Der Landesbeauftragte
für Datenschutz und Informationsfreiheit
im Saarland

22. Tätigkeitsbericht

2007 /2008

22. Tätigkeitsbericht
des

Landesbeauftragten
für Datenschutz und Informationsfreiheit

für die Jahre 2007 und 2008

Der Landesbeauftragte
für Datenschutz und Informationsfreiheit Saarland
Roland Lorenz

Fritz-Dobisch-Str. 12, 66111 Saarbrücken
Postfach 10 26 31, 66026 Saarbrücken
Tel.: 0681/94781-0, Fax: 0681/94781-29
E-Mail-Adresse: poststelle@lfdi.saarland.de
Internet-Angebot unter www.lfdi.saarland.de

Saarbrücken im September 2009

Geleitwort

Auch in diesem Berichtszeitraum bin ich in meiner täglichen Arbeit von Vielen in vielerlei Hinsicht begleitet und unterstützt worden. Mein Dank gilt zunächst allen Abgeordneten des Saarländischen Landtages. Er gilt auch und ganz besonders dem Präsidenten des Saarländischen Landtages, der meine Tätigkeit stets mit Interesse und besonderem Wohlwollen verfolgt hat. Auch allen öffentlichen Stellen und allen Privaten, die Interesse am Datenschutz und an der Arbeit meiner Geschäftsstelle gezeigt haben, die meinen fachlichen Rat gesucht haben oder die meine Tätigkeit gefördert haben, bin ich zutiefst verbunden. Nicht verhehlen will ich, dass es mich ganz besonders motiviert und beflügelt hat, dass dort wo Meinungsunterschiede und divergierende Positionen vorhanden waren, gleichwohl regelmäßig Achtung für meine Aufgaben und meine datenschutzrechtlichen Positionen gezeigt wurde. Nicht vergessen will ich bei meinem Dank die Mitarbeiter und Mitarbeiterinnen meiner Geschäftsstelle, ohne deren Einsatz meine Arbeit und die Legung dieses Berichts nicht möglich wären.

In meinem letzten Bericht hatte ich übrigens darauf hingewiesen, dass die Grenzen der Belastbarkeit meiner Geschäftsstelle bald erreicht sein würden. Nunmehr sind diese Grenzen teilweise schon überschritten. Dies beruht auf der Übertragung der Aufgabe eines Informationsfreiheitsbeauftragten ohne jegliche Personalverstärkung. Dies beruht aber auch auf den zahlreichen Gesetzesvorhaben und datenschutzrechtlichen Regelungen, die im Berichtszeitraum in Angriff genommen wurden, aber auch auf den zahlreichen Datenschutzskandalen, die einerseits durch Aufzeigen der datenschutzrechtlichen Probleme zu einer weiter steigenden Anzahl der Eingaben der Bürgerinnen und Bürger geführt haben, andererseits aber auch eine Intensivierung der Aufklärungs- und der Öffentlichkeitsarbeit aber auch der Kontrolltätigkeit bedingt haben.

Mir erscheint es jedenfalls am Ende des Berichtszeitraumes und fast am Ende meiner laufenden Amtsperiode klar, offenkundig und zwingend, dass soweit tatsächlich die von den Bürgern und Bürgerinnen erwartete Arbeit im Datenschutz geleistet werden soll, die Implementierung des Datenschutzes sich nicht in Sonntagsreden und gut gemeinten Absichtserklärungen erschöpfen kann. Ich appelliere daher an den

Gesetzgeber und an die politisch Verantwortlichen im Lande durch gesetzgeberische, aber auch durch haushalterische Maßnahmen, die objektiven Rahmenbedingungen für einen effektiven und erfolgreichen Datenschutz im Saarland zu verstärken und sich dabei allein von sachlichen Überlegungen leiten zu lassen.

Inhaltsverzeichnis

1 Vorbemerkung

Online-Durchsuchung, Vorratsdatenspeicherung, Automatische Kfz-Kennzeichenerfassung. etc… etc…pp… Gesetzgeberische Projekte im öffentlichen Bereich, die Teile der Öffentlichkeit zutiefst verunsichern, haben auch im Berichtszeitraum nicht abgenommen. Deutsche Bahn, Telekom, Lidl, KiK, Deutsche Bank, etc…etc…pp… Dazu immer wieder neue Datenschutzskandale im privaten Bereich.

Die Kumulierung der gesetzgeberischen Maßnahmen mit einer Vielzahl von Datenschutzskandalen hat das Interesse und das Bewusstsein der Bevölkerung (dies ist also und insbesondere auch der Wählerinnen und Wähler) für den Datenschutz wiederbelebt und entscheidend gestärkt. Datenschutz hat allerorten Konjunktur. Bei den Bürgerinnen und Bürgern, den Medien, der Politik. Nun, jeder Konjunktur folgt erfahrungsgemäß eine Flaute. Es heißt dann, die Blase musste ja irgendwann platzen. Vor diesem Hintergrund komme ich als amtierender Landesbeauftragter für Datenschutz und Informationsfreiheit nicht umhin, die Entscheider in unserem Lande aufzufordern, die Gelegenheit am Schopfe zu packen und die offenkundige Forderung der Bürgerinnen und Bürger nach mehr Schutz und Aufklärung im Bereich der informationellen Selbstbestimmung im Saarland zu befriedigen.

Dazu ist aus meiner Sicht zunächst die Zusammenlegung des privaten und des öffentlichen Datenschutzes im Saarland erforderlich. Die sich daraus ergebenden Synergieeffekte, die man z.B. bei unserem Nachbarland Rheinland-Pfalz schon nach kurzer Zeit beobachten kann, sind zahlreich. Diese Zusammenlegung sollte geschehen, unabhängig von der angekündigten Entscheidung des Europäischen Gerichtshofes in Sachen Unabhängigkeit des Datenschutzes (insbesondere des privaten Datenschutzes) in der Bundesrepublik. Jenseits der europarechtlichen Frage, ob die einschlägige Richtlinie der Europäischen Union eine derartige Zusammenführung gebietet, handelt es sich hier vornehmlich um eine politische Entscheidung. Selbst wenn die Europarichtlinie diese Zusammenlegung nicht gebieten sollte, sie verbietet sie sicherlich nicht. Und das Argument, Deutsches Verfassungsrecht stünde dem entgegen, ist bei näherer Betrachtung alles andere als überzeugend. Tatsache ist, die Mehrheit der Länder dieser Republik, die öffentliche und private Aufsicht zusam-

mengefasst haben, ist sicherlich auch an unser Grundgesetz und an die jeweilige Landesverfassung genauso gebunden und respektiert diese genauso intensiv, wie jene Länder, die auf eine Trennung beharren.
Darüber hinaus ist festzustellen, dass nicht nur das Bundesdatenschutzgesetz (BDSG) überarbeitungsreif gewesen ist. Auch das Saarländische Datenschutzgesetz ist es. Es handelt sich zwar um ein gutes Gesetz. Dieses Gesetz ist aber genauso wie das BDSG hier oder dort durch Zeitablauf überholungsbedürftig. Auch sind die Erfahrungen der 30 vergangenen Jahre seit Schaffung der Institution eines Landesbeauftragten für Datenschutz im Saarland in ein derartiges neues Gesetz einzubringen. Das Bessere ist nun einmal der entschiedene Feind des Guten.

Ähnliches gilt für das Recht der Informationsfreiheit des Saarlandes. Das im Saarland geltende Recht stellt einen Schritt in die richtige Richtung dar. Gleichwohl ist es genauso wie das Informationsfreiheitsrecht des Bundes aufgrund der bei Anwendung gemachten Erfahrungen bürgerfreundlicher und effizienter zu gestalten. Diesbezüglich darf ich auf den ersten und den zweiten Informationsfreiheitsbericht meines Kollegen, Herrn Peter Schaar, dem Bundesbeauftragten für Datenschutz und Informationsfreiheit verweisen.

An dieser Stelle will ich übrigens feststellen, dass meine Mitarbeiter und ich, um den Wünschen einer interessierten und fordernden Öffentlichkeit zu genügen, in dem Berichtszeitraum die öffentlichkeitswirksame Aufklärung intensiviert und die dazu notwendigen Maßnahmen vervielfacht haben. So wurde der Internetauftritt meiner Geschäftsstelle im Berichtszeitraum neu entwickelt. So wurde mit dem Landesjugendring des Saarlandes ein gemeinsames datenschutzrechtlich relevantes und äußerst erfolgreiches Internetportal erarbeitet. So wurden von der Geschäftsstelle und mir eine an Jugendliche, Schülerinnen und Schüler gerichtete Präsentation entwickelt, dem Ministerium für Bildung, Familie, Frauen und Kultur zur Verfügung gestellt und allen Interessenten zugänglich gemacht. So wurde die Zusammenarbeit mit einer Vielzahl von öffentlichen und privaten Stellen im Lande aufgenommen bzw. intensiviert. Ich denke hier z.B. an die Landesmedienanstalt, die Arbeitskammer, die BEST GmbH, das Ministerium für Bildung, Familie, Frauen und Kultur und die Schulen, die saarländische Polizei, eine Vielzahl unserer Gemeinden und weitere private und öffentliche Institutionen. Nicht unerwähnt will ich übrigens meine Vortragstätigkeit las-

sen, die offenkundig einen großen Nachhall hat, einen bedeutsamen Bedarf abzudecken scheint und zum Selbstläufer geworden ist.

2 Technisch-organisatorischer Datenschutz

2.1 Kommunales Netz im Saarland eGo-Net

Im Jahre 2006 entschloss sich der Zweckverband elektronische Verwaltung für saarländische Kommunen (eGo-Saar) dazu, für seine Verbandsmitglieder ein geschlossenes Datennetz unter der Bezeichnung „Kommunales Netz des Saarlandes“ aufzubauen.

Mit Hilfe dieses Datennetzes wird den Kommunen eine ungehinderte und schnelle Kommunikation untereinander sowie ein schneller und sicherer Datenaustausch ermöglicht. Weiterhin werden den Bürgern über dieses Netz durch die Kommunen Dienstleistungen bei Dritten, wie z.B. der Deutschen Rentenversicherung, angeboten.
Das Netz wurde als logisches Netz unter Nutzung des IPSec-VPN Technologie konzipiert und realisiert. Mit Hilfe dieser Technologie ist es möglich, die Vertraulichkeit und Integrität der übertragenen Daten zu gewährleisten.
Die Umsetzung der Absicherung des Netzes wird in zwei Stufen realisiert. In der zweiten und endgültigen Ausbaustufe werden zur Verschlüsselung und Authentifizierung Zertifikate genutzt. Bis zum Zeitpunkt des Einsatzes dieser Zertifikate werden in einer Übergangsphase der Verschlüsselung Pre-Shared-Keys zu Grunde gelegt. Diese Schlüssel werden mehrmals im Jahr ausgetauscht. Die Verwaltung der Schlüssel erfolgt durch den eGo-Saar selbst.
Als Schnittstellen zu externen Netzen wurden Übergänge in das Landesdatennetz des Saarlandes und zu TESTA implementiert.
Als erster Dienst dieses Netzes wurde die Datenlieferung der Melderegisterdaten an den Schattenspeicher realisiert, um eine tägliche Befüllung desselben und somit einen tagesaktuellen Datenbestand sicher zu stellen.
Meine Forderungen nach Gewährleistung der Integrität und Authentizität der übertragenen Daten werden auf Grund der genutzten Topologie und Technologie des Netzes erfüllt.

2.2 Einführung eines Dokumentenmanagementsystems in der Landesverwaltung

Die saarländische Landesverwaltung führte 2007 ein Dokumentenmanagement- und Vorgangsbearbeitungssystem ein. Das System soll eine digitale Registrierung und komfortable Ablage von papierenen und elektronischen Dokumenten mit einer anschließenden Weiterleitung in den Geschäftsgang sicherstellen. Es soll somit die Papierakte durch eine elektronische Akte abgelöst werden.
Die zentrale Datenschutzfrage beim Einsatz eines DMS ist, wie wirksam verhindert wird, dass

- Dokumente unzulässig im DMS gespeichert werden oder bleiben,
- auf im DMS gespeicherte Dokumente unzulässig zugegriffen werden kann,
- Dokumente manipuliert werden und
- auf Protokolldaten der Beschäftigten zur Leistungs- und Verhaltenskontrolle unzulässig zugegriffen wird.

Da meine Dienststelle bereits in einer sehr frühen Phase eingebunden wurde, konnten unsere Anregungen und Forderungen in die Systemarchitektur eingebaut werden.
Die Rechtevergabe ist sehr restriktiv gehalten, so dass nur beteiligte Organisationseinheiten Zugriff auf die entsprechenden Dokumente besitzen. Weitergehende Zugriffsberechtigungen (z. B. externer Organisationseinheiten) müssen gesondert gesetzt werden, werden protokolliert und sind somit jederzeit nachvollziehbar.
Die Protokollierung aller Zugriffe und Änderungsvorgänge werden in der elektronischen Akte selbst realisiert und bleiben somit bis zum Löschen der Akte nachvollziehbar. Die Löschfristen für elektronische Akten sind analog zu den Papierakten festgelegt.
Weiterhin wurde in Dienstvereinbarungen geregelt, dass die Protokolldaten nicht zur Verhaltens- und Leistungskontrolle der Mitarbeiter genutzt werden dürfen, sodass auch der Arbeitnehmerdatenschutz in dieser Beziehung sichergestellt ist.
Ingesamt gelang es durch die Kooperation zwischen der Fachbehörde und meiner Dienststelle bereits ab einem sehr frühen Zeitpunkt, den Einsatz eines Dokumentenmanagementsystems in der saarländischen Landesverwaltung auch aus Sicht des Datenschutzes optimal auf den Weg zu bringen.

2.3 E-Learning Plattform der Universität des Saarlandes - CLIX

Das Kompetenzzentrum Virtuelle Saar-Uni (Visu) begann 2006 mit der Planung einer E-Learning-Plattform an der Universität des Saarlandes. Lehre und Lernen sollen über das Internet und mittels Computer vereinfacht werden. Alle Schritte rund um das Studium sollen über ein zentrales System gesteuert werden, indem verschiedene bereits existierende Datenbanken an ein Kernsystem angebunden werden.

Dies führt durch die Verknüpfung umfangreicher Datensätzen zu einer personenspezifischen Datensammlung über jeden Studenten.

2007 erreichte mich die Eingabe eines Studenten, der darüber berichtete, dass es möglich sei, sich alle Studenten mit den zugehörigen Daten anzeigen zu lassen.

Diese Möglichkeit beruhe auf einer ID-Vergabe für alle Studenten aus einem festen Nummernbereich. Durch Eingabe einer beliebigen ID in der Adresszeile des Webbrowsers sei es möglich, auf die Daten des zugehörigen Studenten zuzugreifen.

Auf Nachfragen durch meine Dienststelle kam es zu mehreren Gesprächen mit der Universität des Saarlandes und der Entwicklerfirma.

Als Ergebnis wurde die von Studenten entdeckte Sicherheitslücke im Zusammenhang mit der URL-Eingabe und der Eingabe der UserID durch die Herstellerfirma beseitigt.

Die Möglichkeit auf Profile Dritter zuzugreifen wurde unterbunden. Weiterhin wurde der Umfang der Möglichkeiten der Nutzer, das Profil entsprechend den eigenen Wünschen zu beeinflussen, vergrößert.

Nachdem alle Änderungen eingearbeitet wurden, ist nun eine E-Learning-Plattform realisiert, gegen deren Einsatz keine datenschutzrechtlichen Bedenken mehr bestehen.

3 Justiz

3.1 Saarländisches Jugendstrafvollzugsgesetz - SJStVollzG

Das Bundesverfassungsgericht (BVerfG) hat mit Urteil vom 31. Mai 2006 den Gesetzgeber aufgefordert, die verfassungsrechtlich erforderliche gesetzliche Grundlage für den Jugendstrafvollzug bis zum 31. Dezember 2007 zu schaffen. Es betonte hierbei ausdrücklich, dass die Ausgangsbedingungen bei den zur Jugendstrafe Verurteilten sich wesentlich von den zur Freiheitsstrafe Verurteilten unterscheiden, da Jugendliche ein anderes Zeitempfinden haben und typischerweise stärker unter der Trennung von ihrem sozialen Umfeld und unter dem erzwungenen Alleinsein leiden. In ihrer Persönlichkeit sind sie regelmäßig weniger verfestigt als Erwachsene. Vor dem Hintergrund, dass das Ziel der Befähigung zu einem straffreien Leben in Freiheit für den Jugendstrafvollzug ein besonders hohes Gewicht hat, wurden durch das Bundesverfassungsgericht konkrete Anforderungen an ein Jugendstrafvollzugsgesetz gestellt. Der zukünftige Jugendstrafvollzug soll human, zeitgemäß und konsequent am Erziehungsgedanken ausgerichtet sein.

Durch die Föderalismusreform ist die entsprechende Gesetzgebungskompetenz im September 2006 vom Bund auf die Länder übergegangen und somit mussten die Landesgesetzgeber entsprechend tätig werden.

Im Februar 2007 wurde mir daher ein erster Referentenentwurf für ein saarländisches Jugendstrafvollzugsgesetz (SJStVollzG) im Rahmen der externen Anhörung zur Stellungnahme aus datenschutzrechtlicher Sicht übersandt. Der vorgelegte Referentenentwurf basierte im Wesentlichen auf dem Musterentwurf einer von dem Strafvollzugsausschuss der Länder eigens eingerichteten Arbeitsgruppe und trug in einigen wenigen Punkten saarländischen Besonderheiten Rechnung. Aufgrund meiner Stellungnahme wurden in den Gesetzesentwurf der Regierung des Saarlandes über den Vollzug der Jugendstrafe vom 29.05.2007 (LT-Drs. 13/1390) einige datenschutzrechtliche Forderungen und Verbesserungsvorschläge eingearbeitet. Allerdings blieben auch einige weitere datenschutzrechtliche Kritikpunkte unberücksichtigt. So blieb beispielsweise die Regelung, bei unüberwindlichen sprachlichen Verständigungsschwierigkeiten andere Mitgefangene zu einem Zugangsgespräch hinzuzuziehen, bestehen. Mittels Erkennungsdienstlicher Maßnahmen gewonnene Unterlagen können auch in kriminalpolizeilichen Sammlungen verwahrt werden. Weder ist hierzu die Erforderlichkeit dieser zusätzlichen Verwahrung erkennbar, noch erscheint sicherge-

stellt, dass bei einer Löschung der gewonnenen Unterlagen in den Gefangenenpersonalakten oder personenbezogenen Dateien ebenso eine zeitgleiche Löschung dieser Unterlagen in den kriminalpolizeilichen Sammlungen erfolgt. Auch sollten die in Dateien gespeicherten personenbezogenen Daten aus erkennungsdienstlicher Behandlung unverzüglich nach Entlassung oder Haftverlegung gelöscht werden und nicht erst nach spätestens 2 Jahren. Das Gesetz ermöglicht die Führung einer zentralen Datei für die Anstalt und die Aufsichtsbehörde, in der die für den Vollzug erforderlichen personenbezogenen Daten gespeichert werden. Leider lässt es jedoch eine normenklare Regelung vermissen, die die Zweckbestimmung und die Datenarten, die in dieser Datei gespeichert werden sollen, bezeichnen. Ebenso wurde in das Jugendstrafvollzugsgesetz eine Norm aufgenommen, die eine Vereinbarung zu einem Datenverbund zwischen Bund und Ländern zur automatisierten Datenerhebung ermöglicht. Weder Zweck des Datenverbundes noch die Form der Vereinbarung sowie die erforderlichen technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes wurden im Regelungswerk konkretisiert.
Das Gesetz ist zum 01.01.2008 in Kraft getreten.

3.2 Neue Telekommunikationsanlage in der Justizvollzugsanstalt Saarbrücken

Im Februar 2007 erlangte ich durch einen Kollegen Kenntnis darüber, dass in dessen Zuständigkeitsbereich in einer dortigen Justizvollzugsanstalt der Einsatz eines neuen Telefonsystems beabsichtigt sei, mit welchem Telefongespräche von Häftlingen aufgezeichnet werden können. Da dies datenschutzrechtlich nicht unbedenklich ist, habe ich das Ministerium für Justiz, Gesundheit und Soziales um Mitteilung gebeten, ob sich in der Justizvollzugsanstalten unseres Landes ein ähnliches Telefonsystem in Betrieb befindet bzw. ob dies beabsichtigt sei und inwieweit gegebenenfalls etwaige Aufzeichnungsmöglichkeiten genutzt werden.
Nach Mitteilung des Ministeriums für Justiz, Gesundheit und Soziales befindet sich seit Mai 2006 eine neue Telefonanlage in der Justizvollzugsanstalt Saarbrücken in Betrieb. Für die Bereiche des offenen Strafvollzuges sowie des Jugendstrafvollzuges ist eine Einführung dieses Telefonsystems nicht geplant.

Ich habe mir die Nutzungsmöglichkeiten des neuen Systems unter datenschutzrechtlichen Gesichtspunkten erläutern lassen.
So ermöglicht die in Rede stehende Telefonanlage, dass ein Gefangener nur nach Eingabe einer persönlichen Kennziffer telefonieren kann. Auf dem Kontrollmonitor des Bediensteten der Justizvollzugsanstalt erscheint sodann der zu der Kennziffer gehörende Name, so dass der Bedienstete ersehen kann, ob der sich einwählende Gefangene auch tatsächlich der Berechtigte ist.
Die Option zur Aufzeichnung von Telefongesprächen der Gefangenen wurde seitens der Anstaltsleitung in der zentralen Steuerung des Telefonsystems bewusst nicht aktiviert. Auch zukünftig ist das Freischalten der vorgenannten Option nicht beabsichtigt.
Weitergehende datenschutzrechtliche Bedenken waren demzufolge nicht gegeben.

3.3 Aktenlagerung bei der Staatsanwaltschaft Saarbrücken

Im August 2007 wurde in den saarländischen Medien darüber berichtet, dass bei der Staatsanwaltschaft beim Landgericht Saarbrücken (StA) wegen laufender Baumaßnahmen seit einiger Zeit - so wörtlich - „Berge von Ermittlungsakten“ auf den Fluren lagerten. Im Übrigen bestünde weder eine Zutrittskontrolle zu den Büros noch eine Zugriffskontrolle zu den Akten. Gleichfalls sei eine Einsicht in die Akten durch unbefugte Dritte jederzeit möglich gewesen.
Die unmittelbar daran anschließend stattgefundene Ortsbesichtigung durch meine Geschäftsstelle sowie eine längere Erörterung sowohl mit dem zuständigen Staatssekretär als auch der Behördenleitung der StA führte zu einer erheblichen Sensibilisierung hinsichtlich der Thematik des Datenschutzes. Die StA hat dann auch sofort nach Bekanntwerden der angesprochenen Zustände Vorsorge getroffen, um für die Zukunft zu verhindern, dass weitere Aktenlagerung auf ihren Fluren erfolgt. Neben der Einrichtung zusätzlicher abschließbarer Lagerräume für die benötigten umfangreichen Aktenbestände gehörte zu den Maßnahmen der Behördenleitung der umgehende Erlass einer entsprechenden Hausverfügung.
Hiernach wurde strikt untersagt, Akten, Beweismittel und dergleichen auf den Fluren zu lagern bzw. die mit Akten beladenen Aktenwagen dort abzustellen.

