarhen Behauptungen und zahlreichen Beschuldigungen an Institutionen gewandt habe, u. a. auch an den TLfD. Die Stadtverwaltung versicherte auf Nachfrage des TLfD zwar, dass sie die Vorschriften des Thüringer Datenschutzgesetzes einhalten wolle, sah sich aber verpflichtet, in der Begründung der Kündigung alle Stellen zu nennen, an die sich der Betroffene wandte und dadurch einen Vertrauensbruch begangen habe.

Nach § 11 Abs. 2 ThürDSG darf niemand benachteiligt oder gemaßregelt werden, weil er von seinem Recht, sich an den TLfD zu wenden, Gebrauch macht oder gemacht hat. Sinn und Zweck dieser Vorschrift als Sonderform des verfassungsrechtlich garantierten Petitionsrechts ist es, das Recht eines jeden zu gewährleisten, sich an den TLfD zu wenden, ohne Nachteile befürchten zu müssen. Deswegen darf eine Kündigung sich weder darauf stützen noch damit begründet werden, dass der Betroffene von seinem Recht nach § 11 ThürDSG Gebrauch gemacht hat. Hier wurde aber gerade dem Betroffenen gekündigt, weil er sich u. a. an den TLfD gewandt hatte. Deshalb wurde diese Verletzung datenschutzrechtlicher Vorschriften nach § 39 ThürDSG förmlich beanstandet. Schließlich hat die Stadtverwaltung Leinefelde-Worbis eingesehen, dass eine solche Verfahrensweise nicht zulässig ist und wies ihre Mitarbeiter an, dies künftig zu beachten.

Die Behörden dürfen Mitarbeiter, die sich beim TLfD wegen der Verletzung datenschutzrechtlicher Vorschriften beschwerten, nicht benachteiligen und schon gar nicht deswegen kündigen.

## **7. Polizei**

### **7.1 Novellierung des Polizeiaufgabengesetzes (Teil II)**

Die bereits im Jahr 2007 in den Landtag eingebrachte Novellierung des Polizeiaufgabengesetzes (7.TB, 7.1) wurde, wie zu erwarten war, erst nach der Entscheidung des Bundesverfassungsgerichts zu den Kennzeichenerkennungssystemen in den Polizeigesetzen von Hessen und Schleswig-Holstein (Urteil vom 11. März 2008, 1 BvR 2074/05 und 1 BvR 1254/07) zu einem Abschluss gebracht. Ungewöhnlich war dabei die Verfahrensweise. Da sich der Gesetzentwurf der Landesregierung bereits in der parlamentarischen Beratung befand, war zwar klar, dass Änderungen an dem Entwurf nur durch Anträge der Landtagsfraktionen vorgenommen werden konnten. Der Änderungsantrag, den die CDU-Landtagsfraktion dann aber im Juni 2008 vorgelegt hat, konnte jedoch kaum mehr als Änderungsantrag angesehen werden. Vielmehr war dies in weiten Teilen eine völlige Neuformulierung der Regelungsgegenstände. Ganz grundlegend wurde insbesondere § 34a PAG überarbeitet, der u. a. um eine Befugnis zur Quellen-TKÜ erweitert wurde. Erfreulich war, dass mit der Überarbeitung eine ganze Reihe von Änderungshinweisen des TLfD aus der Anhörung berücksichtigt worden sind. Zudem wurde die Regelungssystematik zum Kernbereichsschutz sowie zum Schutz der Berufsgeheimnisträger für den Rechtsanwender zumindest etwas verständlicher und klarer als im Regierungsentwurf gefasst, auch wenn nicht alle aufgezeigten Defizite beseitigt worden sind.

Die ursprünglich vorgesehene Regelung zur Kfz-Kennzeichenerkennung ist nach den Vorgaben des Bundesverfassungsgerichts so eingeschränkt worden, dass der konkrete Datenbestand, mit dem ein Abgleich zulässig sein soll, im Gesetz festgelegt sowie ein Einsatz nur noch bei bestimmten Gefahrenlagen und dem Vorhandensein einer Anhaltmöglichkeit zulässig ist. In § 33 Abs. 7 i. V. m. § 43 Abs. 2 PAG ist auch ausgeschlossen, dass ein Abgleich mit anderen polizeilichen Dateien erfolgt sowie die Daten zur Erstellung eines Bewegungsprofils verwendet werden. Was den Schutz des Kernbereichs privater Lebensführung angeht, so ist im Vergleich zum ursprünglichen Entwurf zu begrüßen, dass der Kernbereichsschutz nun auf alle heimlichen Ermittlungsmaßnahmen ausgedehnt wurde und auch ein absolutes Verwertungsverbot kernbereichsrelevanter Informationen festgeschrieben ist. Nach wie vor unbefriedigend ist jedoch das an § 100a Abs. 4 StPO angelehnte nur

relative Erhebungsverbot kernbereichsrelevanter Informationen. So soll nach § 34b Abs. 1 PAG eine Datenerhebung nur dann unzulässig sein, wenn aufgrund von tatsächlichen Anhaltspunkten eine Prognose vor Durchführung der Maßnahme ergibt, dass durch diese „allein“ Kenntnisse aus dem Kernbereich privater Lebensführung erlangt würden. Damit wird aber in Kauf genommen, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden, weil ein Unterlassen der Erhebung nur dann erfolgen würde, wenn die Prognose ergeben sollte, dass mit der Maßnahme ausschließlich kernbereichsrelevante Inhalte erfasst werden. Damit läuft jedoch das Erhebungsverbot faktisch leer, weil nur in den seltensten Fällen eine Unterhaltung ausschließlich kernbereichsrelevante Inhalte umfasst. Selbst wenn gesicherte Erkenntnisse vorliegen, dass der Großteil der Unterhaltung dem Kernbereich zuzuordnen ist, bleibt es der Polizei erlaubt, diese zunächst zu erfassen und erst in einem zweiten Schritt einem Verwertungsverbot zu unterwerfen.

Neu ist in § 34a Abs. 2 Satz 2 PAG die Befugnis zur sog. „Quellen-TKÜ“. Danach darf die Polizei zur Gefahrenabwehr eine laufende Telekommunikation durch Eingriff in ein vom Betroffenen genutztes informationstechnisches System überwachen. Die eingesetzte Technik ist dabei dieselbe wie bei der sog. Online-Durchsuchung. In seiner Grundsatzentscheidung zur Online-Durchsuchung vom 27. Februar 2008 (1 BvR 370/07 und 1 BvR 595/07) hat das Bundesverfassungsgericht die Quellen-TKÜ unter strengen Voraussetzungen für zulässig erachtet. So muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein, dass nur auf Daten der Telekommunikation, nicht aber auf andere auf dem informationstechnischen System gespeicherte Daten zurückgegriffen wird. Diese Anforderungen sind in die Regelung in § 34a Abs. 2 Satz 2 und 3 PAG aufgenommen. Ob und wie dies in der Praxis umgesetzt wird, konnte bislang noch nicht geprüft werden, da von dieser Befugnis nach Kenntnis des TLfD noch nicht Gebrauch gemacht wurde.

Ebenfalls noch nicht zufriedenstellend ist bei den Vorschriften zur Telekommunikationsüberwachung in § 34a PAG nach wie vor die Befugnis, Telekommunikationsüberwachung nicht nur zur Abwehr von Gefahren für hochrangige Rechtsgüter durchzuführen, sondern auch zur Straftatenverhütung, d. h. weit im Vorfeld einer konkreten Gefahrenlage. Außerdem dürfen auch nach wie vor Daten von sog. Nachrichtennetzern erhoben werden, ohne dass diese in irgendeiner Weise in einer verant-

wortlichen Beziehung zu den Gefahren oder geplanten Straftaten stehen müssen und damit auch reine Zufalls- oder Gelegenheitskontakte der Störer von einer Telekommunikationsüberwachung betroffen sein könnten. Hier hat in Teilbereichen zwischenzeitlich das Bundesverfassungsgericht, wenn auch aus anderen Gründen, korrigierend eingegriffen. Nach dem Urteil vom 2. März 2010 (1 BvR 256/08) darf die Thüringer Polizei nicht mehr auf die Telekommunikationsverkehrsdaten aus der Vorratsdatenspeicherung (§ 113a TKG) zur Straftatenverhütung zugreifen (4.1), wobei auch die Daten des Nachrichtennetzmittlers vom Zugriff ausgeschlossen wurden. Erlaubt ist dies nur noch zur Abwehr von dringenden Gefahren für Leib, Leben, Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr. Auch wenn sich dies nur auf die Daten der nicht mehr zulässigen Vorratsspeicherung bezieht, kann doch daraus abgelesen werden, welche allgemeinen Anforderungen das BVerfG an die Schwellen stellt, ab der eine präventive Telekommunikationsüberwachung zulässig sein dürfte, zumal es bei den Verkehrsdaten noch nicht einmal um Gesprächsinhalte geht. So hat das Bundesverfassungsgericht festgestellt, dass für die Gefahrenabwehr eine wirksame Begrenzung des Datenzugriffs durch Bezugnahme auf Kataloge von Straftaten, deren Verhinderung die Datenverwendung dienen soll, eine ungeeignete Regelungstechnik ist. Damit dürfen die in § 34a Abs. 3 Nr. 2 und 3 PAG Thüringen vorgesehenen Befugnisse zur Verhütung von dort aufgeführten Straftaten für einen möglichen künftigen Zugriff auf Vorratsdaten nicht mehr verfassungsgemäß sein und müssen geändert werden. Dem ebenfalls novellierten Thüringer Verfassungsschutzgesetz fehlen nach wie vor vollständig Regelungen zum Schutz des Kernbereichs privater Lebensführung.

Die im Koalitionsvertrag angekündigte Novellierung des PAG sollte genutzt werden, die noch vorhandenen Defizite des Polizeiaufgaben- und des Verfassungsschutzgesetzes beim Datenschutz so schnell wie möglich zu beseitigen.

## **7.2 Kompetenzzuwachs des Bundeskriminalamts**

Im Frühjahr 2008 wurde kurz nach der Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung im Nordrhein-Westfälischen Verfassungsschutzgesetz der Entwurf einer Novelle des Bundeskriminalamtgesetzes von der Bundesregierung vorgelegt. Grundlage hierfür

war die mit der Föderalismusreform geschaffene Gesetzgebungskompetenz des Bundes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalpolizeiamt nach Art. 73 Abs. 1 Nr. 9a GG. Neben der Online-Durchsuchung, die nach einigen Diskussionen ausschließlich auf Anordnung eines Richters zum Einsatz kommen darf, wurde das BKA nun mit fast allen Eingriffsermächtigungen ausgestattet, die sich in den Landespolizeigesetzen zur Gefahrenabwehr finden – nur nicht alle in einem Landespolizeigesetz. Damit ist ein enormer Machtzuwachs verbunden, weil dem BKA bislang neben der Zentralstellenfunktion im Wesentlichen nur Kompetenzen in speziellen Bereichen der Strafverfolgung zustanden. Von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde in einer Entschließung (Anlage 5) gefordert, dass dem BKA nicht mehr Eingriffsmöglichkeiten eingeräumt werden, als den einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Durch das Nebeneinander der z. T. sehr eingriffsintensiven Befugnisse steht insbesondere zu befürchten, dass Eingriffe parallel durch Bundes- und Landesbehörden erfolgen und so unnötig in die Rechte der Betroffenen eingegriffen wird. Diese Argumente wurden jedoch nicht berücksichtigt und das Gesetz insoweit unverändert erlassen.

Aufgrund der anhängigen Verfassungsklagen wird wieder einmal das Bundesverfassungsgericht über die Verfassungsmäßigkeit der erweiterten Eingriffsbefugnisse des Bundeskriminalamts entscheiden.

### **7.3 Ermittlungen wegen Amok-Drohungen gegen eine Erfurter Schule**

Ende 2008 hielt eine durchaus ernst zu nehmende Amok-Drohung gegen eine Erfurter Schule die Sicherheitsbehörden und auch die Öffentlichkeit in Atem. Hinterher stellte sich heraus, dass es sich um einen ziemlich geschmacklosen Streich von zwei Schülerinnen dieser Schule handelte. Auch wegen der schrecklichen Ereignisse am Erfurter Gutenberg Gymnasium im April 2002 mussten die Behörden die Drohung sehr ernst nehmen und fahndeten fieberhaft nach den Tätern, die ihre Drohungen per E-Mail versandt hatten. Als Absendeort dieser E-Mails konnte sehr schnell die Erfurter Stadtbibliothek festgestellt werden. Allerdings handelte es sich um einen öffentlich zugänglichen Computer, so dass hier zunächst die elektronischen Ermittlungsmethoden nicht weiter führten. Sie sollten aber noch ausführlich zum Einsatz kommen. Man entschloss

sich, nun auf das Mittel der DNA-Analyse zurückzugreifen. Dem lag die Annahme zu Grunde, dass die Täter bei der Benutzung des Computers organisches Material an der Tastatur und an den zur Nutzung eingeworfenen Münzen zurückgelassen hatten, das gesichert und molekulargenetisch untersucht wurde. Parallel dazu wurde von 29 Schülern der Schule, die in das vermutete Täterprofil passten und auch zu den Bibliotheksnutzern gehörten, freiwillige Speichelproben zum Zweck der molekulargenetischen Untersuchung entnommen. Zudem wurden auch zwei Beschäftigten der Bibliothek solche Speichelproben entnommen, um deren Spuren von vornherein ausschließen zu können.

Zu einer Untersuchung der Proben ist es jedoch nicht mehr gekommen, da zwischenzeitlich die Täterinnen auf anderem Weg ermittelt werden konnten. Die Proben wurden daraufhin vernichtet und die betroffenen Schüler darüber informiert. Dies führte zu Fragen an den TLfD, ob solche Proben überhaupt mit Einwilligung der Schüler hätten erhoben werden dürfen. Die daraufhin vom TLfD durchgeführte Kontrolle bei der Polizeidirektion Erfurt ergab in Bezug auf die Entnahme der Speichelproben keine Verletzung datenschutzrechtlicher Vorschriften. Die Schüler sind über die Tragweite der Einwilligung nach § 81c StPO sowie über den weiteren Umgang mit Ihren Proben informiert worden. Zuvor waren auch die Eltern in Informationsveranstaltungen über das geplante Verfahren unterrichtet worden. Deren Einwilligung war bei den hier über 17jährigen nicht erforderlich, weil es keine Anzeichen dafür gab, dass sie die Tragweite ihrer Entscheidung nicht überblicken konnten.

Fraglich war, ob die Speichelproben nach den Vorschriften der StPO von den Schülern zum Zweck der molekulargenetischen Untersuchung durch die Polizei erhoben und gespeichert werden durften. Nach der Rechtsprechung kann dies noch auf § 81e Abs. 1 Satz 2 StPO gestützt werden. Allerdings dürfen wegen des Verhältnismäßigkeitsgrundsatzes auf diese Weise nicht beliebig viele und auch nicht willkürlich ausgesuchte Personen untersucht werden. Denn hier besteht die Gefahr, dass man in den Anwendungsbereich einer sog. DNA-Reihenuntersuchung nach § 81g StPO gerät. Eine solche ist aber nur bei bestimmten schweren Delikten und nur mit richterlicher Anordnung zulässig. Da es im Ergebnis zu keiner Untersuchung des Materials kam und zudem schwerste Straftaten zu befürchten waren, wurde diese Maßnahme im Ergebnis nicht kritisiert, auch wenn in künftigen Fällen eine solche Vorgehensweise genau abgewogen werden muss.

Es blieb allerdings nicht nur bei dem Versuch, die Täter mittels DNA-Analyse zu finden. Wie sich bei der Kontrolle durch den TLfD herausstellte, sind die kurz zuvor neu geschaffenen Instrumente des § 34a PAG in großem Umfang, allerdings nur mit sehr mäßigem Erfolg zur Anwendung gekommen. Neben der Verkehrs- und Inhaltsdatenabfrage des Telefonanschlusses der Schule wurden auch die Verbindungs- und Inhaltsdaten der beiden E-Mail-Konten abgefragt, von denen aus die Droh-E-Mails versandt worden waren. Zudem wurde beim Betreiber der Schul-Homepage nach den IP-Adressen gefragt, über die an dem Tag der Drohung auf die Seite zugegriffen wurde. Allerdings waren diese bereits datenschutzgerecht nach einem Tag gelöscht. Alle diese Maßnahmen erfolgten auf der Grundlage des § 34a Abs. 1 PAG mit richterlichen Anordnungen, die dem TLfD auch vorgelegt wurden und gegen deren Durchführung keine Bedenken bestanden.

Eine weitere auf § 34a PAG gestützte Maßnahme stellte sich als sehr umfangreich heraus. So wurden bei einer sog. Funkzellenabfrage im Bereich zwischen Schule und Stadtbibliothek die Mobiltelefonverkehrsdaten von etwa 36.000 Betroffenen erfasst. Ziel war auch hier, die Urheber der Droh-E-Mails ausfindig zu machen. Dazu ging man davon aus, dass die Täter sich an den jeweiligen Tagen zu bestimmten Zeiten sowohl in der Schule als auch in der Stadtbibliothek aufgehalten haben. Deshalb fragte die Polizei bei den Mobilfunkanbietern die Verbindungsdaten derjenigen Mobilfunkgeräte ab, die sich während der fraglichen Zeiträume in den Funkzellen befunden haben und eingeschaltet waren. Aus der Schnittmenge erhoffte man sich weitere Ermittlungsansätze. Da sich jedoch in den abgefragten Funkzellen auch der Erfurter Weihnachtsmarkt befand, war die Anzahl der erfassten Daten zu groß, um sinnvolle Ansätze zu liefern. So wurden sämtliche Daten wieder gelöscht.

Zurück blieben die Fragen, ob aus § 34a PAG die Befugnis für eine solche Funkzellenabfrage abgeleitet werden kann sowie ob die Löschung der Daten erfolgen durfte, ohne dass zuvor die von der Maßnahme Betroffenen darüber unterrichtet worden sind. Inhaltlich war diese Löschung nach § 34 Abs. 7 und 9 PAG ohne Benachrichtigung gerechtfertigt, weil der Aufwand zur Namhaftmachung der Mobiltelefoninhaber nicht nur immens groß gewesen wäre, sondern die Ermittlung der Adressen auch zu einer Intensivierung des Eingriffs gegenüber

diesen Personen geführt hätte. Darüber hinaus kann die Benachrichtigung von Unbeteiligten auch unterbleiben, wenn sie nur unerheblich betroffen waren und anzunehmen ist, dass sie kein Interesse an der Benachrichtigung haben. Auch das konnte bei der Funkzellenabfrage angenommen werden, da mit den Daten keine weiteren Ermittlungen durchgeführt wurden. Etwas irritiert hat jedoch der Umstand, dass die Polizei sich offenbar nicht ganz sicher war und eine Entscheidung beim Amtsgericht Erfurt zur richterlichen Bestätigung ihrer Entscheidung zum Absehen von einer Benachrichtigung der Betroffenen beantragte, was gesetzlich so nicht vorgesehen ist. Noch mehr hat erstaunt, dass vom Amtsgericht Erfurt eine solche Bestätigung ergangen ist, ohne dass es hierzu eine Kompetenzzuweisung im PAG an das Gericht gibt. Die hier praktizierte Verfahrensweise kann dazu führen, dass sich die Polizei auf die Billigung durch das Gericht beruft und so die Möglichkeit des TLfD faktisch beschränkt, Entscheidungen, zu hinterfragen. Das Thüringer Innenministerium hat die Hinweise des TLfD hierzu aufgegriffen und in einer Verwaltungsvorschrift zu § 34a PAG klargestellt, dass richterliche Anordnungen nur in den gesetzlich vorgesehenen Fällen beantragt werden dürfen.

Auch wenn im Gesetzgebungsverfahren zum PAG nie die Rede von einer Befugnis für die Funkzellenabfrage war, so konnte sich der TLfD nicht der Argumentation des Thüringer Innenministeriums verschließen, dass die Befugnis zu einer solchen aus dem Wortlaut des § 34a Abs. 1 Satz 1 Nr. 3 i. V. m. Abs. 3 PAG abgeleitet werden kann. Danach dürfen zur Abwehr einer dringenden Gefahr für hochrangige Rechtsgüter Verkehrsdaten nach § 96 Abs. 1 und § 113a TKG erhoben werden. Bei den 36.000 Datensätzen in den Funkzellen handelt es sich ohne Zweifel um Verkehrsdaten i. S. d. § 96 Abs. 1 TKG, zu denen bei mobilen Anschlüssen auch die Standortdaten (also auch die Funkzellen) gehören. Ein Antrag muss nach § 34a Abs. 6 Satz 2 Nr. 1 PAG nur soweit bekannt den Namen und die Anschrift des Betroffenen enthalten. In § 34a Abs. 6 Satz 2 Nr. 2 wird zusätzlich die Rufnummer oder eine andere Kennung des TK-Anschlusses gefordert, so dass eine Abfrage tausender von Anschlusskennungen ausgeschlossen wäre. Allerdings schränkt das Gesetz diese Anforderung auf die Überwachung oder Datenerhebung der Telekommunikation ein. Hier argumentiert das Thüringer Innenministerium vertretbar, dass die reine Verkehrsdatenerhebung nach § 34a Abs. 1 Nr. 3 PAG nicht unter den Begriff der Überwachung oder Datenerhebung der Telekommunikation falle. Selbst wenn man dieser Argu-

mentation folgt, dann muss aber aus Gründen der Verhältnismäßigkeit eine Begrenzung der Datenerhebung zumindest in zeitlicher und räumlicher Hinsicht erfolgen. Da hier Auslegungsschwierigkeiten bei den Anwendern auftreten können, habe ich das Thüringer Innenministerium aufgefordert, dies zumindest in der Verwaltungsvorschrift zu § 34a PAG näher zu erläutern. Dies ist zwischenzeitlich geschehen.

Der vorliegende Fall kann sicherlich als Ausnahmefall der Gefahrenabwehr angesehen werden. Hier hat der Einsatz eingriffsintensiver Maßnahmen im Ergebnis gerade nicht zur Abwehr der Gefahr geführt. Deshalb sollte genau geprüft werden, ob das Mittel der Funkzellenabfrage zur Gefahrenabwehr geeignet und erforderlich ist. Falls das bejaht werden sollte, müsste bei einer Novellierung des PAG die Befugnis zur Funkzellenabfrage im Interesse der Rechtssicherheit und Anwenderfreundlichkeit entsprechend den Vorschriften in der StPO oder dem BKAG normenklar geregelt werden.

#### **7.4 Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmern**

In den letzten Jahren haben bei Großereignissen wie der Fußball-Weltmeisterschaft, dem Papstbesuch oder der Leichtathletik-Weltmeisterschaft verstärkt Sicherheitsüberprüfungen von Personal stattgefunden, das in sicherheitsrelevanten Bereichen tätig wird. Weil die gesetzlichen Tatbestände zur Zuverlässigkeitsüberprüfung nicht ausgereicht haben, wurde, begründet mit der Einmaligkeit der jeweiligen Großereignisse, kurzerhand auf die Einwilligung der betreffenden Arbeitnehmerinnen und Arbeitnehmer zurückgegriffen. Dieses gegenüber ihren Arbeitgebern erteilte Einverständnis soll die Sicherheitsbehörden (Polizei und Verfassungsschutz) ermächtigen, dem Arbeitgeber Auskünfte zu sicherheitsrelevanten Bedenken gegen die beabsichtigte Tätigkeit des Betroffenen zu erteilen. Gegen diese Tendenzen hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 6) ausgesprochen. Hauptkritikpunkt ist in diesen Fällen, dass man nicht von einer wirksamen Einwilligung aus freien Stücken sprechen kann. Regelmäßig stehen die Betroffenen unter dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes. Zudem darf über solche Einwilligungen auch nicht die Grundentscheidung des Gesetzgebers umgangen werden, wonach über ein Führungszeugnis dem Arbeitgeber nur ganz

bestimmte Informationen über den Betroffenen zugänglich gemacht werden dürfen.

Zuverlässigkeitsprüfungen unter Mitwirkung der Sicherheitsbehörden dürfen nur auf der Grundlage normenklarer Rechtsgrundlagen erfolgen. Eine Einwilligung reicht dafür nicht aus. Wenn auf solche Überprüfungen nicht verzichtet werden kann, müssen die entsprechenden Regelungen dafür geschaffen werden.

### **7.5 Fehlende Rechtsgrundlage für INPOL-Dateien**

Grundlegende Bedeutung hat nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder in einer EntschlieÙung (Anlage 23) das Urteil des Oberverwaltungsgerichts Lüneburg vom 16.12.2008 (11 LC 228/08). Obwohl es sich nur auf die Rechtmäßigkeit der Führung der Verbunddatei „Gewalttäter Sport“ innerhalb des polizeilichen Informationssystems INPOL durch das Bundeskriminalamt bezieht, wirkt sich die bemängelte fehlende Rechtsgrundlage auf alle Verbunddateien aus. Das Gericht hat die von den Datenschutzbeauftragten seit Jahren vertretene Auffassung bestätigt, dass zur Führung der Verbunddateien durch Bund und Länder nicht nur jeweils eine Errichtungsanordnung auf der Grundlage von § 34 BKAG, sondern auch eine Rechtsverordnung nach § 7 Abs. 6 BKAG erforderlich ist. Der Aufforderung durch die Datenschutzkonferenz, die polizeiliche Datenverarbeitung auf den Prüfstand zu stellen, scheint das Bundesministerium des Innern durch den Erlass einer Verordnung nachkommen zu wollen. Bislang ist jedoch noch kein Entwurf vorgelegt worden.

Bei der zu erlassenden Rechtsverordnung wird es nicht nur darum gehen, dass die formelle Voraussetzung nach § 7 Abs. 6 BKAG erfüllt wird. Vielmehr müssen präzise und abschließend die Datenarten bestimmt werden, die im Verbund von Bund und Ländern gemeinsam in den jeweiligen Dateien verarbeitet werden dürfen.

### **7.6 Zugriffsprotokollierung und Kontrolle bei polizeilichen Dateien**

Die bereits dargestellte Problematik der noch unzureichenden Protokollierung der ZEVIS-Abfragen (7. TB, 7.8) hat möglicherweise dazu beigetragen, dass sich in der Folgezeit vermehrt betroffene Bürger an den

TLfD gewandt haben, die einen Missbrauch durch Polizeibeamte vermuteten. Solche Beschwerden sind deshalb für die Kontrolltätigkeit des TLfD so wichtig, weil häufig konkrete Anhaltspunkte für eine zweckwidrige Verwendung dienstlicher Daten durch Polizeibeamte fehlen und Stichprobenkontrollen zu deren Aufdeckung nur begrenzt tauglich sind. Oft sind es belästigende Telefonanrufe bei Betroffenen, deren Telefonnummern nicht in öffentlichen Verzeichnissen enthalten sind und die zu der Vermutung führen, dass auf diese Daten über polizeiliche Datensammlungen zugegriffen wurde. In einem Fall hat sich z. B. ein Bürger an den TLfD gewandt, der von einem pensionierten Polizeibeamten beim Falschparken beobachtet wurde. Er hatte sich dann an einen ehemaligen Kollegen gewandt, der für ihn sozusagen als „Freundschaftsdienst“ die Adresse des Halters in ZEVIS abgefragt und ihm in unzulässiger Weise übermittelt hat. Damit ging er dann in der irrigen Vorstellung, er sei auch nach seiner Pensionierung im Dienst, zur Arbeitsstelle des Bürgers, vor dessen Gebäude er den Parkverstoß beobachtet hatte und stellte den Betroffenen vor seinem Chef auch noch bloß. Der Freundschaftsdienst seines ehemaligen Kollegen wurde jedoch für diesen teuer. Durch die Kontrolle der Protokolldaten konnte dieser ermittelt werden und muss nun mit disziplinarischen und strafrechtlichen Konsequenzen rechnen, da der Betroffene Strafantrag gestellt hat. Nach § 43 Abs. 4 ThürDSG steht das Strafantragsrecht bei Datenschutzverletzungen neben dem Betroffenen auch dem TLfD zu. Auch davon wurde im Berichtszeitraum Gebrauch gemacht. Hier wurde durch polizeiinterne Überprüfungen der Protokolldaten ein Missbrauch entdeckt, jedoch hatten die Abgefragten möglicherweise selbst zu der Tat angestiftet und somit bestand kein Interesse an der Ahndung des Verstoßes.

Allerdings sind auch Überprüfungen von Zugriffsprotokollierungen deshalb ohne Erfolg geblieben, weil die Qualität der Protokollierung noch teilweise unzureichend ist. Wie schon dargestellt (7.TB, 7.8), wird häufig der Grund der Abfrage nicht ausreichend festgehalten, obwohl dies in der Abfragemaske enthalten ist. Gerade dann, wenn der Beamte die Abfrage nicht für seine eigenen Aufgaben durchführt, sondern für einen Kollegen, z.B. wenn dieser über Funk in der Einsatzzentrale ein Kfz-Kennzeichen überprüfen lässt, ist die Dokumentation (aus welchem Grund und auf Veranlassung welches Beamten die Abfrage erfolgt) besonders wichtig. So wurde in einem Fall nach einer Anfrage über Polizeifunk ein Kfz-Kennzeichen durch eine Beamtin in der Einsatzzentrale der Polizeidirektion Nordhausen abgefragt, jedoch nicht doku-

mentiert, zu welchem Zweck und für welchen Kollegen die Abfrage erfolgte. Dass sich diese Beamtin nach über 6 Monaten nicht mehr an den veranlassenden Kollegen erinnern konnte, ist nachvollziehbar. Da auch der aufgezeichnete Funkverkehr datenschutzgerecht nach 3 Monaten gelöscht worden war, konnte in diesem Fall trotz gewichtiger Hinweise für einen Datenmissbrauch ein konkreter Verstoß nicht festgestellt werden. Das darauf vom TLfD eingeschaltete TIM hat einige technische und auch organisatorische Maßnahmen ergriffen, um solche Beweisschwierigkeiten künftig zu minimieren. So wurden die Aufbewahrungsfristen der Aufzeichnungen im Funkverkehr von 3 auf 6 Monate verlängert und damit den Löschrufen der Protokolldaten beim Kraftfahrtbundesamt angeglichen. Damit kann der Fall ausgeschlossen werden, dass im Kraftfahrtbundesamt Zugriffe noch protokolliert sind, aber die dazugehörigen Sprechfunkaufzeichnungen bereits gelöscht wurden. Wegen der besonderen Sensibilität dieser Funkaufzeichnungen bleibt es bei der generellen 3-monatigen Löschrufen. Vom 4. bis zum 6. Monat dürfen diese Daten nur noch zum Nachweis der Abrufberechtigung in zentralen Datenbanken genutzt werden und sind im Übrigen bis zur Löschung für alle anderen Nutzungen gesperrt. Zusätzlich wurden alle Polizeidienststellen angewiesen, bei INPOL- und ZEVIS-Abfragen, die für einen anderen Beamten erfolgen (z. B. bei Einsatzzentralen) in ein eigens hierfür geschaffenes Feld „Veranlasser“ den Namen oder die Funkkennung des Veranlassers und dessen Dienststelle einzutragen. Da dieses Feld mitprotokolliert wird, kann sich der Abfragende künftig nicht mehr darauf berufen, er wisse nicht mehr, für wen die betreffende Abfrage erfolgt ist. Allerdings ist das Feld nicht als Pflichtfeld ausgestaltet. Deshalb kann die Abfrage auch durchgeführt werden, ohne dass der Veranlasser eingetragen ist. Das TIM konnte bislang nicht überzeugt werden, beim INPOL-Land-POLAS Competence Center, dem gemeinsamen Software-Entwickler einiger Landespolizeien, eine solche Umprogrammierung anzustoßen. Das Argument, dass so ein Auftrag bis zu eineinhalb Jahren dauern kann, entbindet jedoch nicht von der Pflicht, zumindest mittelfristig auf dessen Einführung hinzuwirken.