Darüber hinaus wurde auch die Zutrittskontrolle zu den Büros in besagter Dienstanweisung derart geregelt, dass Diensträume selbst bei nur kurzzeitigem Verlassen zu verschließen sind.
Ebenso wurden Maßnahmen zur Entzerrung der Besucherströme in die Wege geleitet. Der Zugang zum Dienstgebäude über die Zähringer Straße ist lediglich den Justizbediensteten vorbehalten, wohin gegen die übrigen Besucher nur über die gemeinsame Pforte im Landgerichtsgebäude Zutritt erhalten.
Auch wurden sodann verschiedene einschlägige Dienstanweisungen überarbeitet und dem aktuellen Rechts- und Sachstand angepasst.

3.4 Fahreridentifizierung mittels einer Frontalfotografie aus einem abgeschlossenen Verwarnungsverfahren

Im Februar 2007 hat ein Petent vorgetragen, dass die Ortspolizeibehörde einer saarländischen Kommune Frontalfotografien aus abgeschlossenen Verwarnungsverfahren im Rahmen von Verkehrsordnungswidrigkeiten speichere und sie bei neuerlichen Verkehrsordnungswidrigkeiten zur Fahreridentifizierung heranziehe. Im weiteren Ermittlungsverfahren legte der Petent die schriftliche Verwarnung der Ortspolizeibehörde vor, aus der zweifelsfrei ersichtlich war, dass die Fahreridentifizierung aufgrund des Fotos einer vorangegangenen Ordnungswidrigkeit erfolgte. Das damals festgesetzte Verwarnungsgeld für diese Ordnungswidrigkeit war bereits beglichen und das Verfahren somit bereits abgeschlossen.
Nach § 94 c des Ordnungswidrigkeitengesetzes (OWiG) gilt für die Verarbeitung und Nutzung personenbezogener Daten die Strafprozessordnung (StPO). Grundsätzlich sind die gespeicherten Daten nach § 483 StPO mit der Erledigung des Verfahrens zu löschen. Die Erledigung des Verfahrens wurde durch das Begleichen des festgesetzten Verwarnungsgeldes erreicht. Mithin wurde seitens der Ortspolizeibehörde der betreffenden Gemeinde in unzulässiger Weise zur Identifizierung des Fahrers auf Daten aus einem abgeschlossenen Verfahren zurückgegriffen. Die Ortspolizeibehörde hat insoweit auch ein Fehlverhalten Ihrer Dienstelle eingeräumt. Von einer weitergehenden Beanstandung konnte ich absehen, da Vorsorge getroffen wurde, um zukünftig personenbezogene Daten nach Abschluss des Verfahrens umgehend zu löschen. Hiermit war die Behebung des Mangels sichergestellt.

3.5 Einführung des Fachmoduls Eureka-Straf

Das damalige Ministerium für Justiz, Gesundheit und Soziales informierte mich erstmals 2005 über den Einsatz der Justizsoftware „EUREKA-Delphi“ für den Bereich der ordentlichen Gerichtsbarkeit. EUREKA steht für EDV-Unterstützung für Rechtsgeschäftsstellen und Kanzleien sowie der Richter- und Rechtspflegearbeitsplätze.
Im November 2007 erhielt ich dann weitere Mitteilung, dass im Rahmen der Anwendung EUREKA-Delphi am 23.11.2007 die Freigabe für den Einsatz des Fachmoduls EUREKA-Straf erfolgt sei. Bei der Datenbank EUREKA-Straf handelt es sich um eine gerichtsinterne Datenbank, deren Nutzung den Bediensteten des Strafsachenbereichs vorbehalten ist. Ich wurde um Mitteilung gebeten, ob meinerseits Bedenken bestehen, auch den Mitarbeitern der Präsidialverwaltung und der Geschäftsleitung Leseberechtigungen für das System einzurichten. Bei Einführung des modularen Programmsystem EUREKA-Delphi wurde mir mitgeteilt, dass die zu speichernden verfahrensbezogenen gerichtlichen Daten streng getrennt nach Fachmodul und zuständigem Gericht in einer zentralen Oracle-Datenbank im Justizrechenzentrum beim Saarländischen Grundbuchamt vorgehalten werden.
Was die Leseberechtigung für Mitarbeiterinnen und Mitarbeiter der Präsidialverwaltung anbelangt, ergaben sich aus meiner Sicht demzufolge erhebliche datenschutzrechtliche Bedenken hinsichtlich der Gewährleistung dieser strikten Trennung. Eine Begründung, die meine Bedenken hätte ausräumen können, wurde mir leider bislang auch nicht vorgetragen.

3.6 Entwurf für ein Saarländisches Gesetz zur Sicherung des Justizvollzuges

Im Rahmen der externen Anhörung wurde mir im Juli 2008 ein Referentenentwurf für ein Saarländisches Gesetz zur Sicherung des Justizvollzuges mit der Bitte um Stellungnahme aus datenschutzrechtlicher Sicht übersandt.
Mit dem Gesetz soll der Mobilfunkverkehr auf dem Gelände der Justizvollzugsanstalten unterbunden und insbesondere eine Rechtsgrundlage für den Betrieb sogenannter Mobilfunkblocker oder ähnlicher Geräte zur Verhinderung unerlaubter Mobilfunkgespräche geschaffen werden. Unerlaubte Mobilfunkgespräche Gefangener stellen

eine erhebliche Gefahr für die Sicherheit und Ordnung in den Justizvollzugsanstalten dar. Die Nutzung von Mobiltelefonen ist bereits nach geltendem Recht in Bereichen des geschlossenen Justizvollzuges untersagt. Das unerlaubte Einbringen von Mobilfunktelefonen in Bereiche des geschlossenen Vollzuges lässt sich trotz sorgfältiger Kontrollen nicht zuverlässig verhindern, zumal solche Geräte immer kleiner werden. Aufgrund der Föderalismusreform sind die Länder seit dem 01. September 2006 für den Strafvollzug gesetzgeberisch verantwortlich.

Das mit den Erfordernissen des Strafvollzuges begründbare Interesse, die Nutzung von Mobilfunk zu unterbinden, ist gemäß § 55 Telekommunikationsgesetz (TKG) auf das Gelände der jeweiligen Justizvollzugsanstalt beschränkt, weshalb der Mobilfunkverkehr außerhalb davon nicht beeinträchtigt werden darf. Nach heutigem Stand der Technik kann auf fünf Meter genau zwischen geblocktem und freiem Mobilfunkverkehr getrennt werden. Die erforderliche Beschränkung der räumlichen Wirkung der eingesetzten Mobilfunkblocker wird durch exaktes Einmessen der installierten Anlagen sichergestellt. Alle Hafthäuser stehen mindestens 7,5 Meter von der Außenmauer entfernt, so dass für die Anwohner der Anstalten bei einer 5 Meter genauen Trennung auch keine Beeinträchtigungen zu erwarten sind.

Da bereits nach geltendem Recht Mobilfunktelefone im geschlossenen Vollzug untersagt sind und nach § 55 Abs.1 S.5 TKG für Behörden zur Ausübung gesetzlicher Aufgaben Ausnahmen von einer Frequenzzuteilung geschaffen wurden, habe ich in meiner Stellungnahme zu dem vorgenannten Referentenentwurf keine datenschutzrechtlichen Bedenken erhoben.

4 Polizei

4.1 Gesetz zur Erhöhung der öffentlichen Sicherheit im Saarland

Bereits im November 2006 wurde mir ein erster Entwurf eines Gesetzes zur Erhöhung der öffentlichen Sicherheit im Saarland im Rahmen des externen Anhörungsverfahrens mit der Bitte um Stellungnahme zugeleitet. Sodann wurde mit Landtagsdrucksache 13/1313 vom 16.04.2007 eine vollständig überarbeitete Fassung des Gesetzentwurfes vorgelegt, der meinen aber auch den Anregungen und Forderungen anderer Angehörter teilweise Rechnung trug. Hinsichtlich meiner damaligen datenschutzrechtlichen Hinweise darf ich auf meinen 21. Tätigkeitsbericht für die Jahre 2005/2006 inhaltlich verweisen (TZ 4.4 Seite 28 ff.). Das Gesetz zur Erhöhung der öffentlichen Sicherheit im Saarland wurde sodann im Berichtszeitraum am 12.09.2007 in zweiter Lesung vom Landtag des Saarlandes verabschiedet und im Amtsblatt des Saarlandes vom 12.11.2007 veröffentlicht. Es trat am 01.01.2008 in Kraft. Vor diesem Hintergrund darf ich wie zuvor erwähnt auf die ausführliche Würdigung dieses Gesetzes im vorgenannten Bericht verweisen. Ungeachtet dessen will ich gleichwohl auf mein datenschutzrechtliches Postulat bezüglich der in § 27 Absatz 3 Saarländisches Polizeigesetz (SPolG) neu eingeführten automatischen Kfz-Kennzeichenerfassung zurückkommen.

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 11.03.2008 die verfassungsrechtlichen Grenzen polizeilicher Kfz-Kennzeichenerfassungen dargelegt (BVerfG 1 BvR 2074/05, 1 BvR 1254/07, NJW 2008, 1505).
Im Rahmen dieses Verfassungsbeschwerdeverfahrens gegen die Vorschriften zur automatisierten Erfassung von Kfz-Kennzeichen in den hessischen und schleswig-holsteinischen Vorschriften hat das Verfassungsgericht deren Rechtsvorgaben für nichtig erklärt. Im Wesentlichen hat es seine Entscheidung damit begründet, dass diese Normen nicht dem Gebot der Normbestimmtheit und Normenklarheit genügen, da sie weder den Anlass noch den Ermittlungszweck benennen. Über dies hinaus sei auch das Gebot der Verhältnismäßigkeit nicht gewahrt.

Im Rahmen des parlamentarischen Anhörungsverfahrens im Saarländischen Landtag habe ich die Unbestimmtheit und Weitläufigkeit des Begriffes „Fahndungsbestand“ bei der Kfz-Kennzeichenerfassung moniert. Dieser war bis dato weder Gegenstand

einer gesetzlichen Definition noch einer Auslegung durch die Rechtsprechung gewesen. Das Bundesverfassungsgericht hat mit seiner nun vorliegenden Entscheidung klargestellt, dass sofern im Gesetz zum Verwendungszweck keine Aussagen getroffen werden, die Ermächtigung alle denkbaren Verwendungszwecke einschließt. Eine Präzisierung wird durch die Verwendung des Begriffes „Fahndungsbestand“ nicht geleistet. Vielmehr hat der Begriff den Charakter einer dynamischen Verweisung, durch die insbesondere nicht ausgeschlossen wird, dass sich der Umfang der einbezogenen Datenbestände laufend und in gegenwärtig nicht vorhersehbarer Weise verändert (BVerfG, NJW 2008, 1505 Rdnr. 131).

Im Saarland wurde nach dem Urteil des Bundesverfassungsgerichtes zwar wohl ein Anpassungsbedarf der bisherigen rechtlichen Grundlagen an die verfassungsrechtlichen Anforderungen erkannt, jedoch wurde bis dato keine neue Regelung vorgelegt. Eine Anpassung des Saarländischen Polizeigesetzes an die Rechtsprechung des Bundesverfassungsgerichtes ist zwingend geboten. Gemäß Artikel 7 Absatz 3 des Gesetzes zur Erhöhung der öffentlichen Sicherheit Nr. 627 tritt das Saarländische Polizeigesetz zum 31. Dezember 2010 außer Kraft. Spätestens bis zu diesem Zeitpunkt muss ein neues Polizeigesetz verabschiedet sein, das verfassungskonform ist. Ich werde die Entwicklung diesbezüglich weiterhin verfolgen. Die Abschaffung verfassungswidriger polizeirechtlicher Ermächtigungsgrundlagen erledigt sich nämlich nicht dadurch, dass sie faktisch nicht angewendet werden.

4.2 Richtlinie für die Zusammenarbeit der Einwohnermeldeämter im Saarland mit der Vollzugspolizei des Saarlandes zur Verhinderung und Bekämpfung der Schleusungskriminalität, der unerlaubten Einreise und des unerlaubten Aufenthaltes

Ziel dieser Richtlinie ist es, die behörden- und ressortübergreifende Zusammenarbeit der Einwohnermeldeämter im Saarland mit der Vollzugspolizei des Saarlandes im Grundsatz zu regeln, um Schleusungskriminalität und unmittelbar damit zusammenhängende Straftaten effektiv und nachhaltig zu bekämpfen, unerlaubte Einreise nach Deutschland zu verhindern sowie den illegalen Aufenthalt von Ausländern in Deutschland zu unterbinden.

Schleusungen nach Deutschland werden in vielfältiger Weise organisiert und häufig über die „grüne“ Grenze versteckt in verschiedenen Verkehrsmitteln sowie unter Verwendung von erschlichenen Visa oder gefälschten Reisedokumenten, durchgeführt. Die Opfer von Schleusungskriminalität werden von den Schleuserorganisationen finanziell ausgebeutet und im Zuge der Schleusungen regelmäßig in menschenunwürdige und sogar lebensgefährdende Lagen gebracht. In Einzelfällen wird selbst der Tod der meist hilflosen Menschen in Kauf genommen.
Im Mai 2007 wurde ich vom damaligen Ministerium für Inneres, Familie, Frauen und Sport gebeten, mich aus datenschutzrechtlicher Sicht zu einem ersten Entwurf der Richtlinie zu äußern. Dieser erste Entwurf hätte es den beteiligten Behörden ermöglicht, bei einem bloßen Vorliegen von nicht näher bezeichneten Anhaltspunkten für einen illegalen Aufenthalt oder einer nur möglicherweise bestehenden Verbindung mit illegal aufhältigen Personen einen entsprechenden Datenabgleich vorzunehmen. Dies hatte erhebliche datenschutzrechtliche Bedenken meinerseits zur Folge. In meiner Stellungnahme habe ich daher gemäß dem Gebot der Normenklarheit gefordert, die anlass- und verfahrensbezogenen Zusammenarbeit zu konkretisieren.
Meine diesbezüglichen Anregungen und Formulierungen haben in dem überarbeiteten Entwurf der Richtlinie ihren Niederschlag gefunden, so dass dieser keinen datenschutzrechtlichen Bedenken mehr begegnete. Die Richtlinie ist nunmehr seit dem 10.07.2008 gültig.

4.3 Auskunftserteilung durch die Polizei

§ 40 des Saarländischen Polizeigesetzes (SPolG) regelt den Anspruch des Betroffenen auf Auskunftserteilung über die zu seiner Person gespeicherten Informationen, sowie deren Zweck und die der Speicherung zugrunde liegende Rechtsnorm. Der Auskunftsanspruch bezieht sich auf Akten und Dateien und kann nur unter den Voraussetzungen des § 40 Abs.2 SPolG eingeschränkt sein.
Die Polizeidienststellen eines Bundeslandes führen einen elektronischen Kriminalaktennachweis Land (Landes-KAN), in dem wesentliche Informationen über Strafverfahren zu einer Person gespeichert werden. In einem für alle Polizeidienstellen bundesweit zugänglichen Kriminalaktennachweis (Bundes-KAN) werden Taten von länderübergreifender, internationaler oder erheblicher Bedeutung gespeichert.

Ein Kollege schilderte mir im November 2007, dass die Polizeidienststellen in seinem Zuständigkeitsbereich den Auskunftsersuchenden lediglich die Eintragungen im Landes-KAN mitteilen. Die Antwort an den Petenten ließe jedoch nicht erkennen, welche dieser Speicherungen auch im Bundes-KAN vorgenommen wurden.
Ich sah ich mich daher veranlasst, das hiesige Ministerium für Inneres und Sport um Stellungnahme hinsichtlich der Auskunftspraxis saarländischer Polizeidienststellen gemäß § 40 SPolG zu bitten. Sofern keine Auskunftsverweigerungsgründe entgegenstehen, werden Auskunftsersuchenden im Saarland sämtliche Daten mitgeteilt, die von der saarländischen Polizei sowohl im saarländischen KAN als auch im Bundes-KAN gespeichert wurden.
Da die Auskunftsersuchenden vielfach nicht über die erforderlichen Kenntnisse hinsichtlich der verschiedenen Datenverarbeitungssysteme der Polizei verfügen, kann ich die Auskunftspraxis der saarländischen Polizei gerade mit Blick auf die Gewährleistung des Rechts auf informationelle Selbstbestimmung als erfreulich bewerten.

4.4 Datenspeicherung der Polizei für Zwecke der Polizeilichen Kriminalstatistik (PKS)

Aufgrund einer Anfrage eines Kollegen habe ich das Ministerium für Inneres und Sport des Saarlandes um Mitteilung gebeten, in welchen Fällen und ggfl., wie lange personenbezogene Daten für Zwecke der Polizeilichen Kriminalstatistik (PKS) im Saarland gespeichert werden. Im Dezember 2007 erhielt ich eine einschlägige Stellungnahme des saarländischen Ministeriums für Inneres und Sport.
Aus technischer Sicht werden hiernach die PKS-Daten nicht mehr eigens erfasst, sondern aus dem Vorgangsbearbeitungssystem POLADIS in Form von Einzeldatensätzen automatisiert zur PKS-Erfassung weitergeleitet. Nach den Richtlinien für die Führung der Polizeilichen Kriminalstatistik i.d.F. vom 01.01.2007 werden Tatverdächtige nur einmal gezählt, unabhängig davon, wie oft sie in Erscheinung getreten sind. Um Mehrfachzählungen während der Erfassungszeit auszuschließen, ist eine Identifizierung der Tatverdächtigen erforderlich. Die personenbezogenen Daten stehen ausschließlich Mitarbeitern der Polizei zur Verfügung, die für die PKS zuständig sind und dürfen von diesen auch nur zu vorgenanntem Zweck genutzt werden. Nach Abschluss des Erfassungszeitraumes von einem Jahr stehen die Daten nur noch ano-

nymisiert zur Verfügung. Daten wie Familienname, Geburtsname, Vorname, Geburtsdatum und der jeweilige Kurzsachverhalt werden in der PKS gelöscht. Anstelle der Personalien wird ein vom Bundesamt für Sicherheit vorgeschlagener BSI-Schlüssel verwendet, mit welchem die maßgeblichen Datensätze dem Bundeskriminalamt zur Auswertung für die bundesweite PKS übermittelt werden. Staatsschutzdelikte und Verkehrsdelikte sind nicht Bestandteil der PKS und werden daher auch nicht erfasst. Zur Berechnung der PKS-Zahlen wurde für das Saarland das IT-Verfahren PKS-net erworben. Der Entwurf einer Errichtungsanordnung für die automatisierte Datei PKS-net wurde mir im Juni 2008 zur datenschutzrechtlichen Bewertung zugeleitet. Die Datei dient der statistischen Erfassung, Zählung und Auswertung von Straftaten und Tatverdächtigen an Tatorten im Saarland. Sie erlaubt die Beobachtung und den Vergleich der Kriminalitätsentwicklung im laufenden Jahr und in den vergangenen fünf Jahren. Während des Erstellungszeitraumes, nämlich dem laufenden Kalenderjahr, stehen die Daten, wie bereits zuvor beschrieben, zum Ausschluss von Mehrfachzählungen in nicht anonymisierter Form einem bestimmten Benutzerkreis zur Verfügung. Anschließend werden sie mittels BSI-Schlüssel anonymisiert. Nach Ablauf von fünf Jahren werden sodann sowohl die anonymisierten Daten als auch die Vorgangs- und Verwaltungsdaten gelöscht. PKS.net wird auf einem eigenen Server betrieben und ist logisch von anderen Anwendungen getrennt. Ebenso lassen sich auch keine Daten aus PKS.net importieren. Da insoweit auch das Gebot der strikten Trennung der Datenbestände beachtet wurde, bestanden aus meiner Sicht keine datenschutzrechtlichen Bedenken gegen die Einrichtung der Datei-Anwendung PKS.net. Sie ist datenschutzverträglich. Nach Mitteilung des Ministeriums für Inneres und Sport wurde daher am 06.08.2008 die entsprechende Freigabe erteilt.

4.5 Einsatz von Hypnose bei Zeugenvernehmungen im Ermittlungsverfahren

Wie mir ein Kollege im Juni 2008 mitteilte, wurde in seinem Zuständigkeitsbereich in den letzten zehn Jahren, in besonders schwierigen Fällen, bei Zeugenvernehmungen das Mittel der Hypnose eingesetzt. Durch diesen Bericht veranlasst, habe ich das

saarländische Ministerium für Inneres und Sport um Stellungnahme gebeten, ob derartige Ermittlungsmethoden auch im Saarland Anwendung finden.

Eine Zeugenvernehmung unter Hypnose ist gemäß §§ 69 Abs.3 i.V.m. 136a Abs.1 StPO nicht zulässig. Hypnose ist die Einwirkung auf einen anderen, durch die unter Ausschaltung des bewussten Willens eine Einengung des Bewusstseins auf die von dem hypnotisierten gewünschte Vorstellungsrichtung erreicht wird (Karlsruher Kommentar zur Strafprozessordnung, StPO, 5. Aufl. 2003, Boujong §136a RN 28). Nach herrschender Meinung verbietet § 136a Abs.1 StPO die Hypnose ohne Ausnahme, selbst dann, wenn sie zur Ausforschung des Gedächtnisses von Zeugen mit deren Einwilligung angewendet werden soll (Beck´sche Kurzkommentare Lutz Meyer-Goßner zur StPO, 51. Auflage, § 136a RN 19).Sollte die verbotene Vernehmungsmethode der Hypnose rechtswidrigerweise zur Anwendung gelangen, so unterliegt sie gemäß § 136a Abs.3 S.2 StPO ausdrücklich einem Verwertungsverbot (Meyer-Goßner aaO § 136a RN 27). Auch aus datenschutzrechtlicher Sicht muss ich eine derartige Beeinträchtigung der freien Willensbildung als unzulässig einstufen. Umso erfreulicher ist es daher, dass nach Mitteilung des hiesigen Ministeriums für Inneres und Sport im Saarland vom Mittel der Hypnose bei Zeugenvernehmungen kein Gebrauch gemacht wird.

5 Steuern

5.1 Datenschutzrechtliche Auskunftsansprüche im Besteuerungsverfahren

Bereits seit vielen Jahren ist der Auskunftsanspruch im Besteuerungsverfahren ein unerledigter und gegensätzlich diskutierter Punkt zwischen Finanzverwaltung und Datenschutzbeauftragten.

Während die Finanzverwaltung gestärkt durch die Rechtsprechung der Finanzgerichte argumentierte, dass ein Auskunftsanspruch nach den abgaberechtlichen Vorschriften nicht existiert und es sich um eine „absichtsvolle Nichtregelung“ in der Abgabenordnung (AO) handele, wurde nun durch das Bundesverfassungsgericht in seinem Beschluss vom 10.03.2008 (1 BvR 2388/03) eindeutig der Auskunftsanspruch nach § 19 Bundesdatenschutzgesetz (BDSG) gegenüber der Finanzverwaltung unmittelbar für anwendbar erklärt.

Nach Mitteilung des Bundesbeauftragten für Datenschutz und Informationsfreiheit wurde die Einführung eines Auskunftsrechts in der AO durch das Bundesministerium der Finanzen wieder aus dem Gesetzentwurf des Jahressteuergesetzes 2009 herausgenommen, obwohl bereits entsprechende Formulierungen vorlagen. Erklärt wurde dies damit, dass mit den Ländern noch Abstimmungsbedarf bestehe.

Stattdessen wurde das Auskunftsrecht in Form einer bundeseinheitlichen Verwaltungsanweisung geregelt, die von den Datenschutzbeauftragten des Bundes und der Länder mit Befremden aufgenommen wurde, da sie die Auskunftserteilung von einem berechtigten Interesse abhängig macht.

Dies steht in einem krassen Widerspruch zum o.g. Beschluss des Bundesverfassungsgerichts. (Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: „Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten.“)

Nicht unerwähnt jedoch darf die Tatsache bleiben, dass bei mir bisher kein Petent vorstellig geworden ist, dem durch die Saarländische Finanzverwaltung Auskunft im Besteuerungsverfahren verweigert worden wäre.

5.2 Steuerliche Identifikationsnummer

Die Einführung der einheitlichen Identifikationsnummer für steuerliche Zwecke (Steuer-ID) wurde von den Datenschutzbeauftragten sehr kritisch gesehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mit ihrer Entschließung aus der 75. Datenschutzkonferenz darauf hingewiesen, dass einheitliche Personenkennzeichen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung bergen. Besondere Gefahren erwachsen daraus, dass sich aus der steuerlichen Identifikationsnummer ein Personenkennzeichen entwickeln könnte, über das alle möglichen Datenbestände verknüpft und umfassende Persönlichkeitsprofile erstellt werden könnten.

Der ständig wachsende Umfang der zu einer Person gespeicherten Daten und die sich stetig verbessernden technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, lassen bei den Behörden Begehrlichkeiten entstehen, die es abzuwehren gilt.

Der im August 2008 gestartete Versand der Steuer-ID durch das Bundeszentralamt für Steuern war auch im Saarland von unerwünschten Pannen begleitet. Die verschickten Mitteilungen enthielten Datensätze die keine Relevanz für die Steuerverwaltung besaßen. Dies war darauf zurückzuführen, dass verschiedene Kommunen Zusatzinformationen in den elektronischen Melderegistern abgelegt hatten, die dort nichts zu suchen hatten (z.B. Vorbesitzer eines Hauses). Andere Mitteilungen enthielten veraltete Informationen. Die unkorrekten Datenfelder wurden dem Bundeszentralamt zugeführt und im Schreiben über die Zuteilung der Steuer-ID mit ausgedruckt.

Die Reklamationen der Bürgerinnen und Bürger bei den Einwohnermeldeämtern und die Aktivitäten der Datenschutzbeauftragten des Bundes und der Länder gegenüber dem Bundesministerium für Finanzen führten zu einer strategischen Analyse der aufgetretenen Fehler und einer nachfolgenden Bereinigung des Datenbestandes bei den Meldeämtern und beim Bundeszentralamt für Steuern.

5.3 Veräußerungsmitteilung für das Veräußererfinanzamt

Nach dem Verkauf eines Hauses erhielt das für den Veräußerer zuständige Finanzamt eine „Veräußerungsmitteilung für das Veräußererfinanzamt“. Daraufhin wurde der Veräußerer angeschrieben mit folgender Aufforderung: „Ich bitte Sie uns die Verwendung des Verkaufserlöses näher zu erläutern.“ Ein Hinweis auf die gesetzlichen Grundlagen für die Erhebung der Daten oder die steuerliche Relevanz der Anfrage fehlte.

Der Petent verlangte telefonisch Auskunft beim zuständigen Finanzamt über

- Zweck und Erforderlichkeit der o.a. Veräußerungsmitteilung,
- Zweck und Erforderlichkeit der Datenerhebung beim Petenten,
- die anschließende Aufbewahrung der Anfrage und
- die Benennung der erforderlichen spezialgesetzlichen Rechtsgrundlagen.

Hierzu wurden ihm nach seinen Angaben keine hinreichenden Antworten gegeben.

Der Petent äußerte zudem die Befürchtung, dass durch die Anfrage der Finanzbehörde, welche er in dieser allgemeinen Form nicht beantworten konnte, in unzulässiger Weise ein Kontendatenabruf vorbereitet werde.

Die sehr allgemein gehaltene Frage nach der Verwendung des Verkaufserlöses halte ich aus datenschutzrechtlicher Sicht für bedenklich, da sie über das erforderliche Maß in den privaten Bereich von Steuerpflichtigen eingreift. Es darf die Finanzbehörde nicht interessieren, ob die Person den Verkaufserlös für steuerlich nicht relevante Vorgänge einsetzt.

Mein Kontrollbesuch beim zuständigen Finanzamt und eine gleichzeitige schriftliche Anfrage beim Ministerium der Finanzen ergaben, dass in reinen Arbeitnehmerfällen ein zeitnahes Auskunftsersuchen beim Steuerpflichtigen gängige Praxis ist. Da bei diesen Steuerpflichtigen keine „Steuerakte“ existiert, will man mit diesem Verfahren einerseits verhindern, dass Kontrollmitteilungen „vergessen“ werden und andererseits erreichen, dass frühzeitig Steuereinnahmen z. B. durch Festsetzung von Steuervorauszahlungen gesichert werden. An die Vorbereitung einer Kontendatenabfrage sei dabei in keiner Weise gedacht.

Nach der Stellungnahme des Ministeriums konnte ich dem Petenten mitteilen, dass die Ermittlungspraxis der saarländischen Finanzämter beim Erwerb/Verkauf von Grundstücken datenschutzrechtlich unbedenklich ist, da sie sich auf entsprechende gesetzliche Vorschriften der Abgabenordnung (§ 88 ff AO) stützt. Meine Auffassung, dass die allgemein gehaltene Frage nach der Verwendung des Verkaufserlöses rechtlich bedenklich ist, wird geteilt.

6 Wahlen

6.1 Einsatz eines Wahlauswertungsprogramms „PC-Wahl“ und eines Wahlhelferprogramms „PC Wahlhelfer“

Gemäß § 7 Abs.2 SDSG bedarf der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, hinsichtlich der in der Verfahrensbeschreibung festzulegenden Angaben (§ 9 SDSG) der schriftlichen Freigabe durch die verantwortliche Stelle. Vor dieser Freigabe ist der Landesbeauftragte für Datenschutz und Informationsfreiheit zu hören.

Im Juli 2008 wurden mir daher die Verfahrensbeschreibungen zu dem Wahlauswertungsprogramm „PC-Wahl“ und dem Wahlhelferprogramm „PC Wahlhelfer“ von einer saarländischen Kommune übersandt.

Gemäß § 9 Abs.4 des Bundeswahlgesetzes (BWG), § 5 Abs. 7 des Landtagswahlgesetzes (LWG) und § 5 Abs. 5 des Kommunalwahlgesetzes (KWG) dürfen lediglich folgende personenbezogene Daten der Wahlhelfer erhoben und verarbeitet werden: Name, Vorname, Geburtsdatum, Anschrift, Telefonnummern, Zahl der Berufungen zu einem Mitglied der Wahlvorstände und die dabei ausgeübte Funktion. Eine weitergehende Speicherung von personenbezogenen Daten wie Geschlecht, Beruf, Parteimitgliedschaft, E-Mail-Adresse, oder gar Bankverbindungsdaten, wie sie im konkreten Fall durch die die Software zur Verfügung stellende Firma vorgesehen war, ist in Ermangelung einer entsprechenden Rechtsgrundlage datenschutzrechtlich unzulässig.

In diesem Zusammenhang sei auch ausdrücklich erwähnt, dass die betroffenen Personen nach § 5 Abs. 5 Satz 3 KWG vorab über Ihr Widerspruchsrecht hinsichtlich einer eventuellen Datenverarbeitung zu informieren sind. Laut Herstellerhinweis zur Zugänglichkeit der Daten enthält die Software eine Schnittstelle zu mehreren Softwareprogrammen des Melderegisters, durch die die in einer programminternen Datenbank abgespeicherten Wahlhelferadressen aktualisiert werden können. Der Gebrauch der erwähnten Schnittstelle zum Melderegister würde einen automatisierten Datenabruf darstellen, der in der derzeit gültigen Fassung weder des Meldegesetzes (MG) noch der Meldedatenübermittlungsverordnung (MeldeDÜV) eine gesetzliche Grundlage fände und daher aus datenschutzrechtlicher Sicht auch nicht toleriert werden könnte.

Auch dem Erforderlichkeitsgrundsatz nach dem MG wird nicht genüge getan, da eine stetige automatisierte Aktualisierung der Wahlhelferdaten außerhalb von Wahlterminen nicht geboten ist. Im Übrigen muss gewährleistet werden, dass der Wahlhelfer über seine gesetzlichen Widerspruchsbefugnisse gegen die Verarbeitung seiner personenbezogenen Daten für künftige Wahlen unterrichtet wird (§ 9 Abs.4 S.2 u. 3 BWG, § 5 Abs.7 S.2 u. 3 LWG, § 5 Abs.5 S.2 u. 3 KWG).
Aufgrund meiner datenschutzrechtlichen Bewertung hat die anfragende Kommune nur die per Gesetz legitimierten personenbezogen Daten der Wahlhelfer gespeichert und auch von der Schnittstelle zum Einwohnermeldeprogramm keinen Gebrauch gemacht. Dem mit mir abgestimmten Einsatz der Software „PC-Wahl“ und „PC Wahlhelfer“ stand daher aus datenschutzrechtlicher Sicht nichts mehr im Wege.

6.2 Gesetz zur Änderung wahlrechtlicher Vorschriften

Im Juni 2008 wurde mir im Rahmen der externen Anhörung ein erster Referentenentwurf eines Gesetzes zur Änderung wahlrechtlicher Vorschriften mit der Bitte um Stellungnahme übersandt.
Aufgrund der Erfahrungen bei den Bundestagswahlen wurden das Bundeswahlrecht und auch das Europawahlrecht durch das Gesetz zur Änderung des Wahl- und Abgeordnetenrechts vom 17. März 2008 fortentwickelt. Das Landtagswahlrecht (LWG) und das Kommunalwahlrecht (KWG) wurden in der Vergangenheit im Interesse der Wahlberechtigten, Wahlvorschlagsträger und der Wahlbehörden mit dem Bundes- und Europawahlrecht harmonisiert, um die Anwendung der Wahlgesetze zu vereinheitlichen und so die Vorbereitung und Durchführung der verschiedenen, teilweise gleichzeitig stattfindenden Wahlen im Saarland zu erleichtern.
Artikel 1 des Referentenentwurfes beinhaltet die vorgesehenen Änderungen im LWG. § 42 des LWG regelt grundsätzlich die Berufung von Listennachfolgern und legt in der beabsichtigten Neufassung fest, dass diejenigen Listenbewerber, die seit dem Zeitpunkt der Aufstellung der Wahlvorschläge aus dieser Partei oder Wählergruppe ausgeschieden oder Mitglied einer anderen Partei oder Wählergruppe geworden sind, bei der Nachfolge unberücksichtigt bleiben.
Im Rahmen der externen Anhörung habe ich gegen den mir vorgelegten Entwurf des § 42 LWG datenschutzrechtliche Bedenken erhoben, da mir nicht allein die Praktika-

bilität, sondern vor allem auch die rechtliche Zulässigkeit der Vorschrift höchst zweifelhaft erschien und auch die Gesetzesbegründung hierzu keinen Aufschluss gab. Es ist mir keine Rechtsgrundlage ersichtlich, die dem Staat die Überprüfung der Mitgliedschaft eines Bürgers in einer Partei bzw. Wählergruppe in verfassungsrechtlich zulässiger Weise möglich machen könnte. Dies gilt aus meiner Sicht auch für die Überprüfung einer „neuen“ Mitgliedschaft. Eine Rechtsvorschrift, die einem Bürger die Offenbarung einer Parteimitgliedschaft, einer Doppelmitgliedschaft bzw. eines Austritts und Neueintritts in Parteien staatlichen Stellen gegenüber begründet, ist dem deutschen Recht unbekannt, ja nach Verfassungsrecht unzulässig. Ebenso gibt es keine Rechtsvorschrift, die es Parteien oder Wahlvereinigungen auferlegt, Auskunft über die Mitgliedschaft von Personen dem Staat gegenüber zu machen.

Es ist im Gegenteil genuine Sache der aufstellenden Vereinigungen und Parteien, dafür Sorge zu tragen, dass es sich bei den von ihnen aufgestellten Kandidaten nicht um sogenannte „U-Boote“ handelt. Ein staatliches Überwachungsrecht, gar eine Überwachungspflicht gibt es nicht und kann es in unserem Staat nicht geben. Dies ergibt sich im Übrigen bereits aus der Verfassungsrechtsprechung zur Frage von gemeinsamen verdeckten Wahlvorschlägen von Parteien.

Das Gesetz Nr. 1657 zur Änderung wahlrechtlicher Vorschriften ist am 06. November 2008 im Amtsblatt des Saarlandes veröffentlicht worden und am darauf folgenden Tag in Kraft getreten. Bedauerlicherweise blieben meine Anmerkungen zu § 42 LWG ungehört. Die Gesetzesbegründung wurde zwar geändert, lässt aber weiterhin die Darstellung einer rechtlichen Zulässigkeit vermissen. Mit Blick auf die zuvor erwähnte bereits ergangene Verfassungsrechtsprechung bleibt ein Aufbäumen der Zivilgesellschaft abzuwarten.

7 Meldewesen

7.1 Elektronischer Reisepass (ePass)

Mit der Verordnung Nr. 2252/2004 des Europäischen Rates aus dem Jahre 2004 wurden die Mitgliedsstaaten verpflichtet, in die Reisepässe einen RFID-Chip zu integrieren. Auf diesem Chip werden neben den allgemeinen Passdaten auch ein Gesichtsbild sowie zwei Fingerabdrücke gespeichert. Mit der Ausgabe der elektronischen Pässe (ePass) der zweiten Generation, auf denen die beiden Fingerabdrücke als biometrisches Merkmal gespeichert sind, wurde am 01.11.2007 begonnen. Gleichzeitig wurde mit den ePässen der zweiten Generation ein erweiterter Zugriffsschutz - Extended Access Control (EAC) - eingeführt. Damit soll zum einen gewährleistet werden, dass nur berechtigte, hoheitliche Lesegeräte auf die im RFID-Chip gespeicherten Fingerabdrücke zugreifen können. Zum anderen soll auch der Schutz aller personenbezogenen Daten entsprechend den Hinweisen des BSI erhöht werden.

Im Rahmen mehrerer Besuche bei verschiedenen Passämtern informierte ich mich über die Ausstellung eines elektronischen Passes von der Beantragung mit der Registrierung der Fingerabdrücke bis hin zur Aushändigung des fertigen Passes.

Besonderes Augenmerk legten meine Mitarbeiter hierbei auf die Erfassung und Speicherung der Passdaten, die Datenübermittlung an die Bundesdruckerei sowie die Zugriffsrechte im Passverfahren.

Zum besseren Verständnis soll der Verfahrensablauf zwischen Passbehörde und Passhersteller kurz erläutert werden:

1. Die Antragsdaten der Bürger werden in der Passbehörde aufgenommen, die erforderlichen biometrischen Daten erfasst und deren Qualität geprüft. Die erfassten Antragsdaten werden zu einem digitalen Datensatz zusammengefasst, signiert und verschlüsselt.
2. Die Passbehörde überträgt den Datensatz integer, authentisch und vertraulich an den Passhersteller.
3. Der Passhersteller nimmt den Datensatz entgegen, entschlüsselt diesen, prüft die digitale Signatur und bestätigt der Passbehörde den sicheren Empfang der Daten.
4. Nach einer zentralen Qualitätsprüfung wird der elektronische Pass produziert und ausgeliefert.

5. Die Passbehörde händigt dem Bürger seinen elektronischen Pass aus. Dem Bürger wird die Möglichkeit geboten, sich einen Überblick über die über ihn auf dem RFID-Chip gespeicherten Daten zu verschaffen. Mit Aushändigung des Ausweises werden die in der Behörde gespeicherten Fingerabdrücke gelöscht.

Bei unseren Besuchen vor Ort zeigte sich, dass die Arbeitsschritte, die in den Passbehörden abgearbeitet werden, sorgfältig in die bisherigen Arbeitsabläufe integriert wurden.

Die Erfassung der Fingerabdrücke stellte sich als unproblematisch dar. Es wurde lediglich von einem Fall berichtet, in dem Fingerabdrücke eines Bürgers nicht erhoben werden konnten. Das Ausstellen eines Passes ohne Fingerabdrücke war in diesem betreffenden Fall allerdings problemlos möglich.

Die Übermittlung der Passdaten zu der Bundesdruckerei erfolgte in allen Passämtern mit Hilfe des D-Safe-Moduls, welches von der Bundesdruckerei zur Verfügung gestellt wird. Ein Umstieg auf das OSCI-Protokoll ist geplant.

Nach Aushändigung des erzeugten Passes an den Bürger werden die Fingerabdrücke automatisch gelöscht. Dieser Löschprozess ist bereits in der von den Meldeämtern genutzten Software berücksichtigt und wird durchgeführt. Allerdings muss vor Ort sichergestellt sein, dass eine Datensicherung auf Band die digitalen Fingerabdrücke nicht einschließt, da ansonsten die archivierten Fingerabdrücke auch nach Aushändigung des Passes noch weiterhin gespeichert bleiben.

Abschließend kann festgestellt werden, dass jedenfalls in den von mir besuchten Kommunen das Verfahren der Beantragung eines elektronischen Passes datenschutzgerecht umgesetzt wurde.

8 Kommunales

8.1 Gesetz zur Reform der saarländischen Verwaltungsstrukturen - Verwaltungsstrukturreformgesetz (VSRG)

Das Gesetz bezweckt die legislative Umsetzung einer umfassenden Reform der Verwaltungsstrukturen im Saarland mit dem Ziel, zukunftsfähige Verwaltungseinheiten zu schaffen, deren Grundvoraussetzungen ein prozessorientierter Aufbau und eine strukturell gesicherte Finanzierung sind.

Im Rahmen der externen Anhörung wurde mir im April 2007 Gelegenheit gegeben, mich zu dem vorgelegten Regierungsentwurf zu äußern. Durch Artikel 1 Nr. 6 des VSRG wurde § 41 Absatz 3 Satz 1 des Kommunalselbstverwaltungsgesetzes (KSVG) dahingehend geändert, dass die Einberufung zur Sitzung des Gemeinderates an dessen Mitglieder zukünftig unter Mitteilung der Tagesordnung auch elektronisch an die Gemeinderatsmitglieder erfolgen kann, sofern die Empfängerin oder der Empfänger hierfür einen Zugang eröffnet. Von einem „eröffneten Zugang“ kann nur dann ausgegangen werden, wenn dies ausdrücklich in schriftlicher Form durch das Gemeinderatsmitglied erklärt worden ist. Die bloße Angabe einer E-Mail-Adresse auf dem Briefkopf genügt beispielsweise nicht.

Zum einen wird mit dieser Gesetzesänderung einer Forderung zahlreicher Kommunen, aber auch Mandatsträger Rechnung getragen, hinsichtlich der Nutzung des elektronischen Rechtsverkehrs durch die Zulassung auch einfacher Verfahren Akzeptanzdefizite abzubauen. Darüber hinaus ist diese Regelung, insbesondere wegen der früher fehlenden Rechtsgrundlage, aufgrund der nun gegebenen Normenklarheit und Rechtssicherheit für die Anwender erforderlich.

Da durch die vorgenannte Formulierung ein Zwang zur Schaffung der Voraussetzung einer elektronischen Kommunikation bei den Ratsmitgliedern vermieden wird, habe ich gleichfalls empfohlen, explizit darauf hinzuweisen, dass auch bei dieser Nutzung einfacher elektronischer Kommunikationsformen die schutzwürdigen Interessen Dritter, deren Angelegenheit in nichtöffentlicher Sitzung behandelt wird, unter allen Umständen zu beachten sind und gewahrt bleiben müssen.

Insbesondere habe ich angeregt, dass durch geeignete technische und organisatorische Maßnahmen der Datenschutz und die –sicherheit zu gewährleisten sind. Das VSRG trat mit Wirkung zum 01.01.2008 in Kraft.

Die faktische Umsetzung der Verwaltungsstrukturreform werde ich ebenfalls zukünftig aus datenschutzrechtlicher Sicht im Rahmen meiner Beratungs- und Kontrollfunktion zeitnah begleiten.

8.2 Erstellung eines qualifizierten Mietspiegels für eine saarländische Kommune

Die Städte und Gemeinden eines saarländischen Landkreises haben sich im Dezember 2006 für die Erstellung eines qualifizierten Mietspiegels ausgesprochen und den Landkreis mit dieser Aufgabe betraut. Dieser hat sich zur Klärung datenschutzrechtlicher Fragen im Mai 2007 an meine Geschäftsstelle gewandt.
Mietspiegel sind Übersichten über die üblichen Entgelte für Wohnraum in einer Gemeinde. Von einem qualifizierten Mietspiegel nach § 558d Bürgerliches Gesetzbuch (BGB) spricht man, wenn er nach anerkannten wissenschaftlichen Grundsätzen erstellt wurde und von der Gemeinde oder den Interessenvertretern der Vermieter und Mieter anerkannt wurde. Ein qualifizierter Mietspiegel ist alle zwei Jahre an die Marktentwicklung anzupassen und nach jeweils vier Jahren neu zu erstellen.
Der Landkreis entschied sich für die Durchführung einer Mieter- bzw. Vermieterbefragung mittels Versand eines Erhebungsbogens. Aus datenschutzrechtlicher Sicht habe ich bei dem angestrebten Verfahren nachdrücklich die Anonymisierung personenbezogener Daten gemäß § 3 Abs.8 SDSG gefordert. Es musste gewährleistet werden, dass eine Bestimmbarkeit des Betroffenen durch die von ihm erteilten Auskünfte über seine persönlichen oder sachlichen Verhältnisse in jedem Fall ausgeschlossen ist. Auf eine zunächst angestrebte Rücklaufkontrolle mittels eines gesondert markierten Rückumschlages wurde daher seitens des Landkreises verzichtet. Auch gegen die Übersendung von weiteren Fragebögen zu den Themen „Wohnpräferenzen“ und „Städtebau“ hatte ich erhebliche datenschutzrechtliche Bedenken, da die bereits zuvor erwähnte Anonymität nach § 3 Abs.8 SDSG nicht sichergestellt werden konnte. Im Übrigen waren einige in diesen Zusatzbögen gestellte Detailfragen mit der ursprünglichen Erhebungsabsicht „Mietspiegel“ nicht in Einklang zu bringen, so dass eine Erhebung diesbezüglich nicht erforderlich war. Auf meine Empfehlung hin wurde daher von der Übersendung der Zusatzfragebögen Abstand genommen. Die schriftliche Mieterbefragung wurde in der Zeit von Dezember 2007 bis März

2008 durchgeführt. Am 01.07.2008 wurde sodann der qualifizierte Mietspiegel veröffentlicht.
Derzeit liegen mir weitere Ersuchen von Städten und Gemeinden zur datenschutzrechtlichen Bewertung hinsichtlich beabsichtigter Befragungsarten im Rahmen einer Mietspiegelerstellung vor.