Durch einige technische und organisatorische Maßnahmen sind die Nachweismöglichkeiten bei Datenmissbrauch innerhalb der Polizei bei „Stellvertreterabfragen“ verbessert worden. Das TIM sollte jedoch auf die Umwandlung des Feldes „Veranlasser“ als Pflichtfeld hinwirken. Wichtig bleiben für die Kontrollarbeit die zeitnahen Hinweise der Betroffenen auf mögliche unbefugte Datenabfragen.

### **7.7 Der oft schwierige Weg vom Blitzfoto zum Verantwortlichen**

Fährt man mal etwas zu schnell und wird dabei auch noch von einem Fotoapparat oder einer Videokamera abgelichtet, dann stellt sich für die Polizei das Problem, das Verwarnungsgeld oder auch das Bußgeld vom Verursacher einzutreiben. Wird nicht am „Tator“ direkt abkassiert, bleibt nur der Weg, den Betroffenen über das fotografierte Kfz-Kennzeichen durch eine Halterabfrage in Verbindung mit dem Beweisfoto ausfindig zu machen. Das gestaltet sich zum Teil nicht ganz einfach und ist wegen der damit verbundenen Datenverarbeitungen auch datenschutzrechtlich nicht immer unproblematisch. Im Berichtszeitraum hat es eine Reihe von Anfragen Betroffener zu verschiedenen Aspekten bei der Fahrerermittlung gegeben, die Anlass geben, einige datenschutzrechtliche Gesichtspunkte einmal etwas näher zu beleuchten.

In einem Fall hatte die Schweizer Polizei bei der Polizeiinspektion Gotha um Amtshilfe gebeten, weil durch das Kraftfahrzeug eines deutschen Halters eine Geschwindigkeitsübertretung festgestellt wurde. Allerdings war noch nicht einmal ein Beweisfoto mitgeschickt worden. Der von der Polizeiinspektion Gotha befragte Halter gab an, dass sein Fahrzeug von seiner Tochter genutzt werde, die den Wagen gelegentlich auch Bekannten überlasse. Daraufhin übermittelte die Polizeiinspektion Gotha diese Information einschließlich des Namens, Geburtsdatums und der Anschrift der Frau in Deutschland an die Kantonspolizei Zürich. Dafür gab es jedoch (noch) keine Rechtsgrundlage. Was unter deutschen Polizeibehörden ohne weiteres möglich wäre, bedarf jedoch bei der Beteiligung ausländischer Behörden einer gesonderten Rechtsgrundlage. Zwar gibt es im deutsch-schweizerischen Polizeivertrag eine solche Befugnis. Diese war aber zum Zeitpunkt der Übermittlung noch nicht in Kraft getreten. Nachdem sich der Betroffene an den TLfD gewandt und dieser die Polizeidirektion Gotha auf die Rechtslage hingewiesen hat, forderte die Polizeidirektion Gotha die Kantonspolizei Zürich auf, die übersandten Unterlagen zu vernichten, was von dort zugesagt wurde. Der ebenfalls vom TLfD informierte Datenschutzbeauftragte des Kantons Zürich sicherte zu, eventuelle Beschwerden oder Anfragen des Betroffenen direkt zu bearbeiten. Zur Vermeidung weiterer Datenschutzverletzungen erging Anfang 2009 ein gemeinsamer Erlass des TIM und des TJM, der bis zum Inkrafttreten des direkten Informationsaustauschs zwischen den Polizeibehörden vorschreibt, dass alle direkt bei den Polizeibehörden

eingehenden Ermittlungersuchen an die zuständige Staatsanwaltschaft zur weiteren Entscheidung weitergeleitet werden müssen.

In einer weiteren Beschwerde, ging es darum, dass der Sohn mit dem Kfz seines Vaters geblitzt wurde. Der Vater reagierte zunächst nicht auf den Anhörungsbogen. Aufgrund des geschätzten Alters des abgebildeten Fahrers war mit sehr großer Wahrscheinlichkeit davon auszugehen, dass nicht er, sondern eine andere Person das Kfz zum Tatzeitpunkt geführt hat. Deshalb wurde die Polizei in Berlin – dem Wohnort von Vater und Sohn, mit der Fahrerermittlung beauftragt. Die dazu erforderliche Datenübermittlung war im Gegensatz zu dem Datenaustausch mit der Schweiz von den Vorschriften der StPO und des OWiG gedeckt. Der Ermittlungsauftrag führte letztlich auch zum Sohn. Entgegen der Ansicht des Beschwerdeführers musste sich die Polizei nicht mit dem zwischenzeitlichen „Geständnis“ des Vaters durch Zahlung des Verwarngeldes zufrieden geben und von weiteren Ermittlungen absehen, da die Verfolgungsbehörden nicht nur belastende sondern auch entlastende Gesichtspunkte bei Ordnungswidrigkeiten zu ermitteln haben. Ob die Fahrerermittlung der Berliner Polizei über einen Lichtbildabgleich mit dem Personalausweisantrag rechtmäßig war, konnte der TLfD nicht prüfen und verwies den Beschwerdeführer an den Berliner Kollegen. In Thüringen wäre dies bei der vorliegenden Konstellation jedoch nach der Verwaltungsvorschrift zur Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten (7. TB, 7.2) wohl nicht zulässig gewesen. Nach 2.3.2.1 dieser Verwaltungsvorschrift darf ein Lichtbildabgleich nur in denjenigen Konstellationen erfolgen, in denen die Anhörung zu keinem Ergebnis führte und es sich bei Fahrer und Halter offensichtlich um Personen unterschiedlichen Geschlechts handelt. Nur in diesen Fällen darf ein Lichtbild und auch nur des Ehepartners angefordert werden. Nicht erfasst sind demnach die Fälle unterschiedlichen Alters. Hier müsste in Thüringen auf andere Ermittlungsmethoden, z. B. die Befragung des Halters, zurückgegriffen werden.

Da mit der in Thüringen regelmäßig praktizierten Übersendung des Anhörungsbogens einschließlich des Frontfotos an den Halter (2. TB, 7.10) auch eine Übermittlung personenbezogener Daten Dritter verbunden sein kann (immer dann, wenn der Halter nicht selbst gefahren ist), stellt sich zum Teil die Frage, ob dies erforderlich und auch verhältnismäßig ist. Ausgangspunkt für diese Verfahrensweise ist der Umstand, dass der Halter im Regelfall wissen darf und auch sollte, wer sein Kraft-

fahrzeug führt. Wird vom berechtigten Nutzer gegenüber dem Halter die Fahrzeugüberlassung an einen Dritten verschwiegen (z. B. Überlassung des Kfz an Geliebten der Ehefrau), so überwiegt das Interesse des Halters an der Kenntnis, wer sein Fahrzeug zum Zeitpunkt der Ordnungswidrigkeit geführt hat, da ihm bei der Unaufklärbarkeit des Verstoßes eine Fahrtenbuchauflage droht. Die rechtliche Befugnis zur Übermittlung des Frontfotos an den Halter ergibt sich aus § 69 Abs. 1 StPO i. V. m. § 46 Abs. 1 OWiG. Danach sind dem Halter als Zeuge, der Hinweise zur Identität des Fahrers machen kann, vor seiner (schriftlichen) Vernehmung der Gegenstand der Untersuchung und die Person des Beschuldigten (hier durch Übermittlung des Fotos) zu bezeichnen. Eine solche Maßnahme ist auch nicht unverhältnismäßig, da das Fahrerfoto gerade nicht einem unbegrenzt großen Personenkreis zugänglich gemacht wird, sondern nur demjenigen, der nach allgemeiner Erfahrung wissen müsste, wer das auf ihn zugelassene Fahrzeug zum Tatzeitpunkt geführt hat. Diese Grundsätze galten auch bei einer Beschwerde, bei der der Anhörungsbogen samt Foto an einen leitenden Mitarbeiter eines Unternehmens versandt worden ist. Ihm war es unangenehm, dass seine Mitarbeiter bei der Öffnung der Post sein Konterfei und damit seine Verkehrsübertretung zur Kenntnis bekamen. Meist stellen sich solche Fälle gerade umgekehrt dar, indem der Chef über die Verkehrsübertretungen seiner Mitarbeiter informiert wird. Aber auch hier gilt, dass der Halter zum einen wissen darf, wer wann mit seinem Kfz unterwegs war und zum anderen nur anhand des Frontfotos der Fahrer ermittelt werden kann, da in Unternehmen häufig kein Fahrtenbuch geführt wird. Dem Beschwerdeführer wurde geraten, die Verteilung von Briefsendungen von der Zentralen Bußgeldstelle unternehmensintern so zu regeln, dass diese ungeöffnet direkt dem Chef vorgelegt werden.

Obwohl in Massenverfahren wie der Geschwindigkeitsüberwachung im Regelfall die Abläufe stark standardisiert sind, gibt es immer wieder besondere Konstellationen, in denen eine konkrete Datenverarbeitung aus besonderen Gründen nicht zulässig ist (z. B. im Rechtsverkehr mit dem Ausland, Lichtbildabgleich bei unterschiedlichem Alter von Fahrer und Halter). Die regelmäßige Vorlage des Frontfotos an den Halter auch in Fällen, in denen von vornherein klar ist, dass Halter und Fahrer nicht identisch sind, ist verhältnismäßig, weil regelmäßig nur der Halter über Hinweise über den Fahrer verfügt.

## **8. Verfassungsschutz**

### **8.1 Kontrolle der Anti-Terror-Datei bei Polizei und Verfassungsschutz**

Nachdem die Anti-Terror-Datei vollständig in Betrieb gegangen und auch die Datensätze aus den Datensammlungen der Polizei und des Verfassungsschutzes in die Anti-Terror-Datei übernommen worden waren, hat der TLfD 2009 eine Kontrolle sowohl beim Landesamt für Verfassungsschutz als auch beim Landeskriminalamt durchgeführt. Dazu wurden zunächst die Protokolldaten zu den Zugriffen durch die jeweiligen Behörden beim Bundeskriminalamt für den Zeitraum eines halben Jahres angefordert. Die übersandten Protokolldaten waren als Verschlussache-vertraulich und zum Teil auch als Verschlussache-geheim eingestuft und lagen demzufolge ausschließlich in Papierform vor. Diese Einstufung wurde damit erklärt, dass es sich nicht nur um eine Vollprotokollierung handelt, sondern gleichzeitig um eine Inhaltsprotokollierung, bei der in den Protokolldaten auch alle in dem jeweiligen Datensatz enthaltenen Inhalte aufgezeichnet werden. Als Hauptproblem stellte sich dabei aber heraus, dass eine Auswertung nach bestimmten Kriterien nur manuell und wegen der Restriktionen der Einstufung als mindestens Verschlussache-vertraulich auch nicht automationsgestützt möglich war. Gerade bei großen Datenmengen ist daher eine Überprüfung, welcher Mitarbeiter welcher Stelle wann auf welche konkreten Inhalte der Anti-Terror-Datei zugegriffen hat in effektiver Weise nicht möglich. Dies wäre nur durch Auswerteprogramme beim BKA als Daten verarbeitende Stelle realisierbar, mit denen die Protokolldaten gruppiert oder nach bestimmten Kriterien durchsucht werden können. Damit erfüllen die derzeit vom BKA verfügbaren Protokolldaten noch nicht ausreichend die Anforderungen von § 9 Abs. 2 ATDG i. V. m. Nr. 3 der Anlage zu § 9 BDSG, da eine effektive Zugriffskontrolle ohne Auswerteprogramme nicht möglich ist. Das TLfV und das TLKA wurden aufgefordert, gegenüber dem BKA darauf hinzuwirken, dass eine entsprechende Software entwickelt wird.

Wegen der sowohl beim TLfV als auch beim TLKA bislang nur sehr kleinen Anzahl an eingespeicherten Datensätzen war der Umgang mit den Protokolldaten bei der aktuellen Kontrolle noch kein allzu großes Problem. Aus diesem Grund war es auch nicht notwendig, eine Stichprobe des Aktenrückhalts zu ziehen. Vielmehr konnten alle eingespei-

cherten Personen hinsichtlich der Rechtmäßigkeit ihrer Speicherung überprüft werden. Dabei haben sich keine Hinweise darauf ergeben, dass die materiellen Voraussetzungen für die Einspeicherung der Haupt- und Kontaktpersonen nicht vorlagen. Ein weiteres Problem hat sich jedoch nicht nur bei den fehlenden automatisierten Auswertungsmöglichkeiten der Protokolldaten ergeben, sondern auch bei der Qualität dieser Daten. So ist der Grund der protokollierten Abfrage nur sehr allgemein umschrieben. Zudem sieht das System keine speziellen Eingabefelder vor, in denen nähere Angaben zur konkreten Zweckbestimmung der Abfrage gemacht werden können, wie z. B. Aktenzeichen oder Bezeichnung von Verfahrenskomplexen. Um eine effektive Kontrolle der Zugriffe erst zu ermöglichen, hat der TLfD gegenüber den Stellen gefordert, gegenüber dem Bundeskriminalamt ebenfalls darauf hinzuwirken, ein zusätzliches Pflichtfeld in den Abfragemasken aufzunehmen, in dem der konkrete Abfrageanlass angegeben werden muss und dieses Feld auch in die Protokollierung nach § 9 Abs. 1 ATDG einzubeziehen. Im TLfV wurde bereits ein Feld in der Abfragemaske dafür verwendet, um die für den Grund der Abfrage erforderlichen Angaben einzutragen. Mit dem BKA wird innerhalb der zuständigen Gremien derzeit erörtert, ob dieses Feld für alle Teilnehmer verbindlich für diesen Zweck umgewidmet und zudem als Pflichtfeld ausgestaltet wird, so dass Zugriffe ohne diese Angaben gar nicht mehr bearbeitet werden.

Bei der noch geringen Zahl der Datensätze aus Thüringer Behörden konnten bislang keine übermäßigen oder unzulässigen Speicherungen dieser Behörden in der Anti-Terror-Datei festgestellt werden. Es bleibt aber die Forderung, dass die Möglichkeiten zur Protokollauswertung und damit die Kontrollbedingungen für den TLfD noch verbessert werden.

## **8.2 Auskunftsanspruch bei der Sicherheitsüberprüfung**

Bei der Sicherheitsüberprüfung durch das Landesamt für Verfassungsschutz werden die zu überprüfenden Personen, meist Beamte, die Zugang zu Verschlussachen haben und ggf. deren Ehepartner auf der Grundlage des Sicherheitsüberprüfungsgesetzes einer sehr genauen Prüfung unterzogen, ob sich in ihrer Person Sicherheitsrisiken ergeben, die den Umgang mit Verschlussachen einer bestimmten Geheimhaltungsstufe ausschließen. Soll beispielsweise der Beamte Zugang zu Verschlussachen der Stufe „Geheim“ oder „Streng Geheim“ erhalten,

so muss nach § 10 ThürSÜG eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen im Umfeld des Beamten durch das Landesamt für Verfassungsschutz durchgeführt werden. Dabei werden auch vom Betroffenen genannte Referenzpersonen oder weitere Auskunftspersonen nach § 12 Abs. 4 ThürSÜG befragt, um zu prüfen ob tatsächliche Anhaltspunkte vorliegen, die auf ein Sicherheitsrisiko schließen lassen. Im Rahmen einer Beschwerde überprüfte der TLfD die Sicherheitsüberprüfungsakte des Betroffenen und dabei auch die erfolgten Befragungen von Auskunftspersonen. Dabei haben sich keine Anhaltspunkte ergeben, dass Angaben erhoben und in den Akten gespeichert worden sind, die für die Sicherheitsüberprüfung nicht erforderlich waren.

Das Recht, sich an den TLfD wenden zu können, ist besonders bei der Sicherheitsüberprüfung wichtig, da es hier weitreichende Auskunftsverweigerungsrechte gibt und nur so eine unabhängige Kontrolle sichergestellt werden kann.

## **9. Finanzwesen**

### **9.1 Steuerbürokratieabbaugesetz und Bürgerentlastungsgesetz Krankenversicherung**

Der Entwurf des Anfang 2009 in Kraft getretenen Gesetzes zur Modernisierung und Entbürokratisierung des Steuerverfahrens sah in einem neu geschaffenen § 150 Abs. 7 Satz 1 Abgabenordnung (AO) vor, die zu übermittelnde Steuererklärung im Falle einer verpflichtenden elektronischen Datenübermittlung mit einer qualifizierten elektronischen Signatur - gem. Signaturgesetz (SignG) - zu versehen. Für bedenklich wurden dagegen seitens der Datenschutzbeauftragten des Bundes und der Länder die Neuregelungen der Nummer 6 und Nummer 7 des § 150 Abs. 7 Satz 2 AO gehalten. Nach Nummer 6 kann das Bundesministerium der Finanzen (BMF) durch Rechtsverordnung mit Zustimmung des Bundesrates im Benehmen mit dem BMI anstelle der qualifizierten elektronischen Signatur ein "anderes sicheres Verfahren" zulassen. Darüber hinaus soll das BMF gem. Nummer 7 auch Ausnahmen von der Pflicht zur Verwendung einer qualifizierten elektronischen Signatur oder eines anderen sicheren Verfahrens zulassen dürfen. Laut Gesetzesbegründung bezweckt die Gesetzesänderung, die Datenübermittlung mittels des elektronischen Personalausweises zu ermöglichen. In Ihrer Entschliebung vom November 2008 „Elektronische Steuererklärung sicher und datenschutzgerecht gestalten“ hat die 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder kritisch zu dem Gesetzentwurf Stellung genommen. Insbesondere wurde betont, dass Steuerpflichtige die Möglichkeit haben müssen, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern. Das Steuerbürokratieabbaugesetz ist jedoch Anfang 2009 mit den o. g. Regelungen in Kraft getreten.

Die elektronische Steuererklärung zum Gegenstand hatten auch zwei Änderungsanträge des Bundesrates (BR-Drs.168/09(B)) vom 3. April 2009 zu einem Entwurf eines Gesetzes zur verbesserten Berücksichtigung von Vorsorgeaufwendungen (Bürgerentlastungsgesetz Krankenversicherung). Danach sollte durch Änderungen in § 87a Abs. 6 AO, § 150 Abs. 6 und 7 AO und Art. 97 § 10a Abs. 1 des Einführungsgesetzes zur AO die bisher geforderte qualifizierte elektronische Signatur sowohl in den Fällen der freiwilligen elektronischen Steuerklärungen

als auch in Fällen, in denen der Steuerpflichtige zu einer Übermittlung nach amtlich vorgeschriebenem Datensatz verpflichtet ist, durch ein anderes sicheres Verfahren – das über das ElsterOnline-Portal genutzte Authentifizierungsverfahren – ersetzt werden. Zugleich sollte die gesetzliche Evaluierungsfrist von Ende 2011 aufgehoben werden. Dies wurde damit begründet, dass das Verfahren Elster bereits als sicher evaluiert worden sei. Dem gegenüber hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in Abstimmung mit den Landesbeauftragten für den Datenschutz gegenüber der Bundesregierung festgestellt, dass einzig die Zertifizierung der Elster-Clearingstellen als ein Beitrag zur Evaluation – allerdings nur dieser einen Komponente - des komplexen IT- Verfahrens angesehen werden konnte. Eine abschließende Evaluation sei hingegen nicht erfolgt. Um die Möglichkeit der elektronischen Kommunikation des Bürgers und der Finanzverwaltung mittels des hierfür geeigneten Verfahrens der qualifizierten elektronischen Signatur nicht einzuschränken, wurde gefordert, auf die vorgesehene Gesetzesänderung zu verzichten. Bedenken begegnete auch der Vorschlag des Bundesrates, wonach für eine Finanzbehörde eines Landes, die als zentrale Stelle - z. B. eine Elster-Clearingstelle- für die Erhebung, Verarbeitung oder Nutzung von Daten im Auftrag anderer Länder oder des Bundes zuständig ist, künftig ausschließlich die datenschutzrechtlichen Vorschriften des Landes gelten sollen, dem die zentrale Stelle angehört. Nach § 2 Abs. 1 ThürDSG ist das ThürDSG auf die Verarbeitung und Nutzung personenbezogener Daten durch die öffentlichen Stellen des Landes – auch der Finanzbehörden – anzuwenden. Daher war die vorgesehene Neuregelung wegen ihrer Unvereinbarkeit mit dem Landesdatenschutzrecht abzulehnen. Im Juni 2009 ist das Bürgerentlastungsgesetz Krankenversicherung verabschiedet worden, ohne dass die datenschutzrechtlich bedenklichen Änderungsanträge des Bundesrates berücksichtigt wurden.

Neben der qualifizierten elektronischen Signatur existiert derzeit kein anderes sicheres Verfahren, das die Authentizität und Integrität eines elektronisch übermittelten Dokumentes sicherstellt. Steuerpflichtige müssen die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das Verfahren der qualifizierten elektronischen Signatur abzusichern.

## 9.2 Haushaltsmanagementsystem (HAMASYS)

Parallel zur Einführung von HAMASYS in weiteren Dienststellen offenbarten sich neue datenschutzrechtliche Probleme. In mehreren HAMASYS nutzenden Behörden war im April 2009 festzustellen, dass personenbezogene Daten von Zahlungsempfängern zu konkreten Zahlungen außerhalb der Zuständigkeit der jeweiligen abrufenden Stelle und damit unberechtigter Weise aufgerufen werden konnten. Auf Grund dessen hatte der TLfD empfohlen, die vorgesehene Einbeziehung weiterer Behörden in das Verfahren HAMASYS bis zur Erledigung der vollständigen Fehlerkorrektur auszusetzen. Nachdem daraufhin das Programmsystem überarbeitet worden war, stellte sich heraus, dass zwar die o. g. Fehlfunktion für die neu erstellten, nicht jedoch für die bis dahin gespeicherten Daten behoben war. Wie das TFM mitteilte, wird nun seit November 2009 eine weitere Programmänderung durch den Softwarehersteller geprüft. Der TLfD sieht bis zu einer endgültigen Klärung des Problems zumindest den Anschluss weiterer Behörden an HAMASYS als bedenklich an. Wie das TFM zudem mitteilte, haben die Partner, d. h. Lieferanten und Kunden, die Möglichkeit, einer Speicherung ihrer Stammdaten (Namen, Adressen, Bankverbindungen und Steuernummern) im allgemeinen Partnerbestand zu widersprechen, wodurch diese Daten ausschließlich für die Buchung eines einzelnen Zahlungsvorgangs verwendbar sind und nicht den zugriffsberechtigten Mitarbeitern aller beteiligten Dienststellen zur Verfügung stehen. Auf Grund von Anfragen an den TLfD wurde das TFM gebeten mitzuteilen, ob und wenn ja in welcher Form die HAMASYS nutzenden Stellen ihre Partner auf das Widerspruchsrecht zur Datenspeicherung im allgemeinen Partnerbestand hingewiesen haben, welche Stellen diese Verfahrensweise anwenden bzw. bereits angewandt haben. Zugleich wurde angeregt zu prüfen, ob ggf. künftig eine Speicherung der Partnerdaten von einer Einwilligung aller „Partner“ gem. § 4 ThürDSG abhängig gemacht werden sollte, sofern keine technische Lösung dieser Problematik möglich sei. Auch ist bisher ungeklärt, welche Rechte und Pflichten das für die zentrale Pflege zuständige Kompetenzzentrum konkret besitzt und ob es neben den Stammdaten der Partnerdatenbank auch alle Buchungssätze einsehen kann. Auf Grund dieser derzeit offenen Fragen wird die Anwendung von HAMASYS weiterhin kritisch gesehen.

Mittels geeigneter technisch-organisatorischer Maßnahmen gem. § 9 ThürDSG ist zu gewährleisten, dass eine Kenntnisnahme personenbezogener Daten durch Unbefugte ausgeschlossen wird.

### 9.3 Auskunftsanspruch im Steuerverfahren

Mit Beschluss des Bundesverfassungsgerichts vom 10.03.2008 (1 BvR 2388/03), wurde fallbezogen zwar ein Auskunftsanspruch im Steuerverfahren wegen § 19 Abs. 4 BDSG abgelehnt, grundsätzlich aber ein solcher Auskunftsanspruch auf § 19 BDSG gestützt. Das BMF hat Ende 2008 eine Verwaltungsanweisung zur Erteilung von Auskünften über Daten, die zu einer Person im Besteuerungsverfahren gespeichert sind, erlassen (Bundessteuerblatt I 2009 S.6). Darin wird entgegen § 19 BDSG der Auskunftsanspruch im Besteuerungsverfahren zusätzlich von der Darlegung eines berechtigten Interesses abhängig gemacht, welches zu Lasten des Betroffenen in der Praxis bisweilen verneint wird. Der TLfD vertritt die Auffassung, der verfassungsrechtlich garantierte Auskunftsanspruch darf nur aufgrund eines Gesetzes eingeschränkt werden. Diese Qualität besitze die Verwaltungsanweisung nicht; zudem verstoße die Verwaltungsanweisung gegen § 19 BDSG, indem sie einen gesetzlich nicht vorgesehenen Ausnahmetatbestand etabliere. Die 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte in einer Entschließung die Rücknahme der Verwaltungsanweisung. Zwischenzeitlich hat der Bundesbeauftragte für Datenschutz und Informationsfreiheit das BMF wegen der fortgesetzten Anwendung der Verwaltungsanweisung beanstandet. Der TLfD fordert weiterhin, dass eine Auskunftserteilung nicht von der Darlegung eines berechtigten Interesses abhängig gemacht werden darf, wie dies die Verwaltungsanweisung jedoch vorschreibt.

Eine Auskunftserteilung über Daten, die zu einer Person im Besteuerungsverfahren gespeichert sind, darf nicht durch eine Verwaltungsanweisung von der Darlegung eines berechtigten Interesses abhängig gemacht werden.

### 9.4 Fragebogen Grunderwerb

Ein Grundstückskäufer ist nach einem Grunderwerb vom Finanzamt Nordhausen zum Ausfüllen eines Fragebogens aufgefordert worden. Die dem Betroffenen übersandten Unterlagen enthielten keine Hinweise darauf, worin die Erforderlichkeit für die Erhebung der einzelnen Daten bestand. Daher wurde die Thüringer Landesfinanzdirektion (LFD) um Stellungnahme zur Rechtsgrundlage der Datenerhebung und zur Erforderlichkeit, insbesondere der Fragen nach den Finanzierungsquellen, den

weiteren Einkünften - auch des Ehepartners - gebeten. Zudem sollte mitgeteilt werden, in welchen Fällen dieser Fragebogen angewandt wird. Die LfD gab an, der Fragebogen sei dann anzuwenden, wenn bisher steuerlich nicht geführte Personen Grundstücke erwerben, da in diesen Fällen keine Angaben vorliegen, um eine Steuererklärungspflicht zu prüfen. Daneben werde der Fragebogen verwendet, wenn sich aus einem Abgleich der Angaben zum Grunderwerb mit einer vorliegenden Steuererklärung neue Fragestellungen, insbesondere zur Finanzierung des Erwerbs und einer etwaigen weiteren Verwertung des Grundstücks ergeben. Das Vorgehen der Finanzverwaltung beruht auf § 85 AO, wonach die Steuern nach Maßgabe der Gesetze gleichmäßig festzusetzen und zu erheben sind. Hierzu ermittelt sie den Sachverhalt von Amts wegen, d. h. sie ist nicht an das Vorbringen und Beweisanträge der Beteiligten gebunden und hat alle für den Einzelfall bedeutsamen, auch für die Beteiligten günstigen Umstände zu berücksichtigen (§ 88 AO). Nach § 93 AO sind der Finanzbehörde die besteuierungsrelevanten Sachverhalte mitzuteilen, wobei verlangt werden kann, die Auskünfte schriftlich zu erteilen. Da jedoch die obigen Erhebungszwecke nicht aus den Unterlagen ersichtlich waren, hat der TLfD darum gebeten, den Fragebogen und das zugehörige Anschreiben entsprechend zu überarbeiten. Mittlerweile wurde eine nachvollziehbare Begründung für die geforderte Datenerhebung in die Unterlagen aufgenommen und damit dem datenschutzrechtlichen Transparenzgebot Rechnung getragen.

Bei der Gestaltung von Formularen ist darauf zu achten, dass der Betroffene nachvollziehen kann, zu welchen Zwecken die Datenerhebung erfolgt (Transparenzgebot). Die Datenerhebung darf den für die Aufgabenerfüllung erforderlichen Umfang nicht überschreiten.