8.3 Videoüberwachung im kommunalen Bereich

Mit Sorge verfolge ich die zunehmende Tendenz in Kommunen, öffentliche Plätze, Gebäude und Einrichtungen mit Videokameras überwachen zu wollen und dieses scheinbar einfache Mittel bei der Bewältigung ihrer Aufgaben einzusetzen. Anlass solcher Überwachungen sind nach Angaben der Gemeinden Ruhestörungen, Schmierereien bis hin zu Vandalismus an kommunalen Bauten und Einrichtungen.

Bereits in meinem 21. Tätigkeitsbericht habe ich im Zusammenhang mit der Einführung einer Rechtsgrundlage im SDSG zur Videoüberwachung durch öffentliche Stellen darauf hingewiesen, dass eine derartig ausgestaltete Legalisierung des Videoeinsatzes für öffentliche Stellen den Anreiz dazu geben wird, alternative und für den Bürger weniger belastende Methoden zur Beseitigung von Alltagsproblemen nicht mehr näher in Betracht zu ziehen. Im Übrigen wird der Einsatz eines Videoüberwachungssystems dem Gebot der Datenvermeidung und Datensparsamkeit (§ 4 Abs. 4 SDSG) regelmäßig nicht gerecht.

Ich kann mich des Eindruckes nicht erwehren, dass in vielen Gemeinden das Bewusstsein noch nicht ausreichend dafür geschärft ist, dass die Beobachtung der Bürger mittels Videokameras einen Eingriff in deren allgemeines Persönlichkeitsrecht darstellt und diese dadurch einem latenten Anpassungsdruck ausgesetzt werden. Durch den Beschluss des Bundesverfassungsgerichts vom 23.02.2007 (1 BvR 2368/06) darf als geklärt angesehen werden, dass Videoüberwachungsanlagen mit Aufzeichnungsoption in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 i.V.m. mit Artikel 1 Absatz 1 GG eingreifen. Dort wurde unter anderem festgestellt, dass „verdachtlose Eingriffe mit großer Streubreite, bei denen zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden,

die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben, grundsätzlich eine hohe Eingriffsintensität aufweisen.“ Daher müssen Kommunen, die den Einsatz einer Videoüberwachung in Betracht ziehen, im Rahmen der Zulässigkeit solcher Überwachungsmaßnahmen stets prüfen, ob die Maßnahme zur Erfüllung des damit angestrebten Zwecks geeignet ist, keine milderen Mittel ergriffen werden können und eine Videoüberwachung die von ihr ausgehenden Grundrechtsbeeinträchtigungen noch rechtfertigt.
In diese Güterabwägung ist einzubeziehen, dass das Recht, sich unbeobachtet im öffentlichen Raum zu bewegen, durch eine Videoüberwachung stets eingeschränkt wird.
Eine Videoüberwachung ist nur in engen Grenzen zulässig, sofern ihre grundsätzliche Geeignetheit zu dem verfolgten öffentlichen Zweck vorausgesetzt werden kann. Gegenüber dem Zweck - gegebenenfalls der Verhinderung von Eigentumsstörungen - sind die Interessen der von der Überwachung betroffenen Bürger in aller Regel dann höher zu bewerten, wenn die Videoüberwachung Bereiche erfasst, die dem höchstpersönlichen oder gar dem Intimbereich der beobachteten Person zuzuordnen sind.

Im Saarland beziehen sich zahlreiche Kommunen bei der Videoüberwachung auf den durch das Gesetz zur Erhöhung der inneren Sicherheit im Saarländischen Datenschutzgesetz neu eingeführten § 34 SDSG.
Einige Fälle bezogen sich auf § 34 Abs. 1 Nr. 1 SDSG „Videoüberwachung zur Wahrnehmung des Hausrechtes“.
Die Wahrnehmung des Hausrechts vermag nun nur dann einen verhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung zu begründen, wenn konkrete Anhaltspunkte für erhebliche hausrechtsrelevante Vorkommnisse in öffentlich zugänglichen Bereichen vorliegen, denen mit dieser Technik wirksam begegnet werden kann.
Zu bedenken ist ebenfalls, dass das Hausrecht nur in seltenen Ausnahmefällen missachtet wird, bei der Videoüberwachung aber eine weit überwiegende Anzahl unbeteiligter Personen beobachtet wird, ohne dass diese zu einer Gefahrenlage auch nur das Geringste beigetragen haben bzw. beitragen werden.
Beschränkungen der Rechte der Bürger stehen unter dem grundsätzlichen Vorbehalt der Verhältnismäßigkeit, so dass stets restriktiv geprüft werden muss, ob die eingrei-

fende Maßnahme, also die Videoüberwachung, zur Wahrung des Hausrechtes, hier insbesondere Wahrung der Funktionsfähigkeit der Gebäude bzw. des Besitztums, erforderlich, geeignet und angemessen ist.

In den Fällen, welche sich auf die Videoüberwachung im Rahmen der „Aufgabenerfüllung“ beziehen (§ 34 Abs. 1 Nr. 2 SDSG), habe ich darauf hingewiesen, dass eine solche Art der Überwachung nur zulässig ist, wenn Anhaltspunkte für eine konkrete Gefährdung von Gesundheit, Leib oder Leben, Eigentum oder sonstigen hochrangigen Rechtsgütern vorliegen. Darüber hinaus dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen betroffener Bürger überwiegen (§ 34 Absatz 1 Satz 3 und 4 SDSG). Durch die meinerseits für unabdingbar erklärte entsprechende Schutzbedarfsanalyse in Verbindung mit geforderten Überlegungen zu Alternativen einer Videoüberwachung haben einige Kommunen von einer geplanten Videoüberwachung Abstand genommen und von Möglichkeiten Gebrauch gemacht, die für ihre Bürgerinnen und Bürger weniger belastend sind.

Festzuhalten bleibt, dass eine Videoüberwachung eine hohe Eingriffsintensität darstellt und zahlreiche Personen in den Wirkungsbereich der Maßnahme einbezogen werden, die zu keinem Zeitpunkt in irgendeiner Beziehung zu einem konkreten Fehlverhalten stehen.
Im Saarland sollte trotz teilweise sinnvoller Möglichkeiten hinsichtlich des Einsatzes moderner Videoüberwachung immer im Auge behalten werden, dass die Persönlichkeitsrechte der freien Bürger unseres Rechtsstaates nicht leichtfertig aufs Spiel gesetzt werden dürfen.
Ich habe bei den mit mir in Erörterung stehenden Kommunen den Eindruck gewonnen, dass nach eingehender Betrachtungsweise des Rechts- und Sachstandes sowie der Alternativen einer Videoüberwachung eine Sensibilisierung dieses Themas ergebnisreich im Sinne der Wahrung der Freiheitsrechte der Bürger gelungen ist.

So konnte in einem Fall die Kommune davon überzeugt werden, im Schwimmbad - insbesondere in den Zugängen zu den Umkleideräumen und zum Saunabereich - von einer Videoüberwachung Abstand zu nehmen. Vor allem die Überwachung des Eingangsbereiches einer Sauna kann regelmäßig nicht verhältnismäßig sein, da davon auszugehen ist, dass hier allein schon wegen der zu wahrenden Intimsphäre der

Betroffenen eindeutige Indikatoren bestehen, die die schutzwürdigen Interessen der Betroffenen überwiegen lassen.

In einem weiteren Fall wurde seitens einer Kommune erwogen, wegen wiederholter Schäden durch Vandalismus an den Schulgebäuden, das Schulhofgelände per Videotechnik zu überwachen. Eine Videoüberwachung an Schulen ist allein deshalb schon kritisch zu beurteilen, da sie sich grundsätzlich nicht mit dem Auftrag der Schule, die Entwicklung der Schüler zu selbstbestimmten, mündigen Persönlichkeiten zu fördern, vereinbaren lässt. Die im konkreten Fall geschilderte Störung, nämlich Schaden durch Vandalismus, rechtfertigt - wegen der enormen Beeinträchtigung der Persönlichkeitsrechte der Schüler und Lehrer - in keinem Maße eine Videoüberwachung während des Schulbetriebes. Auch in diesem Fall verfolgte die betreffende Kommune aufgrund meiner datenschutzrechtlichen Bedenken ihre Pläne hinsichtlich des Einsatzes einer Videotechnik nicht weiter.

Aus der Sicht des Datenschutzes ist nämlich besonders zu beachten, dass der Einsatz von Videotechnik für öffentliche Stellen – betrachtet man zudem die vorstellbaren Anwendungsfälle – für die Bevölkerung regelmäßig keinen objektiven Sicherheitsgewinn bringt, sondern nur Verlagerungseffekte bedingt.
Ich werde jedenfalls gemäß § 7 Abs. 2 SDSG auch weiterhin die zukünftige erstmalige Einführung jeglicher Videoüberwachungsvorrichtungen durch öffentliche Stellen aufmerksam verfolgen.

8.4 Zusammenarbeit der Stadtkasse einer saarländischen Kommune mit privatem Inkassounternehmen

Eine saarländische Stadt hat sich im Januar 2008 an mich gewandt mit der Frage, ob datenschutzrechtliche Bedenken dagegen bestehen, private Inkassounternehmen bei der Durchsetzung von Forderungen der Kommune einzuschalten.
Hierzu hat sie mir den Entwurf einer Vereinbarung zwischen der Stadt und dem in Rede stehenden Inkassounternehmen zugesandt.
Grundlage der Vereinbarung seien die gesetzlichen Vorschriften zur Beitreibung öffentlich rechtlicher Forderungen nach saarländischem Verwaltungsvollstreckungsge-

setz. Eine Abtretung der Forderung an das Inkassounternehmen fände nicht statt, die vereinbarten Tätigkeiten würden im Hinblick auf die Verarbeitung personenbezogener Daten vom Auftragnehmer für den Auftraggeber gemäß den Bestimmungen des § 5 SDSG im Auftrag verarbeitet. Vertragsgegenstand sei die Einziehung von Forderungen des Auftraggebers gegen seine Schuldner, worunter angemahnte und schon mit Vollstreckungsauftrag bezeichnete Forderungen im Sinne des Saarländischen Verwaltungsvollsteckungsgesetzes zu verstehen seien.
Der Auftrag umfasse u. a. im Einzelnen folgende Tätigkeiten:
- Übernahme der Einzugsfälle in das Forderungsmanagement des Auftragnehmers
- Führung der im Einzugsverfahren anfallenden Korrespondenz mit den Schuldnern
- Überprüfung der Bonität des Schuldners durch Einholen einer Wirtschaftsauskunft.
Darüber hinaus sei der Auftragnehmer berechtigt, mit den Schuldnern den Abschluss von Ratenzahlungsvereinbarungen und Vergleichen vorzubereiten.
Das Vorhaben solle derart ausgestaltet werden, dass es den Anforderungen der Auftragsdatenverarbeitung gemäß § 5 SDSG entspricht.

In meiner Stellungnahme hierzu habe ich zunächst dargelegt, dass es wohl zu den primären Aufgaben einer Kommune gehört, ihre öffentlich-rechtlichen und privatrechtlichen Forderungen selbst beizutreiben, weswegen auch der Gesetzgeber ihnen richtigerweise das Verwaltungszustellungs- und Vollstreckungsgesetz als erforderliches rechtliches Instrumentarium zur Verfügung gestellt hat. Um eine verfassungskonforme Antwort auf die im Vertragsentwurf aufgeworfenen datenschutzrechtlichen Fragen – vor allem die grundsätzliche Frage nach der datenschutzrechtlichen Zulässigkeit einer Zusammenarbeit von kommunalen Gebietskörperschaften mit Inkassobüros zwecks Realisierung geldwerter Ansprüche – zu geben, bedarf es aus meiner Sicht einer bereichsspezifischen und normenklaren gesetzlichen Regelung. Insbesondere sollte eine solche Regelung auf einer datenschutzrechtlich tragfähigen Grundlage errichtet und dadurch Datenschutzstandards sichergestellt werden.

Gleichwohl neige ich zu der Auffassung, dass die Einschaltung privater Inkassobüros als echte Verwaltungshelfer bei der Beitreibung kommunaler Forderungen aus datenschutzrechtlicher Sicht nach geltendem Recht nicht von vornherein gänzlich ausgeschlossen ist. Insbesondere der Aspekt, dass die Verwaltungshelfertätigkeit sich ausschließlich auf eine reine Verarbeitung personenbezogener Daten im Sinne einer

Auftragsdatenverarbeitung beschränkt, dieses wiederum in der vertraglichen Vereinbarung klar und deutlich ersichtlich und die praktische Umsetzung der geschlossenen Verträge tatsächlich ihrem Wortlaut entsprechen würde, könnte die Einschaltung privater Inkassounternehmen vertretbar erscheinen lassen. In der besagten Angelegenheit hielte ich denn auch lediglich eine Übertragung von echten Hilfstätigkeiten im Rahmen einer Auftragsdatenverarbeitung nach § 5 SDSG für zulässig. Dem vorgelegten Vertragsentwurf konnte ich jedoch nicht entnehmen, ob es sich hier um eine allumfassende Zusammenarbeit handeln soll, die alle öffentlich rechtlichen Forderungen einschließlich etwaiger Amtshilfeersuchen aber auch alle privatrechtlichen Forderungen erfasst. Jedenfalls erhob ich die Forderung, dass eine hinreichend bestimmte Festlegung von Gegenstand und Umfang der Datenverarbeitung im Rahmen der Auftragsdatenverarbeitung im vorliegenden Fall inhaltlich präzise ausgeführt werden müsse.
Im Übrigen halte ich – wie zuvor ausgeführt – eine Übertragung von echten Hilfstätigkeiten als echte Verwaltungshelfer durch Auftragsdatenverarbeitung für grundsätzlich zulässig. Insofern ist eine ganzheitliche Übertragung von den der Kommune zustehenden hoheitlichen Befugnissen zur Forderungsbeitreibung auf Private unzulässig. Dies impliziert, dass eine Übertragung von Tätigkeiten, bei der das Inkassounternehmen im jeweiligen Einzelfall über das Vorgehen gegen den Schuldner und die Art der konkreten Ausgestaltung der dabei zu treffenden Maßnahmen entscheiden würde, unzulässig ist. Dieser Tatbestand einer konkludenten Aufgabenübertragung spiegelte sich im vorgelegten Vertrag wieder, da meines Erachtens unzulässigerweise dem Auftragnehmer Gestaltungs- und Ermessungsspielräume eingeräumt wurden und der Auftragnehmer dadurch berechtigt sei, mit den Schuldnern den Abschluss von Ratenzahlungsvereinbarungen und Vergleichen vorzubereiten.
Datenschutzrechtlich zulässig wäre es allenfalls, sich als echter Verwaltungshelfer verschärft um Zahlungserinnerungen zu bemühen. Vollstreckungsmaßnahmen einschließlich Billigkeitsmaßnahmen und auch faktische Zahlungsvereinbarungen darf aber ein Inkassobüro auf keinen Fall im Auftrag der öffentlichen Hand vornehmen bzw. abschließen.

Im Übrigen habe ich darauf hingewiesen, dass ein Vertrag gemäß § 5 SDSG (Auftragsdatenverarbeitung) auch die Vorlage von Betriebskonzepten über die praktische Umsetzung und technische Zuverlässigkeit des Inkassobüros vorsehen muss. Auch

hat das beauftragte Unternehmen sich bezüglich der vertraglich übernommenen Aufgabe ebenfalls meiner Kontrolle zu unterwerfen. Auch wäre sicherzustellen, dass durch die Verwaltungshelfertätigkeit gesammelte Daten nicht willentlich oder auch nur versehentlich zweckentfremdet werden. Dies würde – der augenblicklichen saarländischen Rechtslage gemäß – besondere Aufmerksamkeit und besondere Anstrengungen der Stelle für privaten Datenschutz beim saarländischen Innenministerium bedingen.

Gleichwohl mag ich meine Verwunderung darüber nicht verhehlen, dass zum einen sich die betreffende Kommune durch Übertragung reiner Verwaltungshelfertätigkeiten Optimierungserfolge bei der Vollstreckung von Forderungen erwartet, andererseits ein privates Inkassounternehmen sich offenkundig unter den vom geltenden Recht vorgegebenen Voraussetzungen bei der Übernahme reiner Verwaltungstätigkeiten wirtschaftlichen Erfolg verspricht.

Im Dezember 2008 habe ich erfahren, dass die betreffende Kommune ihre Forderungen weiterhin selbst eintreiben wird und diese Aufgabe nicht an ein privatwirtschaftliches Inkassounternehmen abgegeben hat. Jenseits der datenschutzrechtlichen Fragen wird im Übrigen bei derartigen Plänen von Kommunen letztendlich die zuständige Oberste Landesbehörde die Frage beantworten müssen, ob sie die Auffassung des Innenministeriums des Landes Niedersachsen (Erlass vom 30.06.2008) teilt, welches explizit feststellt, dass die zur Betreibung öffentlich-rechtlicher Forderungen der Kommunen vom Landtag des Landes Niedersachsen erlassenen Vorschriften umfassend, detailliert und hiermit abschließend sind, oder ob die Oberste Landesbehörde die Auffassung vertritt, das saarländische Verfassungs-, Zwangsvollstreckungs- und Kommunalrecht eröffne ganz andere Möglichkeiten der Vollstreckungsprivatisierung als in Niedersachsen.

9 Soziales

9.1 Abruf von Kontendaten bei Hartz-IV-Bezug

Wenn jemand einen Antrag auf Arbeitslosengeld II stellt, bekommt er gleichzeitig ein Merkblatt ausgehändigt, in dem er darauf hingewiesen wird, dass die ARGE zur Klärung der Einkommens- und Vermögensverhältnisse beim Bundeszentralamt für Steuern ein Abrufersuchen stellen kann.
Verschiedentlich haben Bürger bei meiner Dienststelle angefragt, was es mit diesem Abrufersuchen auf sich hat, ob ein solcher Datenabruf überhaupt zulässig ist und welche Voraussetzungen gegebenenfalls vorliegen müssen.

Grundsätzlich ist dazu zu sagen, dass ein solches Abrufersuchen seine Rechtsgrundlage in der Abgabenordnung (§ 93 Absatz 8 und 9 AO) hat.
Die ARGEN dürfen das Bundeszentralamt für Steuern ersuchen, bei den Kreditinstituten Kontenstammdaten, wie z.B. Name, Geburtsdatum, Kontonummern und Depots, abzurufen. Dabei werden Kontostände und Umsätze nicht mitgeteilt.
Voraussetzung ist, dass die Daten zur Überprüfung der Anspruchsvoraussetzungen erforderlich sind und ein vorheriges Auskunftsersuchen an den Betroffenen nicht zum Ziel geführt hat oder keinen Erfolg verspricht. Routinemäßige oder anlasslose Abrufe sind demzufolge unzulässig.
Gegenüber dem Antragsteller bestehen Informationspflichten: Vor der Durchführung eines Kontenabrufes ist der Antragsteller auf die Möglichkeit des Kontenabrufs hinzuweisen. Nach der Durchführung eines Kontenabrufes ist der Antragsteller auch über das Ergebnis zu informieren.
Die Erforderlichkeit des Ersuchens muss in der Leistungsakte dokumentiert werden. Dies ermöglicht eine Prüfung der Rechtsmäßigkeit des Kontenabrufverfahrens sowohl durch den Betroffenen als auch die staatlichen Datenschutzaufsichtsbehörden.

Ich habe mir für den nächsten Berichtszeitraum vorgenommen, bei verschiedenen ARGEN im Saarland zu prüfen, ob die Voraussetzungen für einen rechtmäßigen Kontenabruf dort eingehalten werden.

9.2 Akteneinsicht

So vielfältig die Anlässe für Eingaben von Bürgern bei meiner Dienststelle sind, so gibt es eine Thematik, mit der ich mich leider immer wieder beschäftigen muss: Beschwerden über nicht erteilte Akteneinsicht im Sozialbereich.

Es ist sicherlich richtig, dass es Gründe gibt, eine Akteneinsicht zu versagen. Festzustellen ist allerdings auch, dass oft völlig sachwidrige Argumente für eine ablehnende Entscheidung der Behörden herangezogen werden. So habe ich mehr als einmal das Argument gehört, der Datenschutz (bei eigenen Daten!) stehe dem entgegen.

Ich möchte deshalb noch einmal die Rechtslage im Sozialleistungsbereich darstellen. Im Zehnten Buch des Sozialgesetzbuches (SGB X) gibt es zwei Vorschriften, in denen das Akteneinsichts- bzw. Auskunftsrecht geregelt ist.

Gemäß § 25 SGB X hat die Behörde den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Der auf § 25 SGB X gestützte Anspruch auf Akteneinsicht ist wesentliche Voraussetzung dafür, dass die Beteiligten ihren Anspruch auf rechtliches Gehör realisieren können. Voraussetzung ist insofern, dass ein Verwaltungsverfahren anhängig ist, d.h. ein Verfahren, das auf den Erlass eines Verwaltungsaktes gerichtet ist.

Eine andere Zweckrichtung hat der Auskunftsanspruch nach § 83 SGB X, wonach dem Betroffenen Auskunft zu erteilen ist über die zu seiner Person gespeicherten Sozialdaten. Dieses Auskunftsrecht leitet sich unmittelbar aus dem Recht auf informationelle Selbstbestimmung her, nach der eine Gesellschaftsordnung und eine dies ermöglichende Rechtsordnung gegen die Rechte aus Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 Grundgesetz verstoßen würde, wenn der Bürger nicht mehr erfahren kann, wer was wann und bei welcher Gelegenheit über ihn weiß (Urteil des Bundesverfassungsgerichts vom 15.12.1983, Az.: BvR 209/83). Das Auskunftsrecht ist die Grundlage, um weitergehende Datenschutzrechte, wie z.B. Ansprüche auf Schadensersatz oder auf Berichtigung oder Löschung von Daten überhaupt erst geltend machen zu können.

Allerdings unterbleibt eine Auskunftserteilung in bestimmten Fällen, insbesondere soweit die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen, und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

Wenn sich eine Behörde bei einem Antrag auf Akteneinsicht mit diesen Voraussetzungen auseinandersetzt und zu dem Ergebnis kommt, dass die Akteneinsicht im Einzelfall nicht erteilt werden kann, so ist dies nicht zu beanstanden. In diesen Fällen muss ich den Betroffenen mitteilen, dass ein Akteneinsichtsrecht nicht besteht. Kein Ablehnungsgrund ist dagegen das immer wieder vorgebrachte Argument, ein Akteneinsichtsrecht bestehe nicht hinsichtlich solcher Daten, die die Behörde von anderen Stellen erhalten habe; der Betroffene solle sein Akteneinsichtsrecht dort geltend machen. Denn es ist das Recht jedes Bürgers zu erfahren, welche Daten eine Behörde über ihn gespeichert hat, gleichgültig aus welcher Quelle die Angaben stammen.