### **9.5 Unzulässige Offenbarung von Steuerdaten des Finanzamtes Mühlhausen**

Ein Beschwerdeführer teilte mit, dass er in seinem Hausbriefkasten eine handschriftliche Notiz vorgefunden habe, die von einem ihm bekannten Mitarbeiter des Finanzamtes stammen sollte. In der Notiz wurde Aufklärung zu Inhalten seiner Steuererklärung gefordert. Nach Auffassung des Betroffenen bezog sich das Schreiben auf die Entwicklung seiner Kapitalerträge, wobei er vermutete, dass die zugrunde liegenden Kenntnisse mittels unzulässiger Nutzung dienstlicher Möglichkeiten erlangt worden seien. Wegen des Verdachts, dass Daten, die dem Steuergeheimnis ge-

mäß § 30 Abgabenordnung (AO) unterliegen, unbefugt erlangt und verwendet worden sind, wurde das Finanzamt um Überprüfung der Angelegenheit gebeten. Hierbei wurde festgestellt, dass der Verdächtige archivierte Steuererklärungsdaten des Betroffenen in einem privaten Schreiben nutzte und damit gegen seine Verpflichtung zur Wahrung des Steuergeheimnisses gem. § 30 AO verstoßen hat. Nachdem die Angelegenheit im Finanzamt ausgewertet worden war, sind allen Mitarbeitern Hinweise auf die Verpflichtung zur Wahrung des Steuergeheimnisses zur Beachtung datenschutzrechtlicher Bestimmungen zur Verfügung gestellt worden. Wie das Finanzamt mitteilte, hatte die Angelegenheit für den betreffenden Mitarbeiter des Finanzamtes neben arbeitsrechtlichen Konsequenzen auch ein strafrechtliches Verfahren zur Folge.

Insbesondere bei Daten, die dem Steuergeheimnis unterliegen, stellt eine private Nutzung dieser Daten einen Verstoß gegen § 30 AO dar.

## **9.6 Datenlöschung in gepfändeter IuK-Technik**

Ein Thüringer Finanzamt hat nach Mitteilung eines Beschwerdeführers einen Laptop mit personenbezogenen Daten seiner Mitarbeiter und Geschäftspartner beschlagnahmt und nachfolgend versteigert. Wegen der Möglichkeit, dass diese Daten in Folge der Versteigerung gegenüber unberechtigten Dritten offenbart sein könnten, wurde die LFD gebeten, nachzuweisen, dass dem Steuerschuldner vor der Verwertung angeboten wurde, den Datenbestand zu kopieren und zu löschen. Wie festzustellen war, wurde dem Beschwerdeführer lediglich mündlich mitgeteilt, dass er den Datenbestand kopieren und löschen dürfe. Da diese Möglichkeit ungenutzt blieb, ist die Festplatte mittels Festplatten-Löschprogramm VS-Clean V2.1 durch das Finanzamt gelöscht worden, was durch die Vorlage eines Löschprotokolls nachgewiesen wurde. Nachfolgend wurde der Laptop versteigert. Der Verzicht auf eine schriftliche Information des Vollstreckungsschuldners wurde als ein datenschutzrechtlicher Verstoß bewertet, zumal dieses Vorgehen einer Dienstanweisung der Finanzverwaltung widersprach, wonach dem Schuldner vor der Verwertung unter Fristsetzung schriftlich anzubieten ist, die Daten des gepfändeten Computers zu kopieren und zu löschen. Um derartige Datenschutzverletzungen künftig zu vermeiden, ist der Vordruck zur Benachrichtigung im Pfändungsverfahren entsprechend der o. g. Dienstanweisung ergänzt worden.

Vor diesem Hintergrund wurde die Auffassung des TLfD zur Datenlöschung im Zusammenhang mit dem Schutzbedarf der Daten gegenüber der Thüringer Finanzverwaltung wie folgt dargelegt: Die Software VS-Clean V2.1 ist als sehr sicher bei der Löschung magnetischer Datenträger einzustufen, weshalb keine Einwände gegen deren Einsatz bei Daten eines geringen Schutzbedarfs bestehen. Gleichwohl wird empfohlen, bei Daten eines hohen bzw. unbekanntem Schutzbedarfs von einer Weitergabe des Datenträgers abzusehen. Diese Beurteilung stützt sich darauf, dass Festplatten Daten enthalten können, die auch nach einer Löschung rekonstruierbar sind. Dies betrifft insbesondere die folgenden Fälle: Bei Computern mit älteren BIOS-Versionen kann möglicherweise nicht auf die Daten jenseits der 504 MB oder 8.4 GB-Grenze einer Platte löschend zugegriffen werden. Einige IDE/ATA-Platten gestatten es, Bereiche der Festplatte einzuschränken, auf die das Betriebssystem und andere Programme Zugriff haben ("Host Protected Area"), so dass Daten des geschützten Bereichs nicht gelöscht werden können. Moderne, sehr dicht schreibende Platten schreiben Daten von als fehlerhaft erkannten Sektoren in eigens dafür eingerichtete Reservesektoren. Daten fehlerhafter Sektoren werden von den Löschroutinen nicht überschrieben. Wollte man auch diese löschen, müsste die Magnetscheibe der Festplatte entnommen und mit einer Spezialhardware bearbeitet werden. RAID-Systeme müssen vorher deaktiviert werden und die Platten einzeln der Löschroutine unterzogen werden. Von größerer Bedeutung sind die Möglichkeiten, aus Datenspuren Daten zu rekonstruieren. Hierfür lassen sich z. B. die Positionierungstoleranzen der Schreib- und Leseköpfe ausnutzen. Festplatten sind so konstruiert, dass geringfügige Positionsfehler der Schreib- und Leseköpfe in Bezug auf die Spur, in der die Daten gespeichert werden, sich im Laufe der Lebensdauer der Festplatte verändern. Diese Toleranz kann dazu führen, dass Daten, die vor einer Positionsverschiebung des Kopfes auf die Platte geschrieben wurden, von der Löschroutine nicht mehr erfasst werden. Ähnlich aussichtsreich kann eine Analyse des Pufferbereichs zwischen den Spuren sein. Dieser Pufferbereich zwischen den Spuren dient dazu, magnetische Interferenzen zwischen den Mustern der Spuren zu vermeiden. Diese und ähnliche Gegebenheiten dürften Sicherheitsverantwortliche in Hochrisikobereichen bewogen haben, Festplatten mit "streng geheimen" Daten nicht per Software zu löschen, sondern sie gebrauchsunfähig physisch zu vernichten. Es ist natürlich nicht möglich, eine mit VS-Clean gelöschte Festplatte an einen anderen Computer anzuschließen und dadurch diese Effekte auf der Platte auszunutzen. Es ist jedoch nicht

auszuschließen, dass eine Firma mit entsprechender Technik und Know-how von einem Erwerber einer mittels VS-Clean gelöschten Festplatte mit deren Rekonstruktion beauftragt wird, wenn die dadurch gewonnenen Daten ein Vielfaches des Aufwandes einbringen (Technologien, Patente, sensible personenbezogene Daten usw.). Der Gesetzgeber verlangt von den Verantwortlichen sicherzustellen, dass die ihnen anvertrauten Daten der Bürger (einschließlich Klienten oder Patienten) nicht zum Nachteil der Betroffenen missbraucht werden können. Das Verhältnis eines möglichen Schadens durch die Rekonstruktion von hochsensiblen personenbezogenen Daten, Technologien, Patentanmeldungen usw. steht in keinem Verhältnis zum möglichen Versteigerungserlös.

Eine Weitergabe von Datenträgern mit Daten eines hohen oder unbekanntem Schutzbedarfs ist auf Grund moderner Datenrekonstruktionsverfahren zu vermeiden.

Bei Daten eines geringen Schutzbedarfs ist eine Löschung mittels einer zertifizierten Software, bspw. VS-Clean V2.1, als datenschutzrechtlich unbedenklich einzuschätzen.

### **9.7 Verwenden von Kundendaten der Sparkasse Mittelthüringen zu Werbezwecken**

Bereits im 7. TB (9.4) hatte der TLfD zu Sparkassen berichtet, dass eine Nutzung von Kundendaten für Zwecke der Werbung und Beratung nur dann zulässig ist, wenn der Kunde hierin schriftlich einwilligt, wobei die Einwilligung nicht an eine Bedingung für eine Vergünstigung gekoppelt sein darf. Im Jahre 2009 beschwerte sich ein Betroffener darüber, dass eine Werbesendung der Sparkasse Mittelthüringen zugestellt wurde. Zuvor hatte der Petent mit dieser Sparkasse eine Vereinbarung zu einem Online-Konto abgeschlossen, dabei jedoch nicht in eine Nutzung seiner Kundendaten für Werbezwecke eingewilligt. Wie die Sparkasse auf Anfrage des TLfD mitteilte, sei (erst) nach Kenntnis der Beschwerde ein Werbeverbot im EDV-System hinterlegt worden. Die Sparkasse sicherte zu, die von den Kunden erbetenen Werbeverbote zu beachten und Qualitätssicherungsmaßnahmen durchzuführen.

Kundendaten dürfen nur dann für Zwecke der Werbung und Beratung genutzt werden, wenn der Kunde hierin schriftlich einwilligt, wobei die Einwilligung nicht an eine Vergünstigung gekoppelt sein darf.

## 10. Justiz

### 10.1 Einsatz von Videoüberwachung im Strafvollzug

Die Beschwerde eines Bediensteten der Jugendstrafvollzugsanstalt Ichtershausen zeigte, dass die Ende 2007 mit § 67 Thüringer Jugendstrafvollzugsgesetz (ThürJStVollzG) erfolgte Regelung der Videoüberwachung sich als notwendige Handlungsanleitung erwies. Dieser wurde mit einer Videoaufzeichnung konfrontiert, nach der er in einer Nachtschicht nicht die vorgeschriebenen Kontrollgänge durchgeführt haben soll. Er vermutete eine unzulässige Dauerüberwachung und wandte sich an den Petitionsausschuss und die Strafvollzugskommission, die den TLfD informierte. Bei einer auswärtigen Sitzung der Strafvollzugskommission stellte sich heraus, dass der Bedienstete kein Opfer einer planmäßigen Mitarbeiterüberwachung war. Vielmehr wurden die Videoaufnahmen im Jahr 2006 routinemäßig über einen längeren Zeitraum in dieser Nacht angefertigt, um zu überprüfen, ob die Ausleuchtung des Bereichs, in dem normalerweise die Videoüberwachung nur über einen Bewegungsmelder aktiviert wird, noch ausreichend ist. Bei Gelegenheit der Auswertung des Videos zu diesem Zweck wurden die nicht durchgeführten Kontrollgänge des Bediensteten festgestellt und disziplinarische Maßnahmen gegen diesen eingeleitet. Da somit keine zielgerichtete, verdeckte Überwachung von Mitarbeitern erfolgte und diese über die auch zu deren eigener Sicherheit durchgeführten Videoüberwachung der Kontrollgänge informiert waren, war diese Datenerhebung und -verwendung als zulässig anzusehen, auch wenn dies noch vor Inkrafttreten des § 67 ThürJStVollzG erfolgte. Bei einer späteren Kontrolle in der Jugendstrafvollzugsanstalt stellte sich aber heraus, dass die technischen und organisatorischen Maßnahmen zur Durchführung der Videoüberwachung zu Sicherheitszwecken lückenhaft waren. So fehlten konkrete Festlegungen zu Löschrufen, unter welchen Voraussetzungen ein Zugriff auf die Aufzeichnungen möglich ist und wer die Aufzeichnungen unter welchen Voraussetzungen auswerten darf. Dies wurde im Nachgang durch die Anstalt nachgebessert.

Durch die spezialgesetzliche Regelung des § 67 ThürJStVollzG zur Videoüberwachung werden die Grenzen für einen notwendigen Einsatz dieser Technik in Jugendstrafvollzugsanstalten aus Sicherheitsgründen normenklar aufgezeigt.

## **10.2 Abfrage von Telekommunikations-Verkehrsdaten einschränken**

Unter dieser Überschrift hatten die Datenschutzbeauftragten des Bundes und der Länder in einer EntschlieÙung (Anlage 15) im November 2008 den Gesetzgeber aufgefordert, die Konsequenzen aus einem Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg zur Nutzung von Telekommunikations-Verkehrsdaten für Zwecke der Strafverfolgung zu ziehen. Dieses vom Bundesministerium der Justiz in Auftrag gegebene Gutachten war zum Schluss gekommen, dass die Verkehrsdatenabfragen erheblich und kontinuierlich zugenommen haben, dabei jedoch gravierende Defizite bei der Begründung der jeweiligen Maßnahmen sowie bei den Benachrichtigungs-, Löschungs- und Dokumentationspflichten bestehen. Zudem wurde der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung in Frage gestellt, weil bereits bei 98 % der Abfragen die frühere Höchstspeicherdauer von 3 Monaten ausreichend war. Gerade letztere Erkenntnis wäre für das Gesetzgebungsverfahren zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung äußerst hilfreich gewesen, wurde doch das Gutachten erst nach dessen Abschluss veröffentlicht. Bislang hat der Bundesgesetzgeber diese Forderung nicht aufgegriffen. Allerdings ist der Handlungsdruck durch die Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung (4.1) nicht geringer geworden. Nach dem Urteil stehen den Strafverfolgungsbehörden bis zur Schaffung eines neuen Gesetzes zunächst die Daten aus der Vorratsdatenspeicherung nicht mehr zur Verfügung. Für eine künftige Regelung hat das Bundesverfassungsgericht jedoch u. a. eine der Forderungen in der EntschlieÙung bestätigt und für den Zugriff auf die Verkehrsdaten eine Anhebung der Straftatenschwelle gefordert. Danach ist künftig für einen Abruf zumindest der durch bestimmte Tatsachen begründete Verdacht einer auch im Einzelfall schwerwiegenden Straftat notwendig.

Nicht nur durch das Rechtsgutachten, sondern vor allem aufgrund des Urteils des Bundesverfassungsgerichts, muss die Abfrage von Telekommunikations-Verkehrsdaten auf ein verhältnismäßiges Maß eingeschränkt und mit Verfahrenssicherungen versehen werden.

### **10.3 Justizzahlstellenverfahren speichert längst erledigte Forderungen**

Aufgrund einer Beschwerde wurde der TLfD auf einen Mangel in dem von der Justizzahlstelle in Gera betriebenen automatisierten Kosteneinziehungsverfahren aufmerksam. Der Beschwerdeführer sah sich bei einer Vollstreckungsankündigung durch den Gerichtsvollzieher einer ganzen Liste von Forderungen gegenüber, die in den letzten 12 Jahren angefallen, jedoch zum größten Teil bereits beglichen waren. An erster Stelle befand sich eine Forderung aus dem Jahr 1996, die ebenfalls längst bezahlt worden war. Bei einer aktualisierten Aufstellung ein halbes Jahr später tauchte bei dieser Forderung plötzlich ein erhöhter Betrag an Nebenkosten auf sowie eine daraus resultierende offene Restforderung. Der Beschwerdeführer konnte sich nicht erklären, weshalb nun plötzlich eine seit vielen Jahren beglichene Forderung wieder offen sein sollte. Durch die falsche Zuordnung war es ihm auch nicht möglich nachzuvollziehen, um welche Forderung es sich handelte. Eine Nachfrage bei der Landesfinanzdirektion angesiedelten Justizzahlstelle ergab Erstaunliches. Das eingesetzte System sei in zweierlei Hinsicht Mängel behaftet. Eine Löschung der ersten eingetragenen Forderung nach der gesetzlichen Frist von 10 Jahren sei systembedingt nicht möglich, weil zu diesen Datensätzen ein „führendes Kassenzeichen“ vergeben werde und zur ordnungsgemäßen Aufgabenerledigung erforderlich sei, da andernfalls z. B. Verbindungen zwischen Forderungen und Erstattungen nicht mehr möglich seien. Zudem sehe das System keine gesonderte Möglichkeit vor, Nebenkosten, die durch die Vollstreckung verursacht wurden, gesondert zu verbuchen. Deshalb hat man kurzerhand diese Nebenkosten, ohne dies für den Betroffenen zu erläutern, immer wieder der bereits beglichene ersten Forderung (im vorliegenden Fall aus dem Jahr 1996!) zugeordnet.

Das ist aus mehreren Gründen ein unhaltbarer Zustand. Zunächst sind die gesetzlichen Löschfristen umzusetzen und können nicht mit der willkürlichen Begründung verlängert werden, dass ein automatisiertes Verfahren sonst nicht mehr ordentlich funktionieren würde. Würde man sich dieser Argumentation anschließen, dann könnte man bewusst schlecht programmierte Software anschaffen, um gesetzliche Löschfristen zu umgehen. Zudem sind nach § 14 ThürDSG personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Daraus ergibt sich aber auch, dass die Verwaltung nicht bewusst unrichtige Daten in automati-

sierten Verfahren erzeugen darf. Aber als solches muss die erneute Zu-  
speicherung von Nebenkosten zu Aktenzeichen verstanden werden, die  
längst beglichen worden sind, ohne dies zu erläutern. Die Justizzahlstel-  
le hat allerdings erst nach dem Eingreifen des TLFID eingesehen, dass  
hier die Technik dem Datenschutzrecht angepasst werden muss und  
nicht umgekehrt. So wurde die Absicht geäußert, dass ein neues Kosten-  
einziehungsverfahren angeschafft werden soll, das die beschriebenen  
Mängel nicht mehr hat. Als erste Maßnahmen wurden in einem Löschauf-  
lauf die alten Forderungen entfernt. Allerdings nicht die Datensätze zum  
führenden Kassenzeichen, da ansonsten ein Zugriff auf die Personen-  
konten nicht mehr möglich wäre. Es wurde veranlasst, dass der Ge-  
richtsvollzieher und auch der Schuldner in der Übersicht nicht mehr die  
beglichenen Forderungen, die Angabe der Gläubiger sowie die alten  
Aktensätze vorgelegt bekommen. Vielmehr wird nur noch das füh-  
rende Kassenzeichen angegeben. Weil nach wie vor kein gesonderter  
Datensatz für die Nebenkosten angelegt werden kann, sollen diese künf-  
tig nicht mehr beim führenden Kassenzeichen, sondern bei einer der  
auslösenden Forderungen verbucht und mit einer erklärenden Fußnote  
versehen werden. Diese Maßnahmen können allerdings nur übergangs-  
weise geduldet werden. Von der zuständigen Landesfinanzdirektion war  
zu hören, dass sich die angestrebte Einführung des neuen Verfahrens aus  
haushaltsrechtlichen Gründen verzögern könnte.

Wenn der Staat aufgrund seines Gewaltmonopols gegen den Bürger  
Forderungen zwangsweise vollstrecken kann, dann müsste es eine  
Selbstverständlichkeit sein, dass ein Verfahren verwendet wird, in dem  
dieser einfach und transparent nachvollziehen kann, welche Summe in  
welchem Verfahren von ihm verlangt wird. Das ist im derzeitigen Ver-  
fahren nicht gewährleistet. Hier ist dringend eine Technik einzusetzen,  
die den rechtlichen Anforderungen entspricht.

## **11. Gesundheits- und Sozialdatenschutz**

### **11.1 Arbeitshilfe "Außendienst" der Bundesagentur für Arbeit**

§ 7 Abs. 3a SGB II stellt die gesetzliche Vermutung an, dass Partner, die länger als ein Jahr oder mit einem Kind zusammenleben oder sich Vermögensverfügungsbefugnisse eingeräumt haben, als sog. Bedarfsgemeinschaft zu qualifizieren sind (7. TB, 11.1). Folge ist, dass Partner einer solchen Bedarfsgemeinschaft füreinander einzustehen haben, insbesondere in finanzieller Hinsicht. Diese Regelung stellt beispielsweise bloße Wohngemeinschaften vor große Probleme, diese gesetzliche Vermutung zu widerlegen, also zu beweisen, dass eine Bedarfsgemeinschaft nicht besteht. In der Praxis werden insbesondere nach der Verweigerung einer Wohnungsbesichtigung die Leistungen mit der zuvor meist angebotenen Begründung eingeschränkt bzw. eingestellt, der Sachverhalt könne nicht weiter aufgeklärt werden. Dabei erfolgt die Leistungsbeschränkung gerade auch in denjenigen Fällen, in denen die Voraussetzungen für die gesetzliche Vermutung des Bestehens einer Bedarfs-/Einstehens-/Verantwortungsgemeinschaft im Sinne von § 7 Abs. 3a SGB II noch nicht vorliegen, also insbesondere im zeitlichen Vorfeld der gesetzlichen Fiktion. Die Arbeitshilfe „Außendienst“ der Bundesagentur für Arbeit, die auch von den ARGEn als Handlungsgrundlage herangezogen wird, führt hierzu unter 2.1, Absatz 8 aus: „Wegen der Verweigerung des Zutritts zur Wohnung als solcher ist es nicht möglich, einen Leistungsanspruch nach § 66 SGB I zu versagen, da für Hausbesuche keine Mitwirkungspflicht im Rahmen des § 60 SGB I besteht. Es ist allenfalls möglich, die beantragte Leistung abzulehnen, wenn der Sachverhalt nicht anderweitig aufgeklärt werden kann.“ Während in älteren Arbeitshilfen noch von einer zwingenden Leistungseinstellung nach Ausschöpfung der Möglichkeiten der Sachverhaltsaufklärung die Rede war, wird nunmehr zu Recht auf die fehlende Mitwirkungspflicht des Betroffenen bei Hausbesuchen hingewiesen. Allerdings wird weiterhin betont, es sei möglich, die Leistungen einzustellen, wenn der Sachverhalt nicht anderweitig aufgeklärt werden könne. Diese Sichtweise fußt auf dem Gedankengang, dass der Antragsteller das Vorliegen der anspruchsbegründenden Tatsachen (Anspruchsvoraussetzungen) nachzuweisen hat. Gelingt ihm dieses nicht, geht das zu seinen Lasten. Die beantragte Leistung wird also verweigert. Vor dem Hintergrund neuerer Rechtsprechung erscheint diese Auffassung aus folgenden Erwägungen nicht mehr differenziert genug:

- Existenzsichernde Leistungen dürfen nicht auf Grund bloßer Mutmaßungen verweigert werden (BVerfG vom 12. Mai 2005 1 BvR 569/05).
- Eine Rechtsvorschrift, die dem Leistungsempfänger auferlegt, eine Wohnungsbesichtigung zu dulden, existiert nicht, auch nicht in den §§ 20, 21 SGB X (SG Lübeck vom 14. Februar 2008; S 27 AS 106/ 08 ER).
- Das Vorliegen einer Einstehensgemeinschaft (Bedarfsgemeinschaft) muss im Vorfeld der gesetzlichen Fiktion des § 7 Abs. 3a SGB II als anspruchsvernichtende Tatsache bewiesen sein. Hierfür trägt die Behörde die objektive Beweislast (LSG Baden-Württemberg vom 12. Januar 2006, L 7 AS 5532/05 ER-B; LSG Sachsen-Anhalt, a. a. O.). Das SG Lübeck (a. a. O.) fügt erläuternd hinzu, der Gesetzesbegründung zu § 7 Abs. 3a SGB II (BT-Drs. 16/1410, Seite 40, 48 f.) sei zu entnehmen, dass erst mit Vorliegen der mit dieser Norm eingeführten Vermutungstatbestände eine Beweislastumkehr zu Lasten des Leistungsempfängers eintreten soll. Daher trage vor Eintritt dieser gesetzlichen Fiktion (Beweislastumkehr) nicht der Antragsteller die Beweislast für das Vorliegen der anspruchsbegründenden Tatsachen, sondern der Leistungsträger für das Vorliegen der anspruchsvernichtenden Tatsachen.
- Eine Darlegungslast trifft den Leistungsempfänger erst dann, wenn gewichtige Tatsachen für eine Verantwortungsgemeinschaft vorliegen. Erst dann hat der Leistungsempfänger plausible Gründe darzulegen, die das Zusammenwohnen lediglich als reine Zweck- /Wohngemeinschaft erkennen lassen (SG Lübeck, a. a. O.). Als solche gewichtigen Tatsachen reichen z. B. weder das Zusammenleben unter einer Meldeanschrift noch das gemeinsame Nutzen von Teilen der Wohnungseinrichtung allein aus, weil dies auch für eine Wohngemeinschaft typisch ist. Auch geschlechtliche Beziehungen sind nicht maßgeblich, da die Intimsphäre zur Feststellung einer Verantwortungsgemeinschaft gar nicht ausgeforscht werden darf (LSG Sachsen-Anhalt, a. a. O.).

Mithin darf die Leistungsgewährung vor Eintreten der gesetzlichen Fiktion des § 7 Abs. 3a SGB II nicht wegen Unaufklärbarkeit des Sachverhalts quasi automatisch eingestellt werden.

Die Arbeitshilfe „Außendienst“ sollte auch als Arbeitsgrundlage der ARGEn die differenzierende Rechtsprechung zum zeitlichen Vorfeld der gesetzlichen Fiktion des § 7 Abs. 3a SGB II aufnehmen, um damit sowohl Außendienstmitarbeitern als auch Sachbearbeitern eine Grundlage zur rechtssicheren Behandlung von Leistungsanträgen an die Hand zu geben

## 11.2 DDR-Heimkinder

Der „Runde Tisch Heimerziehung in den 50er und 60er Jahren“ verfolgt das Ziel, bei der Heimerziehung in Deutschland begangenes Unrecht umfassend aufzuarbeiten. Dabei ist es zentrales Anliegen der ehemaligen Heimkinder, Einsicht in die sie betreffenden Akten nehmen zu können. Mit diesem Anliegen setzt sich auch der Arbeitskreis Gesundheit und Soziales der Datenschutzbeauftragten des Bundes und der Länder auseinander. Ein Auskunftsanspruch der Betroffenen ist in § 83 SBG X spezialgesetzlich geregelt. Nach dieser Vorschrift ist dem Betroffenen Auskunft über die zu seiner Person gespeicherten Sozialdaten, deren mögliche Empfänger und den Zweck der Speicherung zu erteilen. Auf welche Art und Weise die Behörde – i. d. R. das Jugendamt - diese Informationen zur Verfügung zu stellen hat, lässt § 83 SGB X offen. In der Praxis kann neben der Einsicht vor Ort auch die Zusendung der Unterlagen in Betracht kommen. Vor dem Hintergrund einer bestmöglichen Zweckerfüllung hat das Jugendamt über die Art des Auskunftsersuchens zu entscheiden. Das Einsichtsrecht findet ausschließlich dort seine Schranken, wo diesem Begehren bei der Akten führenden Behörde ein unverhältnismäßiger Aufwand gegenüber stehen würde. Das Jugendamt wird sich nur ausnahmsweise hierauf zurückziehen können, da dieses Kriterium eng auszulegen ist, denn das Recht auf Auskunft ist Ausfluss des Grundrechts auf informationelle Selbstbestimmung. Keinen unverhältnismäßigen Aufwand stellt vor diesem Hintergrund dar, dass im Rahmen des Auskunftsrechts die Rechte Dritter an ihren personenbezogenen Daten und deren Geheimhaltung u. U. arbeitsaufwendig zu berücksichtigen sind. Für die Praxis bedeutet dies, dass die entsprechenden Daten von anderen ehemaligen Heimkindern unkenntlich zu machen sind. Dies gilt indes nach allgemeiner Auffassung nicht für Erzieher oder sonstige Angestellte der Heime, sofern sie in Ausübung und Funktion ihres Berufes genannt werden, denn das Informationsinteresse des Betroffenen überwiegt das Geheimhaltungsinteresse eines Funktionsträgers.

Der Auskunftsanspruch kann nach § 13 SGB X auch durch einen Bevollmächtigten geltend gemacht werden. Der konkrete Umfang der Vollmacht ist dabei in schriftlicher Form ausdrücklich zu regeln. Die Auskunft an sich hat unentgeltlich zu erfolgen (§ 83 Abs. 7 SGB X). Eine Löschung der fraglichen Daten ist nach § 16 Abs. 4 Satz 1 Thüringer Datenschutzgesetz solange unzulässig, als hierdurch schutzwürdige Interessen der Auskunftssuchenden beeinträchtigt würden.

In Kooperation mit dem Thüringer Ministerium für Soziales, Familie und Gesundheit verfolgt der TLfD auch künftig die Entwicklungen in diesem sensiblen Bereich und wird in Abstimmung mit den Datenschutzbeauftragten des Bundes und der Länder Lösungen finden, die den beteiligten Personen die Wahrnehmung ihres Auskunftsrechts und den Behörden datenschutzrechtssicheres Handeln weiterhin ermöglichen.

### **11.3 Thüringer Initiative zur Integration und Armutsbekämpfung - Nachhaltigkeit (TIZIAN)**

Ziel des TIZIAN-Projektes soll zur Armutsbekämpfung insbesondere die Steigerung der Erwerbsfähigkeit von Bedarfsgemeinschaften und Alleinerziehenden mit Kindern sein. Die für das Projekt geeigneten Personen werden von den Arbeitsgemeinschaften (ARGEn) und Jugendämtern ermittelt und sodann von einem sogenannten Projektträger näher betreut. Die Datenverarbeitung - hier vor allem die Erhebung und Übermittlung von sensiblen Sozialdaten - zwischen den beteiligten Stellen ist Gegenstand von Beratungen, in die der TLfD frühzeitig eingebunden wurde. Die datenschutzrechtlichen Fragen erscheinen derzeit lösbar, sodass erneut deutlich wird: Kinderschutz und Datenschutz von Kindern und Eltern stellen keine Gegensätze dar, sondern sind zur Verfolgung sinnvoller Ziele regelmäßig auch miteinander vereinbar.

Durch die konstruktive Kooperation des TMSFG mit dem TLfD wird auch das Projekt TIZIAN datenschutzrechtskonform ausgestaltet werden können.

### **11.4 Gemeinsame Empfehlung zur Verbesserung der ressortübergreifenden Kooperation beim Kinderschutz in Thüringen**

Kinderschutz und Datenschutz sind dank der guten Zusammenarbeit zwischen TLfD und dem Thüringer Ministerium für Soziales, Familie

und Gesundheit auf gutem Wege (vgl. im 7. TB Punkt 11.4). Erkannt wurde der Datenschutz als Förderer des Kinderschutzes und nicht als dessen Widersacher. Dem gemäß hat der Datenschutz in der Gemeinsamen Empfehlung zur Verbesserung der ressortübergreifenden Kooperation beim Kinderschutz in Thüringen eine breite Darstellung gefunden. Anhand von praxisrelevanten Darstellungen und Übersichten werden Jugendhilfe, Justiz, Polizei, Gesundheitswesen, Schulen und Kindertageseinrichtungen in die Lage versetzt, das Grundrecht auf informationelle Selbstbestimmung von Eltern und Kindern in ihre Entscheidungswägungen rechtssicher einzubeziehen. In der Praxis ist diese Aufhellung der bisherigen rechtlichen Grauzone „Kinderschutz-Datenschutz“ auf hohe Akzeptanz gestoßen. Bevor der gebündelte Sachverstand die Gestalt der gemeinsamen Empfehlungen annehmen konnte, mussten diskursiv wechselseitige Vorbehalte abgebaut und Kenntnisse aufgebaut werden. Alle an der Arbeitsgruppe Beteiligten haben sich diesem Prozess gestellt und so konnte nach konstruktiver, offener und vor allem ressortübergreifender Diskussion ein Ergebnis präsentiert werden, das auch in anderen problematischen Bereichen zu ähnlichen Vorgehensweisen ermutigt.