9.3 ELENA (Elektronischer Einkommensnachweis)

Bereits in meinem 20. Tätigkeitsbericht 2003/2004 (TZ. 8.4) habe ich über das Projekt des Bundesministeriums für Wirtschaft und Arbeit berichtet, das die Speicherung der Einkommensdaten aller Beschäftigten bei einer zentralen Speicherstelle zum Gegenstand hat. Dadurch sollen die Arbeitgeber von ihrer Verpflichtung entlastet werden, für die verschiedensten Sozialleistungen Verdienstbescheinigungen in Papierform auszustellen.

Im Berichtszeitraum wurde nunmehr der Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492).

Die Brisanz des Vorhabens war Anlass für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, sich in zwei Entschließungen vom 8./9.03.2007 (Anlage 21.3) sowie vom 6./7.11.2008 (Anlage 21.26) mit der Thematik zu befassen.

Die Bedenken der Datenschutzbeauftragten resultieren einmal aus Zweifeln an der Verfassungsmäßigkeit des Gesetzes und hier speziell unter dem Gesichtspunkt der Erforderlichkeit. Es ist davon auszugehen, dass ein großer Anteil der Betroffenen die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals geltend machen wird.

Auf jeden Fall sind unter dem Gesichtspunkt des technisch-organisatorischen Datenschutzes noch Verbesserungen erforderlich, wozu z.B. gehört, dass die Schlüssel zur Ver- und Entschlüsselung der bei der zentralen Speicherstelle gespeicherten Daten nicht in der Verfügungsgewalt der zentralen Speicherstelle liegen dürfen. Im Übrigen

verweise ich speziell zu diesem Punkt auf die oben erwähnte Entschließung vom 6./7.11.2008.

9.4 Kontrollanrufe der Krankenkassen bei Krankengeldbeziehern

Eine besorgte Krankengeldbezieherin wandte sich mit einer Eingabe an mich, in der sie anfragte, ob es zulässig sei, dass ihre Krankenkasse bei ihr zu Hause mehrmals angerufen habe, um sich über Ihren aktuellen Gesundheitszustand zu informieren und die Behandlungsvorschläge des Hausarztes zu erfragen. Darüber hinaus sei ihr Arbeitgeber von der Krankenkasse um eine Arbeitsplatzbeschreibung gebeten worden.

Die betreffende Krankenkasse um Stellungnahme zu den Vorwürfen gebeten, gab in ihrer Antwort als Begründung für die Anrufe an, es sei Ihre Pflicht gemäß §§ 13 ff. SGB I ihre Versicherten über Anspruch und Zahlungsweise des Krankengeldes zu informieren.

Diese Antwort konnte ich so nicht ganz nachvollziehen. Zwar obliegt der Krankenkasse eine Informationspflicht der Versicherten gem. §§ 13 ff. SGB I, jedoch kommt sie dieser Pflicht in ausreichender Form nach, wenn durch Angebote im Internet, Anschreiben oder per Flyer die Versicherten über die beantragten Leistungen informiert werden. Sollten weitere Informationen gewünscht sein, obliegt es dem Versicherten, mit der Krankenkasse Kontakt aufzunehmen. Eine telefonische Kontaktaufnahme ohne den Zweck des Gespräches offen zu legen und auf die Freiwilligkeit zur Beantwortung der Fragen hinzuweisen, stellt einen tiefen Eingriff in die Privatsphäre der Versicherten dar und ist nicht durch die §§ 13 ff. SGB I legitimiert. Sollten Zweifel an der Arbeitsunfähigkeit bestehen, hat die Krankenkasse gem. § 275 Absatz 1 Nummer 3 Buchstabe a SGB V den Medizinischen Dienst der Krankenkassen zu Klärung der Arbeitsunfähigkeit einzuschalten. Ich habe die Krankenkasse gebeten, von der geübten Praxis der Telefonanrufe abzusehen.

Die Arbeitsplatzbeschreibung des Arbeitgebers wurde nach Auskunft der Krankenkasse benötigt, da die Beurteilung der Arbeitsunfähigkeit unter anderem auch von der Beschaffenheit des Arbeitsplatzes abhänge. Als rechtliche Grundlage wurde hier § 98 SGB X angeführt, wonach der Arbeitgeber auf Verlangen des Leistungsträgers Auskunft über die Art und Dauer der Beschäftigung erteilen muss, soweit es in der

Sozialversicherung einschließlich der Arbeitslosenversicherung im Einzelfall für die Erbringung von Sozialleistungen erforderlich ist.
Die Gewährung der Sozialleistung muss maßgebend von der Auskunft des Arbeitgebers abhängen. Dies ist zum Beispiel der Fall, wenn zur Berechnung der Höhe des Krankengeldes eine Entgeltbescheinigung des Arbeitgebers angefordert wird, nicht aber bei einer Arbeitsplatzbeschreibung. Eine Anfrage beim Arbeitgeber ist hier für die Erbringung der Sozialleistung Krankengeld nicht erforderlich. So sind in den §§ 44 ff. SGB V keine Voraussetzungen zur Zahlung von Krankengeld aufgeführt, die eine Krankengeldgewährung vom jeweiligen Arbeitsplatz abhängig machen. Vielmehr entsteht der Anspruch auf Krankengeld für Pflichtversicherte gemäß § 46 Satz 1 Nummer 2 SGB V von dem Tag an, der auf den Tag der ärztlichen Feststellung der Arbeitsunfähigkeit folgt. Voraussetzung für die Entscheidung ob ein Krankengeldanspruch vorliegt, ist hier lediglich die Vorlage der ärztlichen Feststellung, dass eine Arbeitsunfähigkeit vorliegt. Es fehlt die Erforderlichkeit, um § 98 SGB X als rechtliche Grundlage der Datenübermittlung heranziehen zu können. Sicherlich gibt es unterschiedliche Anforderungen an unterschiedlichen Arbeitsplätzen; letztendlich muss jedoch ein Mediziner die Entscheidung vertreten, ob an diesem Arbeitsplatz eine Arbeitsunfähigkeit vorliegt oder nicht. Die Einschaltung des Medizinischen Dienst der Krankenkassen in dieser Frage ist gemäß § 275 Absatz 1 Nummer 3 Buchstabe b SGB V für die Krankenkasse verpflichtend, soweit Zweifel an der Arbeitunfähigkeit bestehen.
Ich habe die Krankenkasse gebeten, Anfragen an den Arbeitgeber auf die in § 98 SGB X aufgeführten Fallkonstellationen zu beschränken.

9.5 Rückforderung überzahlter Rentenbeträge vom Vermieter

Nach dem Tode ihrer Mieterin wurden die Vermieter der Wohnung von der Deutschen Rentenversicherung (DRV) Saarland mit einem Anhörungsschreiben konfrontiert, in dem sie zur Rückzahlung der nach Ablauf des Todesmonats überzahlten Rente aufgefordert werden sollten, weil nach dem Todesmonat die Miete weiterhin per Dauerauftrag auf das Konto der Vermieter angewiesen wurde. In dem Anschreiben der DRV Saarland wurden den Vermietern alle rentenrechtlich relevanten Daten der Verstorbenen wie Höhe der Rente, Kontonummer, Bankleitzahl, Abzüge zur

Kranken- und Pflegeversicherung offenbart. Diesen Umstand beanstandend wandten sich die Vermieter an meine Geschäftsstelle mit der Bitte, zu überprüfen, ob das Anhörungsschreiben der DRV Saarland datenschutzgerecht gestaltet sei.
Es handelt sich bei dieser Sachlage um eine Übermittlung von Sozialdaten der Mieterin an die Vermieter durch die DRV Saarland. Eine solche Datenübermittlung ist gemäß § 67 d SGB X nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder einer anderen Rechtsvorschrift dieses Gesetzbuches vorliegt. Das Fehlen einer Übermittlungsbefugnis im Sinne des § 67 d SGB X veranlasste mich, die DRV Saarland um Stellungnahme zu bitten.
Im Ergebnis teilte mir die DRV Saarland mit, dass die von ihr eingesetzten Vordrucke zur Anhörung und Rückforderung eines nach dem Tode der Versicherten zu Unrecht gezahlten Betrages nach § 118 Absatz 4 SGB VI tatsächlich Angaben zum Überweisungsweg sowie zur Rentenzahlung der Leistungsberechtigten enthielten, die zur Rückforderung der zu Unrecht erbrachten Leistungen nicht erforderlich seien. Es wurde umgehend eine Überarbeitung der Vordrucke veranlasst, womit in Zukunft eine datenschutzkonforme Regelung gewährleistet ist.

9.6 Stellungnahme einer Firma zur Bewerbung eines ALG-II-Beziehers

Ein Arbeitslosengeld-II-Bezieher hat sich über die Vorgehensweise einer Firma, bei der er sich auf eigenes Betreiben hin beworben hatte, bei meiner Geschäftsstelle beschwert. Nachdem er sich bei der Firma aufgrund einer selbst gesuchten Stellenanzeige beworben hatte, wurde er von Seiten seines Sachbearbeiters bei der zuständigen ARGE über die Art und Weise seiner Bewerbung angesprochen. Die Firma hatte die Bewerbung des Petenten ohne dessen Einwilligung an die ARGE übersandt und darauf hingewiesen, dass die Art und Weise, wie der Arbeitslosengeld-II-Bezieher an die Firma herangetreten sei, dazu geführt habe, von einem möglichen Vorstellungsgespräch abzusehen. Sollten dem Arbeitsvermittler andere arbeitswillige und motivierte Bewerber bekannt sein, so würde man sich über eine Rückmeldung der ARGE freuen.

Ich habe die ARGE um Stellungnahme gebeten, ob von ihrer Seite aus eine Datenübermittlung von potentiellen Arbeitgebern in solchen Fällen gefordert wird oder ob die Firma aus eigenem Antrieb tätig wurde.
Aus der Antwort der ARGE ergibt sich, dass keine Dienstanweisung existiert, von möglichen Arbeitgebern zu verlangen, eventuell missbräuchliche Bewerbungen von Arbeitslosengeld-II-Beziehern zu melden. Die Firma informierte die ARGE also aus eigenem Interesse heraus. Ich habe den Petenten daraufhin informiert, dass hier die Datenübermittlung der Firma an die ARGE datenschutzrechtlich zu bewerten ist. Gegenüber der Firma habe ich keine Aufsichtsbefugnis. Wenn er die Zulässigkeit der Datenübermittlung datenschutzrechtlich überprüfen lassen wolle, müsse er sich an die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich beim Ministerium für Inneres und Sport wenden.

9.7 Steuerungsprogramme der Krankenkassen

Die Aufgaben der Krankenkassen beschränken sich nicht auf die Abrechnung der von ihren Versicherten in Anspruch genommenen Leistungen; sie sind vielmehr vom Gesetzgeber gehalten, ihren Versicherten ein Versorgungsmanagement anzubieten, z.B. in Form von Patientenschulungsmaßnahmen oder strukturierten Behandlungsprogrammen für chronisch kranke Patienten. Die Inanspruchnahme solcher Angebote erfolgt in unserem Gesundheitssystem auf freiwilliger Basis. Festzustellen ist demgegenüber, dass einzelne Krankenkassen – durchaus in bester Absicht – versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen.
Vielfach bedienen sich die Krankenkassen bei Durchführung dieser Maßnahmen privater Dienstleister. Hier stellt sich das Problem der Übermittlung der Versichertendaten an diese privaten Stellen.
Die Datenschutzbeauftragten des Bundes und der Länder haben sich auf ihrer Konferenz am 6. und 7. November 2008 mit dieser Thematik befasst und in einer Entschließung (Anlage 21.30) Eckpunkte formuliert, die die Krankenkassen bei gesundheitlichen Steuerungsprogrammen zu beachten haben.

9.8 Unzulässige Anforderung der Schwerbehindertenakte durch die Aufsichtsbehörde

Eine Beschwerde gegen die Vorgehensweise einer ARGE an die zuständige Aufsichtsbehörde beim damaligen Ministerium für Justiz, Gesundheit und Soziales, führte dazu, dass das Ministerium vom Landesamt für Soziales, Gesundheit und Verbraucherschutz die Schwerbehindertenakte des Petenten anforderte. Gegen diese Übermittlung sensibler Sozialdaten richtete sich die Eingabe an meine Geschäftsstelle.

Zur Begründung für die Anforderung der Schwerbehindertenakte gab das Ministerium an, der Petent hätte als Eingangsformel seiner Beschwerde den Umgang der Behörden mit Schwerbehinderten angeführt. Als Rechtsgrundlage führte das Ministerium § 69 Absatz 5 SGB X an, wonach eine Datenübermittlung von Sozialdaten unter anderem dann zulässig ist, wenn die zuständige Aufsichtsbehörde Ihrer Aufsichtspflicht nachkommen muss.

Hier lag aber keine Beschwerde gegen das Landesamt für Soziales, Gesundheit und Verbraucherschutz als zuständige Behörde für die Schwerbehindertenangelegenheit des Petenten vor. Vielmehr sollte das Verhalten der ARGE durch das Ministerium überprüft werden. Die Schwerbehinderteneigenschaft des Petenten hatte mit dem eigentlichen Anliegen der Eingabe nichts zu tun. Die Übermittlung der Schwerbehindertenakte wäre aufgrund der fehlenden Übermittlungs- und Erhebungsbefugnis nur mit Einwilligung des Petenten zulässig gewesen. Diese lag hier aber unstrittig nicht vor.

Ich habe das Ministerium für Justiz, Gesundheit und Soziales über die unrechtmäßige Datenerhebung informiert. Von einer Beanstandung habe ich aufgrund der nicht eindeutigen Formulierung des Anliegens durch den Petenten abgesehen.

9.9 Vorlage der ersten Gehaltsabrechnung an die ARGE

Nachdem ein Bezieher von Arbeitslosengeldgeld II zum 10. eines Monats wieder Arbeit gefunden hatte, wurde sein neuer Arbeitgeber von Seiten der ARGE mit der Bitte angerufen, mitzuteilen, wann die erste Lohnauszahlung erfolge. Wenig später erhielt der Petent ein Schreiben der ARGE, in dem er gebeten wurde, seine vollständige

erste Gehaltsmitteilung an die ARGE zu übersenden. Durch die Vorgehensweise der ARGE irritiert, wandte sich der Petent an meine Geschäftsstelle, um überprüfen zu lassen, ob dieses Vorgehen datenschutzrechtlich zulässig sei. Schließlich werde der neue Arbeitgeber durch den Anruf über die vorhergehende Arbeitslosigkeit informiert und durch die Übersendung der kompletten, ungeschwärzten Gehaltsmitteilung würden der ARGE Daten bekannt gegeben, die für ihre Aufgabenerfüllung nicht erforderlich seien.

Auf meine Bitte um Stellungnahme antwortete mir die ARGE, dass das erzielte Einkommen gemäß § 11 SGB II im Rahmen der Gewährung von Arbeitslosengeld II in dem Kalendermonat berücksichtig und auf die Leistungen der Sozialbehörde angerechnet wird, in dem das Arbeitsentgelt tatsächlich gezahlt wird (Zuflussprinzip).

Da eine Befragung des Betroffenen nicht erfolgen konnte, da er sich zu diesem Zeitpunkt im Ausland aufhielt und seine fehlende Erreichbarkeit der ARGE mitgeteilt hatte, war die Nachfrage beim Arbeitgeber gemäß § 67a Absatz 2 Satz 2 Nummer 2 SGB X aus datenschutzrechtlicher Sicht zulässig, da die unmittelbare Beantwortung für die Aufgabenerfüllung der ARGE erforderlich war.

Die Anfrage beim Betroffenen nach der ersten Gehaltsmitteilung begründete die ARGE damit, dass sie über die Gewährung ergänzender Leistungen zum Arbeitslosengeld II in Form eines Darlehens (§ 23 Abs.1 SGB II) bis zur ersten Auszahlung des Lohnes nur entscheiden könne, wenn ihr eine Gehaltsbescheinigung und eine Kostenübersicht vorgelegt werde.

Allerdings hat der Petent keinen Antrag auf ergänzende Leistungen zum Arbeitslosengeld II gestellt. Auch wurde von Seiten der ARGE weder der Zweck der Anforderung der Gehaltsbescheinigung angegeben, noch auf die Möglichkeit des Schwärzens von nicht erforderlichen Daten in der Gehaltsbescheinigung hingewiesen. Eine Kostenübersicht wurde von Seiten der ARGE ebenfalls nicht angefordert.

Als Konsequenz stellte ich folgende datenschutzrechtliche Forderungen an die ARGE:

1. Die ARGE muss ausdrücklich darauf hinweisen, dass die Vorlage einer Gehaltsbescheinigung nur für den Fall der Beantragung von ergänzenden Leistungen bis zur ersten Gehaltsauszahlung und nur im Zusammenhang mit einer Kostenaufstellung erforderlich ist.
2. Im Vorfeld der Übersendung von Gehaltsbescheinigungen muss von Seiten der ARGE auf die Möglichkeit des Schwärzens einiger, für die Leistungsge-

währung nicht relevanter Daten, wie zum Beispiel Religionszugehörigkeit, hingewiesen werden.

9.10 Vorlage von Kontoauszügen bei Hartz IV

Auch im Berichtszeitraum haben wieder mehrere Bürger bei meiner Dienststelle angefragt, ob sie bei Beantragung von Arbeitslosengeld II zur Vorlage von Kontoauszügen verpflichtet sind.

Bei dem Verlangen nach Vorlage von Kontoauszügen handelt es sich um einen recht tiefgehenden Eingriff in die Privatsphäre der Betroffenen. Dies gilt in besonderem Maße bei Abbuchungen, bei denen meist der Verwendungszweck angegeben ist, z.B. Mitgliedsbeiträge an Parteien oder Spenden für bestimmte Organisationen.
Klare gesetzliche Vorgaben ob, und in welchem Umfang der Leistungsträger bei der Beantragung von Sozialleistungen die Vorlage von Kontoauszügen verlangen darf, gibt es nicht, was in der Vergangenheit zu divergierenden Gerichtsurteilen zu der Problematik geführt hat.
Aufgrund der Klage eines Betroffenen musste sich das Bundessozialgericht mit der umstrittenen Frage befassen. Mit Urteil vom 19. September 2008 hat das Bundessozialgericht (Az.: B14 AS 45/07 R) entschieden, dass eine grundsätzliche Pflicht zur Vorlage von Kontoauszügen besteht. Das Gericht leitet diese Verpflichtung her aus § 60 Absatz 1 Nr. 3 SGB I, wonach derjenige, der Sozialleistungen beantragt oder erhält, die Beweismittel zu bezeichnen und auf Verlangen des zuständigen Leistungsträgers Beweisurkunden vorzulegen hat.
Die Vorlagepflicht sei nicht auf konkrete Verdachtsfälle beschränkt. Hinsichtlich der zeitlichen Erstreckung sei die Vorlage von Kontoauszügen jedenfalls der letzten drei Monate nicht unverhältnismäßig.
Das Gericht hat sich auch mit der strittigen Frage beschäftigt, ob eine Vorlagepflicht nur bei dem Erstantrag oder auch bei der Stellung weiterer Folgeanträge besteht. Auch die Aufforderung bei Stellung eines Folgeantrages wurde als rechtmäßig angesehen.
Das Gericht hat allerdings die Rechte der Antragsteller in einem wichtigen Punkt gestärkt: Aus den Regelungen des Sozialdatenschutzes ergebe sich, dass der Grundsi-

cherungsempfänger die Möglichkeit habe, auf der Ausgabenseite die Empfänger von Zahlungen zu schwärzen oder unkenntlich zu machen, wenn diese Zahlungen besondere personenbezogene Daten betreffen (etwa Beiträge für Gewerkschaften, politische Parteien, Religionsgemeinschaften usw.). Allerdings müssten die überwiesenen Beträge auch in diesen Fällen für den Grundsicherungsträger erkennbar bleiben.

Ich begrüße diese Klarstellung durch das Bundessozialgericht und werde die Maßstäbe des Gerichts meiner zukünftigen Beratungspraxis zugrunde legen.

9.11 Wahrung des Sozialdatenschutzes bei Vorsprache

Auch im letzten Berichtzeitraum habe ich mehrere Eingaben erhalten, der Datenschutz sei in sogenannten „Servicecentern“ nicht gewährleistet. Auf die Eingaben der Petenten reagierend, haben Mitarbeiter meiner Geschäftstelle bei Vorortbesuchen die Situation in Augenschein genommen.
Bei den Ortsbesichtigungen wurde festgestellt, dass ein Mithören von Anliegen der Antragsteller durch die vorhandenen Schallschutzmaßnahmen in den meisten Fällen nicht verhindert wird. Aufgrund dieser Tatsache musste ich aus datenschutzrechtlicher Sicht feststellen, dass die dem Sozialgeheimnis (§ 35 SGB I) unterliegenden persönlichen Daten im Bereich der Sachbearbeitung der Behörden nicht ausreichend gegen unbefugte Kenntnisnahme geschützt werden.
Ich habe deshalb gefordert, dass geeignete Maßnahmen zu treffen sind, die eine Beachtung des Sozialgeheimnisses gewährleisten.
Vorsorglich habe ich in diesem Zusammenhang schon darauf hingewiesen, dass ich die Anbringung von Hinweisschildern, wonach auf Wunsch eine Beratung in einem separaten Raum geführt werden kann, in diesem Zusammenhang nicht für geeignet halte. Es ist Aufgabe des Sozialleistungsträgers, die Wahrung des Sozialgeheimnisses von vornherein uneingeschränkt zu gewährleisten. Die Wahrung des Sozialgeheimnisses darf nicht von einem entsprechenden Wunsch des Bürgers abhängig gemacht werden.

Die betroffenen Behörden haben auf meine Forderung reagiert und für eine datenschutzgerechtere Gestaltung der Beratungsräume, zum Beispiel durch das Aufstellen von Trennwänden oder Umorganisation der Beratungsräume, gesorgt.
Meine Mitarbeiter haben sich nach den durchgeführten Maßnahmen von der datenschutzgerechteren Gestaltung der Behördenräumlichkeiten überzeugen können.

10 Gesundheit

10.1 Schweigepflichtentbindungserklärung einer Krankenkasse

Aufgrund des Anrufes eines saarländischen Allgemeinmediziners, der sich über eine zu pauschale Gestaltung der Schweigepflichtentbindungserklärung einer meiner Aufsicht unterliegenden Krankenkasse beschwerte, erfolgte die Kontaktaufnahme zum behördlichen Datenschutzbeauftragten der betroffenen Krankenkasse.
Der bis dato verwendete Vordruck zur Entbindung von der ärztlichen Schweigepflicht enthielt weder eine sachliche Begrenzung auf die aktuell vorliegende Erkrankung, noch eine zeitliche Befristung bis zum Ende der Erkrankung. Die Erklärung war zudem mit dem Hinweis versehen, dass die ärztlichen Unterlagen zur Einsichtnahme der Krankenkasse bzw. zur Weiterleitung an den Medizinischen Dienst der Krankenkassen (MDK) überlassen werden dürfen.
Durch die Zusammenarbeit von behördlichem Datenschutzbeauftragten, der Fachabteilung der Krankenkasse und meiner Geschäftsstelle konnte eine datenschutzgerechte Entbindungserklärung von der ärztlichen Schweigepflicht entwickelt werden, die eine zeitliche und sachliche Begrenzung beinhaltet.
Da medizinische Unterlagen wie Röntgenbilder und fachärztliche Gutachten nur von einem dafür ausgebildeten Mediziner ausgewertet werden können, wurde auf den Zusatz der Einsichtnahme durch die Krankenkasse gänzlich verzichtet. Es wurde von meiner Seite auf die datenschutzrechtlich unbedenkliche Praxis bei anderen Krankenkassen verwiesen, dass die angeforderten Unterlagen in einem verschlossenen Umschlag direkt an den MDK weiterzuleiten sind und nicht von der Krankenkasse geöffnet werden dürfen.
Hervorzuheben ist hierbei die vorbildliche Kooperationsbereitschaft der Krankenkasse mit meiner Geschäftsstelle.

10.2 Weitergabe von Patientendaten an Krankenkassen im Zusammenhang mit Disease-Management-Programm

Eine Krankenkasse hatte niedergelassene Ärzte im Saarland angeschrieben und eine Liste der Patienten, die bei der betreffenden Krankenkasse versichert waren, bei-

gefügt. Der Arzt sollte zu jedem Patienten angeben, ob der Patient an Asthma leidet, ob er DMP-fähig (d.h. ob der Patient geeignet ist, an einem systematischen Behandlungsprogramm für chronisch kranke Menschen teilzunehmen) bzw. ob er einer chronisch obstruktiven Lungenerkrankung leidet. Die Angaben sollten dazu dienen, in Frage kommende Patienten zu einer Vortragsveranstaltung zum Thema Asthma einzuladen.
Einige Ärzte hatten Zweifel, ob sie ohne entsprechende Einverständniserklärungen dazu berechtigt sind, die erbetenen Informationen über ihre Patienten weiterzugeben und hatten sich ratsuchend an die Ärztekammer des Saarlandes gewandt. Die Ärztekammer kam bei ihrer rechtlichen Überprüfung zu dem Ergebnis, dass es keine Rechtsgrundlage für die fragliche Datenübermittlung gibt und daher eine Datenweitergabe nicht zulässig ist. Ich habe die Ärztekammer in dieser Auffassung bestätigt. Im Recht der gesetzlichen Krankenversicherung gibt es zwar eine Vorschrift (§ 284 Absatz 1 Nr. 14 SGB V), wonach die Erhebung und Speicherung von Versichertendaten zur Gewinnung für Disease-Management-Programme und zur Vorbereitung und Durchführung dieser Programme zulässig ist. Hier ging es aber lediglich um die Vorbereitung einer Vortragsveranstaltung zum Thema Asthma, also einem Zweck, der von vornherein nicht unter die fragliche Vorschrift fällt. Hinzu kommt, dass ich keine entsprechende Befugnisnorm erkennen konnte, die es den angefragten Ärzten erlaubt hätte, die fraglichen Daten ohne Einwilligung ihrer Patienten zu übermitteln.

Ich habe deshalb der Ärztekammer auch im Hinblick auf die Gefahr der Verletzung der strafbewehrten ärztlichen Schweigepflicht geraten, ihren Mitgliedern zu empfehlen, auf die Anfrage nicht zu reagieren und keine Daten der betroffenen Patienten an die Krankenkasse weiterzugeben.

11 Schule und Bildung

11.1 Arbeitskreis Schule/Bildung der Datenschutzbeauftragten

Seit Beginn ihrer Tätigkeit arbeiten die Datenschutzbeauftragten des Bundes und der Länder in verschiedenen Arbeitskreisen zu unterschiedlichen Themenbereichen zusammen.

Im Berichtszeitraum wurde 2008 nach Durchführung des zweiten europäischen Datenschutztages – auch in Saarbrücken – mit dem Motto „Bildung macht Schule“ ein neuer Arbeitskreis Schule/Bildung errichtet. Zielrichtung dieser neuen Arbeitsgruppe soll es sein, das Datenschutzbewusstsein von Schülerinnen und Schülern zu schärfen und zu verbessern. Denn die Datenschutzbeauftragten erfüllt die Beobachtung mit Sorge, dass eine neue Generation heranwächst, die sehr sorglos mit ihren persönlichen Daten umgeht, ohne sich der daraus resultierenden Gefahren bewusst zu sein.

Man hat sich insbesondere vorgenommen, die Jugendlichen durch Informationen, wie z.B. Unterrichtsmaterialien, Flyer oder jugendgerechte Internetangebote aufzuklären. Geeignete Instrumente sind auch die Durchführung von Veranstaltungen oder Wettbewerben.

Die Arbeitsgruppe hat sich im Berichtszeitraum wiederholt getroffen. Schwerpunkt war dabei der gegenseitige Informationsaustausch über bisherige Aktivitäten zur Förderung des Datenschutzbewusstseins von Kindern und Jugendlichen sowie das gemeinsame Durchdenken neuer Aktivitäten.

Ich begrüße sehr diese neu gegründete Plattform für einen gegenseitigen Gedankenaustausch und erwarte mir für die Zukunft entscheidende Impulse für meine Arbeit in diesem Bereich. Erste Anregungen für die Arbeitsgruppe hatte ich bereits im Internetportal „Datenparty“ – über das ich anderweitig berichte – sowie in meiner dem Ministerium für Bildung, Familie, Frauen und Kultur und der interessierten Öffentlichkeit zur Verfügung gestellten Präsentation „Den Daten auf der Spur“ gegeben. Die Teilnahme meiner Geschäftsstelle an der Messe „Welt der Familie“ ist ebenfalls durch Erfahrungen in dieser Arbeitsgruppe bedingt.

11.2 Bilder auf der Homepage einer Grundschule

Eine Grundschule stellte mir ihre Homepage vor, um sicherzugehen, dass sie die Datenschutzbelange der Lehrkräfte sowie der Schüler und Schülerinnen ausreichend berücksichtigt hatte.

In einem Punkt gab es Anlass zur Diskussion: Unter welchen Voraussetzungen dürfen Fotos von Schülern und Schülerinnen veröffentlicht werden?

Die Schule meinte zunächst, sie dürfe Klassenfotos oder Fotos von schulischen Veranstaltungen auch ohne Einwilligung der Erziehungsberechtigten ins Internet stellen. Dadurch werde die Homepage viel interessanter – wer habe sich früher nicht selbst schon gern mal in der Zeitung gesehen?

Auf meinen Einwand, dass mangels einer gesetzlichen Grundlage eine Veröffentlichung von Fotos Minderjähriger nur mit Einverständnis der Erziehungsberechtigten zulässig sei, kam der Vorschlag, die Eltern über die Klassenfotos im Internet zu informieren und einen fehlenden Widerspruch innerhalb einer bestimmten Frist als Zustimmung zu werten.

Dieser Verfahrensweise konnte ich nicht zustimmen, denn eine Einwilligung setzt eine ausdrückliche – im Regelfall schriftliche – Erklärung voraus, mit einer bestimmten Datenverarbeitung einverstanden zu sein. Bloßes Schweigen erfüllt diese Voraussetzung nicht.

Ich habe als Alternative vorgeschlagen, bei Bildern von Schulveranstaltungen die Gesichter etwas zu verfremden, so dass man die Schüler nicht erkennen kann, oder Bilder zu verwenden, auf denen keine erkennbaren Schüler abgebildet sind.

Schließlich hat die Schule eine „Einwilligung zur Verwendung von Personenabbildungen und personenbezogenen Daten von Schülerinnen und Schülern“ entwickelt, die auch meine Zustimmung fand und künftig vor einer geplanten Veröffentlichung den Erziehungsberechtigten oder volljährigen Schülern zur Unterschrift vorgelegt wird.

Verschweigen möchte ich allerdings nicht, dass damit das Problem der Veröffentlichung von Fotos schulischer Veranstaltungen, auf denen auch Schülerinnen und Schüler erkennbar sind, nicht befriedigend gelöst ist. Denn, worauf die Schule zutreffend hingewiesen hat, wird es aus praktischen Gründen schwierig bzw. unmöglich sein, bei der Vielzahl der Betroffenen die Einwilligungserklärungen einzuholen. Hier bleibt mir allerdings nur der Hinweis auf die Rechtslage, wonach eine Verarbeitung personenbezogener Daten durch Schulen nur zulässig ist, wenn entweder eine ent-

sprechende Rechtsvorschrift die Veröffentlichung erlaubt oder die Einwilligung der Betroffenen vorliegt.

11.3 Datenerhebung zur Ausstellung von Abo-Karten für Grundschulkinder

Eine Schule wandte sich mit folgender Frage an mich: Die Schule liefert einem öffentlichen Verkehrsunternehmen zur Ausstellung der Fahrkarten verschiedene Daten ihrer Grundschulkinder. Während sich die Datenweitergabe bisher im Wesentlichen auf Name und Wohnort des jeweiligen Kindes beschränkte, sollten im neuen Schuljahr darüber hinaus Geburtsdatum und genauer Wohnort mit Straße und Postleitzahl übermittelt werden. Der Schule war die Erforderlichkeit dieser Daten für die Fahrkartenausstellung nicht einsichtig. Sie hatte deshalb Zweifel, ob sie berechtigt war, die zusätzlich gewünschten Informationen über ihre Schüler zu liefern.

Auf meine Nachfrage erklärte das Verkehrsunternehmen, die Informationen zu Geburtsdatum und genauer Anschrift seien keine Pflichtfelder, dienten aber insbesondere in zwei Fällen zur schnelleren und kundenfreundlicheren Reaktion: Bei Verlust einer Karte könne die Ersatzkarte direkt an die Privatadresse der Eltern geschickt werden, ohne Umweg über die Schule. Es komme oft vor, dass Eltern direkt bei dem Verkehrsunternehmen eine Abo-Karte bestellten. Sei der Schüler aber schon mit Name und Geburtsdatum im System eingegeben, falle eine Zweitabgabe direkt auf.

In meiner Stellungnahme habe ich zugestanden, dass in den geschilderten Fallkonstellationen eine schnellere und kundenfreundlichere Reaktion möglich ist, wenn das Verkehrsunternehmen über die fraglichen zusätzlichen Angaben verfügt. Erforderlich zur Aufgabenerfüllung (§ 14 Absatz 1 Saarländisches Datenschutzgesetz) seien die Daten allerdings nicht, was allein schon die Tatsache belege, dass die Entscheidung über die Angabe der Daten der Entscheidung der jeweiligen Schule überlassen bleibe. Im Übrigen habe ich Zweifel an der Verhältnismäßigkeit der Erhebung der fraglichen Daten unter dem Gesichtspunkt geäußert, dass die Daten von allen Schülern erhoben werden sollen, obwohl nur in einem Bruchteil der Fälle auf die Daten zurückgegriffen werden müsse.

Abschließend habe ich darauf hingewiesen, dass ich aus datenschutzrechtlicher Sicht keine Einwände hätte, wenn es gelinge, das Einverständnis der Eltern in die Erhebung der fraglichen Daten zu erlangen.

11.4 Datenweitergabe durch den schulpsychologischen Dienst

Eine Mutter beschwerte sich bei mir darüber, dass der schulpsychologische Dienst einen Bericht über ihren Sohn an die ARGE weitergegeben habe, ohne zuvor ihr Einverständnis eingeholt zu haben. Sie wollte von mir wissen, ob dies datenschutzrechtlich zulässig gewesen sei.

Was war geschehen? Die Petentin ist Hartz-IV-Bezieherin und hatte nach einem Schulwechsel ihres Sohnes höhere Fahrtkosten geltend gemacht, da der Schulwechsel aufgrund einer Empfehlung des schulpsychologischen Dienstes erforderlich geworden sei.

Die ARGE hatte daraufhin den schulpsychologischen Dienst um Übersendung der entsprechenden Unterlagen gebeten, ohne vorher das Einverständnis der Petentin einzuholen.

Auf meine Frage nach der Rechtsgrundlage für die fragliche Datenübermittlung berief sich der schulpsychologische Dienst auf den im Verwaltungsverfahrensrecht geltenden Untersuchungsgrundsatz, der besagt, dass die Behörden den Sachverhalt von Amts wegen zu ermitteln haben und für Art und Umfang der Ermittlungen nur die Entscheidungserheblichkeit, nicht aber das jeweilige Vorbringen der Beteiligten oder deren Beweisanträge maßgebend sind.

Hier musste ich allerdings darauf hinweisen, dass alle Behörden bei ihren Ermittlungen zur Beachtung der geltenden Gesetze verpflichtet sind. Maßgebend ist in diesem Zusammenhang § 20a Schulordnungsgesetz, der sich mit der Datenverarbeitung beim schulpsychologischen Dienst befasst und in Absatz 4 regelt, dass die Verarbeitung personenbezogener Daten durch den schulpsychologischen Dienst grundsätzlich nur mit Einwilligung der Erziehungsberechtigten oder des volljährigen Schülers zulässig ist. Etwas anderes gilt nur dann, wenn der schulpsychologische Dienst aufgrund besonderer gesetzlicher Vorschriften zur Vorbereitung schulischer Entscheidungen tätig wird.

Der schulpsychologische Dienst hätte somit vor Weitergabe seines Berichts das Einverständnis der Petentin einholen müssen.

11.5 Einsatz von „moodle“ an saarländischen Schulen

Der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf hinsichtlich der in der Verfahrensbeschreibung festzulegenden Angaben der schriftlichen Freigabe. Vor der Entscheidung ist der Landesbeauftragte für Datenschutz zu hören (§ 7 Absatz 2 SDSG).

Die oben zitierte Rechtsvorschrift war einigen Mitarbeitern des Ministerium für Bildung, Familie, Frauen und Kultur leider nicht bekannt, denn erst durch ein Telefonat eines Lehrers mit einem Mitarbeiter meiner Geschäftsstelle habe ich vom Einsatz einer „Moodleplattform“ in saarländischen Schulen erfahren.
Bei „moodle“ handelt es sich um eine virtuelle unterrichtsbegleitende Lernumgebung, in der Schülern die Möglichkeit für interaktives Lernen geboten wird. Arbeitsmaterialien aus dem Unterricht, Bildbeschreibungen, Hörverstehensaufgaben, Multiple-Choice-Tests, Abstimmungen, Foren, aber auch die Möglichkeit persönliche Profile anzulegen, wie es in sozialen Netzwerken möglich ist, sind nur einige der Einsatzmöglichkeiten dieser Plattform. „moodle“ wird bundesweit an Schulen zu E-Learningzwecken eingesetzt und somit besteht auch die Möglichkeit bundesweit mit Usern der Plattform zu kommunizieren.
Dass beim Einsatz einer solchen Plattform auch datenschutzrechtliche Belange tangiert werden, ergibt sich allein aus der Tatsache, dass personenbezogene Daten der Schüler und Lehrer abgespeichert werden.
Nachdem ich die verantwortlichen Stellen auf die fehlende Beteiligung meiner Geschäftsstelle aufmerksam gemacht hatte, wurde umgehend ein Termin zur Einsichtnahme in die Möglichkeiten und den Aufbau von „moodle“ vereinbart. Dabei konnten meine Mitarbeiter den verantwortlichen Stellen die rechtlichen und technisch-organisatorischen Voraussetzungen für den Einsatz von „moodle“ näher erläutern. Die Vorgaben meiner Geschäftstelle wie Passwortschutz und Freiwilligkeit der Eingabe persönlicher Daten wurden von Seiten des Ministeriums umgesetzt und mündeten in einer Verfahrensbeschreibung gemäß § 9 SDSG. Auch wurde mir zugesagt, sowohl die Eltern als auch die Schüler im Vorfeld des Einsatzes von „moodle“ in ausreichender Form über datenschutzrechtliche Belange beim Arbeiten mit der Plattform zu unterrichten. So konnte im Nachhinein durch eine effektive Zusammenarbeit die datenschutzkonforme Einsatzmöglichkeit von „moodle“ an saarländischen Schulen umgesetzt werden.

11.6 Notenlisten im Altpapiercontainer

Ein anonymer Petent übersandte mir die Entwürfe zur Festsetzung von Zeugnisnoten einer Grundschulklasse, die er laut eigenen Angaben im Einfüllschlitz eines fast gefüllten Containers für Altpapier gefunden hat. Auf den Entwürfen waren die Namen der Schüler, die Klasse und die betroffene Grundschule aufgeführt. Ebenfalls zu sehen waren die Zeugnisnoten in verschiedenen Fächern, die Beurteilung der Mitarbeit und des Verhaltens sowie die entschuldigten und unentschuldigten Fehltage im Beurteilungszeitraum.

Unter Berufung auf die mir zugesandten Unterlagen bat ich den Rektor der verantwortlichen Schule um Stellungnahme. Gemäß § 3 Absatz 2 der Verordnung über die Verarbeitung personenbezogener Daten in den Schulen im Saarland ist sicherzustellen, dass Unbefugte keinen Zugang zu Schülerdaten, wozu auch die Notenlisten zählen, erhalten.

Der Rektor berichtete daraufhin, dass er die zuständige Lehrerin, von der die fragliche Liste stammte, zu den Vorwürfen befragt hat. Der Lehrerin sei völlig unklar, wie diese Listen in die Hände des Anzeigeerstatters gelangen konnten. Sie habe diese Dokumente nicht auf diesem Wege entsorgt.

Der Schulleiter teilte mit, dass die erste Dienstbesprechung des Kollegiums der Schule nach Bekanntwerden des Vorfalles dazu genutzt worden sei, ausführlich auf die Bedeutung des Datenschutzes und die damit verbundene korrekte Vorgehensweise hinzuweisen.

Ich erwarte von allen saarländischen Schulen, dass sich ein solcher Vorfall nicht mehr wiederholt und die Regelungen der Verordnung über die Verarbeitung personenbezogener Daten in den Schulen im Saarland jedem saarländischen Lehrer bekannt sein müssen.

11.7 Novellierung der Verordnung über die Verarbeitung personenbezogener Daten in den Schulen

Im Berichtszeitraum wurde die aus dem Jahre 1986 stammende Verordnung über die Verarbeitung personenbezogener Daten in den Schulen novelliert. Eine Novellierung war – auch aus meiner Sicht – unter anderem erforderlich geworden, weil die Restrik-

tionen, die die alte Verordnung für die elektronische Datenverarbeitung vorgesehen hatte, aus heutiger Sicht nicht mehr nachvollziehbar waren. So ist die elektronische Datenverarbeitung (unter sicheren Rahmenbedingungen) heute die Regel und nicht mehr, wie noch 1986, die Ausnahme.

Es durften beispielsweise in einem Grundschulverwaltungsprogramm keine Gesundheitsdaten der Schüler gespeichert werden. Nicht mehr zeitgemäß war auch die Regelung, dass bei der Verarbeitung von Schülerdaten nur automatische Datenverarbeitungsanlagen eingesetzt werden durften, die nicht mit anderen vernetzt waren.

Weggefallen sind im Rahmen der Novellierung die Anlagen zu der Verordnung, in denen die Art der zulässigen Schülerdaten im Einzelnen aufgezählt waren. Auch gegen diese Maßnahme der Deregulierung habe ich keine Einwände erhoben, da eine zu detaillierte Datenbeschreibung bei neuen Erkenntnissen zwangsläufig aufwändige Fortschreibungen erforderlich macht.

Entgegen treten musste ich allerdings Forderungen von Lehrerverbänden und Personalräten:

So war die Erforderlichkeit eines schriftlichen Antrages bei der Schulleitung für die Datenverarbeitung der Lehrer im häuslichen Bereich in Frage gestellt worden. Darüber hinaus hielt man die Unterwerfung unter die Kontrolle durch den Landesbeauftragten für Datenschutz in diesem Fall für überzogen.

Festzuhalten ist demgegenüber, dass die Verlagerung dienstlicher Tätigkeiten in den häuslichen Bereich den für die Datenverarbeitung verantwortlichen Schulleiterinnen und Schulleitern die Kontrolle bezüglich des Umfangs, der Rechtmäßigkeit und der Ordnungsmäßigkeit der Datenverarbeitung entzieht. Durch die Datenverarbeitung im häuslichen Bereich steigt das Risiko, dass Unbefugte Zugang zu dienstlichen personenbezogenen Daten erhalten. So ist in vielen Fällen davon auszugehen, dass der PC auch von anderen Familienmitgliedern mitbenutzt wird und darüber hinaus auch mit dem Internet verbunden ist.

Angesichts dieser Gefährdungslage kann die Frage gestellt werden, ob eine Verarbeitung von Schülerdaten durch die Lehrkräfte außerhalb der Schule überhaupt unter Datenschutzgesichtspunkten gestattet werden soll. Um hier ein Mindestmaß an Kontrollmöglichkeiten zu haben, erscheinen die getroffenen Regelungen angemessen. Die Unterwerfung unter die Kontrolle des Landesbeauftragten für Datenschutz ist erforderlich, weil ansonsten wegen des Grundrechts der Unverletzlichkeit der Wohnung eine Kontrolle durch den Landesbeauftragten nicht stattfinden könnte. Auch

sonst unterliegt die Datenverarbeitung aller öffentlichen Stellen im Saarland meiner Kontrolle. Die Möglichkeit einer Kontrolle der Datenverarbeitung durch die Lehrkräfte ist somit keineswegs Zeichen eines besonderen Misstrauens, dass dort mit personenbezogenen Daten nicht ordnungsgemäß umgegangen wird, sondern entspricht der geltenden Gesetzeslage.

Es war die Forderung erhoben worden, dass bis auf den Schülerbogen und die Abschrift des Abgangszeugnisses bei einem Schulwechsel alle Schülerunterlagen an die aufnehmende Schule im Original weitergegeben werden sollen.

Dieser Vorschlag mag zwar im Sinne der Erleichterung der Verwaltungsarbeit sinnvoll sein, aus Datenschutzsicht konnte ich dem jedoch nicht zustimmen. Für die aufnehmende Schule sind nur ganz bestimmte Informationen von Bedeutung und somit erforderlich. Bei einer Abgabe der Originalunterlagen würden auch Daten weitergegeben, deren Kenntnis für die aufnehmende Schule nicht von Belang ist. Insofern würde gegen einen der prägenden Grundsätze des Datenschutzes verstoßen, der besagt, dass jede öffentliche Stelle nur über die Informationen verfügen darf, die sie für die Erfüllung ihrer Aufgaben benötigt.

Erfreulicherweise ist das Ministerium in diesen Punkten meiner Argumentation gefolgt und hat es bei den vorgesehenen Regelungen belassen.

Insgesamt begrüße ich die Novellierung der Verordnung, weil sie die vielfach schon übliche Verwaltungspraxis in den Schulen auf eine sichere und zeitgemäße rechtliche Grundlage stellt.