Mit der gemeinsamen Empfehlung zur Verbesserung der ressortübergreifenden Kooperation beim Kinderschutz in Thüringen ist allen beteiligten Ressorts ein großer Wurf gelungen. Vorhandene Reibungspunkte konnten zugunsten des Kinderschutzes „plan geschliffen“ werden und sämtliche mit der Aufgabe des Kinderschutzes betrauten Stellen sind mit diesem Leitfaden in der Lage, rechtssicher und damit im Sinne des Kinderschutzes und des Datenschutzes zu agieren. Eine Vorgehensweise, die auch in anderen Problembereichen Schule machen sollte.

### 11.5 Arge ARGEn?

Im Berichtszeitraum wurde die ARGE Saalfeld-Rudolstadt datenschutzrechtlich häufiger auffällig: Zur Sachverhaltsermittlung, etwa bei Mietverhältnissen, wurden Erkundigungen zum Leistungsempfänger bei Vermieter, Nachbarn und Behörden eingezogen, ohne dass der Betroffene selbst zuvor hierzu befragt wurde. Insbesondere waren hierbei Verstöße gegen § 67a Abs. 2 Satz 1 SGB X festzustellen. Denn die ARGE hatte wiederholt verkannt, dass sie zwar zur Ermittlung des Sachverhalts Beweise – einschließlich Zeugenaussagen – erheben darf (§ 21 SGB X), dieser Grundsatz jedoch durch § 67a Abs. 2 Satz 1 SGB X eingeschränkt

wird. Danach sind Sozialdaten zunächst beim Betroffenen (Leistungsempfänger) zu erheben; insoweit wird die „Ermittlungsfreiheit“ nach § 21 SGB X eingeschränkt (wenn – wie hier – die Ausnahmeregelungen des § 67a Abs. 2 Satz 2 SGB X nicht einschlägig sind). Zu dem wurden unter Verstoß gegen § 67a Abs. 1 SGB X Sozialdaten erhoben, die zur Aufgabenerfüllung nicht erforderlich waren. Ein thüringisches Sozialgericht hatte zur Frage des Bestehens einer Bedarfsgemeinschaft (§ 7 Abs. 3a SGB II) folgendes ausgeführt: Einer reinen Wohngemeinschaft, die keinen erkennbaren Willen für eine Einstehensgemeinschaft (Bedarfsgemeinschaft) habe, könne auch bei einem Zusammenwohnen über ein Jahr hinaus nicht der Wille unterstellt werden, dass die Mitglieder dieser Wohngemeinschaft füreinander eintreten und Verantwortung füreinander tragen wollen. Ermittelte Indizien und Informationen wie Gegenstände, Zeitschriften, Kleidung, Bettbezüge, gelegentliche Übernachtungen oder Urlaubsreise mit gemeinsamen Kindern ließen hier nicht den Schluss zu, dass eine Bedarfsgemeinschaft vorliegt. Trotz dieser sozialgerichtlichen Entscheidung beauftragte die ARGE jedoch – unter zusätzlichem Verstoß gegen § 80 SGB X (Auftragsdatenverarbeitung) – eine Detektei mit einer mehrtägigen Observation der vermeintlichen Mitglieder der Bedarfsgemeinschaft, obwohl die Observation lediglich Daten zu Tage fördern sollte und konnte, die im Sinne der sozialgerichtlichen Entscheidung irrelevant waren. Die ARGE Saalfeld-Rudolstadt wurde mehrfach beanstandet, auch weil sie sich unkooperativ zeigte. Inzwischen konnten diese gravierenden Defizite in Folge entsprechender Schulungsmaßnahmen und intensiverer Kommunikation mit Blick in die Zukunft behoben werden.

Hingegen positiv gestaltete sich im Berichtszeitraum das datenschutzrechtliche Zusammenwirken mit der ARGE Erfurt. Auf Grund berechtigter Eingaben Betroffener fiel hier zwar auf, dass Leistungsempfänger Angaben über sich oder Dritte machen sollten, obwohl die Kenntnis dieser Daten zur Aufgabenerfüllung der ARGE bzw. der von ihr eingeschalteten Privatfirmen nicht erforderlich war. Durch datenschutzrechtskonforme Änderung des Verfahrens und von Formularen und Vertragsmustern konnte jedoch Abhilfe geschaffen werden. Insbesondere in solchen Fällen, in denen sich die ARGE für Coaching- oder Profilingmaßnahmen privater Firmen bediente, hat sie auf die datenschutzgerechte Ausgestaltung der Vertragsbeziehungen zwischen den Privatfirmen und den Betroffenen (Leistungsempfängern) zu achten. In Kooperation mit dem TLfD konnten Mängel hinsichtlich des Umfangs der Datener-

hebung und der weiteren Datenverarbeitung einschließlich Löschung in den beauftragten Privatfirmen erhoben werden.

Die datenschutzrechtlichen Grundsätze der Datenerhebung zunächst beim Betroffenen selbst und der Erhebung nur der zur Aufgabenerfüllung erforderlichen Daten müssen von ARGEN intensiver beachtet werden. Insbesondere der letztgenannte Grundsatz gilt auch für Privatfirmen, die im Auftrag der ARGE Sozialdaten verarbeiten. Die ARGEN haben hier eine Kontrollpflicht auszuüben. Wünschenswert wäre eine datenschutzrechtliche Kommunikation zwischen den ARGEN, damit im Einzelfall festgestellte Mängel landesweit kommuniziert und abgestellt werden können.

### **11.6 Patientenarmbänder in Krankenhäusern**

Dank eines Hinweises aus dem Journalistenkreis wurde der TLfD auf sogenannte Patientenarmbänder aufmerksam. Dabei handelt es sich um einen Kunststoffstreifen, der dem Patienten während des Klinikaufenthalts um das Handgelenk gebunden wird. In diesem Kunststoffstreifen kann ein Chip eingesetzt oder ein Strichcode aufgedruckt sein, sodass verschiedene Datensätze gespeichert werden können. Das Krankenhauspersonal soll durch einen Handscanner die so gespeicherten Informationen abrufen können. Problematisch sind dabei insbesondere die RFID-Chips. Durch das Auslesen dieser Informationen besteht die Möglichkeit, einen kompletten Überblick über Untersuchungsergebnisse, die Therapieanweisungen und sonstige Informationen, die auf dem Armband gespeichert sind, abzurufen. Der TLfD hat daraufhin eine flächendeckende Anfrage bei allen seiner Zuständigkeit unterliegenden Krankenhäusern gestartet. Ziel dieser Anfrage war es, ein detailliertes Bild über den Einsatz solcher Armbänder zu erhalten. So stand im Vordergrund, ob und welche Daten auf welche Weise auf dem Patientenarmband hinterlegt werden, ob die Patienten Ihre Einwilligung hierzu erklärt haben, wer zum Datenzugriff berechtigt ist und wie die Löschung der so gespeicherten Daten erfolgt. Nach dem bisherigen Ergebnis der Anfrage werden in Thüringen gegenwärtig keine Armbänder mit den erwähnten problematischen Funktionen eingesetzt, sondern lediglich solche mit Aufschrift oder Strichcode. Verwendung finden diese Armbänder allein in verschiedenen Geburtsstationen und zur Identifikation desorientierter Patienten. Die Einwilligungsberechtigten müssen hierzu ihre Zustimmung erteilen. Da die Armbänder allein der Identifikation der Per-

sonen dienen sollen, werden neben dem Namen, dem Geburtsdatum und der Fallnummer regelmäßig keine weiteren Informationen notiert.

Da das Interesse der Krankenhäuser am künftigen Einsatz von digitalen Patientenarmbändern indes groß ist, wird der TLfD diesen Prozess weiterhin aufmerksam beobachten und auch begleiten.

### **11.7 Krankenhausinformationssysteme**

Die Datenschutzbeauftragten des Bundes und der Länder haben sich der Problematik des Datenschutzes in Krankenhäusern verstärkt zugewandt. Der Abruf elektronisch gespeicherter Patientendaten ist mittels moderner Krankenhausinformationssysteme (KIS) jederzeit, ortsungebunden und schnell möglich. Einerseits liegen hierin Vorteile für eine effiziente Behandlung. Andererseits stehen dem jedoch Missbrauchsmöglichkeiten gegenüber, die in anderen Bundesländern bereits in die Tat umgesetzt wurden. Die Problematik gewinnt noch dadurch an Brisanz, dass der Europäische Gerichtshof für Menschenrechte am 17.10.2008 (20511/03) die Überprüfbarkeit der Zugriffe auf Krankenhausdaten (Protokollierung) zu einem Teil des Menschenrechts auf Achtung des Privatlebens gem. Artikel 8 der Europäischen Menschenrechtskonvention erklärt hat. Dem entsprechend fordert die 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (Anlage 28), die internen Abläufe und die Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern datenschutzkonform zu gestalten. Um diese datenschutzkonforme Ausrichtung zu begleiten, wurde von den Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe einberufen, die die Seite der Krankenhäuser und der Softwarehersteller in den Problemlösungsprozess einbindet. Ziel muss sein, die Krankenhausinformationssysteme für datenschutzgerechte Lösungen fit zu machen.

Um die Krankenhausinformationssysteme datenschutzkonform auszurichten, wird sich die von den Datenschutzbeauftragten des Bundes und der Länder ins Leben gerufene Arbeitsgruppe mit den Krankenhäusern und Softwareherstellern ins Benehmen setzen. Ein Prozess, der Zeit in Anspruch nehmen wird.

## **12. Wirtschaft, Arbeit, Bau und Verkehr**

### **12.1 Geodaten und Persönlichkeitsrecht**

Unter Geodaten werden Daten jeglicher Art verstanden, die in irgendeiner Weise einen Orts- oder Raumbezug haben. Die Bedeutung von Geodaten und Geoinformationen wird sowohl von den öffentlichen Verwaltungen als auch von der Privatwirtschaft als sehr hoch angesehen. Zahlreiche Verwaltungsentscheidungen haben einen Orts- oder Raumbezug, sei es bei der Erstellung eines Bebauungsplans, eines Flurbereinigungsverfahrens, der Abgrenzung von Schutzgebieten, der Feststellung von tatsächlichen Verläufen von Ver- und Entsorgungsleitungen, der Erschließung von Bodenschätzen, der Überwachung etc.

Klassische Darstellungsmöglichkeiten von Geodaten sind Landkarten in verschiedenen Maßstäben, das Grundbuch und die Liegenschaftskarten. Bedingt durch den technischen Fortschritt werden solche Orts- und Raumberechnungen inzwischen ergänzt von Luftbildern, die beim Überfliegen mit Flugzeugen oder Erdbeobachtungssatelliten entstanden sind. Insbesondere durch diese neuen Verfahren besteht die Gefahr, dass zunächst nur raum- und sachbezogene Daten so detailliert dargestellt werden, dass sich nunmehr bereits hieraus ein direkter Personenbezug ergeben kann, etwa weil die Auflösung von Luftbildaufnahmen so genau ist, dass Personen oder Kfz-Kennzeichen erkannt werden können. Kann durch Zusatzwissen ein bestimmtes Grundstück einem bestimmten privaten Grundstückseigentümer zugeordnet werden, so werden personenbezogene oder zumindest personenbeziehbare Daten zu diesem Grundstück öffentlich, die mit bisherigen Mitteln der Wahrnehmung der Öffentlichkeit entzogen sind. Dies können Form, Größe, Bewuchs des Grundstücks oder auch ein erkennbarer Swimmingpool, eine Terrasse, ein Gewächshaus, ein Autoabstellplatz etc. sein. Es stellt sich die Problematik, mit den gesetzlichen Zugangsregelungen zu Geodaten einen akzeptablen Ausgleich zu schaffen zwischen den Interessen der Verwaltungen sowie der Wirtschaft und dem Schutz der Persönlichkeitsrechte des Einzelnen.

Um die Voraussetzungen für den Aufbau einer europäischen Geodateninfrastruktur zu schaffen, trat am 15. Mai 2007 die INSPIRE-Richtlinie (Infrastructure for Spatial Information in Europe; "Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemein-

schaft", ABI EU Nr. L 108 S. 1) in Kraft. Diese Geodateninfrastruktur soll sich aus den nationalen Geodateninfrastrukturen der Mitgliedsstaaten zusammensetzen. Damit dies möglich wird, müssen die organisatorischen, technischen und rechtlichen Grundlagen in den Mitgliedsstaaten weitgehend angepasst werden. Zur Umsetzung der INSPIRE –Richtlinie trat am 31. Juli 2009 das Thüringer Geodateninfrastrukturgesetz vom 08.07.2009 (ThürGDIG, GVBl. S. 574) in Kraft. Sinn des Gesetzes ist es, neben der o. g. Interoperabilität mit allen Mitgliedsstaaten, die Nutzung von Geodaten für Bürger, Verwaltung und Wirtschaft zu vereinfachen. Dabei hatte sich der TLfD bei seiner Beteiligung im Vorfeld dafür eingesetzt, dass den schutzwürdigen Interessen des Betroffenen ein hohes Gewicht eingeräumt wird. Soweit durch den Zugang zu Geodaten schutzwürdige Interessen der Betroffenen beeinträchtigt werden, war deshalb der Zugang zu diesen Daten zu beschränken, was der Gesetzgeber jetzt auch berücksichtigt hat.

Am 1. Januar 2010 trat das Thüringer Gesetz zur Zusammenfassung der Rechtsgrundlagen und zur Neuausrichtung des Vermessungs- und Geoinformationswesens vom 16. Dezember 2008 (GVBl. S. 574) in Kraft. Im unter Artikel 1 aufgeführten Thüringer Vermessungs- und Geoinformationsgesetz werden die Aufgaben und Ziele des amtlichen Vermessungswesens vorgegeben, etwa die Bereitstellung der Geodaten in einer Datenbank. Weiterhin werden alle Landesverwaltungen dazu verpflichtet, die eigenen Geoinformationssysteme entsprechend kompatibel zu dieser Datenbank zu gestalten. Der TLfD hatte an dem zur Kenntnis erhaltenen Gesetzentwurf kritisiert, dass zwar die Aufgaben des amtlichen Vermessungswesens beschrieben werden, die hierfür erforderliche Verarbeitung personenbezogener Daten aber nicht ausdrücklich angesprochen wird. Dies ist inzwischen geschehen.

Nunmehr hat der Freistaat Thüringen einen für jedermann freien Zugang zu Geodaten von Thüringen in einem sog. „Geoproxy“-System bereitgestellt. Hierin können Grundstücke nach Flurstückangaben oder nach der postalischen Adresse in Form des Liegenschaftskatasters oder als Luftbild in einer Auflösung von nicht mehr als 20 cm pro Pixel abgerufen werden. Der TLfD hatte mehrfach gegenüber dem TMBV hingewiesen, dass höhere Auflösungen aus den genannten datenschutzrechtlichen Gründen keinesfalls ohne spezielle Rechtsgrundlage eingestellt werden dürfen.

Bei aller Euphorie über die Effizienzvorteile für die Verwaltung und das hohe Wertschöpfungspotential für die Wirtschaft bei der Nutzung von Geodaten darf das informationelle Selbstbestimmungsrecht des Bürgers nicht auf der Strecke bleiben.

## 12.2 Deutschland-Online Kfz-Wesen

Im Rahmen der Deutschland-Online-Initiative wird der Einführung des Vorhabens „Kfz-Wesen“ Priorität bei der Realisierung dieses Systems eingeräumt. Für die Prozesse der An-, Ab- und Ummeldung in den ca. 440 örtlich zuständigen Zulassungsbehörden in der Bundesrepublik Deutschland werden jährlich etwa 24 Mio. Transaktionen ausgeführt, die von dem einzelnen Bürger verlangt, bei der für ihn zuständigen Zulassungsstelle vorstellig zu werden. Durch die zukünftige Durchführung einer Online Kfz-Zulassung ohne Medienbruch, also durchgängig am Computer über das Internet, sollen dem Bürger Wege und Zeit erspart werden.

Um in der Praxis zu erproben, in wieweit sich das Zulassungsverfahren auf elektronischen Weg bewährt, haben sich die Bundesländer Bayern, Baden-Württemberg, Hamburg, Hessen und Nordrhein-Westfalen zur Einführung eines Pilotprojektes mit Echtdaten bereit erklärt.

Derzeit liegt ein Feinkonzept zu einem zweistufigen Verfahren vor, wobei ab dem Jahre 2010 in einer ersten Stufe in den genannten Pilotländern der Bürger Fahrzeugzulassungen internetbasiert beantragen kann. Eine Authentifizierung ist mit dem elektronischen Personalausweis möglich. Der Antragsteller kann sich nach der Bearbeitung und Bezahlung der anfallenden Gebühren und Kosten die Fahrzeugdokumente und Schilder an den Ort seiner Wahl liefern lassen. Ab dem Jahre 2013 sollen dann die bisherigen Fahrzeugdokumente durch solche, die elektronisch aus- und einlesbar sind, ersetzt werden.

Der TLfD wird die Entwicklung des Vorhabens aus datenschutzrechtlicher Sicht weiterhin begleiten und bei einer zukünftigen Umsetzung in Thüringen die bei dem Pilotprojekt gemachten Erfahrungen der anderen Bundesländer einfließen lassen.

## 12.3 Falsche Adressaten für Gasliefervertrag

Aufgrund mehrerer Beschwerden wurde dem TLfD bekannt, dass die Stadtwerke Erfurt Energie GmbH Briefe versandt hatte, die u. a. Gasver-

träge enthielten, die dritte Personen betrafen. Die daraufhin vom TLfD unverzüglich eingeleitete Kontrolle der Energie GmbH ergab, dass in 26 Fällen menschliches Versagen Ursache für die fehlerhaften Datenübermittlungen war. Da jeweils mehrere Unterlagen an die Adressaten zu versenden waren und diese Unterlagen nicht maschinell zusammengestellt werden konnten, hatten Auszubildende die Sendungen manuell zusammengestellt. Hierbei wurden Adressaten fälschlicher Weise Gaslieferverträge zugeordnet, die für Dritte Personen bestimmt waren. Zusätzliche Brisanz erhielt das Geschehen dadurch, dass die an den falschen Adressaten versandten Gaslieferverträge teilweise Kontodaten enthielten. Schließlich wurden im Zuge der Kontrolle Auftragsdatenverarbeitungsverhältnisse sichtbar, die den datenschutzrechtlichen Anforderungen des § 11 BDSG nicht genügten. Im Wege konstruktiver Kommunikation zwischen dem TLfD und der Stadtwerke Erfurt Energie GmbH konnten die datenschutzrechtlichen Mängel behoben werden.

Die Verarbeitung sensibler personenbezogener Daten muss mit entsprechenden Kontrollmaßnahmen einhergehen. Auch verschachtelte gesellschaftsrechtliche Verhältnisse sind am Datenschutzrecht, insbesondere an den Vorgaben zur Auftragsdatenverarbeitung auszurichten.

#### **12.4 Intelligente Stromzähler**

Der Bundesgesetzgeber hat in § 21b Abs. 3a und 3b Energiewirtschaftsgesetz ab dem 01.01.2010 den obligatorischen (in Neubauten und umfangreich sanierten Gebäuden) bzw. fakultativen Einbau von elektronischen Energiezählern, sog. „Smart Metern“ vorgesehen, um die angebotene Energie besser ausnutzen zu können. Darüber hinaus müssen die Energieversorger ab Ende 2010 last- und zeitvariable Tarife anbieten.

Diese intelligenten Stromzähler können den gesamten und den momentanen Stromverbrauch sowie die Nutzungszeit anzeigen. Die Werte werden in den Geräten gespeichert, so dass es möglich ist, ein Energienutzungsprofil des jeweiligen Stromabnehmers zu erstellen. Dabei bieten die neuen Zähler die Möglichkeit, dass sie die Verbrauchsdaten selbstständig, z. B. über das Internet oder mit einer Funkverbindung, an den Stromanbieter bzw. Netzanbieter übertragen. Während bei den herkömmlichen Stromzählern lediglich abrechnungsrelevante Daten abzulesen sind, wie viel Strom innerhalb des jeweiligen Ablesezeitraums verbraucht wurde, zeigen die neuen Zähler an, zu welchen Zeiten, welche Strommengen durch den angeschlossenen Haushalt verbraucht wur-

den. In der Begründung der Bundestagsdrucksache 16/8306 wird auf S. 7 ausgeführt, dass die Einführung innovativer Zähler eine Grundlage für ein energiesparendes Verhalten schaffen, Konzepte für intelligente Netze fördern und preisliche Vorteile für den Verbraucher erschließen soll. Da öffentliche Stellen mit der Bereitstellung von Strom am Wettbewerb teilnehmen, gilt für sie gemäß § 26 ThürDSG mit einigen Ausnahmen das Bundesdatenschutzgesetz. Die von den intelligenten Stromzählern erstellten Nutzungsprofile sind deshalb personenbezogene Daten i. S. von § 3 Abs. 1 BDSG. Die Zulässigkeit, den Stromverbrauch innerhalb eines bestimmten Abrechnungszeitraums abzulesen, um für den Kunden eine Abrechnung zu erstellen, ergibt sich aus § 28 Abs. 1 Nr. 1 BDSG, wonach dies für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient. Hingegen ist die datenschutzrechtliche Zulässigkeit der Erhebung und Verarbeitung von Verlaufsdaten des Stromverbrauchs und dies ggf. auch über eine o. g. Funkverbindung ohne Wissen des Betroffenen nicht gegeben.

Aus datenschutzrechtlicher Sicht ist zu fordern, dass die Geräte technisch so gestaltet sind, dass nur hierfür ausdrücklich autorisiertes Personal und der Betroffene selbst an die im Strommessgerät gespeicherten Daten gelangen. Hierfür sind die nach § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen zu treffen. Der Kunde muss darüber informiert sein, zu welchen Zeitpunkten ein Zugriff auf das Messgerät stattfindet. Die Erforderlichkeit der Zugriffsintervalle muss sich dabei eindeutig aus dem Vertragsverhältnis ergeben. Weiterhin besteht auch die Möglichkeit, auf der Grundlage einer Einwilligung des Betroffenen nach § 4a BDSG einer Lastprofilablesung durch das Energieunternehmen zuzustimmen, etwa bei der Nutzung besonders günstiger Stromtarife zu bestimmten Tageszeiten oder die Zählerdaten in pseudonymisierter Form zum Test der Zähler und zum Zweck der Berechnung neuer Tarife für die Nutzung freizugeben. Die gleichen Probleme und Lösungsmöglichkeiten bestehen auch bei den zukünftig zu erwartenden intelligenten Gas-, Wasser- und Wärmehählern.

Die neuen intelligenten Stromzähler bieten die Möglichkeit eines wirtschaftlichen Umgangs mit Strom. Gleichzeitig besteht die Gefahr der Erstellung von Nutzungsprofilen. Dieser Gefahr muss durch das Ergreifen von technischen und organisatorischen Maßnahmen durch den Messstellenbetreiber begegnet werden. Ob intelligente Stromzähler

überhaupt oder deren volle Funktionalität genutzt werden, so ist dies nur im Rahmen des Vertragsverhältnisses mit dem Energieversorger oder aber aufgrund einer schriftlichen Einwilligung möglich.

## 12.5 Videoüberwachung in Wohngebäuden

Die Präsenz von Videokameras hat nicht nur im Bereich öffentlich zugänglicher Räume zugenommen. Auch Vermieter versuchen immer öfter, ihr Eigentum durch den Einsatz von Videoüberwachung vor Vandalismusschäden und unerwünschten Personen zu schützen. Nicht immer werden dabei die gesetzlichen Voraussetzungen für die Zulässigkeit eingehalten. Ende 2009 wandte sich ein Bürger an den TLfD, weil er Zweifel daran hatte, ob die in einem Mietshaus installierten Kameras rechtmäßig zum Einsatz kamen. In dem Wohnhaus wurden insgesamt 11 Kameras installiert, mit denen der äußere Wohnungseingangsbereich, die Treppenaufgänge im Erdgeschoss, der Fahrstuhlvorraum jeder Etage und der Fahrstuhl selbst überwacht wurden.

Im Außenbereich ist eine Überwachung unter den besonderen Voraussetzungen des BDSG zulässig. Nach § 26 ThürDSG i. V. m. § 6b Absatz 1 Nr. 3 BDSG ist eine Beobachtung von öffentlich zugänglichen Räumen mit optisch elektronischen Mitteln dann zulässig, wenn dies zur Wahrnehmung berechtigter Interessen erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Kontrolle ergab, dass diese Voraussetzungen hier erfüllt sind. Die Videoüberwachung des Außenbereiches soll sowohl präventive als auch repressive Wirkung entfalten. Sie soll Eigentumsbeeinträchtigungen verhindern und die Verfolgung strafrechtlich relevanter Störungen ermöglichen. Die nach § 6b BDSG vorzunehmende Güterabwägung führte hier zu einem Überwiegen der Interessen der Wohnungsgesellschaft. Sie wies durch eine umfangreiche Schadensaufstellung nach, dass die Eigentumsverletzungen in diesem Bereich nicht nur sehr häufig, sondern auch die Reparaturen sehr kostenintensiv waren.

Die dauernde Überwachung im Innenbereich ist jedoch nach wie vor ungeklärt. Da bezüglich der Innenraumüberwachung § 6b BDSG nicht anwendbar ist und auch keine Einwilligung aller Mieter zur Durchführung dieser Maßnahme vorlag, ist zur Beurteilung der Zulässigkeit neben § 28 BDSG auch die Rechtsprechung zu den §§ 823 Absatz 1, 1004 analog BGB i. V. m. Art. 1, 2 Absatz 1 GG zu beachten. Eine Rundumüberwachung des sozialen Lebens ist danach nicht gerechtfertigt, wenn

hierdurch Graffiti-schmierereien, Verschmutzungen oder einmaliger Vandalismus verhindert werden sollen. Im Rahmen der Kontrolle wurde durch den TLfD zunächst festgestellt, dass die kontrollierte Wohnungsgesellschaft nahezu ausschließlich solche Schäden durch die Überwachung verhindern will. Derartige Eigentumsstörungen rechtfertigen aber, wie in zahlreichen Gerichtsverfahren entschieden (AG Schöneberg, 10.05.2000 – 12 C 69/00; KG Berlin, 04.08.2008 – 8 U 83/08; LG Berlin, 31.10.2000 - 65 S 279/00), einen derart tiefen Eingriff in das allgemeine Persönlichkeitsrecht nicht. Zwischenzeitlich hat die Wohnungsgesellschaft weitere Argumente vorgetragen, die datenschutzrechtlich noch zu bewerten sind.

In nicht öffentlich zugänglichen Räumen müssen Mieter eine dauernde Videoüberwachung ihres unmittelbaren Wohnungsumfeldes durch den Vermieter nur dulden, wenn erhebliche Eingriffe in das Eigentum des Vermieters die schutzwürdigen Interessen der Mieter überwiegen.

## **13. Bildung, Wissenschaft, Forschung**

### **13.1 2. Europäischer Datenschutztag mit Folgen**

Für den 28. Januar 2008 kamen auf Initiative des TLfD die Datenschutzbeauftragten des Bundes und der Länder überein, sich Deutschland weit unter dem Motto „Datenschutz macht Schule“ dem Datenschutzbewusstsein von Schülern und Jugendlichen zuzuwenden. Der TLfD besuchte mit seinen Mitarbeitern Thüringer Schulen, um rechtliche Grundlagen und aktuelle jugendrelevante Aspekte des Datenschutzes zu diskutieren. Themen wie die Bedrohung der Privatsphäre durch argloses Agieren im Internet, z. B. in den sogenannten Communities wie SchülerVZ oder MySpace oder Facebook, und wie man sich vor Gefährdungen schützen kann, fanden das Interesse der Schüler ebenso wie die sich vor diesem Hintergrund stellenden (grund-) rechtlichen Zusammenhänge. Diese Veranstaltungen offenbarten einerseits großen Zuspruch seitens der Schüler, andererseits jedoch ein gerüttelt Maß an Unwissenheit. Um diese Lücken zu schließen, unterstützt der TLfD weitere Initiativen zur Stärkung der Medienkompetenz von Kindern und Jugendlichen, z. B. den Arbeitskreis Schule/Bildung der Datenschutzbeauftragten des Bundes und der Länder sowie in Thüringen die in dieser Form bundesweit einmalige Kooperation mit dem Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM; siehe dazu auch 13.2).

Datenschutzbewusstsein und Medienkompetenz junger Leute sollten Gegenstand intensiverer staatlicher Anstrengungen sein. Der TLfD widmet diesem Tätigkeitsfeld seine besondere Aufmerksamkeit und unterstützt die beteiligten Stellen bei ihren Bemühungen.

### **13.2 Kooperationsvertrag TLfD/ThILLM: Ein Erfolgsmodell**

Aus dem 2. Europäischen Datenschutztag (13.1) resultierte die Erkenntnis, dass Datenschutzbewusstsein und Medienkompetenz bei Schülern und Jugendlichen in Thüringen stärker gefördert werden müssen. Angesichts begrenzter Personalressourcen musste der TLfD für seine Vorstellungen zu Datenschutzvorträgen an Schulen, zur Ausbildung von Lehrermultiplikatoren, zur Erstellung von Unterrichtsmaterial etc. einen starken Verbündeten gewinnen, den er im Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) gefunden hat.