11.8 Verhaltensbericht vom Kinderhort an die Grundschule

Im Berichtszeitraum erreichte mich die Eingabe eines Petenten, in dem es um folgenden Sachverhalt ging: Der Sohn des Petenten besucht die erste Klasse einer Grundschule; nach der Schule besucht das Kind einen Hort, in dem eine Aufgabenbetreuung stattfindet. Im Rahmen einer Besprechung in der Schule erfuhr der Petent zufällig, dass die Schule bei dem Hort einen Verhaltensbericht angefordert hatte, der von dort auch erstellt worden war.

Der Petent wollte wissen, ob die Erstellung eines solchen Verhaltensberichtes durch den Hort für die Schule ohne das Einverständnis der Eltern zulässig ist.

Auf meine Nachfrage bei der Schule nach dem Zweck dieses Verhaltensberichtes hat mir die Schule mitgeteilt, dass der Bericht angefordert worden sei, um eine sonderpädagogische Förderungsbedürftigkeit bei dem Sohn des Petenten zu prüfen. Die Schule hatte sich dazu aufgrund der „Bekanntmachung der Empfehlungen der Kultusministerkonferenz zur sonderpädagogischen Förderung in den Schulen in der Bundesrepublik Deutschland“ vom 8. Juni 1994 für berechtigt gehalten. Dort heißt es unter anderem: „Sonderpädagogischer Förderbedarf lässt sich nicht allein von schulfachbezogenen Anforderungen her bestimmen. Seine Klärung und Beschreibung müssen das Umfeld des Kindes bzw. Jugendlichen einschließlich der Schule und die persönlichen Fähigkeiten, Interessen und Zukunftserwartung gleichermaßen berücksichtigen. Daher sind Voraussetzungen und Perspektiven der elementaren Bereiche … in eine Kind-Umfeld-Analyse einzubeziehen.“ Abgesehen davon, dass Beschlüssen der Kultusministerkonferenz keine Rechtsnormqualität zukommt, auf die eine Datenerhebung gestützt werden könnte, enthält die fragliche Passage in dem Beschluss auch keine ausdrückliche Ermächtigung zur Erhebung personenbezogener Daten ohne Einverständnis der Erziehungsberechtigten.
Es gibt allerdings eine Verordnung zur Ausführung des Schulpflichtgesetzes vom 23. Juni 2004, in der das Verfahren zur Feststellung eines sonderpädagogischen Förderungsbedarfes detailliert geregelt ist. Aber auch diese Verordnung lässt die in Frage stehende Datenverarbeitung nicht zu.

Die zuständige Schulaufsichtsbehörde beim damaligen Ministerium für Bildung, Kultur und Wissenschaft hat veranlasst, dass das fragliche Gutachten vernichtet wurde. Damit wurde der Vorschrift des § 21 Absatz 3 Saarländisches Datenschutzgesetz Rechnung getragen, wonach personenbezogene Daten zu löschen sind, wenn ihre Speicherung unzulässig war.

11.9 Datenparty (www.datenparty.de)

In Zusammenarbeit mit dem Landesjugendring des Saarlandes entwickelte ich im Berichtszeitraum das Internetportal www.datenparty.de. Am 27.10.2008 wurde dieses Internetportal im Illtal-Gymnasium im Beisein des Bundesdatenschutzbeauftrag-

ten Peter Schaar unter großer Anteilnahme der Medien und der Öffentlichkeit präsentiert.

Das Portal Datenparty richtet sich an Jugendliche und junge Erwachsene. Sie soll sie im Umgang mit ihren persönlichen Daten sensibilisieren. In leicht verständlichen Worten und mit lebensspezifischen Praxisbeispielen wird gezeigt, wer wo Daten sammelt und was damit gemacht werden kann. Vor allem Bereiche wie Internet / Soziale Netzwerke, Handy oder Fotografie sind hierbei für Jugendliche relevant und werden beispielgebend besprochen. Daneben wird darauf eingegangen, wer welche Daten sammeln darf, was für Gesetze ausschlaggebend sind und an wen man sich mit Datenschutzfragen wenden kann. Eine Sammlung von Datenpannen sowie Hilfen für Eltern / Pädagogen und Pädagoginnen runden das Angebot ab. In der Jugendarbeit Tätige, Lehrer, Schulworker und Eltern können selbständig mit Kindern und Jugendlichen unter Einbeziehung dieser Internetseite zum Thema Datenschutz arbeiten und informieren.

Die Seite ist ein hervorragender Erfolg geworden. Bemerkenswert für saarländische Verhältnisse ist die Anzahl der Aufrufe (per heute knapp 400.000). Bemerkenswert ist auch, dass am Eröffnungstag, nach Berichterstattung im ZDF, der Server dieser Internetseite wegen der bis zu diesem Zeitpunkt über 50.000 Aufrufe zusammenbrach.

12 Forschung

12.1 Übermittlung von Videodaten im Rahmen einer Forschungskooperation

Folgende Problematik aus dem Bereich der wissenschaftlichen Forschung wurde an mich herangetragen:

Im Rahmen einer wissenschaftlichen Studie waren im Jahre 2003 Videoaufnahmen von 56 Kindern im Alter von 6 Monaten bei einer 5-10minütigen Spielsituation mit ihrer Mutter erstellt wurden. Anhand dieser Videoaufnahmen sollte der Interaktionsstil der Mutter mit ihrem Kind analysiert sowie der Zusammenhang des mütterlichen Interaktionsstils mit dem Blickverhalten der Kinder in einer Aufgabe zur kognitiven Entwicklung untersucht werden.

Im Rahmen eines aktuellen Projekts sollten nun diese Aufnahmen an eine andere Forschergruppe übermittelt und erneut analysiert werden. Es sollte unter anderem geprüft werden, ob sensitive Mütter sich auch dadurch auszeichnen, dass sie in besonderer körperlicher Art und Weise mit ihren Kindern interagieren. Aus derartigen Befunden sollten auch Erkenntnisse für die Diagnostik defizitärer Mutter-Kind-Interaktionen abgeleitet werden.

Die Frage war nun, ob die Videoaufnahmen aus dem Jahre 2003 zulässigerweise für die neue Studie Verwendung finden konnten. Die Eltern hatten damals eine Erklärung unterschrieben, in der sie sich mit der Speicherung des Videomaterials zu Zwecken der Auswertung und Archivierung einverstanden erklärt haben.

Auch wenn es viel Arbeit erspart hätte, wenn man die Videoaufnahmen für die aktuelle Fragestellung hätte verwenden können, konnte ich aus datenschutzrechtlicher Sicht dieser Zweckänderung der einmal erstellten Aufnahmen nicht zustimmen. Eine Rechtsgrundlage, wonach eine Verpflichtung besteht, Videoaufnahmen für wissenschaftliche Zwecke zu dulden, gibt es in unserer Rechtsordnung nicht. Die Wissenschaft ist insofern auf das Einverständnis der Betroffenen angewiesen. Wesentlich für die Entscheidung, ob das Einverständnis erteilt wird, ist der Zweck, der mit der Datenverarbeitung auf Seiten der datenverarbeitenden Stelle verfolgt wird.

Vorliegend waren die Teilnehmerinnen darüber informiert worden, welche Fragestellung anhand der Videoaufnahmen erforscht werden sollten. Nur hierauf bezog sich ihre Einwilligungserklärung.

Ich musste den Forschern deshalb mitteilen, dass eine Auswertung der Videoaufnahmen für die neue Fragestellung ohne entsprechende Einwilligungserklärungen der damaligen Teilnehmerinnen nicht zulässig ist.

13 Öffentlicher Dienst

13.1 Automatisiertes Meldeverfahren bei Krankendaten an die zentrale Vergütungsstelle

Die für die Mitarbeiter des Landes zuständige Vergütungsstelle des Landesamtes für Zentrale Dienste hat im Berichtszeitraum, aufgrund einer Forderung des Rechnungshofes, die Umstellung der Meldung über Fehlzeiten vom postalischen Weg auf ein automatisiertes Meldeverfahren aus dem Zeiterfassungsprogramm „bedatime“ durchgeführt. Da es sich hierbei um ein automatisiertes Verfahren handelt, in dem personenbezogene Daten von den einzelnen Dienststellen des Landes an die Vergütungsstelle übermittelt werden, war meine Geschäftstelle vorab gemäß § 7 Absatz 2 SDSG zu hören.

Die Meldung der Krankheitstage von Landesbediensteten ist erforderlich, um die Lohnfortzahlungsansprüche zu berechnen und Fälle, die in den Krankgeldbezug gem. §§ 44 ff SGB V fallen, schneller zu erkennen und an die zuständige Krankenkasse zur Zahlung des Krankengeldes abzutreten. Ist ein Mitarbeiter innerhalb eines Jahres an mehr als 42 Tagen wegen der gleichen Erkrankung nicht zum Dienst erschienen, so endet in der Regel der Lohnfortzahlungsanspruch und die zuständige Krankenkasse übernimmt die daran anschließende Krankengeldzahlung. Welche Fehlzeiten auf eine Erkrankung angerechnet werden, ermittelt die Krankenkasse anhand der dort gespeicherten Diagnosen der behandelnden Ärzte auf Ersuchen der Vergütungsstelle.

Bei der Überprüfung der mir zur Verfügung gestellten Unterlagen zum Programm fiel mir auf, dass neben den Krankheitstagen, die per Arbeitsunfähigkeitsbescheinigung nachgewiesen wurden, auch Fehltage übermittelt werden sollten, für die keine Arbeitsunfähigkeitsbescheinigung vorliegt. Da hier eine Verknüpfung mit möglichen Vorerkrankungen aufgrund fehlender Diagnose bei der zuständigen Krankenkasse zur Berechnung der 42-Tage-Frist ausscheidet, habe ich bei der Vergütungsstelle interveniert und die Erforderlichkeit dieser Erhebung in Frage gestellt.

Die Begründung der Vergütungsstelle, wonach die Erhebung aller Krankheitszeiträume erforderlich sei, um der Regelung des § 22 Absatz 3 Satz 3 TVL gerecht zu werden, konnte überzeugen. In besagter Vorschrift, kommt es für die Festsetzung des Höchstzeitraumes zur Gewährung eines Krankengeldzuschusses nicht auf die Zusammenhangserkrankung an, sondern auf die Anzahl aller im Berechnungszeit-

raum anfallender Fehlzeiten. Daraufhin habe ich das automatisierte Übermittlungsverfahren aus datenschutzrechtlicher Sicht für unbedenklich erklärt.

13.2 Daten von Mitarbeitern im Intranet, Internet, an Türschildern

Immer wieder muss ich mich mit der Frage beschäftigen, ob und unter welchen Voraussetzungen die Veröffentlichung von persönlichen Daten von Mitarbeitern im Intranet einer Behörde oder im Internet zulässig ist.

So wurde ich durch eine Anzeige darüber informiert, dass ein Verband neben Bildern seiner Mitarbeiter auch weitere Informationen, wie Eintritt in den Ruhestand oder Mutterschaftsurlaub, ins Internet gestellt hatte.

In einem anderen Fall wollte ein Ministerium ebenfalls die Bilder seiner Mitarbeiter zunächst im Intranet, später im Internet und sogar auf den Türschildern der jeweiligen Büros veröffentlichen.

Ich habe darauf hingewiesen, dass solche Veröffentlichungen allenfalls mit Einwilligung der betreffenden Mitarbeiter zulässig sind. Allerdings muss darauf geachtet werden, dass die entsprechenden Einwilligungen auf der freien Entscheidung der Betroffenen beruhen, denn nur dann kann von einer wirksamen Einwilligung ausgegangen werden. Abhängigkeitsverhältnisse, wie sie in der Beziehung zwischen Arbeitgebern und ihren Bediensteten bestehen, begründen meines Erachtens Zweifel an einer solchen freien Entscheidung. Vielmehr ist davon auszugehen, dass sich zumindest ein Teil der Mitarbeiter einem faktischen Zwang ausgesetzt sieht, die entsprechende Einwilligungserklärung zu unterzeichnen. Das gilt auch und gerade vor dem Hintergrund, dass das Interesse an der Veröffentlichung der Fotos einseitig auf Seiten der Behördenleitung liegt.

Vor jeder Veröffentlichung persönlicher Daten der Mitarbeiter, und gerade von Bildern, sollte sorgfältig überlegt werden, ob auf eine solche Veröffentlichung nicht genauso gut verzichtet werden kann.

13.3 Dienstvereinbarung zur Gesundheitsförderung sowie zum Fehlzeiten- und betrieblichen Eingliederungsmanagement

Ein Sozialversicherungsträger machte sich Gedanken darüber, wie er die Gesundheit seiner Mitarbeiter fördern und den Krankenstand senken könnte. Als Maßnahmen zur Erreichung dieses Ziels sollten eine aktive Gesundheitsförderung, ein Fehlzeitenmanagement sowie ein betriebliches Eingliederungsmanagement eingeführt werden. Der Entwurf der entsprechenden Dienstvereinbarung wurde mir zur datenschutzrechtlichen Bewertung vorgelegt.

Während die angedachten Maßnahmen der Gesundheitsförderung, wie z.B. innerbetriebliche Gesundheitsprogramme, Ernährungsberatung, Gesundheitstage, Informationsveranstaltungen über gesunden Lebensstil mit medizinischen Hintergrundinformationen, zu begrüßen sind, stehe ich den im Rahmen des Fehlzeitenmanagements geplanten Krankenrückkehrgesprächen äußerst skeptisch gegenüber.

Ich halte die Führung von Krankenrückkehrgesprächen für ein bei Beachtung aller datenschutzrechtlichen Kautelen ungeeignetes, nicht erforderliches und unverhältnismäßiges Mittel zur Senkung des Krankenstandes und demzufolge die damit verbundene Datenerhebung in den Gesprächen und den anzufertigenden Protokollen für datenschutzrechtlich unzulässig.

In den vorgesehenen Rückkehrgesprächen sollen als mögliche Ursachen für häufige Erkrankungen Ursachen im persönlichen, familiären Umfeld oder in den Arbeitsbedingungen ermittelt werden.

Es kann zwar nicht bestritten werden, dass Erkrankungen ihre Ursache in diesen Bereichen haben können.

Was persönliche oder familiäre Probleme als Ursache für Erkrankungen betrifft, stellt sich allerdings die Frage, ob ein Mitarbeiter bereit ist, diese Probleme seinem Vorgesetzten anzuvertrauen und, was noch zweifelhafter erscheint, wie der Vorgesetzte bei der Bewältigung dieser Probleme behilflich sein kann.

Was Probleme im Arbeitsumfeld betrifft (in Form von Arbeitsüberlastung, Ausstattung des Arbeitsplatzes oder persönlicher Umgang mit Kollegen und Vorgesetzten), gibt es meines Erachtens andere, die Mitarbeiter weniger belastende Maßnahmen, als die Führung von Rückkehrgesprächen, um hier Verbesserungen zu schaffen. So ist es Aufgabe des Fachvorgesetzten, von vornherein für eine gleichmäßige Arbeitsbelastung zu sorgen; der arbeitsmedizinische Dienst hat für eine ergonomische Ausstattung jedes Arbeitsplatzes zu sorgen; für Probleme im persönlichen Umgang mit

Mitarbeitern und Vorgesetzten kann eine Stelle eingerichtet werden, an die sich jeder Mitarbeiter vertrauensvoll und auf eigenen Wunsch wenden kann.
Auch wenn in dem Entwurf der Dienstvereinbarung der Eindruck vermieden werden sollte, Rückkehrgespräche sollten als disziplinierendes Mittel bei „häufigen“ Erkrankungen dienen, so werden diese Gespräche doch von den meisten Mitarbeitern regelmäßig so empfunden. Es mag sein, dass sich einzelne Mitarbeiter, die sich „häufig“ krank melden, ohne arbeitsunfähig zu sein, von solchen Rückkehrgesprächen abschrecken lassen. (Auch hier sind allerdings Zweifel angebracht, ob sich gerade Mitarbeiter, die häufig „krank feiern“ von Rückkehrgesprächen beeindrucken lassen.) Auf der anderen Seite steht demgegenüber die überwiegende Mehrheit der rechtstreuen und korrekten Mitarbeiter, die sich nur krank melden, wenn sie tatsächlich erkrankt sind. Diese Mitarbeiter würden sich zu Recht als diskriminiert fühlen, wenn sie aufgrund „häufiger“ Erkrankungen in den Verdacht des unberechtigten Fernbleibens vom Dienst gerieten.

Neben diesen grundsätzlichen Erwägungen habe ich verschiedene Punkte in der Dienstvereinbarung angesprochen, die deutlich machen, dass eine datenschutzgerechte Organisation von Krankenrückkehrgesprächen eigentlich nicht möglich ist:

- In dem Entwurf wird zutreffender Weise davon ausgegangen, dass Diagnosen entsprechend der geltenden Rechtslage nicht erfragt werden dürfen. Dieser Hinweis ist für mich allerdings nur theoretischer Natur, denn selbst wenn der Vorgesetzte nicht ausdrücklich nach der Diagnose fragt, ist es lebensfremd anzunehmen, dass in einem solchen Gespräch nicht auch über die Art der Erkrankung gesprochen wird.
- Für fragwürdig halte ich die Einbeziehung des unmittelbaren Vorgesetzten unter dem Gesichtspunkt, dass diesem eine Aufstellung der Krankheitstage seiner Mitarbeiter zur Verfügung gestellt wird. Gegen eine solche Unterrichtung der Fachvorgesetzten durch eine Übersicht, wie oft und wie lange die einzelnen Mitarbeiter in bestimmten Zeiträumen gefehlt haben, habe ich größte Bedenken. Die Sammlung der Fehlzeitendaten ist Aufgabe der jeweiligen Personalabteilung, wo die Angaben für die Dienstaufsicht, Personalplanung (z.B. Ermittlung einer Ausfallquote) oder für die Vorbereitung von Personalmaßnahmen im Einzelfall (z.B. Einschaltung des Amtsarztes, Veranlassung der Überprüfung der Dienstfähigkeit)

benötigt werden. Unterlagen über Erkrankungen sind Teil der Personalakte, zu der nur Beschäftigte Zugang haben dürfen, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind. Diesen Grundsatz, wonach der Zugriff auf sensible Personaldaten restriktiv zu handhaben ist, würde es widersprechen, wenn es im Belieben des Dienstherrn stünde, welchen Personenkreis er mit der Wahrnehmung von Personalverwaltungsaufgaben betraut.

- Größte Bedenken habe ich gegen die Regelung in der Dienstvereinbarung, wonach ein Fehlzeitengespräch auch dann zu führen ist, wenn Zweifel an der Arbeitsunfähigkeit bestehen, die sich daraus ergeben sollen, dass ein Mitarbeiter „auffällig häufig“ oder „auffällig häufig nur für kurze Dauer“ arbeitsunfähig ist oder dass der Beginn der Arbeitsunfähigkeit „häufig“ auf einen Arbeitstag am Beginn oder Ende der Woche oder vor oder nach Urlaubszeiten fällt. Ich halte die Begriffe „häufig“ oder „auffällig häufig“ wegen ihrer Unbestimmtheit als Voraussetzung für eine Datenerhebung – unter anderem durch Anfertigung eines Protokolls, das zur Personalakte genommen werden soll – für nicht geeignet. Ich bin der Auffassung, dass es kein Mitarbeiter dulden muss, dass Zweifel an seiner Arbeitsunfähigkeit geäußert werden und dass dies auch noch in der Personalakte festgehalten wird, allein aufgrund des Umstandes, dass er je nach Auslegung seines Vorgesetzten „häufig“ arbeitsunfähig ist.

  Ich gehe davon aus, dass sich solche Krankenrückkehrgespräche zunehmender Beliebtheit in den Personalabteilungen der Privatwirtschaft und des öffentlichen Dienstes erfreuen und appelliere an die Arbeitgeber, von diesem Instrumentarium keinen Gebrauch zu machen bzw. an die Personalvertretungen, ihre Zustimmung zu verweigern.

13.4 Mitteilung an Arbeitgeber bei mehreren Minijobs

Die Universität des Saarlandes beschäftigt vielfach Studenten als studentische Hilfskraft in einem sogenannten Minijob**.** Bei der Einstellung muss der zukünftige Mitarbeiter unter anderem angeben, ob noch weitere sozialversicherungsrelevante Beschäftigungsverhältnisse ausgeübt werden. Wird dies bejaht, so muss der Student den

zeitlichen und finanziellen Umfang der anderen Tätigkeit angeben, damit die Universität des Saarlandes die Beiträge zur Sozialversicherung ordnungsgemäß entrichten kann. Dabei muss auch eine Meldung an die Minijob-Zentrale von Knappschaft-Bahn-See erfolgen, der die Überprüfung der Rechtmäßigkeit der Zahlungen obliegt.
Durch die Eingabe eines Studenten wurde ich auf die Praxis der Universität des Saarlandes aufmerksam, in Fällen, in denen mehrere Beschäftigungsverhältnisse angegeben wurden, den jeweils anderen Arbeitgeber um Bestätigung der Angaben des Studenten zu bitten.
Dabei handelt es sich um eine Datenerhebung im Sinne des § 12 SDSG. Eine Datenerhebung ist aber grundsätzlich nach dieser Vorschrift nur zulässig, wenn sie direkt beim Betroffenen erfolgt (§12 Abs.1 Satz 2 SDSG). Ausnahmen von dieser Regelung lagen im vorliegenden Fall nicht vor. Es ist nicht Aufgabe der Universität des Saarlandes, die Einhaltung der Meldepflichten des geringfügig Beschäftigten zu überwachen.
Durch die reine Abfrage bei dem Studenten, in welchem Umfang er noch weitere sozialversicherungsrechtlich relevante Beschäftigungsverhältnisse ausübt, erfüllt die Universität ihre Pflicht im Sinne des Sozialgesetzbuches. Nach § 280 Absatz 1 SGB IV ist der Beschäftigte zur Auskunft über alle notwendigen Angaben verpflichtet, die es dem Arbeitgeber ermöglichen, seiner Meldepflicht gegenüber der Minijob-Zentrale nachzukommen. Die Plausibilitätsprüfung der Angaben des Studenten obliegt der Minijob-Zentrale.
Ich habe den Datenschutzbeauftragten der Universität des Saarlandes zur Vorgehensweise in seinem Hause um Stellungnahme gebeten. Durch den Austausch mit meiner Dienststelle hat er die Personalabteilung der Universität darauf hingewiesen, zukünftig keine anderen Arbeitgeber von geringfügig Beschäftigten zur Bestätigung der Angaben des Studenten anzuschreiben.