Am 13. Mai 2009 schlossen ThILLM und TLfD einen Kooperationsvertrag mit dem Ziel, die genannten Vorhaben gemeinsam anzugehen. Zwischenzeitlich haben die kooperativen Aktivitäten dazu geführt, dass das Thüringer Ministerium für Bildung, Wissenschaft und Kultur in den Kursplan Medienkunde den Lernbereich „Recht, Datensicherheit und Jugendmedienschutz“ aufgenommen hat. Damit können nunmehr auch (grund-) rechtliche und sicherheitsrechtliche Aspekte des Datenschutzes vermittelt werden. Dabei sollen die konkreten Unterrichtsinhalte den Schülern nicht einfach übergestülpt werden – viel mehr können und sollen die Schüler vorab die sie in diesem Zusammenhang bewegenden Themen einbringen. Insoweit speziell fortgebildete Lehrermultiplikatoren werden sodann ihre Kollegen in die Lage versetzen, den neuen Unterrichtsstoff anhand neuer Unterrichtsmaterialien an die Schüler zu bringen.

Die Kooperation zwischen TLfD und ThILLM hat das TMBWK als Gefährten gewinnen können für einen neuen Weg, dessen zukunftsweisende Weichen jetzt gestellt worden sind: Rechtskenntnisse, Datenschutzbewusstsein und Medienkompetenz sollen die Schüler auf ihrem Werdegang in ein mündiges Erwachsenenleben unterstützend begleiten. Ein bedeutendes Ziel, dass den Einsatz auch weiterer Stellen lohnt!

### 13.3 Der gläserne Schüler

Ungebrochen ist das wissenschaftliche Interesse an Schülern und Ihren Elternhäusern. Mit ganzen Paketen von Fragestellungen -zuweilen seltsam anmutenden Inhalts- werden Schüler unter massivem Einsatz personeller und materieller Ressourcen von mehreren Seiten bombardiert. Diese Aktionen sind datenschutzrechtlich mitunter angreifbar:

Der Thüringer Jugendmonitor ist eine Online-Befragung aller Schüler der Klassenstufen 5 – 8 zu ihren Freizeitaktivitäten; verantwortlich ist das Thüringer Ministerium für Bildung, Wissenschaft und Kultur. Gegen diese Befragung machten besorgte Eltern Front: Angesichts von in die Intimsphäre ragenden Fragestellungen (Vorhandensein der weiblichen Brust, Küssen, Menstruation, etc.) hätte vor Beantwortung der Fragen die elterliche Einwilligung zur Teilnahme der Schüler an der Befragung eingeholt werden müssen. Das ist auch die Ansicht des TLfD. Der Auffassung des Ministeriums, die Freiwilligkeit der Angaben wäre dadurch gewahrt, dass der Schüler am Ende der Befragung entscheiden könne, ob seine Antworten ausgewertet werden sollen oder

nicht, konnte sich der TLfD nicht anschließen. Denn in den hier betroffenen Altersklassen ist die Einwilligung der Erziehungsberechtigten (noch) erforderlich. Auch der seitens des Ministeriums gegenüber einer bestimmten Schule erteilte Hinweis auf die Verpflichtung zur Teilnahme an der Befragung gem. §§ 30 Abs. 2; 57 Abs. 2, Abs. 6 ThürSchulG konnte nicht überzeugen, da eine Befragung zu Freizeitaktivitäten die Vorgaben dieser Normen nicht erfüllt. Das Ministerium sicherte daraufhin die Einholung der schriftlichen Einwilligungserklärungen von Eltern und Schülern zu.

Befragungen von Kindern in einem Alter von bis zu 14 Jahren sind bei Fehlen einer Rechtsgrundlage datenschutzrechtlich nur mit Einwilligung der Erziehungsberechtigten zulässig.

Der Kompetenztest des Thüringer Ministeriums für Bildung, Wissenschaft und Kultur für die Schüler der Klassenstufen 3 und 6 sah im Mathematiktest eine Frage nach dem Bücherbestand im elterlichen Hausstand vor. Der Schüler konnte dabei eine passende Bücherregal-Grafik ankreuzen. Hierdurch sah sich ein Elternteil in seinem Recht auf informationelle Selbstbestimmung verletzt, zumal diese Angabe nicht anonym erfolgte. Zu Recht: Die „Bücherfrage“ tangiert die (Rechts-) Sphäre der Eltern (Betroffene) und gem. § 19 Abs. 2 Satz 1 ThürDSG sind personenbezogene Daten beim Betroffenen und nicht bei Dritten (Schülern) zu erheben. Zudem besteht nach den §§ 30, 57 ThürSchulG für Eltern gerade keine Pflicht zur Angabe solcher Daten. Zwischenzeitlich ist dieser Mangel behoben: Die „Bücherfrage“ wird nunmehr anonym beantwortet und vom übrigen Kompetenztest getrennt verarbeitet.

Die personenbezogene Frage nach dem Bücherbestand im elterlichen Haushalt in einer Schülerbefragung tangiert das Recht auf informationelle Selbstbestimmung der Eltern und ist nicht durch eine Rechtsgrundlage gerechtfertigt. Eine derartige Datenerhebung darf daher nur in anonymisierter Form bzw. mit Einwilligung der Erziehungsberechtigten erfolgen.

### **13.4 Befragung von Kindern und Jugendlichen der Stadt Jena**

In einer Eingabe beschwerten sich Eltern über eine in Schulen durch ein privates Forschungsinstitut im Auftrag der Stadt Jena durchgeführte Befragung von Kindern und Jugendlichen. Danach wurden die Schüler

der Klassenstufen 6, 8 und 10 über ihre Lebensbedingungen und den Bedarf an Freizeitangeboten befragt. In einem dem Erhebungsbogen beigegefügt Erläuterungsblatt wird u. a. ausgeführt, dass die Befragung auch dann durchgeführt werden soll, wenn die Eltern der Teilnahme nicht in einer Erklärung widersprechen.

Der TLfD wandte sich daraufhin an das zuständige Schulamt und wies darauf hin, dass bei der in Rede stehenden Befragung aufgrund der fehlenden umfassenden Aufklärung sowie der fehlenden Einwilligung der Betroffenen die Bestimmungen der §§ 4 und 19 Abs. 3 ThürDSG nicht eingehalten wurden. Das Schulamt wurde dazu aufgefordert, bis zu einer abschließenden Klärung der Rechtmäßigkeit der Datenverarbeitung von weiteren Befragungen und einer Nutzung der Daten abzusehen.

Wie sich dann aus den von dem Schulamt übersandten Unterlagen zu dieser Studie ergab, wurden keine schriftlichen Festlegungen für die Schulen zur Art und Weise des Verfahrens bzw. zur Beteiligung des Schulpersonals getroffen. Voraussetzung für die Genehmigung einer solchen Untersuchung an Schulen durch das Schulamt ist ein Erlass vom 6. August 1993 zur Genehmigung von Erhebungen, Umfragen und wissenschaftlichen Untersuchungen gemäß § 57 Abs. 5 ThürSchulG. Danach ist ein entsprechender schriftlicher Antrag, in dem das Projekt präzise beschrieben ist (Inhalt, Umfang und Zielstellung, Verfahrensweise der Datenerhebung bzw. Behandlung der Erhebungspapiere und deren Verbleib, Inhalt der Erhebungsunterlagen, der zeitliche Ablauf, die Verantwortlichkeiten und die Beteiligten) Voraussetzung für eine solche Genehmigung. Ebenfalls ist durch Auflagen sicherzustellen, dass aus der Erhebung keine Rückschlüsse auf einzelne Schüler, Eltern oder Lehrer möglich sind. Solche Antragsunterlagen konnten für die Schülerstudie nicht vorgelegt werden. Statt einer Verpflichtung zur Einholung einer Einwilligung bei den Eltern wurde es den jeweiligen Schulen überlassen, ob sie von den Eltern eine Einwilligung verlangten oder lediglich in einem Informationsschreiben den Eltern ein Widerspruchsrecht eingeräumten. Insbesondere, wenn den Eltern lediglich ein Widerspruchsrecht eingeräumt wird, ist nicht gesichert, dass die Eltern von dieser Information nachweisbar Kenntnis hatten. Ebenso wurde nicht beachtet, dass nicht nur die Eltern, sondern gleichfalls und vor allem auch die tatsächlich betroffenen und bereits grundrechtsmündigen Schüler entscheiden konnten, ob sie an einer freiwilligen Befragung teilnehmen möchten. Weiterhin sind gemäß § 19 Abs. 3 ThürDSG die Betroffenen auf die Freiwilligkeit ihrer Angaben ausdrücklich hinzuweisen. Diese für die Rechtmäßigkeit der Datenerhebung maßgebliche Information wurde den

Betroffenen weder in den schriftlichen Hinweisen zur Ausfüllung der Fragebögen für die Schüler noch in den Informationsschreiben zum Widerspruch für die Eltern gegeben. Das Informationsschreiben an die Eltern enthielt zuwenig Aufklärung über Zweck, Inhalt und Durchführung der Studie, sodass eine rechtswirksame Einwilligung nicht erteilt werden konnte. Darüber hinaus war durch die Kennzeichnung jedes Einzeldatensatzes mit einem schülerbezogenen Pseudonym eine personenbezogene Zusammenführung der Daten über mehrere Jahre für Längsschnittuntersuchungen vorgesehen. Hierüber, sowie über die Tatsache, dass für diese Zwecke die Daten schülerbeziehbar praktisch unbefristet bei den Jugendämtern aufgehoben werden sollten und damit auch schülerbezogene Persönlichkeitsentwicklungsprofile hätten erstellt werden können, wurde den Sorgeberechtigten nichts mitgeteilt.

Der TLfD hatte im Ergebnis das betroffene staatliche Schulamt gemäß § 39 Abs. 1 ThürDSG beanstandet, weil das Erhebungsverfahren genehmigt wurde, obwohl hierzu die gesetzlichen und die vom TMBWK vorgegebenen Voraussetzungen nicht erfüllt waren.

Da das Forschungsinstitut im Auftrag der Stadt tätig wurde, beanstandete der TLfD wegen der festgestellten schwerwiegenden Verstöße gegen das informationelle Selbstbestimmungsrecht und Bestimmungen zum Datenschutz durch die Jugendstudie auch die Stadt als insoweit verantwortliche Stelle (§ 8 Abs. 1 ThürDSG). Die Stadt Jena hat daraufhin sofort veranlasst, alle Einzeldaten aus der Umfrage sowie aus den Umfragen der vergangenen Jahre unverzüglich zu löschen. Gleichzeitig versicherten sowohl das staatliche Schulamt als auch die betroffene Stadt, bei künftigen Befragungen die datenschutzrechtlichen Bestimmungen umfassend zu beachten.

Schülerbefragungen, die nicht verpflichtend sind, bedürfen stets der schriftlichen Einwilligung durch die Sorgeberechtigten und die bereits grundrechtsmündigen Schüler. Diese Einwilligung wird nur dann rechtswirksam erteilt, wenn der Einwilligende aus dem Informationsschreiben zu der Studie die Bedeutung und die Tragweite seiner Entscheidung zu überblicken vermag. Den Sorgeberechtigten muss die Möglichkeit zur vorherigen Einsichtnahme in die Fragebögen zur Entscheidungsfindung über die Teilnahme ihres Kindes eröffnet werden.

### 13.5 Lebenslauf von Studienbewerbern?

Dem TLfD gelangte zur Kenntnis, dass Studienbewerber an der Berufsakademie Gera neben den üblichen Unterlagen, wie Nachweisen über die Hochschulreife und einen Ausbildungsplatz, auch einen Lebenslauf beifügen müssen. Ob sich diese Forderung auf eine Rechtsgrundlage stützen kann und ob die Abgabe des Lebenslaufs zur Aufgabenerfüllung der Berufsakademie Gera erforderlich ist, beantwortet sich nach dem Thüringer Berufsakademiegesetz (ThürBAG vom 24. Juli 2006; GVBl. 381). § 7 ThürBAG (Zugang zum Studium) sowie § 8 ThürBAG (Zulassung zum Studium) sind bereits erfüllt, wenn die dort geforderten Zeugnis-, Vertrags- sowie sonstigen Unterlagen vorgelegt werden. Ein Lebenslauf kann danach indes nicht verlangt werden. Zur Erfassung etwaiger Tatbestände, die im Sinne von § 8 Abs. 2 ThürBAG einen Studienbewerber vom Studium an der Berufsakademie ausschließen könnten, ist ein Lebenslauf ungeeignet, denn zum einen können diese Angaben im Lebenslauf nicht enthalten sein, zum anderen werden mit dem Lebenslauf Daten erhoben, die über die Erfassung von Ausschlussstatbeständen hinausgehen und daher nicht erforderlich sind. Das Ziel der Erfassung von Ausschlussstatbeständen könnte bereits durch eine entsprechende Versicherung des Studienbewerbers erreicht werden. Auch der ins Feld geführte § 31 ThürBAG (Datenverarbeitung, Datennutzung) rechtfertigt die Forderung nach einem Lebenslauf nicht. Weder wird die Abgabe eines Lebenslaufes in dieser Norm erwähnt, noch ist eine solche Datenverarbeitung zur Aufgabenerfüllung erforderlich – wie erwähnt, würde eine entsprechende Versicherungserklärung des Studienbewerbers ausreichen. Mit der Staatlichen Studienakademie Thüringen haben sich inzwischen die Berufsakademien Gera und Eisenach der Auffassung des TLfD angeschlossen.

Wer sich um ein Studium bei den Berufsakademien Gera und Eisenach bewirbt, muss einen Lebenslauf nicht (mehr) vorlegen. Für eine solche Forderung findet sich im Thüringer Berufsakademiegesetz keine Rechtsgrundlage. Zudem ist die Abgabe eines Lebenslaufs zur Erfüllung der Aufgaben der Berufsakademien nicht erforderlich, da Ausschlussstatbestände bereits von einer entsprechenden Versicherungserklärung des Studienbewerbers erfasst werden können.

## **14. Entwicklungen der automatisierten Datenverarbeitung**

### **14.1 Datenschutzförderndes Identitätsmanagement**

Unter Identitätsmanagement versteht man eine sichere Verwaltung von elektronischen Identitäten, den Identifizierungsprozess einer Identität und die entsprechenden Informationen, die damit verbunden werden können. Eine Identität ist immer einer Person zugeordnet, wobei eine Person mehrere Identitäten besitzen kann. Solch eine Identität kann aus verschiedenen Attributen wie bspw. Name, Bild, Adresse, Kontonummer, Kundennummer usw. bestehen. Für die Akzeptanz von elektronischen Prozessen innerhalb eines Unternehmens oder einer Behörde, als auch bei der Erstellung von E-Government-Anwendungen über das World Wide Web, ist ein datenschutzförderndes Identitätsmanagement von enormer Bedeutung. So haben im Rahmen der E-Government-Konferenz „Teaming up for the eUnion“ im November 2009 in Malmö die EU-Mitgliedsstaaten einer gemeinsamen Entwicklung des europäischen E-Government bis 2015 zugestimmt. Ziel ist es, neben der Interoperabilität ein durchgängiges E-Government in Europa zu schaffen, in dem die Mobilität für Bürger und Wirtschaft gewährleistet ist. Des Weiteren hat die EU verschiedene Projekte hinsichtlich des Identitätsmanagement ins Leben gerufen, an denen zum Teil Mitarbeiter des Unabhängigen Landesbeauftragten für den Datenschutz Schleswig-Holstein beteiligt waren. Die in diesem Zusammenhang entstandene Studie „Identity Management Systems (IMS): Identification and Comparison“ befasst sich mit technischen, juristischen und soziologischen Problemstellungen des technisch gestützten Identitätsmanagements ([www.uld-i.de/gutachten/idm/](http://www.uld-i.de/gutachten/idm/)).

In Deutschland fördert der Bund die Interoperabilität, Plattformunabhängigkeit und Investitionssicherheit von Softwaresystemen durch regelmäßige Veröffentlichungen von Standards und Architekturen für e-Government-Anwendungen (SAGA). Seit März 2008 liegt SAGA in der Version 4.0 vor (7.TB 15.2). Entsprechend SAGA 4.0 ist nunmehr die Einführung eines elektronischen Identitätsmanagement unter Verwendung der zukünftigen Funktionen und Anwendungen z. B. durch den elektronischen Personalausweis (ePA) sowie die Erarbeitung von E-Identity-Konzepten geplant. Somit rückt in Zukunft das Bedürfnis der

Nutzer, vor Identitätsbetrug geschützt zu sein, bei E-Government-Anwendungen stärker in den Mittelpunkt.

Auch das nationale Spiegelgremium zu ISO/IEC JTC 1/SC 27/WG 5 mit Sitz beim Deutschen Institut für Normung (DIN) befasst sich mit dem Thema Identitätsmanagement, die zukünftige ISO/IEC CD 24760 "A framework for identity management" wird voraussichtlich 2011 veröffentlicht. Eine Studie des ISPRAT-Institutes und Fraunhofer-Institutes zum Thema „Bürgerfreundliches Identitätsmanagement“, vom Juni 2009, untersucht das Modell am Beispiel der EU-Dienstleistungsrichtlinie.

Mit den Plänen zur Einführung eines Bundesmeldegesetzes im Jahr 2007 entstand auch die im April 2008 durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedete Entschließung „Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen“ (Anlage 3). Ausgehend davon, dass die Wirtschaft und die Verwaltung immer mehr digitale Daten mit direktem Personenbezug speichern, fordern die Datenschutzbeauftragten ein datenschutzförderndes Identitätsmanagement, um den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten zu schützen und zugleich eine moderne und effektive Datenverarbeitung zu ermöglichen. Dabei ist auch sicherzustellen, dass kein unkontrollierter Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann, sondern dies nur erfolgt, wenn der Nutzende es wünscht. Die Konferenz forderte die Bundesregierung auf, den Absichtserklärungen des dritten IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Mittlerweile liegen die Ergebnisse des vierten IT-Gipfels vom Dezember 2009 vor. Auch dort wurde noch einmal die Notwendigkeit der Zusammenarbeit von Politik und Wirtschaft betont, um Rahmenbedingungen zu schaffen, welche die Bürger zum Gebrauch des Internets ermutigen.

Um den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten zu schützen und zugleich eine moderne und effektive Datenverarbeitung zu ermöglichen, bedarf es datenschutzfördernder Identitätsmanagementsysteme.

## 14.2 Biometrische Authentisierung

Mit der Einführung des neuen Personalausweises 2010, auf dem die Speicherung der biometrischen Merkmale vom Gesicht und optional von einem Fingerabdruck erfolgen wird, wird die flächendeckende Erfassung biometrischer Merkmale von Bürgern der Bundesrepublik Deutschland weiter schrittweise umgesetzt (5.9). Unabhängig von dieser Entwicklung im öffentlichen Bereich hat auch die Wirtschaft Interesse, Authentisierungsverfahren unter Nutzung biometrischer Merkmale einzusetzen. Denn im Gegensatz zur UserID und Passwort und zu Verfahren von Besitz und Wissen sind biometrische Merkmale eindeutig und potenziell lebenslang mit der betroffenen Person verbunden. Begriffe wie Iriserkennung, Stimmbiometrie und Gangerkennung könnten alltäglich werden. Selbst beim Handgeometrieverfahren, bekannt durch den Fingerabdruck, sind weitere Einzel-Verfahren getestet worden. So kann nicht nur das Muster der Handvenen, sondern auch die Dicke, Länge, Breite und Fläche der Hand beziehungsweise der Finger der Erkennung eines Menschen dienen. Man darf also auf die Entwicklung der nächsten Jahre gespannt sein.

Jedes System zur Authentisierung hat allerdings auch seine Grenzen. Diese Grenzen ergeben sich bspw. aus den jeweils speziell für das System vor Ort festzulegenden Fehlertoleranzen (False Acceptance Rate (FAR) und False Rejection Rate (FRR)) und aus der Stabilität oder Veränderung der Merkmale selbst. Aber selbst wenn das für den jeweiligen Zweck ausgesuchte Authentisierungsverfahren mit seinen Fehlertoleranzen optimal eingestellt ist, ergeben sich aus datenschutzrechtlicher Sicht weitere zu beachtende Grundsätze, die regelmäßig überprüft werden müssen.

Der AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist deshalb in seiner Orientierungshilfe „Biometrische Authentisierung – Möglichkeiten und Grenzen“ bspw. darauf hin, dass unabhängig vom verwendeten biometrischen Authentisierungsverfahren Folgendes beachtet werden sollte:

- Die Verbindung zwischen biometrischen und anderen Identitätsdaten muss sicher geschützt werden.
- Es sollte keine zentrale, sondern eine dezentrale Speicherung der Referenzdaten, z. B. auf einer Chipkarte, realisiert werden.

- Die Speicherung und Übertragung der biometrischen Daten müssen gegen Abhören, unbefugte Offenbarung und Modifikation geschützt werden.
- Die Vertraulichkeit der Daten erfordert den Einsatz kryptografischer Verfahren.

Eine höhere Sicherheit vor Kompromittierung erlangen biometrische Authentisierungsverfahren, wenn zusätzlich zu den o. g. Anforderungen diese mit der Methode Besitz und Wissen (bspw. Chip mit PIN) ergänzt wird. Im Übrigen bedürfen Systeme, die der Mitarbeitererkennung dienen, zusätzlich der Mitbestimmung des Personalrates oder des Betriebsrates. Die vollständige Orientierungshilfe kann unter [www.lfd.mv.de/dschutz/informat/biometrie/oh-biometrie.pdf](http://www.lfd.mv.de/dschutz/informat/biometrie/oh-biometrie.pdf) eingesehen werden.

Jedes System, so auch ein Authentisierungsverfahren, entfaltet seine Stärken allerdings nur, wenn die damit verbundenen Risiken insgesamt wirksam beherrscht werden. Dies setzt ein umfangreiches Wissen bei den eigenen Mitarbeitern und eine kompetente Schulung und Beratung voraus. Zur Aneignung notwendiger technischer und organisatorischer Grundlagen stellt u. a. das Bundesamt für Sicherheit in der Informationstechnik einige Informationen bereit (<https://www.bsi.bund.de>). Auch die TeleTrust Deutschland e.V., bestehend aus Mitgliedern der Industrie, Wissenschaft/ Forschung und Behörden, hat bspw. neben ihrem „White Paper Datenschutz in der Biometrie“ ([www.teletrust.org/uploads/media/Datenschutz-in-der-Biometrie-080521\\_01.pdf](http://www.teletrust.org/uploads/media/Datenschutz-in-der-Biometrie-080521_01.pdf)) mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. eine „Landkarte Biometrie Deutschland 2008“ veröffentlicht ([www.teletrust.org/uploads/media/Flyer\\_Landkarte\\_Biometrie\\_-\\_V7\\_0\\_de1.pdf](http://www.teletrust.org/uploads/media/Flyer_Landkarte_Biometrie_-_V7_0_de1.pdf)).

Werden biometrische Authentisierungsverfahren eingesetzt, so ist neben der dezentralen Speicherung jederzeit die Vertraulichkeit der Daten durch den Einsatz sicherer kryptografischer Verfahren sicherzustellen.

### 14.3 Kennzeichnung von Daten

Bereits im Jahr 2003 wies die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass die Pflicht zur Kennzeichnung der Daten nicht auf den Bereich der Fernmeldeüberwachung beschränkt werden sollte.

Die nun in den letzten Jahren aufgetretenen Datenschutzskandale, wie beispielsweise das illegale Handeln mit Millionen von Kundendaten

oder mit Adressdaten gaben Anlass, erneut diese Forderung zu erheben. So hat der Bundesgesetzgeber mit der Novellierung des Bundesdatenschutzgesetzes im Jahr 2009 rechtliche Rahmenbedingungen geschaffen, um den illegalen Datenhandel, zumindest bei Werbung einzuschränken. Ab dem 1. April 2010 ist nach § 34 Abs. 1a BDSG vorgeschrieben, dass bei listenmäßiger Werbung die Herkunft der Daten und der Empfänger für die Dauer von 2 Jahren nach der Übermittlung zu speichern sind. Zudem ist dem Betroffenen auf Verlangen darüber Auskunft zu erteilen. Dies gilt entsprechend für den Empfänger.

Der AK Technik der Datenschutzbeauftragten des Bundes und der Länder wurde gebeten, zu untersuchen, ob derzeit schon geeignete Verfahren zur Kennzeichnung von Daten existieren. Im Ergebnis kam dieser zu dem Schluss, dass grundsätzlich solche Verfahren vorhanden, allerdings zurzeit noch sehr aufwändig und langwierig sind. Problematisch ist auch, dass bei Datenweitergabe stets neue Daten generiert werden, so dass die jeweiligen Quellenangaben um ein vielfaches größer sein können als die einzelne Datenangabe selbst. Unabhängig vom anfallenden Datenvolumen ist eine Kennzeichnung der zu schützenden Daten auch nur sinnvoll, wenn diese Kennzeichnung selbst auch vor Manipulationen oder ungewollter Veränderung bei Umwandlung in unterschiedliche Formate geschützt werden kann. Aus datenschutzrechtlicher Sicht erscheint es derzeit nicht unangemessen, alternativ eine manuelle Dokumentationspflicht festzulegen. Perspektivisch sind die erforderlichen technischen Lösungen voranzutreiben.

Sind technische Möglichkeiten, mit denen die gesetzlichen Vorgaben zur Kennzeichnung der Herkunft der Daten manipulationssicher und datensparsam umgesetzt werden können nicht ausreichend vorhanden, ist die geforderte Kennzeichnung manuell vorzunehmen.

#### **14.4 Protokollierung**

Öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die Revisionsfähigkeit (wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat) mittels technischer und organisatorischer Maßnahmen sicherzustellen (§ 9 Abs. 2 ThürDSG). Geeignete Maßnahmen hierfür sind bspw. die Protokollierung von Zugriffen und Zugriffsversuchen (Zugriffskontrolle), die Pro-

tokollierung der Übermittlungen von Daten (Weitergabekontrolle) und die Protokollierung der Eingaben (Eingabekontrolle).

Gemäß § 20 Abs. 4 ThürDSG dürfen Protokolldateien mit personenbezogenen Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, nur für diese Zwecke verwendet werden. Diese strikte Zweckbindung ergibt sich aus der Tatsache, dass mittels Protokollierungsdaten die Tätigkeiten aller Nutzer (Administratoren und Anwender) nachvollzogen werden können. Vor einer Protokollierung ist der Zweck der Protokollierung festzulegen und das Gebot der Datensparsamkeit und Datenvermeidung zu befolgen. Der Inhalt der Protokolldaten orientiert sich hierbei am Schutzbedarf der zu verarbeitenden Daten und gegebenenfalls an speziellen gesetzlichen Vorschriften (bspw. § 2 ThürMeldeVO). Zudem ist sicherzustellen, dass Protokolldaten nachträglich nicht verändert werden können und nur Berechtigten zugänglich sein dürfen. Diese Berechtigungen sind schriftlich festzulegen, wobei die Zugriffsmöglichkeiten so minimal wie nötig zu halten sind. Für die berechtigte Kontrollinstanz müssen Protokolldaten so aufbereitet werden, dass diese dann auch einen Sachverhalt rekonstruieren und bewerten kann.

Ebenfalls ist bereits vor der Erzeugung von Protokolldateien die Aufbewahrungsdauer festzulegen. Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Pflicht zur Löschung, wobei das Verfahren zum Löschen beschrieben sein muss. Es ist auch darauf zu achten, dass der Ereignisauslöser (i. d. R. eine Person) eindeutig bestimmbar sein muss. Deshalb widerspricht die Möglichkeit, personenbezogene Daten mit einer Gruppenkennung zu verarbeiten, der gesetzlich vorgeschriebenen Revisionsfähigkeit. Bei einem ändernden Zugriff ist zu beachten, dass klar erkennbar sein muss, um welches Datenfeld es sich hierbei handelt. Je nach Schutzwürdigkeit der personenbezogenen Daten sollten diese vor und nach der Änderung protokolliert werden.

Werden Protokolldaten mit personenbezogenen Daten und/oder erhöhtem Schutzbedarf über Netze übertragen, sind auch zur Wahrung der Vertraulichkeit, Integrität und Authentizität dieser Protokolldaten geeignete und für den Schutzbedarf angemessene kryptografische Verfahren nach dem Stand der Technik einzusetzen. Da Protokolldateien geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen oder zu erfassen, ist gemäß § 74 Abs. 2 Nr. 11 ThürPersVG der Perso-

nalrat zu beteiligen. Der AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die o. g. und weitere Hinweise in einer Orientierungshilfe „Protokollierung“ zusammengefasst, die unter [www.lfd.m-v.de/dschutz/informat/protokol/oh-proto.pdf](http://www.lfd.m-v.de/dschutz/informat/protokol/oh-proto.pdf) einsehbar ist.

Bei einer Protokollierung sind vorab schriftlich der Zweck, die hierzu notwendigen zu erfassenden Daten, die Auswertungsmodalitäten, die Löschfristen und der zugriffsberechtigte Personenkreis festzulegen.

#### **14.5 Datenschutz im Projekt- und Produktivbetrieb**

Zur Beantwortung der Frage, wann ist der Datenschutz im Projekt- und Produktivbetrieb umzusetzen, stellt der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe „Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb“ bereit. Der AK Technik weist darauf hin, das ungeachtet der Frage, ob die Datenverarbeitung mit personenbezogenen Daten bereits im Produktivbetrieb oder noch in einer Projektphase erfolgt, die Regelungen der jeweiligen Landesdatenschutzgesetze anzuwenden sind.

Zudem ist darauf zu orientieren, dass in der Projektphase nach Möglichkeit nicht mit personenbezogenen Daten gearbeitet werden sollte. Grundlegende Funktionen müssen bereits im Funktionstest mit ausreichend anonymisierten Daten überprüft werden. Nur im Ausnahmefall, wenn trotz Nachbildung im Funktionstest ein Fehler aus dem Produktivbetrieb nicht ermittelt werden kann, sondern sich nur mit Originaldaten aufklären lässt, sollten personenbezogene Daten zu Testzwecken verwendet werden. Der Kopiervorgang der personenbezogenen Originaldaten ist dabei zu protokollieren. Nach Beendigung der Tests ist die benutzte Kopie der Originaldaten unverzüglich aus dem Testbereich zu löschen bzw. im Testbereich zu anonymisieren. Bei der Verwendung von Originaldaten ist der Anlass, die Begründung, Umfang und Dauer, die getroffenen Sicherheitsmaßnahmen sowie die vorgesehenen Tests mit Testdaten revisionssicher zu dokumentieren. Ebenfalls wird darauf hingewiesen, dass es für die Testphase mit personenbezogenen Daten zumindest einer Kurzfassung eines Sicherheitskonzeptes bedarf. Wird das Verfahren vom Projektbetrieb in den Produktivbetrieb, also in den Pilotbetrieb, und später in den Regelbetrieb überführt, ist das Sicherheitskonzept vollständig, aufbauend auf eine Risikoanalyse, zu erstellen.

Abzurufen ist die Orientierungshilfe unter [www.lfd.m-v.de/dschutz/informat/projekt/oh\\_projekt.pdf](http://www.lfd.m-v.de/dschutz/informat/projekt/oh_projekt.pdf)).

Die Regelungen des ThürDSG sind ungeachtet der Frage, ob die Datenverarbeitung mit personenbezogenen Daten im Produktivbetrieb oder bereits in einer Projektphase erfolgt, anzuwenden.

#### **14.6 Anschluss von Netzen der öffentlichen Verwaltung an das Internet**

Der TLfD berichtete bereits über die „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ (7.TB, 4.3). Nunmehr liegt auch die überarbeitete „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ mit Stand November 2008 vor. Insbesondere die Ausführungen zur Protokollierung und Inhaltskontrolle mittels einer Firewall (Kapitel 6) mussten aufgrund der zwischenzeitlich geänderten gesetzlichen Grundlage durch das Inkrafttreten des Telemediengesetzes überarbeitet werden. Die Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder weisen in dieser Orientierungshilfe u. a. ausdrücklich noch einmal darauf hin, dass der Schutzzweck einer Firewall, als Teil eines Sicherheitsgateways, maßgeblich Art und Umfang der Protokollierung bestimmt: Wird beim Einsatz einer Firewall davon ausgegangen, dass diese in erster Linie dem Schutz der „hinter“ dem Webserver liegenden technischen Systeme und weniger dem auf dem Webserver gespeicherten Internet-Angebot der Stelle selbst dient, ist diese nicht unmittelbar selbst Bestandteil des Telemediums. Für Zwecke der Datensicherheit kommt daher eine Protokollierung auf der Grundlage von § 9 BDSG und Anlage bzw. die entsprechenden Vorschriften der Landesdatenschutzgesetze in Betracht. Da die Firewall weniger der Identifizierung von Angreifern als vielmehr deren Abwehr dient, ist die Abwehr von Zugriffen der Protokollierung vorzuziehen.

Dient die Firewall dem Schutz des eigenen Internet-Angebotes/Webservers einer öffentlichen Stelle, richtet sich die Zulässigkeit und der Umfang der Protokollierung von Nutzungsdaten ausschließlich nach § 15 TMG. Eine Speicherung personenbezogener Daten über das Ende des Nutzungsvorgangs hinaus ist nur zu Abrechnungszwecken erlaubt. Die IP-Adressen der Nutzer sind für diesen Zweck nicht erforderlich. Deshalb dürfen bei unproblematischen Zugriffen auf

das Angebot des Webserver selbst die IP-Adressen nicht gespeichert werden. Soweit eine Protokollierung auf der Firewall personenbezogen erfolgen darf, ist sie auf das zur Abwehr von Angriffen unabdingbare Notwendige zu begrenzen. Hierzu bedarf es allerdings einer Ermächtigung. Als Beispiel sei hier das BSI-Gesetz genannt. Kritisch bewertete die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den BSI-Gesetzentwurf, der dem BSI u. a. die Ermächtigung einräumen sollte, die gesamte Sprach- und Datenkommunikation aller Unternehmen, Bürgerinnen und Bürger mit Bundesbehörden ohne Anonymisierung bzw. Pseudonymisierung der Daten zu überwachen und auszuwerten. In der Entschließung „Stärkung der IT-Sicherheit – aber nicht zu Lasten des Datenschutzes!“ forderten die Datenschutzbeauftragten strengere Sicherheitsstandards und soweit möglich die Protokoll- und Inhaltsdaten vor der Auswertung durch das BSI zu anonymisieren bzw. zu pseudonymisieren (Anlage 20). Diese Forderung wurde in § 5 Abs. 2 des Gesetzes umgesetzt, welches seit 14. August 2009 in Kraft ist. Somit liegt hier keine Ermächtigung zur personenbezogenen Protokollierung vor.

Liegt eine Ermächtigung vor, unterliegen die dabei erhobenen Daten zur Gewährleistung der Datensicherheit oder des Datenschutzes der besonderen Zweckbindung gem. § 20 Abs. 4 ThürDSG (14.4). Die Behörde muss darüber hinaus die Informationspflichten nach § 13 Abs.1 TMG auch hinsichtlich der Protokollierung personenbezogener Daten beachten.

Die überarbeitete Orientierungshilfe, die auch auf die Planung einer sicheren Internetanbindung, Sicherheitsgateways, Zusatzmaßnahmen bei der Verarbeitung sensibler Daten, die Protokollierung von Mitarbeiterdaten und auch auf die Kontrolle von Inhaltsdaten bei E-Mail-Kommunikation eingeht, ist abrufbar unter ([www.thueringen.de/imperia/md/content/datenschutz/orientierungshilfe/oh\\_arbeitsplatz.pdf](http://www.thueringen.de/imperia/md/content/datenschutz/orientierungshilfe/oh_arbeitsplatz.pdf)).

Die mit dem Anschluss „interner“ Netze an das Internet verbundenen Sicherheitsrisiken sind zu analysieren und im gesetzlich vorgeschriebenen Rahmen zu begrenzen.

## 14.7 Cloud Computing

Der Begriff des Cloud Computing hat in den letzten Monaten sprunghaft Verbreitung gefunden. Es handelt sich dabei um eine IT-Strategie, die sich seit der kommerziellen Verwendung neuer Virtualisierungstechniken und im Verbund mit anderen, bereits bekannten Prinzipien, wieder neu am Markt bewirbt. Sie beinhaltet neue Herausforderungen, birgt aber auch neue Risiken. Die IT-Leistungen kommen quasi aus der „Steckdose“ direkt ins Haus. Sie werden bedarfsgerecht und flexibel über das Netz bereitgestellt, ohne dass der Nutzer sich weiter um die Beschaffung jeglicher Betriebsmittel kümmern muss. Die Abrechnung erfolgt nach tatsächlicher Nutzung, entweder nach Inanspruchnahme von CPU-Zeit, Speicherplatz, Transfervolumen oder nach Einheiten, die sich über mehrere Komponenten definieren. Das Netzwerk ist Bestandteil der „Wolke“, es setzt sich fort über Router, Switches, Repeater, Kabel- oder Richtfunkstrecken, Satellitenverbindungen bis zu den Servern, die irgendwo auf der Welt ihren Standort haben, entweder als physische Rechner, als Rechnerverbund oder als eine von mehreren virtuellen Maschinen - nur noch aus Software bestehend – auf einem gemeinsamen Hardware-Host. Virtuelle Server haben außerdem die Eigenschaft, ihren Host wechseln zu können je nach Auslastung, Ausfall, Speicherbedarf oder auf Vorgabe eines Administrators. Cloud Computing ist eigentlich nichts anderes, als eine besondere Form des Client-Server-Prinzips, wobei der Server durch die „Wolke“ - eine komplexere Struktur - und der Client durch ein mehr oder weniger intelligentes Anzeigergerät ersetzt werden. Die dem Client zugeordnete Intelligenz wiederum kann aber auch Bestandteil einer (anderen) „Wolke“ sein. Innerhalb einer Cloud hat sich eine Dreiteilung in Ebenen durchgesetzt. Diese aus fachlicher Sicht erstellte Einteilung erfolgt nach der Art der angebotenen IT-Leistungen für potentielle Nutzergruppen: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) und SaaS (Software as a Service).

Nach der Zugehörigkeit der Wolke zum Nutzer unterscheidet man in Public, Private und Hybrid Cloud. Werden bei einer Public Cloud die IT-Leistungen ausschließlich von einem oder mehreren externen Anbietern bezogen, stellt bei einer Private Cloud in der Regel die behördeninternen IT-Abteilung oder das unternehmenseigene Rechenzentrum die Leistung über das interne LAN bereit. Als wichtigster Vorteil für den Nutzer der Cloud-Services gilt, dass er sich nicht um die Abarbeitung

seiner Anwendung und um die dazu erforderliche EDV-Umgebung kümmern muss. Alle EDV-relevanten Vorgänge werden von einem oder mehreren Service-Providern übernommen. Die Datenverarbeitung vollzieht sich scheinbar ortsunabhängig auf weltweit verteilten Servern, ohne dass es dem Nutzer genau bekannt sein muss, wo sich seine Daten im Augenblick befinden. Es besteht also eine Abhängigkeit von den Providern, insofern wird von jenen ein besonderes Vertrauensverhältnis abverlangt. Überprüfungen der Systemsicherheit durch unabhängige Stellen und die Vorlage von Sicherheitszertifikaten können dabei von Vorteil sein. Kompliziert gestalten sich außerdem die rechtlichen Verhältnisse. Zweifellos handelt es sich beim behördlich oder auch geschäftlich genutzten Cloud Computing formal um eine Datenverarbeitung im Auftrag, wenn sie nicht im eigenen Rechenzentrum (private Cloud) oder auf den eigenen Rechnern stattfindet. Wenn dabei der Leistungsanbieter genau bekannt und im gleichen Rechtsraum angesiedelt ist, sind die Vertragsverhältnisse statischer Natur und nicht anders als bisher.

Beim effektiven Cloud Computing jedoch stehen Wirtschaftlichkeit und Flexibilität im Vordergrund, so läuft eine rechenintensive Anwendung sinnvollerweise auf den Servern desjenigen Anbieters, der freie Kapazitäten und die günstigsten Preise hat. Dieser wiederum könnte Unterauftragnehmer ins Spiel bringen, die wiederum selbstständig flexibel operieren und versuchen, den erhaltenen Auftrag für sich selbst so effektiv als möglich umzusetzen. Spätestens dann gibt es vermehrt Unsicherheiten bei der Vertraulichkeit, der Revisionsfähigkeit und der Transparenz der Auftragsgestaltung. Der Aspekt des schnellen Wechsels von Unterbeauftragungen verträgt sich nicht mit statischen Vertragsbeziehungen. Demgegenüber steht eine rechtliche Bindung an den Ort der Verarbeitung. Mit dem Wegfall der Georeferenz geht der am Ursprungsort bestehende Rechtsrahmen verloren. Diese Situation dürfte die Nutzung einer Public Cloud für eine ganze Reihe von Anwendungen erheblich einschränken, zumindest überall dort, wo personenbezogene und sensible Daten verarbeitet werden. Eine direkte Lösung ist noch nicht in Sicht. Der Rechtsraum müsste über Ländergrenzen erweitert werden, das derzeit im Datenschutzrecht gültige Territorialprinzip wäre aufzugeben. Alle Anbieter von Cloud Services müssten sich untereinander verständigen (Service Level Agreements), um ihren Kunden umfassende Vertrauensgarantien bieten zu können. Es besteht die Tendenz, mit Erteilen des Auftrags auch die IT-Sicherheit den Dienstleistern zu übertragen. Inso-

fern müssten sich die Service-Provider untereinander auf ein gemeinsames Sicherheitskonzept verständigen.

Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat 2009 eine Arbeitsgruppe Cloud Computing gebildet. Ziel ist, eine Orientierungshilfe zu erarbeiten.

## 14.8 Viren

Viren, die wahllos Daten auf dem eigenen PC löschen oder ihn aus Spaß Programme starten lassen, sind seltener geworden. Zunehmend sind es Trojaner und Würmer, die bspw. mittels SPAM, manipulierten Internetseiten oder Bild-/Filmdateien auf die PCs geschleust werden, um diese auszuspionieren oder für Großangriffe (Bildung von Bot-Netzen) auf Server im Internet zu missbrauchen. Auch Sicherheitslücken von Betriebssystemen und Anwendungssoftware sind beliebte Angriffsziele zur Übermittlung von Schadsoftware geworden. Allerdings hat noch nicht jeder Bürger, jedes Unternehmen oder jede Behörde die Notwendigkeit einer zeitnahen Aktualisierung (Update) erkannt. Deshalb konnte bspw. der Conficker-Wurm weltweit den Erfolg von mehreren Millionen infizierten PCs erzielen. Auf Grund dieser Entwicklung hat das BSI bereits im Juni 2008 seinen Newsletter zu Virenmeldungen eingestellt und drei neue Informationsdienste im kostenlosen Abonnement bereitgestellt ([www.buerger-cert.de/abonnieren.aspx](http://www.buerger-cert.de/abonnieren.aspx)).

Mit den „technischen Warnungen“ werden Abonnenten einmal pro Woche über Sicherheitslücken und andere Bedrohungen informiert. Zusätzlich erfolgt eine sofortige Benachrichtigung per E-Mail, wenn kritische Gefahren auftauchen. Der Newsletter "Sicher • Informiert" berichtet alle zwei Wochen über Wissenswertes und Tipps zur Computersicherheit. Abonnenten der Extraausgabe "Sicher • Informiert" werden sofort per E-Mail über kritische Gefahren für Computer informiert. Nicht nur Unternehmen und Behörden, sondern insbesondere die Bürger, die z. B. zukünftig den neuen Personalausweis zu Hause für Internet-Anwendungen nutzen wollen (5.9), sind gut beraten, diese Informationsdienste zur IT-Sicherheit zu nutzen.

Um das Risiko zu minimieren, Opfer von Schadsoftware zu werden, ist die tägliche Aktualisierung des Virenschanners und Sicherheitsupdates von Betriebssystemen und Anwendungssoftware unverzichtbar.

## **15. Technische Entwicklung in der Thüringer Landesverwaltung**

### **15.1 Umsetzung EU-Dienstleistungsrichtlinie in Thüringen - ThEA**

Entsprechend dem Thüringer Gesetz zur Umsetzung der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates der Europäischen Union über Dienstleistungen im Binnenmarkt vom 8. Juli 2009 werden die Einheitlichen Stellen bei den Thüringer Kammern eingerichtet. Damit folgt der Gesetzgeber einem umfangreichen Konzept, das unter der Federführung der sechs Wirtschaftskammern in Zusammenarbeit mit den Thüringer Kammern der Freien Berufe sowie dem Landesverband der Freien Berufe Thüringen e.V. erstellt wurde. Art. 8 EG-DLR sieht unter anderem vor, dass alle Verfahren und Formalitäten, die die Aufnahme oder Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch abgewickelt werden können. Hierzu wurde Anfang 2009 eine Projektgruppe zur Einführung des **Thüringer Erfassungs- und Antragsystem (ThEA)** gebildet. Das Verfahren, welches bis zum 28.12.2009 in Deutschland umzusetzen war, dient der elektronischen Verfahrensabwicklung, um Anträge und Formulare online zu verwalten sowie den zuständigen Stellen (ZS) zur Verfügung zu stellen. Dies kann direkt geschehen oder mit Hilfe der Einheitlichen Stelle (ES) der jeweiligen Kammern. Bei dem elektronischen Verfahren handelt es sich um eine webbasierte Portal-Lösung für den Antragsteller, die Einheitlichen Stellen und für die zuständigen Stellen.

Bei dem Verfahren ist aus datenschutzrechtlicher Sicht auf den Umgang mit personenbezogenen Daten der Antragsteller durch die ES als Dienstleister und durch die zuständige Behörde zu achten. Um datenschutzrelevante Vorentscheidungen zeitnah im Verfahren mit aufzunehmen, wurde der TLfD in zwei Projektuntergruppen mit einbezogen. Fragen, die u. a. geklärt werden mussten, betrafen die Übermittlungsbefugnisse, Speicher- und Löschfristen, Bestimmung der speichernden Stelle, Rechte der Antragsteller sowie datenschutzrechtliche Kontrollrechte. In Thüringen sind 6 ES-Geschäftsstellen eingerichtet worden, die bei der Datenerhebung und Datenspeicherung im Serviceportal als eigenständige öffentliche Stellen gegenüber dem Antragsteller auftreten. Deshalb hat jede dieser Stellen einen schriftlichen Vertrag zur Auftragsdatenverarbeitung nach § 8 ThürDSG mit dem TLRZ/ZIV als Betreiber

des IT-Systems abzuschließen. Die datenschutzrechtliche Verantwortlichkeit der ES ist auf die erforderlichen Informationen der über ihre Stelle geleiteten Anträge beschränkt. Die ES hat keinerlei Zugriff auf die Verfahren und Daten, welche auf den behördeninternen Informationssystemen gespeichert sind. Sofern für eine elektronische Verfahrensabwicklung die Schriftform erforderlich ist, müssen alle eingestellten Daten sowohl vom Antragsteller, als auch von der ES oder der ZS mit einer qualifizierten elektronischen Signatur im Sinne des Signaturgesetzes versehen werden. Die Löschfristen nach Antragserteilung müssen entsprechend § 16 ThürDSG festgelegt werden. Nach spätestens einem Jahr nach Antragsstellung sind die Daten zu löschen. Hierbei sind auch die Datensicherungssysteme mit einzubeziehen. Der Antragsteller muss auch die Möglichkeit haben, seine Daten löschen zu lassen, wenn der Antrag abgebrochen wird. Die bei den Statusanzeigen entstehenden Protokolldateien dienen der Dokumentation des Verfahrensablaufes. Werden weitere Protokolldateien erzeugt, ist dies unter Angabe der konkreten Zweckbestimmung zu dokumentieren. Für die Erstellung und die Auswertung dieser Protokolle müssen datenschutzrechtliche Prinzipien beachtet werden (6. TB, 1.5). Nach § 10 ThürDSG ist von der Daten verarbeitenden Stelle ein Verfahrensverzeichnis zu erstellen und nach § 34 Abs. 2 ThürDSG das Verfahren freizugeben. Auf die Umsetzung dieser Vorgaben durch die beteiligten Stellen, die noch nicht vollständig erfolgt ist, wird der TLfD in den nächsten Monaten achten.

Auch wenn das Thüringer Erfassungs- und Antragssystem (ThEA) fristgerecht Online gegangen ist, ist es ein System, welches permanent angepasst und überprüft werden muss. Neben der Umsetzung der bestehenden datenschutzrechtlichen Vorgaben, müssen Änderungen von Verfahren und Verfahrensabläufen, die durch neue Entwicklungen oder der Erweiterung von IT-Modulen erforderlich werden, jeweils den datenschutzrechtlichen Anforderungen angepasst werden.

## 15.2 Einsatz EiCoNeD in Thüringen

Im Freistaat Thüringen ist das Corporate Network (CN) seit 1996 die zentrale Netzplattform für alle Verwaltungsbereiche des Landes. Es sind derzeit ca. 350 Verwaltungsdienststellen eingerichtet, von denen einige das CN auch für die Sprachkommunikation nutzen. Da viele aktuelle Sprach- und Datenverträge Ende 2011 auslaufen, wird derzeit von der IuK-Leitstelle eine Ausschreibung eines zentralen Sprach- und Daten-

dienstes sowie der mobilen Kommunikation vorbereitet. Hierzu wurde Anfang des Jahres 2009 das Projekt „**Einkauf Corporate Network und Dienste**“ mit dem Ziel eingerichtet, ab 2012 mit einer neuen Infrastruktur in den Bereichen Sprache, Daten, mobile Kommunikation und Dienste zu arbeiten.

Die Leistungen für Sprach- und Datennetz, Mobilfunk und der zentrale Internetzugang werden Anfang 2010 europaweit ausgeschrieben. Hierbei sollen über einen gemeinsamen Landesvertrag Einzelverträge abgelöst werden, um wirtschaftlichere Einkaufskonditionen zu bekommen und somit zur Entlastung des Haushaltes beizutragen. Mit der neuen Netzstruktur und den neuen Diensten wird die Leistungsfähigkeit des gesamten Corporate Network (CN) erweitert und mit zukunftsfähigen Technologien nachhaltig ausgestaltet. Das neue CN muss nicht nur leistungsfähiger sondern auch sehr sicher sein, um auch zukünftig den hohen Anforderungen einer zeitgemäßen und nachhaltigen Behördenkommunikation zu genügen. Entsprechend den gesetzlichen Regelungen des ThürDSG ist ein umfassendes Sicherheitskonzept zu erarbeiten. Dabei sollte sich u. a. an der „VoIPSec-Studie zur Sicherheit von Voice over Internet Protocol“ und den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientiert werden. Im Sicherheitskonzept müssen alle angebotenen Dienste im CN mit einer ausführlichen Beschreibung von potenziellen Bedrohungen sowie der Maßnahmen, die zur Vermeidung oder Abwehr zu ergreifen sind, aufgeführt werden. Weiterhin muss sichergestellt werden, dass alle Sicherheitsmaßnahmen laufend an die aktuellen technischen und technologischen Entwicklungen angepasst werden und das Sicherheitskonzept in seiner Gesamtheit ständig aktualisiert wird. Als Ersatz für die veralteten/abgeschriebenen TK-Anlagen sind Vermittlungssysteme vorgesehen, die auf Basis des IP-Netzwerkprotokolls arbeiten. Diese Systeme dienen als Vermittlungsstellen für Datenverbindungen und können Sprachkommunikation über kostengünstige IP-Telefonie (VoIP - Voice over IP) abwickeln. Bei der IP-Telefonie werden, entgegen dem heute üblichen leitungorientierten Sprachkanal im ISDN (Integrated Services Digital Network), VoIP Datenpakete mit einem Gesprächsabschnitt, der Zieladresse und einer laufenden Nummer durch ein auf dem Internet-Protokoll (IP) basierendes Netz geschickt. Sprache und Steuerinformationen werden dabei als digitale Daten im Netzwerk transportiert. Die Pakete können auf den unterschiedlichsten Wegen zum jeweiligen Empfänger übertragen und dort an Hand der laufenden Nummer wieder in der richtigen Reihenfol-

ge zusammengesetzt werden. Schon im Oktober 2005 hat die 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit ihrer EntschlieÙung „Telefonieren mit Internet-Technologie (Voice over IP – VoIP)“ auf die besonderen Risiken hingewiesen, die mit der Internettelefonie verbunden sind. Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen (6. TB, 1.10).

Bei der Umsetzung sollten zum Schutz sensibler und schutzwürdiger Kommunikation die Verschlüsselung der Datenpakete möglich sein, sowie VPN (Virtual Private Networks) - Verbindungen zur Anbindung von verschiedenen Standorten in speziell gesicherten logischen Netzwerken eingesetzt werden. Bei den verbreiteten Protokollen für Voice-over-IP wie SIP (Session Initiation Protocol – Protokoll zum Aufbau einer Verbindung) und RTP (Real-Time Transfer Protocol – Protokoll zur Datenübertragung in Echtzeit) ist die Verschlüsselung möglich. Bei dem Projekt EiCoNeD handelt es sich um Auftragsdatenverarbeitung gemäß § 8 ThürDSG. Wegen der Verarbeitung von personenbezogenen Daten, die besonderen Geheimhaltungsbestimmungen unterliegen, gelten Einschränkungen für die Auftragsdatenverarbeitung, so dass das Betreiben und Verwalten des „neuen“ CN außerhalb der Thüringer Landesverwaltung als kritisch angesehen werden müsste.

Die vielfältigen Risiken bei der Nutzung von VoIP sind durch konkrete Analysen zu Datenschutz und Datensicherheit und die Umsetzung der daraus resultierenden Maßnahmen zu minimieren.

### **15.3 Protokollierung von Zugriffen auf Internetangebote in der Thüringer Landesverwaltung**

In der Thüringer Landesverwaltung gibt es Überlegungen, die Auswertung über Zugriffe auf deren Internetangebot zu verbessern. Hierzu wurde der TLfD um Beratung zur datenschutzgerechten Ausgestaltung gebeten. Es soll eine spezielle Software angeschafft werden, die unabhängig von der technischen Infrastruktur Echtzeitstatistiken über das Besucherverhalten auf Webseiten liefert, um diese kontinuierlich zu verbessern und die Brauchbarkeit zu steigern.

Wird eine Webseite aufgerufen, werden eine Reihe von Informationen über die einzelnen Zugriffe wie Datum und Uhrzeit, die Bezeichnung des abgerufenen Dokuments, Browsertyp und Betriebssystem des

zugreifenden Computers, von welcher Suchmaschine man weitergeleitet wurde und natürlich auch die IP-Adresse des abrufenden Computers protokolliert. Die IP-Adressen haben datenschutzrechtlich eine besondere Bedeutung, da mit den protokollierten Informationen und zusätzlichem Wissen diese Adresse bestimmten Personen zugeordnet werden könnte.

Das Telemediengesetz verbietet im § 15 die personenbeziehbare Protokollierung des Nutzungsverhaltens, sofern diese nicht zur Nutzung der Telemedien selbst oder zu Abrechnungszwecken erforderlich sind. Zur bedarfsgerechten Gestaltung der Telemedien dürfen Nutzungsprofile unter Verwendung von Pseudonymen und nach vorheriger Unterrichtung der Betroffenen unter Hinweis auf eine Widerspruchsmöglichkeit erstellt werden (14.6). In der juristischen Diskussion ist derzeit noch umstritten, ob IP-Adressen als personenbezogene Daten zu werten sind und insoweit datenschutzrechtliche Relevanz haben. Beispielsweise vertrat das Amtsgericht Berlin Mitte in einem Urteil vom 27. März 2007 (5 C 314/06) die Ansicht, dass auch vom Provider nur zeitweise zur Verfügung gestellte, also dynamische IP-Adressen, als personenbezogene Daten gelten und damit nur nach ausdrücklicher Zustimmung des Nutzers erfasst und protokolliert werden dürfen. Dieses Urteil wurde durch das Landgerichts Berlin am 6. September 2007 (23 S 3/07) bestätigt. Dagegen heißt es in einem Urteil des Amtsgerichts München vom 30.09.2008 (133 C 5677/08), die IP-Adresse sei kein personenbezogenes Datum im Sinne des § 3 Abs. 1 BDSG. Der TLfD geht davon aus, dass es sich bei der IP-Adresse um ein personenbezogenes Datum handelt. Natürlich sind die Betreiber von Webangeboten bestrebt, über eine Analyse der aufgerufenen Webseiten Aussagen über die Qualität des Angebotes und des Besucherverhaltens zu bekommen. Des Weiteren gibt es auch Tools, die IP-Adressen anonymisieren, indem der letzte Teil der IP-Adresse auf „0“ gesetzt wird. Somit steht dem Statistikprogramm eine anonyme IP-Adresse zur Verfügung, welche ohne Personenbezug zur Auswertung genutzt werden kann.

Die öffentlichen Stellen Thüringens müssen bei ihren eigenen Webauftritten auf die Speicherung von IP-Adressen der Besucher ihrer Internetseiten verzichten, da es dafür keine Rechtsgrundlage gibt.

#### **15.4 Einsatz BlackBerry in der Thüringer Landesverwaltung**

Seit September 2007 bietet das Thüringer Landesrechenzentrum die BlackBerry-Technologie für die Thüringer Landesverwaltung an. Hierzu berichtete der TLfD im 7. TB (15.6). Zu diesem Zeitpunkt lief bereits die dreistufige Sicherheitsüberprüfung im Auftrag der Herstellerfirma RIM durch das Fraunhofer-Institut für Sichere Informationstechnologie hinsichtlich der Sicherheit der Kommunikation mit dem BlackBerry.

Die damals vom Institut abgeschlossene erste Untersuchungsphase ergab, dass keine Hinweise auf einen beim Produzenten liegenden Master-Key oder andere Möglichkeiten vorhanden sind, die eine unberechtigte Kenntnisnahme durch Manipulation von Dritten ermöglichen. Die dahingehenden Bedenken wurden auch nicht durch die nun zwischenzeitlich vorliegenden Ergebnisse der zweiten und dritten Überprüfungsphase belegt. Das Fraunhofer SIT stellte am 24.11.2008 der Firma RIM für das Produkt „BlackBerry Enterprise Solution for Microsoft Exchange“ in der Version „Enterprise Server 4.1.6 Pearl™ 8110 v4.3.0.104“ ein entsprechendes IT Security Zertifikat aus (Zertifikate 06-104302).

Dieses softwareabhängige Zertifikat gilt bis Dezember 2010 und nur für diese überprüfte Version. Änderungen an Endgeräten und an der Software sind nicht durch das Zertifikat gedeckt. So wird derzeit die BlackBerry Enterprise Server Version v5.0 vertrieben. Behörden wird empfohlen, vom Hersteller eine verbindliche Erklärung abzuverlangen, ob und ggf. ab welchem Sicherheitsupdate im Rahmen des Zertifikats getroffene Aussagen analog Bestand haben.

Wird nicht die zertifizierte Version der BlackBerry-Technologie eingesetzt, ist ggf. deren Sicherheitsniveau abzuklären. Behörden mit einem besonders hohen Schutzbedarf sollten sich generell bei der Wahl von mobilen Endgeräten, abhängig von ihrem Verwendungszweck, hinsichtlich der aktuellen Sicherheitsstandards vom BSI beraten lassen.

## Anlage 1

**Entschließung**

der 75. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 3./4. April 2008 in Berlin

**Berliner Erklärung:  
Herausforderungen für den Datenschutz zu Beginn  
des 21. Jahrhunderts**

Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste Quantensprung der Informationstechnik steht unmittelbar bevor: Die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nicht-öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoringverfah-

ren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zu schulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und –sparsamkeit Rechnung getragen werden.

## Anlage 2

**Entschließung**

der 75. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 3./4. April 2008 in Berlin

**Keine Vorratsspeicherung von Flugpassagierdaten**

Die EU-Kommission hat den Entwurf eines Rahmenbeschlusses des Rates zur Speicherung von Flugpassagierdaten und zu deren Weitergabe an Drittstaaten vorgelegt. Künftig sollen die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast insgesamt 19 Datenelemente, bei unbegleiteten Minderjährigen sechs weitere Datenelemente, an eine von dem jeweiligen Mitgliedstaat bestimmte „Zentralstelle“ übermitteln. Die Daten sollen bei den Zentralstellen anlass- und verdachtsunabhängig insgesamt 13 Jahre lang personenbezogen gespeichert werden und zur Durchführung von Risikoanalysen dienen. Unter im Einzelnen noch unklaren Voraussetzungen sollen die Daten an Strafverfolgungsbehörden von Nicht-EU-Staaten (z. B. die USA), übermittelt werden dürfen. Neben Grunddaten zur Person, über Reiseverlauf, Buchungs- oder Zahlungsmodalitäten und Sitzplatzinformationen sollen auch andere persönliche Angaben gespeichert werden. Unklar ist, welche Daten unter „allgemeine Hinweise“ gespeichert werden dürfen. Denkbar wäre, dass beispielsweise besondere Essenswünsche erfasst werden.

Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und –Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsdatenspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe „ins Blaue hinein“, also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr sind unzulässig.

Der Vorschlag für den Rahmenbeschluss erfolgte, ohne den Nutzen der erst jüngst in nationales Recht umgesetzten Richtlinie 2004/82/EG<sup>2</sup>, die bereits alle Beförderungsunternehmen verpflichtet, die Daten von Reisenden an die Grenzkontrollbehörden zu übermitteln, auszuwerten. Hinzu kommt, dass der Vorschlag kaum datenschutzrechtliche Sicherungen enthält. Er bezieht sich nur auf eine bisher nicht bestehende und im Entwurf mit Mängeln behaftete EU-Datenschutzregelung. Diese Mängel wirken sich dadurch besonders schwerwiegend aus, dass in den Drittstaaten ein angemessenes Datenschutzniveau nicht immer gewährleistet ist und eine Änderung dieser Situation auch in Zukunft nicht zu erwarten ist.

Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen und des Europäischen Datenschutzbeauftragten sowie der Art. 29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.

---

<sup>2</sup> RL 2004/82 EG v. 29.4.2004 Amtsbl. L 261 (2004) S. 24 ff., Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die Beförderten zu übermitteln

## Anlage 3

**Entschließung**

der 75. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 3./4. April 2008 in Berlin

**Datenschutzförderndes Identitätsmanagement  
statt Personenkennzeichen**

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steueridentifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft“ gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z. B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-

Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.

## Anlage 4

**Entschließung**

der 75. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 3./4. April 2008 in Berlin

**Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet mit Sorge, dass die Datenschutzrechte der Bürgerinnen und Bürger im Rahmen der internationalen Zusammenarbeit der Sicherheitsbehörden immer häufiger auf der Strecke bleiben. Aktuelles Beispiel ist das am 11.3.2008 paraphierte deutsch-amerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität. Die Konferenz fordert Bundestag und Bundesrat auf, dem Abkommen solange nicht zuzustimmen, bis ein angemessener Datenschutz gewährleistet ist.

Mit dem Abkommen wurde ein gegenseitiger Online-Zugriff auf Fundstellendatensätze von daktyloskopischen Daten und DNA-Profilen im hit/no-hit-Verfahren nach dem Muster des Prümer Vertrages vereinbart. Zudem wurden dessen Regelungen über den Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten weitgehend übernommen. Eine Übertragung des als Bedingung für diese umfangreichen Zugriffs und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregimes erfolgte jedoch nicht.

Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terrorismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind, wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Daten-

übermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hintergrund sind die im Abkommen enthaltenen weiten Öffnungsklauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.

## Anlage 5

**Entschließung**

der 75. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 3./4. April 2008 in Berlin

**Mehr Augenmaß bei der Novellierung des BKA-Gesetzes**

Der vom Bundesministerium des Innern erarbeitete Referentenentwurf eines Gesetzes zur Abwehr des internationalen Terrorismus durch das Bundeskriminalamt hat zum Ziel, das Bundeskriminalamt mit umfassenden polizeilichen Befugnissen zur Verhütung von terroristischen Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit in diesem Zusammenhang auszustatten. Insbesondere sind Befugnisse zur Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung vorgesehen. Außerdem will das Bundesinnenministerium eine Befugnis zum heimlichen Zugriff auf informationstechnische Systeme („Online-Durchsuchung“) in das BKA-Gesetz aufnehmen.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diene auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d. h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.

Dem Referentenentwurf zufolge soll die Aufgabenwahrnehmung durch das Bundeskriminalamt die Zuständigkeit der Landespolizeibehörden auf dem Gebiet der Gefahrenabwehr unberührt lassen. Dies führt zu erheblichen datenschutzrechtlichen Problemen, da nach geltendem Recht auch die Länder bei Abwehr einer durch den internationalen Ter-

rorismus begründeten Gefahr parallele Abwehrmaßnahmen ergreifen können. Angesichts der Weite der für das Bundeskriminalamt vorgesehenen und den Landespolizeibehörden bereits eingeräumten Datenerhebungs- und Datenverarbeitungsbefugnisse steht zu befürchten, dass es zu sich überlappenden und in der Summe schwerwiegenderen Eingriffen in das informationelle Selbstbestimmungsrecht Betroffener durch das Bundeskriminalamt und die Landespolizeibehörden kommen wird.

Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z. B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes.

Das Bundesverfassungsgericht hat in seinem Urteil zur „Online-Durchsuchung“ vom 27.02.2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur „Online-Durchsuchung“, sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln.

## Anlage 6

**Entschließung**

der 75. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 3./4. April 2008 in Berlin

**Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern**

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Übermittlung polizeilicher und nachrichtendienstlicher Erkenntnisse an Arbeitgeber zur Überprüfung von Bewerberinnen und Bewerbern, Beschäftigten und Fremdpersonal (z. B. Reinigungskräfte) außerhalb gesetzlicher Grundlagen. In zunehmendem Maß bitten Arbeitgeber die Betroffenen, in eine Anfrage des Arbeitgebers bei der Polizei oder dem Verfassungsschutz zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft („fremdbestimmte Selbstauskunft“) selbst einholen und ihrem Arbeitgeber vorlegen. Eine solche „Einwilligung des Betroffenen“ ist regelmäßig keine wirksame Einwilligung. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes ausgesetzt.

Die gesetzliche Grundentscheidung, in einem „Führungszeugnis“ dem Arbeitgeber nur ganz bestimmte justizielle Informationen zu einer Person verfügbar zu machen, wird dadurch unterlaufen. Es stellt einen Dammbbruch dar, wenn jeder Arbeitgeber durch weitere Informationen direkt oder indirekt an dem Wissen der Sicherheitsbehörden und Nachrichtendienste teilhaben kann. Die Übermittlung dieser Informationen an Arbeitgeber kann auch den vom Bundesarbeitsgericht zum „Fragerecht des Arbeitgebers“ getroffenen Wertentscheidungen widersprechen. Danach darf der Arbeitgeber die Arbeitnehmerinnen und Arbeitnehmer bei der Einstellung nach Vorstrafen und laufenden Ermittlungsverfahren fragen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert.

Polizei und Nachrichtendienste speichern – neben den in ein „Führungszeugnis“ aufzunehmenden Daten – auch personenbezogene Daten, die in

das Bundeszentralregister gar nicht erst eingetragen werden oder Arbeitgebern in einem „Führungszeugnis“ nicht übermittelt werden dürfen. Es stellt eine grundsätzlich unzulässige Durchbrechung des Zweckbindungsgrundsatzes dar, wenn ein Arbeitgeber diese Daten – über den Umweg über die Polizei oder einen Nachrichtendienst – für Zwecke der Personalverwaltung erhält. Dabei ist besonders zu beachten, dass polizeiliche oder nachrichtendienstliche Daten nicht zwingend gesicherte Erkenntnisse sein müssen, sondern oftmals lediglich Verdachtsmomente sind. Die Folgen von Missdeutungen liegen auf der Hand.

## Anlage 7

**Entschließung**

der 75. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 3./4. April 2008 in Berlin

**Vorgaben des Bundesverfassungsgerichts bei der Online-  
Durchsuchung beachten**

1. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.
2. Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer „elektronischen Ausforschung“ schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hiermit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government- und E-Commerce-Verfahren herzustellen.
3. Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.

4. Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste aus.
5. Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.
6. Auch wenn Online-Durchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Online-Durchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenüber steht.
7. Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:
  - Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Art. 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.
  - Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.

- 
- Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.
  - Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.
  - Für die Durchführung von „Quellen-Telekommunikationsüberwachungen“, die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.
8. Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstechnische Systeme, z. B. bei der Überwachung der Telekommunikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.

### **Entschließung**

der 75. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 3./4. April 2008 in Berlin

### **Medienkompetenz und Datenschutzbewusstsein in der jungen „online-Generation“**

1. Die Nutzung moderner Informationssysteme ist auch mit Risiken verbunden. Diese begründen ein besonderes Schutzbedürfnis der Bürgerinnen und Bürger. Dieses verlangt aber nicht nur rechtliche Vorkehrungen und Sicherungen, sondern auch Aufklärung und Information darüber, mit welchen Risiken die Nutzung dieser Informationssysteme verbunden sind. Dies gilt vor allem für die junge „online-Generation“, die in der Altersgruppe der 14- bis 19-Jährigen zu 96 % regelmäßig das Internet nutzt und zwar im Durchschnitt länger als zweieinhalb Stunden täglich.
2. Die Datenschutzbeauftragten des Bundes und der Länder sehen es daher als wichtige Aufgabe an, Kinder und Jugendliche für einen sorgsam und verantwortungsbewussten Umgang mit den eigenen Daten und den Daten anderer zu sensibilisieren. Diese Aufgabe obliegt gesellschaftlichen Einrichtungen ebenso wie staatlichen Organen.

Die Erfahrungen, die anlässlich des 2. Europäischen Datenschutztages am 28. Januar 2008 gemacht wurden, stützen dies. Zu dem Motto "Datenschutz macht Schule" wurde von den Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl von Veranstaltungen und Schulbesuchen organisiert. Eltern, Lehrkräfte, Schülerinnen und Schüler, aber auch Studierende hatten dabei die Möglichkeit, sich z.B. bei Podiumsdiskussionen, Rollenspielen und Workshops über datenschutzrelevante Fragen bei der Nutzung moderner Medien zu informieren. Die dabei gewonnenen Erfahrungen lassen nicht nur einen enormen Informationsbedarf, sondern auch ein großes Informationsinteresse erkennen, und zwar bei allen Beteiligten, bei den Jugendlichen ebenso wie bei ihren Eltern und den Lehrkräften.

Bei den Informationsangeboten, die derzeit den Schulen angeboten werden, um die Medienkompetenz junger Menschen zu verbessern, spielt das Thema „Datenschutz“ aber nur eine untergeordnete Rolle. Es beschränkt sich überwiegend auf Fragen der Datensicherheit und wird zudem häufig von Fragen des Jugendmedienschutzes und des Verbraucherschutzes überlagert.

3. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für notwendig, dass die für die schulische Bildung zuständigen Ministerinnen und Minister der Landesregierungen bei der Förderung der Medienkompetenz von Kindern und Jugendlichen – schon im Grundschulalter - deren Datenschutzbewusstsein stärken. Der Datenschutz muss bei den Angeboten und Projekten zur Förderung der Medienkompetenz eine größere Rolle spielen. Die bisherigen Ansätze reichen bei weitem nicht aus. Gerade bei jungen Menschen muss das Bewusstsein über den Datenschutz als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker gefördert werden.

## **Entschliefungen zwischen den Konferenzen 2007/2008**

### **Entschlossenes Handeln ist das Gebot der Stunde** (Umlaufentschließung/16. September 2008)

Nie haben sich in der jüngeren Geschichte die Skandale um den Missbrauch privater Daten in der Wirtschaft so gehäuft wie heute und damit deutlich gemacht, dass nicht nur im Verhältnis Bürger- Staat das Grundrecht auf informationelle Selbstbestimmung bedroht ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt zuletzt in ihrer Berliner Erklärung vom 4. April dieses Jahres auf die Gefahren hingewiesen, die von massenhaften Datensammlungen privater Unternehmen und ihrer unkontrollierten Nutzung ausgehen. Sie hat auch deshalb den Gesetzgeber zu einer grundlegenden Modernisierung und Verbesserung des Datenschutzrechts aufgefordert und eine neue Datenschutzkultur angemahnt.

Dass jetzt endliche im politischen und gesellschaftlichen Raum die Problematik erkannt und diskutiert wird, ist zu begrüßen. Dabei kann und darf es aber nicht bleiben, nur entschlossenes Handeln kann die Bürgerinnen und Bürger vor weiterem Missbrauch ihrer persönlichen Daten schützen und das verlorene Vertrauen wiederherstellen.

Das vom Grundgesetz garantierte Recht eines Jeden, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden, muss endlich die ihm gebührende Beachtung finden. Die Weitergabe von persönlichen Angaben zu Werbezwecken darf nur mit ausdrücklicher Einwilligung der Betroffenen zulässig sein. Daten sind mit einem Vermerk über ihre Quelle zu kennzeichnen. Der Abschluss von Verträgen darf nicht von einer Einwilligung in die Datenübermittlung zu Werbezwecken abhängig gemacht werden. Verstöße gegen den Datenschutz dürfen nicht ohne Konsequenzen bleiben, sondern müssen strikt geahndet werden. Deshalb müssen die bestehenden Lücken in den Bußgeld- und Strafbestimmungen geschlossen und der Bußgeld- und Strafrahmen für Datenschutzverstöße deutlich erhöht werden. Diese Sofortmaßnahmen, die bereits Gegenstand des Spitzentreffens im Bundesministerium des Innern am 4. September 2008 waren, können vom Deutschen Bundestag noch in den bereits vorliegenden Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes aufgenommen werden.

Gesetzgeberische Maßnahmen allein helfen aber nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht sanktioniert werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, die Datenschutzaufsichtsbehörden endlich organisatorisch, personell und finanziell in die Lage zu versetzen, ihren Beratungs- und Kontrollaufgaben flächendeckend, unabhängig und wirkungsvoll nachkommen zu können, und entsprechend der EU-Datenschutzrichtlinie mit wirksamen Einwirkungsbefugnissen auszustatten, die sie bisher nicht haben.

Außerdem müssen Konzepte zur grundlegenden Modernisierung des Datenschutzes entwickelt und umgesetzt werden. Wichtige Themen sollen dabei noch in dieser Legislaturperiode angegangen werden:

- Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren
- Stärkung der datenschutzrechtlichen Auskunftsrechte
- Pflicht zur Information der betroffenen Personen und der Aufsichtsbehörde bei Datenpannen und missbräuchlicher Datennutzung
- Gewinnabschöpfung aus unbefugtem Datenhandel
- Einführung eines gesetzlich geregelten Datenschutzaudits, mit dem unabhängig und qualifiziert die Datenschutzkonformität von Verfahren und Produkten bestätigt wird
- Stärkung der betrieblichen Datenschutzbeauftragten als Organ der Selbstkontrolle
- Spezialisierung der Strafverfolgungsbehörden
- Anerkennung von Datenschutzbestimmungen als verbraucherschützende Normen

Nur wenn jetzt den Ankündigungen Taten folgen und entschlossen gehandelt wird, können die Bürgerinnen und Bürger künftig vor Datenmissbrauch und Verletzung ihres Grundrechts auf informationelle Selbstbestimmung besser als in der Vergangenheit geschützt werden.

Anlage 10

**Entschließung**

der 76. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 6./7. November 2008 in Bonn

**Mehr Transparenz durch Informationspflichten bei  
Datenschutzpannen**

In den letzten Monaten hat eine Reihe von gravierenden Datenschutzverstößen die Aufmerksamkeit der Öffentlichkeit und der Medien gefunden. In vielen dieser Fälle lag der Verlust oder Missbrauch personenbezogener Daten längere Zeit zurück und war der verantwortlichen Stelle bekannt, ohne dass die Betroffenen oder die zuständige Datenschutzaufsichtsbehörde hierüber informiert worden wären. Dadurch wurde ihnen die Möglichkeit genommen, Sicherheitsmaßnahmen zu ergreifen und mögliche Schäden zu begrenzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt deswegen die Forderung, alle verantwortlichen Stellen - grundsätzlich auch alle öffentlichen Stellen - gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen. Hinter diesem Interesse hat der Wunsch der entsprechenden Stellen zurückzustehen, solche Vorkommnisse geheim zu halten, um keinen Imageschaden oder keine wirtschaftlichen Nachteile zu erleiden.

Etliche Staaten haben bereits entsprechende Regelungen. Eine solche Informationspflicht würde die Transparenz erhöhen und das Vertrauen der Betroffenen in eine korrekte Datenverarbeitung stärken. Darüber hinaus würde sie einen wichtigen Anstoß geben, mehr für Datenschutz und Datensicherheit zu tun.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, entsprechende umfassende Informationspflichten für Unternehmen und öffentliche Stellen im Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zu schaffen. Die übrigen aus Anlass der Datenschutzskandale in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16.09.2008 erläuterten Forderungen zur Novellierung des Bundesdatenschutzgesetzes werden bekräftigt.

**Entschließung**

der 76. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 6./7. November 2008 in Bonn

**Angemessener Datenschutz bei der polizeilichen und justiziellen  
Zusammenarbeit in der EU dringend erforderlich**

Auf europäischer Ebene ist eine Vielzahl von Vorhaben beschlossen bzw. initiiert worden, die in ihrer Gesamtheit zu erheblichen Eingriffen in die Persönlichkeitsrechte führt:

- Die Telekommunikationsunternehmen in den Mitgliedstaaten der EU sind verpflichtet, die bei der Nutzung öffentlich zugänglicher Telekommunikationsdienste anfallenden Verkehrsdaten über das Kommunikationsverhalten der Einzelnen für die Sicherheitsbehörden ohne konkreten Anlass auf Vorrat zu speichern.
- Die Pässe der Bürgerinnen und Bürger der EU-Mitgliedstaaten werden mit biometrischen Merkmalen ausgestattet.
- Fluggastdaten (PNR) werden in die USA übermittelt, um sie den dortigen Behörden zur Verfügung zu stellen. Die Nutzung von Fluggastdaten zu Strafverfolgungszwecken wird auch in der Europäischen Union vorbereitet.
- Der Vertrag von Prüm, der in den Rechtsrahmen der Union überführt wird, ermöglicht den Polizei und Strafverfolgungsbehörden der Mitgliedstaaten einen gegenseitigen Zugriff auf Fingerabdruck, DNA und Kfz-Daten.
- Es soll ein Europäisches Strafregisterinformationssystem geschaffen werden, mit dem Informationen über strafrechtliche Verurteilungen zwischen den Mitgliedstaaten ausgetauscht werden können.

- Das Schengener Informationssystem wird weiter ausgebaut, u.a. durch die Speicherung von biometrischen Merkmalen. Zudem wird der Kreis der Nutzer erweitert um das Europäische Polizeiamt EUROPOL und die Einheit für justizielle Zusammenarbeit in der EU (EUROJUST).
- Ein Europäisches Visa-Informationssystem (VIS) wird eingeführt, um den Austausch von Visa-Daten zwischen den Mitgliedstaaten zu erleichtern. Auch für EUROPOL, die Sicherheitsbehörden und die Nachrichtendienste soll dieser Datenbestand zugänglich sein.
- Das europäische Verfahren EURODAC, in dem die Fingerabdrücke von Asylbewerberinnen und Asylbewerbern gespeichert sind, soll auch von der Polizei und den Strafverfolgungsbehörden genutzt werden können.
- Der Aufgabenbereich von EUROPOL soll über die Bekämpfung der Organisierten Kriminalität hinaus auch auf andere Formen der schweren Kriminalität erweitert werden. Außerdem soll EUROPOL erstmals die Befugnis erhalten, Daten auch von privaten Stellen entgegenzunehmen und Zugriff auf alle polizeilich relevanten Datenbanken in der EU bekommen.
- Der Informationsaustausch zwischen den Strafverfolgungsbehörden der EU wird entsprechend dem Rahmenbeschluss des Rates vom 18. Dezember 2006 („Schwedische Initiative“) ausgebaut. Danach soll der Austausch verfügbarer Daten innerhalb der EU zu den gleichen Bedingungen erfolgen wie nach nationalem Recht.

Neben diesen Vorhaben gibt es zudem Abkommen auf bilateraler Ebene zwischen EU-Mitgliedstaaten und Drittstaaten, wie z.B. das Abkommen der Bundesrepublik Deutschland mit den Vereinigten Staaten für einen erweiterten Informationsaustausch zwischen den Sicherheitsbehörden.

Der Aufbau zentraler Datenbestände und der Ausbau der grenzüberschreitenden Datenübermittlung greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung ein und führen dadurch zu Gefahren für jede Einzelne und jeden Einzelnen. Diese werden noch gesteigert durch die angestrebte Verknüpfbarkeit der bestehenden und geplanten Datenbanken.

Umso wichtiger ist deshalb ein hoher und gleichwertiger Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Europa. Dies wurde von den Datenschutzbeauftragten auf nationaler und europäischer Ebene mehrfach angemahnt. Der hierzu im Oktober 2005 vorgelegte Rahmenbeschluss-Vorschlag genügt diesen Anforderungen nicht (siehe dazu die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 „Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen“). Zur Wahrung des erforderlichen Gleichgewichts zwischen Freiheit und Sicherheit sollten die Parlamente und Regierungen ihre Einflussmöglichkeiten bei europäischen Vorhaben stärker nutzen und dabei auch datenschutzrechtliche Aspekte einbringen. Wie notwendig ein angemessener Datenschutz ist, hat sich beim Verfahren der Aufnahme Verdächtiger in die so genannte EU-Terrorliste gezeigt, das durch den Europäischen Gerichtshof für rechtswidrig erklärt wurde.

Die Datenschutzbeauftragten fordern deshalb:

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

Ein unabhängiges, beratendes Datenschutzgremium sowie eine unabhängige und umfassende datenschutzrechtliche Kontrolle müssen für die

polizeiliche und justizielle Zusammenarbeit eingerichtet bzw. gewährleistet werden.

### **Entschließung**

der 76. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 6./7. November 2008 in Bonn

#### **Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten**

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. „Schwedische Initiative“) vom 18.12.2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der „Schwedischen Initiative“ verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

- 
- Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln.
  - Eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,
  - Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,
  - Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,
  - normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,
  - vollständige Umsetzung der Datenschutzbestimmungen in Art. 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,
  - normenklare Bestimmung welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,

normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.

### **Entschließung**

der 76. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 6./7. November 2008 in Bonn

### **Datenschutzgerechter Zugang zu Geoinformationen**

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potential an volkswirtschaftlichem Nutzen und ist geeignet, vielen E-Government und E-Commerce-Anwendungen die erforderliche Infrastruktur zur Verfügung zu stellen. Als einen ersten Schritt regelt das europäische Recht mit der so genannten INSPIRE-Richtlinie, die bis Mai 2009 in nationales Recht umgesetzt werden muss, die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben auf Grund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer bzw. Standortdaten als personenbezogene Daten zur Verfügung gestellt. Diesem Umstand müssen die gesetzlichen Regelungen gerecht werden und angemessene Datenschutzregelungen enthalten.

Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (BT-Drs. 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das Umweltinformationsgesetz ist nach Ansicht der Konferenzen der Datenschutz und der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb nicht interessengerecht. Ein Geodatenzugangsgesetz muss einen differenzierenden Ausgleich zwischen Informations und Schutzinteressen für die spezielle Problematik der Geobasis und der Geofachdaten

vornehmen. Es ist insbesondere zu berücksichtigen, dass nach der IN-SPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

### **Entschließung**

der 76. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 6./7. November 2008 in Bonn

#### **Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren**

Die Bundesregierung hat am 25.06.2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492). Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an die Zentrale Speicherstelle zu dulden, obwohl zurzeit nicht verlässlich abgeschätzt werden kann, in welchem Umfang die Speicherung der Daten tatsächlich erforderlich ist. Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substantiierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.

Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des *technisch-organisatorischen Datenschutzes* noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

- 
- Es muss sichergestellt werden, (z. B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauftragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.
  - Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.
  - Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver- und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.
  - Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.
  - Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Lösungskonzept muss weiterentwickelt und umgesetzt werden.
  - Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen.
  - Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

### **Entschließung**

der 76. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 6./7. November 2008 in Bonn

#### **Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen**

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100g, 100h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotential in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10.200 (2002) auf 40.000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.

Das Bundesministerium der Justiz hat die Studie erst im Februar dieses Jahres und somit nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung im Gesetz vom 21. Dezember 2007 erforderlich gewesen wäre. Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch die Studie in ihrer schon früher geäußerten Kritik (vgl. ihre Entschließung vom 8./9. März 2007) bestätigt. Sie fordern den Gesetzgeber auf, die gesetzliche Regelung unter folgenden Aspekten nun zügig nachzubessern:

- Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.

- Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.
- Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der StPO vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z. B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.
- Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.
- Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 % der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substantiierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grundrechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen - trotz hoher Belas-

tungen in der Praxis - unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können. Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen.

Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage ist unter den neuen rechtlichen Rahmenbedingungen und aufgrund der Weiterentwicklung der Technik unerlässlich. Insbesondere sollten dabei Notwendigkeit und Nutzen der Verkehrsdatenabfrage auch im Vergleich zu anderen möglichen Maßnahmen mit Blick auf den Verhältnismäßigkeitsgrundsatz auf den Prüfstand gestellt werden.

### **Entschließung**

der 76. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 6./7. November 2008 in Bonn

#### **Adress- und Datenhandel nur mit Einwilligung der Betroffenen**

Der auf dem „Datenschutzgipfel“ im September 2008 gefundene Konsens, den Adress- und Datenhandel zukünftig nur auf der Grundlage einer Einwilligung zuzulassen, ist in Politik und Gesellschaft auf breite Zustimmung gestoßen. Nur eine solche Lösung respektiert das informationelle Selbstbestimmungsrecht und damit die Wahlfreiheit der Verbraucherinnen und Verbraucher. Wer davon jetzt abrücken will, verkennt die auf Grund der jüngsten Datenskandale ans Licht gekommenen Missstände, deren Ursache nicht nur in der kriminellen Energie Einzelner zu suchen ist. Um die Daten der Betroffenen tatsächlich wirksam schützen zu können, muss die Wahlmöglichkeit der Menschen von Maßnahmen flankiert werden, die die Herkunft der Daten jederzeit nachvollziehbar machen.

Die von der Werbewirtschaft gegen die Einwilligungslösung ins Feld geführten Argumente sind nicht überzeugend. Die behaupteten negativen Folgen für den Wirtschaftsstandort sind nicht zu belegen. Unabhängig davon gilt: Es gibt keine schutzwürdigen Interessen für die Beibehaltung von Geschäftsmodellen, die darauf beruhen, hinter dem Rücken und ohne Information der Betroffenen mit deren Daten Handel zu treiben. Die Einführung des Einwilligungsprinzips würde im Gegenteil zielgenaueres und wirksames Direktmarketing erlauben. Die Bundesregierung sollte sich deshalb nicht von ihrer Absicht abbringen lassen, die beim „Datenschutzgipfel“ gegebenen Zusagen zur schnellen Verbesserung des Datenschutzes einzulösen. Sie würde es sonst versäumen, die notwendigen Lehren aus den jüngsten Skandalen zu ziehen. Der Referentenentwurf des Bundesinnenministeriums zur Änderung des Bundesdatenschutzgesetzes im Bereich des Adress- und Datenhandels (Stand: 22.10.2008) zieht mit der Einwilligungslösung – bei aller Verbesserungswürdigkeit im Detail – die einzig richtige und notwendige Konsequenz aus den zahlreichen Datenskandalen und darf nicht verwässert werden.

### **Entschließung**

der 76. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 6./7. November 2008 in Bonn

### **Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten**

Mit der Gesundheitsreform soll über die Einführung von Wettbewerbsmechanismen die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert werden. Die Kassen sind daher bemüht und auch vom Gesetzgeber gehalten, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und strukturierte Behandlungsprogramme für chronisch kranke Versicherte, die jedoch lediglich Angebotscharakter haben dürfen. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Diese Vorgaben werden von einzelnen Krankenkassen nicht beachtet, wenn sie versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen.

Um Teilnehmerinnen und Teilnehmer zu gewinnen und um Maßnahmen durchzuführen, bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutzrechtlich nach dem Sozialgesetzbuch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält die Einhaltung insbesondere der folgenden Eckpunkte bei gesundheitlichen Steuerungsprogrammen der Krankenkassen für unerlässlich:

- Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.

- Die erstmalige Kontaktaufnahme mit potenziell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.
- Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.
- Wenn Versicherte - zu welchem Zeitpunkt auch immer - eindeutig zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.

### **Entschließung**

der 76. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 6./7. November 2008 in Bonn

#### **Elektronische Steuererklärung sicher und datenschutzgerecht gestalten**

Mit dem Steuerbürokratieabbaugesetz (BR-Drs. 547/08) sollen u.a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Abs. 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Abs. 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens anstelle der qualifizierten elektronischen Signatur ein so genanntes anderes sicheres Verfahren im Benehmen mit dem Bundesinnenministerium zuzulassen oder sogar auf beide Verfahren vollständig zu verzichten. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalausweises möglich sein soll.

Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentifizierungs- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronisch übermittelten Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

- 1) Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit alternativlos.
- 2) Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.

Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

### **Entschließung**

der 76. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 6./7. November 2008 in Bonn

### **Gegen Blankettbefugnisse für die Software-Industrie**

Gegenwärtig wird auf europäischer Ebene über Änderungen der Richtlinie zum Datenschutz in der elektronischen Kommunikation (2002/58/EG) beraten. Dabei geht es auch um die Frage, ob in Zukunft einzelfallunabhängig Verkehrsdaten zur Gewährleistung der Netz- und Informationssicherheit, also etwa zur Verfolgung von Hackerangriffen, verarbeitet werden dürfen.

Bereits auf der Grundlage der geltenden Richtlinie erlaubt § 100 Telekommunikationsgesetz den Telekommunikationsdiensteanbietern eine zielgerichtete, einzelfallbezogene Datenverarbeitung zur Fehlerbeseitigung und Missbrauchsbekämpfung. Diese Regelung hat sich in der Praxis bewährt. Es ist daher nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.

Obwohl die Europäische Kommission eine Änderung der bisherigen Rechtslage nicht für erforderlich hält, schlagen mehrere Mitgliedstaaten bei den gegenwärtigen Beratungen im Rat vor, entsprechend den Vorstellungen der Software-Industrie (Business Software Alliance) eine generelle Ermächtigung in die Richtlinie aufzunehmen, wonach „jede natürliche oder juristische Person mit einem berechtigten Interesse“ berechtigt sein soll, Verkehrsdaten zu verarbeiten, um „technische Maßnahmen zur Gewährleistung der Sicherheit eines öffentlichen Telekommunikationsdienstes, eines öffentlichen oder privaten Telekommunikationsnetzes, eines Dienstes der Informationsgesellschaft oder von Endgeräten zu deren Nutzung“ zu ergreifen. Damit wäre nicht nur der jeweilige Diensteanbieter, der Maßnahmen zum Schutz des eigenen Angebots treffen will, zur einzelfallunabhängigen Speicherung von Verkehrsdaten berechtigt, sondern praktisch jeder mit einem wirtschaftlichen Verarbei-

tungsinteresse, insbesondere auch die Hersteller von Sicherheitssoftware.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt eine solche zeitlich unbegrenzte und inhaltlich unbestimmte Blankett-Ermächtigung als inakzeptabel ab. Der Hinweis auf die „Informationssicherheit“ rechtfertigt es nicht, dass Verkehrsdaten nahezu uferlos auch von Dritten verarbeitet werden. Die Bundesregierung wird aufgefordert, einer derartigen Aufweichung des Telekommunikationsgeheimnisses im Rat ihre Zustimmung zu verweigern.

## **Entschließungen zwischen den Konferenzen 2009**

### **Stärkung der IT-Sicherheit – aber nicht zu Lasten des Datenschutzes!**

(Entschließung zum BSI-Gesetzesentwurf vom 18.02.2009)

Das Bundeskabinett hat am 14. Januar 2009 den Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes beschlossen (BR-Drs. 62/09). Mit dem Gesetz sollen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) umfassende Befugnisse eingeräumt werden, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Weiter sollen aber zugleich auch das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG) geändert werden.

Angriffe auf die IT-Sicherheit können nicht nur die ordnungsgemäße Abwicklung von Verwaltungsaufgaben beeinträchtigen, sondern auch Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger mit sich bringen. Daher sind Konzepte zu entwickeln und umzusetzen, die sowohl die IT-Sicherheit stärken als auch den Schutz der Privatsphäre gewährleisten.

In weiten Bereichen wurden in der jüngsten Vergangenheit Maßnahmen zur Stärkung der IT-Sicherheit getroffen, die eine detaillierte Registrierung und Auswertung des Nutzerverhaltens und sogar der Inhalte der Kommunikation ermöglichen. Entsprechende Ansätze gibt es nun auch in der Bundesverwaltung. So sieht der Gesetzesentwurf vor, dem BSI sehr weitgehende Befugnisse einzuräumen. Kritisch sind insbesondere

1. die Ermächtigung des BSI, die gesamte Sprach- und Datenkommunikation aller Unternehmen, Bürgerinnen und Bürger mit Bundesbehörden ohne Anonymisierung bzw. Pseudonymisierung zu überwachen und auszuwerten (§ 5),
2. die vorgesehene Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen werden (§ 5 Abs. 4) und
3. die fehlende Verpflichtung des BSI, Informationen über ihm

bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Unternehmen, Bürgerinnen und Bürger vor zu (erwartenden) Angriffen (Spionage und Sabotage) zu warnen (§ 7).

Äußerst bedenklich ist darüber hinaus die Regelung, dass im Zweifelsfall allein das Bundesministerium des Innern entscheiden darf, ob Daten dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind und wie damit weiter zu verfahren ist (§ 5 Abs. 6). In solchen Zweifelsfällen sollten diese Daten gelöscht oder einem Richter zur Entscheidung vorgelegt werden.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen zwar grundsätzlich alle Aktivitäten, in den gewachsenen, vernetzten IT-Strukturen des Bundes das Niveau der IT-Sicherheit zu erhöhen. Sie fordern aber auch, dass die zur Risikobegrenzung eingeführten Maßnahmen nicht den Datenschutz der Nutzerinnen und Nutzer beeinträchtigen. Deshalb ist schon bei der Konzeption von IT-Sicherheitsmaßnahmen vorzusehen, dass das erforderliche Sicherheitsniveau nur mit datenschutzgerechten Lösungen gewährleistet wird. Die Datenschutzbeauftragten fordern strengere Sicherheitsstandards und soweit möglich die Protokoll- und Inhaltsdaten vor der Auswertung durch das BSI zu anonymisieren bzw. zu pseudonymisieren. Damit ließen sich eine unnötige Registrierung des Nutzerverhaltens und Überwachung von Kommunikationsinhalten vermeiden. Die Auswertung der Daten durch das BSI muss reversionssicher ausgestaltet werden. Der vorgelegte Gesetzentwurf enthält keine solchen Regelungen.

Die Gesetzesänderung des Telemediengesetzes böte öffentlichen und privaten Anbietern von Telemedien die Möglichkeit einer umfassenden Protokollierung des Surfverhaltens ihrer Nutzer im Internet, da sie entsprechend der Gesetzesbegründung weit auslegbar ist. Der Gesetzgeber muss unmissverständlich klarstellen, dass die Erhebung und Auswertung personenbezogener Daten ultima ratio ist.

Sowohl die Betreiber der „Netze des Bundes“ als auch die Verantwortlichen für die übergreifenden Netze der Verwaltung in Europa sind aufgefordert, bei allen Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und den Datenschutz der Nutzerinnen und Nutzer zu gewährleisten.

### **Entschließung**

der 77. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 26./27. März 2009 in Berlin

#### **Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz**

Datenskandale der letzten Zeit haben deutlich gemacht, dass bei der Verarbeitung von Beschäftigtendaten weder Transparenz noch Rechtssicherheit besteht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, nach jahrelanger Untätigkeit jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen.

Ziel des neuen Beschäftigtendatenschutzgesetzes muss sein, Rechtssicherheit herzustellen, Regelungslücken zu schließen und bereits vorhandene Regelungsaspekte sowie Vorgaben der Rechtsprechung in einem Spezialgesetz zusammenzufassen. Die Konferenz der Datenschutzbeauftragten hält deshalb vor allem folgende Eckpunkte für unverzichtbar:

- Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.
- Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festlegungen im Hinblick auf Gesundheitsdaten (u. a. zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen, etc.)
- Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z. B. der Innenrevision auf erhobene Personaldaten bedarf enger gesetzlicher Vorgaben.
- Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da die Nutzung von Telefon, Internet und

E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kommunikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand ggf. Dritte (z. B. Mitarbeitervertretungen oder Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.

- Der Einsatz von Überwachungssystemen, wie z. B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.
- Es bedarf der Festlegung der Rechte der Beschäftigten, z. B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.
- Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.
- Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.
- Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch erworbenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

### **Entschließung**

der 77. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 26./27. März 2009 in Berlin

#### **Defizite beim Datenschutz jetzt beseitigen**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Deutschland auf, endlich die nötigen Konsequenzen aus den nicht mehr abreißenden Datenskandalen zu ziehen. Dazu sind mindestens folgende Schritte geboten:

1. Der Deutsche Bundestag wird aufgefordert, noch in dieser Legislaturperiode die von der Bundesregierung vorgelegten Gesetzentwürfe für erste notwendige Korrekturen des Bundesdatenschutzgesetzes im Bereich der Auskunfteien und des Adresshandels zu verabschieden. Ansonsten verlieren die Bürgerinnen und Bürger das Vertrauen in die Zusagen der Bundesregierung nach den Skandalen des Jahres 2008. Insbesondere mit Adressen darf nur noch mit ausdrücklicher Einwilligung der Betroffenen Handel getrieben werden. Der Entwurf für ein Datenschutzauditgesetz muss gründlich überarbeitet werden, damit dieser notwendige Schritt hin zu einem modernen Datenschutzrecht von der Praxis auch umgesetzt werden kann.
2. Mit Beginn der nächsten Legislaturperiode muss endlich eine grundlegende Modernisierung des Datenschutzrechts in Angriff genommen werden, die bereits zu lange aufgeschoben wurde. Nur so kann das Datenschutzrecht den Herausforderungen der Informationsgesellschaft zu Beginn des 21. Jahrhunderts gerecht werden.
3. Der Einsatz datenschutzfreundlicher Technik muss vorangetrieben und rechtlich verpflichtend vorgeschrieben werden. Darin liegt auch eine Chance für den Wirtschaftsstandort Deutschland in Zeiten der Krise.

Anlage 23

**Entschließung**

der 77. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 26./27. März 2009 in Berlin

**Die polizeiliche Datenverarbeitung in INPOL hat keine Rechts-  
grundlage**

Die Speicherung von Daten im polizeilichen Informationssystem INPOL durch die Polizeien des Bundes und der Länder ist nur dann rechtmäßig, wenn eine Rechtsverordnung gemäß § 7 Abs. 6 Bundeskriminalamtsgesetz das Nähere über die Art der Daten bestimmt, die in dieser Datei gespeichert werden dürfen. Eine solche Rechtsverordnung existiert nicht. Mit Urteil vom 16. Dezember 2008 (Az. 11 LC 229/08) hat das Niedersächsische Obergericht dies in Bezug auf die Verbunddatei „Gewalttäter Sport“ bekräftigt. Das Urteil ist nicht nur für die Rechtmäßigkeit der Hooligan-Datei bedeutsam, sondern hat Auswirkung auf alle im Rahmen von INPOL geführten Verbunddateien.

Mit der Entscheidung des Gerichts wird die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt. Die vom Bundesministerium des Innern bisher vertretene Auffassung, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, wird durch die einschlägigen Regelungen nicht gestützt.

## Anlage 24

**Entschließung**

der 77. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 26./27. März 2009 in Berlin

**Auskunftsanspruch der Steuerpflichtigen  
im Besteuerungsverfahren gewährleisten!**

Das Bundesministerium der Finanzen (BMF) hat mit einer einfachen Verwaltungsanweisung den Auskunftsanspruch der Bürgerinnen und Bürger im Besteuerungsverfahren weitgehend eingeschränkt. Es macht die Auskunftserteilung von einem „berechtigten Interesse“ abhängig, was zu einer Einschränkung des Auskunftsrechts führt.

Die Vorgehensweise des BMF steht im krassen Widerspruch zum Beschluss des Bundesverfassungsgerichts vom 10. März 2008 (1 BvR 2388/03). Danach sind auch von der Finanzverwaltung die Grundrechte auf informationelle Selbstbestimmung und auf effektiven Rechtsschutz zu gewährleisten. Der in § 19 Bundesdatenschutzgesetz (BDSG) verankerte umfassende Auskunftsanspruch findet auch im Besteuerungsverfahren unmittelbare Anwendung.

Es ist inakzeptabel, dass verfassungsrechtlich garantierte Auskunftsrechte der Steuerpflichtigen ausgehebelt werden. Auch die Finanzverwaltung ist an Recht und Gesetz gebunden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

## Anlage 25

**Entschließungen zwischen den Konferenzen 2009****Datenschutz beim vorgesehenen Bürgerportal unzureichend**

(Entschließung vom 16. 04. 2009)

Der Gesetzentwurf zur Regelung von Bürgerportalen (BR-Drs. 174/09) soll rechtliche Rahmenbedingungen für eine sichere und vertrauenswürdige elektronische Kommunikation zwischen Bürgerinnen und Bürgern und der Wirtschaft und Verwaltung im Internet schaffen. Private Anbieter sollen die Portale betreiben, über die der sichere E-Mail-Verkehr De-Mail, eine sichere Dokumentenablage De-Safe und ein Identitätsbescheinigungsdienst abgewickelt werden sollen. Eine solche Infrastruktur stellt hohe Anforderungen an die IT-Sicherheit und den Datenschutz.

Der Gesetzentwurf wird diesen Anforderungen noch nicht gerecht und ist zumindest in folgenden Punkten zu korrigieren:

- Der Entwurf sieht vor, dass nur akkreditierte Anbieter Portale betreiben dürfen. Voraussetzung für die Akkreditierung darf nicht allein der Nachweis der technischen und administrativen Sicherheit, sondern muss auch die tatsächliche Einhaltung datenschutzrechtlicher Standards sein. Die dabei zu erfüllenden Mindestanforderungen müssen verbindlich im Gesetz vorgegeben werden. Portalbetreiber sollten zudem erst dann die Akkreditierung erhalten, wenn die Umsetzung dieser Anforderungen durch unabhängige Prüfstellen bescheinigt wurde.
- Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Dienst-Anbietern und durch die Sicherung des Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte gelesen oder verändert werden können. Deshalb muss die Kommunikation standardmäßig durch eine Ende-zu-Ende-Verschlüsselung zwischen Absendenden und Empfangenden nach dem Stand der Technik gesichert und nicht nur als Option angeboten werden.

- Das Bürgerportal soll gerade zwischen Bürgerinnen und Bürgern und Verwaltung eine rechtlich gesicherte Kommunikation ermöglichen. Insbesondere sind über das Bürgerportal förmliche Zustellungen mit den entsprechenden Rechtsfolgen beabsichtigt. Dies darf nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort wird abgelehnt.
- Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. Das ermöglicht Angriffe durch Schadsoftware auf dem Rechner der Nutzenden. So könnten Zugangsdaten beschafft und widerrechtlich dazu verwendet werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern oder unberechtigt auf Daten im De-Safe zuzugreifen. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen.
- Die Möglichkeit, eine pseudonyme Bürgerportaladresse zu nutzen, muss – entgegen der Stellungnahme des Bundesrates vom 3.4.2009 – erhalten bleiben. Denn die pseudonyme Nutzung ermöglicht gerade einen sinnvollen Kompromiss zwischen hinreichender Identifizierbarkeit im Rechtsverkehr und Datenschutz für die Nutzerinnen und Nutzer.
- Die Nutzerinnen und Nutzer müssen bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen – etwa zur verbindlichen Kommunikation mit staatlichen Stellen - hingewiesen werden. Die Aufklärungs- und Informationspflichten müssen im Gesetzestext klarer als bislang geschehen gefasst werden. Gleiches gilt für die Feststellung von Identitätsdaten und der Aufdeckung von Pseudonymen.
- Eine Benachteiligung von Bürgerinnen und Bürgern, die über kein Bürgerportalkonto verfügen, muss ausgeschlossen werden. Auch dürfen Bürgerportale nicht dazu führen, dass staatliche Stellen dazu übergehen, bei jeder Inanspruchnahme einer E-Government-Anwendung eine persönliche Identifizierung zu verlangen, selbst wenn dies für die konkrete Dienstleistung nicht erforderlich ist.

- Der Entwurf sieht vor, dass grundsätzliche Fragen der technischen Ausgestaltung der Bürgerportale und der darüber angebotenen Dienste in einer Rechtsverordnung geregelt werden sollen. Dies widerspricht der Rahmenkonzeption des Art. 80 GG und dient auch sonst nicht der Normenklarheit des Gesetzes. Zumindest die grundsätzlichen technisch-organisatorischen Anforderungen an die Eröffnung des Kontos, den Postfach- und Versanddienst, den Speicherplatz, den Identitätsbescheinigungsdienst und das Akkreditierungsverfahren sollten in das Gesetz selbst aufgenommen werden.
- Der Entwurf des Bürgerportalgesetzes sieht jetzt auch vor, dass nicht nur die Datenerhebung, sondern auch die Verarbeitung und Nutzung der erhobenen Daten durch den akkreditierten Dienstanbieter an eine enge Zweckbestimmung gebunden ist. Allerdings ist der pauschale Verweis auf die Regelungen des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes in diesem Zusammenhang zu weitgehend, da so für die Dienste-Anbieter die Möglichkeit eröffnet wird, die personenbezogenen Daten für Werbung oder Marktforschungszwecke zu nutzen. Die Bürgerinnen und Bürger müssen jedoch sicher sein können, dass ihre Daten ausschließlich zur Teilnahme am Bürgerportal genutzt werden.

### **Entschließung**

der 78. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 8./9. Oktober 2009 in Berlin

#### **Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur**

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

- Das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z. B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;
- die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;
- ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;

- die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;
- die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;
- auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z. B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;
- im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;
- die Videoüberwachung in Staat und Gesellschaft einzuschränken;
- den Schutz der Meldedaten zu verbessern;
- ein praktikables Datenschutzaudit zu schaffen;
- die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

## Anlage 27

**Entschließung**

der 78. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 8./9. Oktober 2009 in Berlin

**Datenschutzdefizite in Europa auch nach Stockholmer Programm**

Die Europäische Union will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem „Europa der Bürger“. Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von zum Teil äußerst eingriffsintensiven Maßnahmen, wie z. B. ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

- Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.
- Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.
- Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.
- Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.
- Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen - auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL und EUROJUST - im weiteren Verfahren einzusetzen.

## Anlage 28

**Entschließung**

der 78. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 8./9. Oktober 2009 in Berlin

**Krankenhausinformationssysteme datenschutzgerecht gestalten!**

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.

Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.

Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechend Systeme anzubieten.

### **Entschließung**

der 77. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 8./9. Oktober 2009 in Berlin

### **Staatsvertrag zum IT-Planungsrat – Datenschutz darf nicht auf der Strecke bleiben**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die informationstechnische Kooperation von Bundes- und Landesbehörden zunehmend die Verarbeitung von personenbezogenen Daten betrifft, die durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen sind, etwa durch wirksame Verschlüsselungsverfahren.

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen.

Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrats teilnehmen soll. Sie hält es für geboten, auch die Landesdatenschutzbeauftragten einzubeziehen.

Anlage 30

### **Entschließung**

der 78. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 8./9. Oktober 2009 in Berlin

#### **"Reality-TV" – keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen**

"Reality-TV"-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige "Lieferanten" für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen Haftbefehl gegen einen Schuldner zu vollziehen - wobei auch schon einmal eine Wohnung zwangsgeöffnet wird - oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mitverfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleibt oder gar ausfällig werden. Aufgrund des Erfolgs derartiger "Unterhaltungssendungen" ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

Presse- und Öffentlichkeitsarbeit sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und den Informationsanspruch der Öffentlichkeit zu erfüllen. Dabei muss aber das Persönlichkeitsrecht der Betroffenen gewahrt werden, gerade wenn Unterhaltung und Befriedigung von Sensationslust im Vordergrund stehen.

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen

wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb alle Behörden auf, grundsätzlich von der Mitwirkung an solchen "Reality" Reportagen Abstand zu nehmen.

### **Entschließung**

der 78. Konferenz der Datenschutzbeauftragten  
des Bundes und der Länder  
am 8./9. Oktober 2009 in Berlin

#### **Kein Ausverkauf von europäischen Finanzdaten an die USA!**

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglichkeiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungen wegen verwehrt sind.

Ein derartiger weit reichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachts wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig. Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängige Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

## Abkürzungsverzeichnis

<b>Abkürz.</b>	<b>Bedeutung</b>
AEUV	Vertrag über Arbeitsweise der Europäischen Union
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaft
ATDG	Antiterrordateigesetz
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BeamStG	Beamtenstatusgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BMF	Bundesministerium für Finanzen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
CN	Corporate Network
CPU	Central Processing Unit
DIN	Deutsches Institut für Normung
DNA	deoxyribonucleic acid
DuD	Datenschutz und Datensicherheit
EG	Europäische Gemeinschaft
eGovernment	electronic Government
EiCoNeD	Einkauf Corporate Network und Dienste
eID	Identität elektronisch
ELENA	elektronischer Entgeltnachweis
E-Mail	Elektronic-Mail (elektronische Post)
ePass	elektronischer Pass
EU	Europäische Union

---

EuGH	Europäischer Gerichtshof
GG	Grundgesetz
HAMASYS	Haushaltsmanagementsystem
INPOL	Informationssystem der Polizei
ISDN	Integrated Services Digital Network
ISO	Internationale Organisation für Normung
IT	Informationstechnik
IuK	Informations- und Kommunikationstechnik
Kfz	Kraftfahrzeug
KIS	Krankenhausinformationssystem
LFD	Thüringer Landesfinanzdirektion
LRA	Landratsamt
LSG	Landessozialgericht
nPA	neuer Personalausweis
OWiG	Gesetz über Ordnungswidrigkeiten
PAG	Polizeiaufgabengesetz
PAuswG	Personalausweisgesetz
PC	Personal Computer
PIN	Persönliche Identifikationsnummer
SAGA	Standards und Architekturen für E-Government-Anwendungen
SGB	Sozialgesetzbuch
SG	Sozialgericht
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TB	Tätigkeitsbericht
TFM	Thüringer Finanzministerium
ThEA	Thüringer Erfassungs- und Antragsystem
ThILLM	Thüringer Institut für Lehrplanentwicklung, Lehrerfortbildung und Medien
ThürBAG	Thüringer Berufsakademiegesetz
ThürBG	Thüringer Beamtengesetz
ThürDSG	Thüringer Datenschutzgesetz
ThürGDIG	Thüringer Geodateninformationssystem
ThürJStVollzG	Thüringer Jugendstrafvollzugsgesetz
ThürKO	Thüringer Kommunalordnung

---

ThürMeldeG	Thüringer Meldegesetz
ThürMeldeVO	Thüringer Meldeverordnung
ThürOBG	Thüringer Ordnungsbehördengesetz
ThürPersVG	Thüringer Personalvertretungsgesetz
ThürSchulG	Thüringer Schulgesetz
ThürSÜG	Thüringer Sicherheitsüberprüfungsgesetz
ThürVerf	Verfassung des Freistaates Thüringen
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
TIZIAN	Thüringer Initiative zur Integration und Armuts- bekämpfung - Nachhaltigkeit
TIM	Thüringer Innenministerium
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TLfD	Thüringer Landesbeauftragter für den Daten- schutz
TLfV	Thüringer Landesamt für Verfassungsschutz
TLKA	Thüringer Landeskriminalamt
TLRZ	Thüringer Landesrechenzentrum
TMBV	Thüringer Ministerium für Bau und Verkehr
TMBWK	Thüringer Ministerium für Bildung, Wissen- schaft und Kultur
TMG	Telemediengesetz
TMSFG	Thüringer Ministerium für Soziales, Familie und Gesundheit
USB	Universal Serial Bus
VG	Verwaltungsgemeinschaft
VIS	Visa-Informationssystem
ZensG	Zensusgesetz
ZEVIS	Zentrales Verkehrsinformationssystem beim Kraftfahrtbundesamt

## Sachregister

Abfallsatzung	5.16
Abfallwirtschaftsgesellschaft	5.16
Abwasserzweckverband	5.13
Akteneinsicht	5.15
Alleinerziehende	11.3
Anti-Terror-Datei	8.1
Arbeitnehmerdatenschutz	6.1
Arbeitskreis Schule/Bildung	13.1
	11.3; 11.5;
ARGE	11.1
Arztgeheimnis	5.17
Asylbewerberunterkunft	5.11
Aufenthaltsstatus	5.12
Aufsichtsbehörde	5.10
Auftragsdatenverarbeitung	2; 5.1; 5.11;
	12.3; 15.2
Auskunftsrecht	5.5
Ausländerbehörde	5.12
Außendienst	11.1
Authentifizierung	9.2
Authentisierung	14.2
<b>Bankverbindung</b>	9.4
Bauantrag	5.3
Beanstandung	1.; 5.1; 5.3;
	5.10; 5.13;
	6.2; 6.5; 11.5;
	13.4
	11.3; 11.5;
Bedarfsgemeinschaft	11.1
Behördeninterner Datenschutzbeauftragter	5.1
Benachteiligungsverbot	6.5
Berechnungsunterlagen	5.15
berechtigtes Interesse	9.5
Beschäftigtendatenschutz	6.1

Bestimmtheitsgrundsatz	5.7; 5.13
Beweis	7.6; 7.7; 11.5
Beweislastumkehr	11.1
Bildauflösung	12.1
Biometrie	14.2
BlackBerry	15.4
Briefumschlag	5.14
BSI-Gesetz	14.6
Bücherfrage	13.3
Buchung	9.4
Bundesagentur für Arbeit	11.1
Bundeskriminalamt	7.2
Bürgerportalgesetz	4.2
Cloud Computing	14.7
Coaching	11.5
Corporate Network (CN)	15.2
	7.6; 9.2; 9.4;
Datenbank	12.1
Datenentsorgung	5.11
Datenerhebung	5.7; 5.16
Datenmissbrauch	2.; 6.4; 7.6
Datenschutz und Kinderschutz	11.4
Datenschutzabkommen	3.2
Datenschutzaudit	2.
Datenschutzbewusstsein	13.1; 13.2
Datensicherheit	13.2
Datenskandal	2.
Datenübermittlung	5.10; 9.2; 5.5
De-Mail	4.2
Detektei	11.5
Deutschland-Online	12.2
	5.2; 5.6; 6.4;
Dienstanweisung	9.6
DNA-Analyse	7.3
Doktorgrad	5.10

Dritte Säule	3.3
<b>EiCoNeD</b>	15.2
Einheitliche Stelle (ES)	15.1
Einkommenssteuer	9.7
Einwilligung	5.3; 5.8; 5.16; 7.4; 9.2; 9.7; 11.6; 12.4; 12.5; 13.3; 13.4
Elektronischer Personalausweis	9.2
Elektronische Signatur	9.2
Eltern	13.4; 13.3
Energiewirtschaftsgesetz	12.4
ePass	5.9
Ermittlungsfreiheit	11.5
Erschließungsträger	5.6
Ersterhebung beim Betroffenen	11.5
EU-Dienstleistungsrichtlinie	15.1
Europäischer Datenschutztag	13.1
Europäischer Gerichtshof für Menschenrechte	11.7
<b>Fahrerermittlung</b>	7.7
Finanzamt	9.7; 9.5; 9.6
Firewall	14.6
Flugpassagierdaten	3.1
Fragebogen	9.6; 5.16
Freiwilligkeit	5.3; 5.9; 7.3; 13.3; 13.4
Fremdenverkehrsabgabe	5.7
Funkzellenabfrage	7.3
<b>Gasliefervertrag</b>	12.3
Geburtenstation	11.6
Gemeindeblatt	5.3
Gemeinderatsbeschlüsse	5.5
Gemeinderatssitzung	5.3

Gemeinsame Empfehlung	11.4
Geoproxy	12.1
Geschäftsordnung	5.4
Grunderwerb	9.6
Grundrechtseingriff	5.2
Grundstückseigentümer	5.13; 5.15
Grundstückskaufvertrag	5.6
<b>HAMASYS</b>	9.2
Hausbesuch	11.1
Hochschule	5.12
<b>Identifikation</b>	11.6
Identität	5.8; 5.9
Identitätsmanagement	14.1
INPOL	7.5
Inspire-Richtlinie	12.1
Integrität	9.2
Intelligente Stromzähler	12.4
Internet	1.; 2.; 5.3; 6.4; 12.2; 12.4; 13.1; 14.1; 14.6; 14.8; 15.2; 15.3
IT-Grundrecht	2.
<b>Jugendamt</b>	11.3
Jugendliche	13.1
Justizzahlstelle	10.3
<b>Kennzeichenerkennungssystem</b>	7.1
Kernbereich privater Lebensführung	7.1
Kfz-Kennzeichnung	12.2
Kinderschutz	11.4
Kommunalkontrolle	5.1
Kompetenztest	13.3
Kontrollrecht des TLfD	5.17

Kooperation	11.4
Krankenhaus	11.7; 11.6
Krankenhausinformationssystem	11.7
Krankmeldung	6.2
Kreisausschuss	5.10
Kündigung	6.5
Landratsamt	5.11; 5.13
Lebenslauf	13.5
Lehrerfortbildung	13.2
Lichtbildabgleich	7.7
Löschung	7.3; 7.6; 9.6; 10.3; 10.5; 11.2; 11.5
Luftbilder	12.1
Medienkompetenz	13.1; 13.2
Meldebehörde	5.10
Menschenrecht auf Achtung des Privatlebens	11.7
Mitarbeiterüberwachung	6.2; 6.4
Modernisierungsbedarf	2.
Mülltonnennutzung	5.16
Multiplikatoren	13.2
Neuer Personalausweis	5.9
Niederschlagswassergebühren	5.13
Niederschrift	5.4
Notarztprotokoll	5.17
Observation	6.2; 11.5
Öffentliche Sicherheit und Ordnung	5.2
Online-Durchsuchung	2.; 7.2
Online-Melderegisterauskunft	5.8
Online-Petition	2
Ordnungsbehörde	5.2

<b>Patientenarmband</b>	11.6
Patientendaten	11.7
Personalakten	6.3
Personalausweis	5.9
Personalrat	6.4; 14.4 5.4; 6.4; 12.1;
Persönlichkeitsrecht	12.5
Polizeirechtsnovelle	7.1
Postzustellung	5.14
Presseauskünfte	5.10
Private Nutzung	9.7
Privater Betreiber	5.11
Privatrechtliche Verträge	5.5
Profiling	11.5
Projekt- und Produktivbetrieb	14.5
Projektträger	11.3
Protokollierung	8.1; 14.4; 7.6
<b>Quellen-TKÜ</b>	7.1
<b>RFID-Chip</b>	11.6
<b>SAGA</b>	14.1
Sanierungsträger	5.6
Satzung	5.7; 5.13; 5.6
Schulamts	13.4; 6.3
Schülerbefragung	13.4
Schuluntersuchungen	13.4
Schwedische Initiative	3.3
Sicherheitskonzept	5.1
Sicherheitsüberprüfung	8.2
Sitzungsprotokoll	5.4
Softwarehersteller	11.7
Sozialdaten	11.3; 11.5
Sozialgericht	11.5
Sparkasse	9.7

---

Stadtratsbeschluss	5.6
Strafverfahren	5.10
Steuerdaten	9.5
Steuergeheimnis	9.5
Steuerverfahren	9.5
Stockholmer Programm	3.5
Strafantrag	7.6
Strafverfolgung	5.2
Straßenausbaubeitrag	5.15
Strichcode	11.6
Telekommunikationsüberwachung	7.3
Telekommunikations-Verkehrsdaten	10.3
Terrorismusbekämpfung	3.1
ThEA	15.1
Thüringer Jugendmonitor	13.3
TIZIAN	11.3
Transparenzgebot	9.6
Umsatz	5.7
Verbunddatei	2.; 7.5
Verfahrensfreigabe	5.1
Verfahrensverzeichnis	5.1
Verkehrsdaten	4.1
Verkehrsordnungswidrigkeiten	7.7
Versteigerung	9.8
Vertrag von Lissabon	3.3
Vertragsklausel	9.9
Vertragsverletzungsverfahren	2.
Videoclip	5.3
Videüberwachung	12.5; 10.1; 5.2
Viren	14.8
VoIP	15.2
Vollstreckung	9.8; 10.5
Vorkaufsrecht	5.6

---

---

Vorratsdatenspeicherung	5.13; 4.1; 10.3
VS-Clean	9.8
<b>Web 2.0</b>	2.
WEB-Access	15.3
Webanalytics	15.3
Webcam	5.2
Werbeverbot	9.9
Widerspruchsrecht	13.4; 9.4
Widerspruchsverfahren	5.15
Wohnanschrift	5.14
Wohngebäude	12.5
Wohngemeinschaft	11.1
Wohnungsgesellschaft	12.5
Wortprotokoll	5.4
<b>Zensus, registergestützter</b>	2.
Zentrale Stelle	9.2
ZEVIS-Abfrage	7.6
Zugriffsrecht	9.4
Zuverlässigkeitsprüfungen	7.4

## Thüringer Landesbeauftragter für den Datenschutz (TLfD)