13.5 Ortung von Rettungsfahrzeugen mittels GPS

Um die Einsatzdisposition in der Notfallrettung und im öffentlich-rechtlichen Krankentransport weiter zu optimieren, hat der Rettungszweckverband Saar als Aufgabenträger des Rettungsdienstes ein System eingeführt, welches mittels GSM/GPRS neben dem Einsatzstatus auch die Fahrzeugstandorte als GPS-Daten der Einsatzzentrale

übermittelt und diese in die EDV-gestützte Dispositionsliste des Einsatzleitsystems implementiert.
Die so zur Verfügung stehenden Daten zusammen mit einer erweiterten Leitstellensoftware ermöglichen es dem Disponenten, die dem Einsatzort nächstgelegenen und verfügbaren Fahrzeuge zum Einsatz anzubieten. Circa 120 Fahrzeuge sollen im Saarland schrittweise mit dieser Technik ausgestattet werden.
Die datenschutzrechtliche Problematik stellt sich hier in einer lückenlosen Überwachung und der Möglichkeit, Bewegungsprofile von Mitarbeitern zu erstellen. Bei einem Vorortbesuch und mehreren Beratungen meiner Geschäftsstelle beim Rettungszweckverband Saar konnte man sich auf eine datenschutzgerechte Umsetzung der Technik einigen. So kann sich der Fahrer eines Einsatzfahrzeuges auf freiwilliger Basis persönlich auf dem Bordcomputer einloggen, er hat aber auch die Möglichkeit, sich anonym beim Fahrzeug anzumelden.
Durch die Besonderheit, dass der Rettungszweckverband Saar nicht gleichzeitig als Arbeitgeber der Fahrzeugbesatzung auftritt, kann der jeweilige Arbeitgeber, zum Beispiel ein Krankenhaus, ein Bewegungsprofil zur Leistungs- und Verhaltenskontrolle seiner Mitarbeiter nur per Datenübermittlung durch den Rettungszweckverband erstellen. Durch die gute Kooperation zwischen Rettungszweckverband und meiner Geschäftsstelle wurde anhand eines Fragekataloges die Zulässigkeit oder Unzulässigkeit einer Datenübermittlung an den Arbeitgeber geregelt. In Fällen, die nicht von diesem Katalog erfasst wurden und Zweifel an der Zulässigkeit bestehen, habe ich mit dem Rettungszweckverband vereinbart, vorab eine datenschutzrechtliche Beurteilung der Frage vorzunehmen.

13.6 Outlookinformation einer Behördenabteilung über Abwesenheitsgründe der Beschäftigten

Durch die Eingabe eines Behördenbediensteten wurde ich darauf aufmerksam gemacht, dass es in dieser Behörde Usus sei, Fehlzeiten von Bediensteten mit Dauer und Grund der Abwesenheit auch den Kollegen der Behörde mitzuteilen, die nicht im direkten dienstlichen Kontakt zum Abwesenden stehen. Mit dem Hinweis, dass der Grund der Abwesenheit in solchen Mitteilungen nicht aufgeführt werden darf und lediglich die Personen über das Fehlen ihres Kollegen zu informieren sind, die zu ihm

im direkten dienstlichen Kontakt stehen, erhielt ich von Seiten der Behördenleitung eine Stellungnahme, die eine Information der Belegschaft über die Dauer der Abwesenheit eines Beschäftigten, sei es krankheits- oder urlaubsbedingt, als erforderliche und damit nach § 31 Saarländisches Datenschutzgesetz (SDSG) datenschutzrechtlich zulässige Maßnahme zum Zwecke des Personaleinsatzes sieht. Auf diese Stellungnahme reagierend verwies ich darauf, dass zum Zwecke des Personaleinsatzes im Sinne des § 31 SDSG die Mitteilung der Dauer der Abwesenheit an den direkt betroffenen Mitarbeiterkreis als ausreichend anzusehen ist. Weder der Grund der Abwesenheit noch die Information von Mitarbeitern, die nicht direkt vom Ausfall des Bediensteten betroffen sind, diene dem Zweck des Personaleinsatzes.

Leider sind meine Mahnungen nicht ernst genommen worden, was mir der Petent mit erneuten Abwesenheitsmeldungen dokumentierte. Erneut auf diesen Missstand aufmerksam gemacht, bat ich die Behördenleitung darum, dafür Sorge zu tragen, dass Meldungen in der vorgelegten Form nicht mehr in Umlauf gelangen und verwies auf mein vorangegangenes Schreiben. Die erneute Ermahnung wurde von der Behördenleitung zum Anlass genommen, alle Mitarbeiter der Behörde über ihre Datenschutzrechte zu informieren und zukünftig von einer Outlookmitteilung, die den Grund der Abwesenheit eines Behördenbediensteten beinhaltet sowie die Information von Personen, die nicht im direkten dienstlichen Kontakt zum Abwesenden stehen, zu unterlassen. Bis dato sind keine weiteren Verstöße gegen den Datenschutz aus dieser Behörde gemeldet worden.

13.7 Personaldatenbanken der saarländischen Polizei

Im Berichtszeitraum kamen mehrere Organisationseinheiten der saarländischen Polizei ihrer Verpflichtung gemäß § 7 Absatz 2 SDSG nach, mich vor dem Einsatz eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, zu hören. Die Zulässigkeit der vorgelegten Datenbanken ergab sich hierbei aus § 31 SDSG, wonach die Daten von Bewerbern und Beschäftigten verarbeitet werden dürfen, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personel-

ler und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist.

Bei der Überprüfung der Programme habe ich unter anderem die Regelung der Löschfristen bei Ausscheiden aus dem Dienst zu beurteilen. Hier stand die Bitte vieler ehemaliger Polizisten im Raum, noch an diversen Veranstaltungen ihrer früheren Dienststelle teilnehmen zu dürfen und über solche Veranstaltungen informiert zu werden, was natürlich nur möglich ist, wenn die Daten der Polizisten auch nach Ausscheiden aus dem Dienst gespeichert bleiben. Nach Rücksprache mit meiner Geschäftsstelle wurde vereinbart, dass die Daten der ehemaligen Polizisten nur dann weiterhin gespeichert bleiben dürfen, wenn die betroffenen Beamten im Vorfeld Ihrer Ruhestandsversetzung die Einwilligung zur weiteren Speicherung der Daten erteilt haben und die Daten nur zum Zwecke der Information über geplante Veranstaltungen der Dienststelle genutzt werden.

13.8 Weitergabe von Daten durch Sicherheitsbehörden an Arbeitgeber

Auf ihrer Konferenz am 3. und 4. April 2008 haben sich die Datenschutzbeauftragten des Bundes und der Länder mit der Problematik befasst, dass Arbeitgeber in zunehmendem Maß ihre Mitarbeiter dazu auffordern, 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 selbst einholen und ihrem Arbeitgeber vorlegen. In einer Entschließung (Anlage 21.15) wenden sich die Datenschutzbeauftragten entschieden gegen diese Praxis, mit der die gesetzgeberischen Wertungen, welche justiziellen Informationen anderen Stellen zur Verfügung gestellt werden dürfen, in eklatanter Weise unterlaufen wird.

13.9 Zusammenarbeit mit dem Arbeitskreis Datenschutz und Datensicherheit

Die Beratungsstelle für sozialverträgliche Technologiegestaltung e.V. (BEST) der Arbeitskammer des Saarlandes bietet einen Arbeitskreis zu Datenschutz und Datensicherheit an. Der Arbeitskreis dient als Plattform zum Wissens- und Erfahrungsaustausch von betrieblichen und behördlichen Datenschutzbeauftragten. Es werden Orientierungshilfen erstellt und aktuelle datenschutzrechtlich relevante Themen diskutiert.

Seit September 2007 nimmt ein Mitarbeiter meiner Geschäftsstelle als ständiges Mitglied an den Sitzungen des Arbeitskreises teil.

In dieser Zeit wurden Themen wie z.B. betriebliches Eingliederungsmanagement, Telearbeit, Internet und E-Mail am Arbeitsplatz, eGovernment oder Datenschutz und Mitbestimmung im Kreise der betrieblichen und behördlichen Datenschutzbeauftragten diskutiert, wichtige Erfahrungen zu diesen Themen ausgetauscht und in verwertbarer Form zusammengetragen.

Der Arbeitskreis stellt eine interessante Plattform für Personen dar, die beruflich mit dem Datenschutz verbunden sind. Er findet in unregelmäßigen Abständen im Hause der Arbeitskammer in Saarbrücken statt. Mehr dazu finden Sie im Internet unter der Adresse: www.best-saarland.de.

14 Rundfunk und Medien, Telekommunikation

14.1 Anonyme Nutzung des Fernsehens

Die Bundesländer haben sich im Rundfunkstaatsvertrag verpflichtet, dass jeder Rundfunkprogramme anonym in Anspruch nehmen kann.
Dem laufen Bestrebungen der großen privaten Fernsehveranstalter entgegen, ihre Programme nur noch verschlüsselt zu übertragen. Es sollen dabei vorrangig solche Geschäftsmodelle favorisiert werden, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.
In einer Entschließung vom 8./9. März 2007 (Anlage 21.2) erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

14.2 Arbeitsgruppe Internet für Schüler

Im Frühjahr 2008 gründete sich eine Arbeitsgruppe aus Vertretern des Landeskriminalamtes, des Ministeriums für Bildung, Familie, Frauen und Kultur, der Landesmedienanstalt, der Europäischen EDV-Akademie des Rechts GmbH, der Landespolizeidirektion, des Landesjugendringes Saar, der Hochschule für Technik und Wirtschaft (HTW), des Landesinstituts für Pädagogik und Medien und meiner Geschäftsstelle. Ziel der Arbeitsgruppe ist es, Schüler im Umgang mit dem Internet zu sensibilisieren, Eltern auf die Gefahren der Internetnutzung hinzuweisen und Lehrern eine Hilfestellung zu geben, wie sie Schüler im Unterricht auf die richtige Nutzung des Internet vorbereiten können. Das Internet bietet sehr viele positive Aspekte für Schüler, birgt aber auch die Gefahr in sich, dass sie beim Umgang mit dem Internet negative Erlebnisse erfahren. So kann zum Beispiel das Herunterladen von MP3-Dateien eine Klage wegen Urheberrechtsverletzungen nach sich ziehen. Die eigene Präsentation in einem sozialen Netzwerk kann schädlich für die berufliche Zukunft eines Schülers sein, wenn der mögliche neue Arbeitgeber von seltsamen Vorlieben seines Bewer-

bers erfährt. Auch das reale Treffen mit einem angeblich gleichaltrigen Chatfreund kann anders als gewollt enden.
Diese und andere Themen wurden in einer Power Point Präsentation zusammengestellt und bei Informationsveranstaltungen in verschiedenen Schulen Lehrern und Eltern vorgestellt.
Schulklassen wurden unter anderem zur Saarmesse eingeladen, um an einem Quiz zum Thema Internet teilzunehmen, das von Vertretern der Arbeitsgruppe erstellt und präsentiert wurde.
In den regelmäßig stattfindenden Sitzungen der Arbeitsgruppe werden unter anderem Verbesserungsvorschläge zur Power Point Präsentation diskutiert, weitere Maßnahmen zur Veröffentlichung des Angebotes der Arbeitsgruppe getroffen und aktuelle Themen in die Arbeit der Arbeitsgruppe eingebunden.
Durch die Gründung des Landesinstitutes für präventives Handeln im Januar 2009 sollen die Aufgaben der Arbeitsgruppe mittelfristig auf dieses Institut übertragen werden.

14.3 Datenpanne bei „Programmbeschwerde.de“

Die Landesmedienanstalt des Saarlandes betreibt federführend ein Beschwerdeportal der Arbeitsgemeinschaft der Landesmedienanstalten zum Privatrundfunk. Unter der Adresse www.programmbeschwerde.de können Verbraucher Kritik an Inhalten von Fernseh- und Rundfunkanstalten üben. Die Landesmedienanstalt Saarland leitet die Beschwerden an die zuständigen Sender weiter und bittet um Stellungnahme zu den Äußerungen. Um der Landesmedienanstalt ihre Kritik zugänglich zu machen, müssen die Verbraucher in einem Beschwerdebogen im Internetangebot unter anderem persönliche Daten sowie die Sendung, gegen die sich die Beschwerde richtet, angeben.
Durch einen ungeklärten Umstand wurden Ende 2008 sämtliche Beschwerdevorgänge frei zugänglich und die personenbezogenen Daten der Beschwerdeführer samt der Beschwerdeinhalte für Dritte im Internet abrufbar.
Es dauerte nicht lange, bis sich gleich mehrere Beschwerdeführer in Ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt fühlten und sich hilfesuchend an meine Geschäftsstelle wandten.

Durch mein schnelles Handeln und die Kooperationsbereitschaft der Landesmedienanstalt wurde das Internetangebot nach Bekanntwerden des Vorfalls direkt gesperrt. Das Problem bestand aber weiter, da über die Cache-Funktion mehrerer Suchdiensteanbieter nach wie vor Daten der Beschwerdeführer abrufbar waren. Die Landesmedienanstalt hat daraufhin den Kontakt zu den Suchdiensten aufgenommen und auf eine Löschung der Daten hingewirkt.

Es wurde vereinbart, dass das Angebot der Beschwerdeplattform erst wieder aktiviert werden darf, wenn nach Abstimmung mit meiner Geschäftsstelle eine datenschutzgerechte Lösung gefunden wird.

Im Rahmen der Neukonzeption des Portals „programmbeschwerde.de“ wurden die beiden Teile Web-Server und Datenbankserver physikalisch voneinander getrennt. Ein Durchgriff aus dem Internet auf den Datenbankserver wird mit Hilfe mehrerer Sicherheitsmechanismen wie zum Beispiel Firewall, Authentifizierungsmechanismen und Zugriffskontrollen verhindert. Das auf dem Webserver erzeugte Formular mit den dazugehörigen Angaben wird nach der Eingabe umgehend verschlüsselt und an den jeweiligen Sender, gegen den sich die Beschwerde richtet, versendet. Eine Speicherung auf dem Webserver erfolgt nicht. Somit ist ein Zugriff auf Programmbeschwerden von Verbrauchern nicht mehr möglich. Auch ein Suchen bei Suchmaschinenanbietern liefert kein Ergebnis.

Nach Realisierung dieser technischen Konzeption standen dem erneuten Einsatz des Portals keine datenschutzrechtlichen Bedenken entgegen.

15 Wirtschaft

15.1 Überweisungsdaten für Sparkassenwerbung genutzt?

Ein Sparkassenkunde eröffnete bei einer Internetbank ein weiteres Konto um die dort günstigeren Guthabenzinsen zu nutzen. Von seinem Sparkassengirokonto überweist er einen höheren Betrag auf das Konto der Internetbank.

Kurz darauf erhält er ein Werbeschreiben seiner Sparkasse mit einem guten Zinsangebot. Werbung ist im stark umkämpften Kapitalmarkt ein notwendiges zulässiges Mittel um eigene Marktanteile zu erhöhen. Die Umstände, wie die vorliegende Werbeaktion zustande gekommen ist, sprechen allerdings für eine datenschutzrechtlich unzulässige Auswertung von Kontenbewegungsdaten.

Bereits der Betreff „Ihr Extra-Konto der X.Bank“ ließ den Sparkassenkunden stutzig werden. Woher konnte die Sparkasse diese Information haben? Er hatte der Sparkasse nichts von dem neuen Konto gesagt. Dass ihm ein gutes Zinsangebot („Da haben wir doch das bessere Angebot“) gemacht wurde, dagegen hatte er nichts einzuwenden. Er fand es jedoch befremdlich, dass Überweisungsdaten ausgewertet werden, um gezielte und persönliche Werbeaktionen durchzuführen.

Ich habe die zuständige Sparkassenhauptstelle unter Hinweis auf einen möglichen Verstoß gegen die Zweckbindungsvorschriften des § 28 Bundesdatenschutzgesetz um Stellungnahme ersucht. Von dort teilte mir der betriebliche Datenschutzbeauftragte mit, dass Überweisungsdaten grundsätzlich nicht zu Werbezwecken zweckentfremdet werden. Im vorliegenden Fall habe eine Zweigstelle eigenmächtig gehandelt. Die Zweigstelle werde auf ihren Datenschutzverstoß aufmerksam gemacht und angewiesen, solche Werbeaktionen zu unterlassen.

16 Statistik

16.1 Volkszählung 2011

Das Bundeskabinett hat am 29. August 2006 beschlossen, dass sich Deutschland an der Volkszählungsrunde der EU im Jahr 2011 beteiligt.

Die Volkszählung wird registergestützt durchgeführt, d.h. die Basisdaten für die Volkszählung werden aus den Melderegistern gewonnen. Da die Melderegister abhängig vom Meldeverhalten der Bürgerinnen und Bürger sowie dem Bearbeitungsstand in den Kommunen in einem qualitativ nicht ausreichenden Zustand waren, wurde mit wissenschaftlicher Begleitung ein Verfahren entwickelt, um mit dem Abgleich verschiedener bereits vorhandener Datenquellen und stichprobenartiger Befragung zu einem Datenbestand zu gelangen, der den Qualitätsanforderungen einer Volkszählung genügt. Als zentrales Hilfsmittel dient ein Anschriften- und Gebäuderegister, das beim Statistischen Bundesamt aufgebaut werden wird. Die rechtliche Basis für das Verfahren wurde im September 2007 durch das Zensusvorbereitungsgesetz geschaffen.

Die Datenschutzbeauftragten des Bundes und der Länder haben das Gesetzgebungsverfahren begleitet und mit ihren Anregungen z. B. erreicht, dass Anschriften und Gebäuderegister zum frühest möglichen Zeitpunkt nach Abschluss des Zensus, spätestens jedoch sechs Jahre nach dem Zensusstichtag gelöscht werden.

Zwischenzeitlich (seit April 2009) sind die ersten Datenerhebungen bei den Ver- und Entsorgungsbetrieben erfolgt.

17 Umwelt

17.1 Geodateninfrastrukturgesetz

Am 15. Mai 2007 trat die Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE-Richtlinie) in Kraft. Damit wurde ein Instrument geschaffen um den Zugang und die Nutzung von Geodaten für Wirtschaft und Verwaltung und für Bürgerinnen und Bürger zu vereinfachen. Zur Umsetzung der Richtlinie haben die Mitgliedsstaaten innerhalb von zwei Jahren die erforderlichen Rechts- und Verwaltungsvorschriften zu erlassen.

Die datenschutzrechtliche Aufarbeitung der Thematik legte besonderen Wert auf ein handhabbares Verfahren und einen angemessenen Ausgleich zwischen Informations- und Geheimhaltungsinteressen. Durch die neue Infrastruktur werden georeferenzierbare Angaben auf Grund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten zu personenbezogenen Daten. Bei der an sich begrüßenswerten Bereitstellung amtlicher Geodaten ist der Schutz personenbezogener Daten angemessen zu gewährleisten.

In ihrer 76. Konferenz haben die Datenschutzbeauftragten des Bundes und der Länder eine Entschließung „Datenschutzgerechter Zugang zu Geoinformationen“ verfasst. Die Entschließung wurde dem saarländischen Ministerium für Umwelt zur Beachtung übersandt. Der mittlerweile vorliegende Gesetzentwurf zum Saarländischen Geodateninfrastrukturgesetz berücksichtigt die datenschutzrechtlichen Aspekte.

17.2 Katasterinhalts- und Datenübermittlungsverordnung

Bereits 2006 wurden erste Schritte zur Neufassung der Katasterinhalts- und Datenübermittlungsverordnung (KaInDÜV) unternommen. Der endgültige Verordnungsentwurf wurde mir im Juni 2008 durch das Ministerium für Umwelt zur Stellungnahme vorgelegt. Leider musste ich feststellen, dass nicht alle von mir eingebrachten Anregungen aus 2006 in den neuen Entwurf übernommen wurden.

Entgegen meinem Votum wurde der Vermessungs- und Katasterbehörde ein Dauerzugriff auf die Datenbank zur Wahrung der Fachaufsicht eingeräumt. Die Notwendigkeit hierfür wurde mir nicht erläutert.
Weiterhin wurde der Vollzugspolizei neben den unbestritten notwendigen Zugriffsmöglichkeiten bei polizeilichen Sofort- und Sonderlagen auch der Onlinezugriff zur Durchführung von Ermittlungsverfahren zugestanden. Diesen halte ich für unverhältnismäßig.
Die Katasterinhalts- und Datenübermittlungsverordnung wurde im Amtsblatt des Saarlandes vom 25. September 2008 (S. 1543) veröffentlicht.

18 Internationaler Datenschutz

18.1 Errichtung eines gemeinsamen Zentrums für länderübergreifende Polizei- und Zollzusammenarbeit in Luxemburg (GZPZ)

Erst aus diversen Presseberichten erfuhr ich im Juli 2008, dass in Luxemburg ein gemeinsames länderübergreifendes Zentrum der Polizei- und Zollzusammenarbeit unter Mitwirkung des Saarlandes eingerichtet worden sei. Divergierende Aussagen hinsichtlich einer etwaigen Rechtsgrundlage für die Schaffung einer solchen Stelle stimmten mich bedenklich, so dass ich eine entsprechende Anfrage an das hiesige Ministerium für Inneres und Sport richtete.

Im September 2008 wurde mir mitgeteilt, dass die GZPZ bereits seit dem 19.03.2003 in einem „vorläufigen Wirkbetrieb“ arbeite. Die Dienstverrichtung der vertretenen Behörden der vier Vertragspartner Deutschland, Luxemburg, Belgien und Frankreich erfolge gegenwärtig auf der Grundlage des Entwurfs eines trilateralen Abkommens zwischen dem Königreich Belgien, dem Großherzogtum Luxemburg und der Bundesrepublik Deutschland. Zwischen Frankreich und Luxemburg bestehe darüber hinaus eine bilaterale Vereinbarung. Beide Verträge waren zum damaligen Zeitpunkt zwar formuliert, von den jeweiligen Ländern im Hinblick auf die Erarbeitung einer quatrolateralen Vereinbarung nicht ratifiziert. Am 24. Oktober 2008 haben die Innenminister aus Belgien, Deutschland, Frankreich und Luxemburg dann das Abkommen am Rande der Ratssitzung der EU-Innenminister in Brüssel unterzeichnet.

An der Arbeit des GZPZ beteiligt sich das Saarland neben Rheinland-Pfalz und der Bundespolizei mit einem Beamten der im Saarland stationierten Polizei.

Da die maßgebliche Rechtsnorm für die Errichtung des GZPZ unter Beteiligung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ausgearbeitet und zwischenzeitlich ratifiziert wurde, konnten meine anfänglichen datenschutzrechtlichen Bedenken nunmehr ausgeräumt werden.

Gleichwohl halte ich es für bezeichnend, dass derartige Unternehmungen zunächst ohne gesetzliche bzw. vertragliche Grundlage implementiert werden. Dass ich nicht im Vorfeld unterrichtet worden bin, überrascht mich weniger.

19 Sonstiges

19.1 Unzulässige Datenübermittlung durch Versorgungsunternehmen

Ein Petent musste, nachdem er sein Eigenheim im Zwangsversteigerungsverfahren verloren hatte, eine neue Bleibe für seine Familie suchen. Er fand ein kleines Eigenheim, das er anmieten konnte. Um notwendige Umbau- und Renovierungsmaßnahmen in der neuen Wohnung durchführen zu können, übergab die Vermieterin schon vor Beginn des Mietverhältnisses den Hausschlüssel, mit der Auflage, ab diesem Zeitpunkt auch die anfallenden Nebenkosten wie Wasser und Strom zu übernehmen. Da er bei der Kündigung der Verbraucherstellen seines versteigerten Hauses keinen Nachbesitzer benennen konnte, schaltete das zuständige Versorgungsunternehmen einen Außendienstmitarbeiter zur Klärung der Eigentumsverhältnisse ein. Der Mitarbeiter des Versorgungsunternehmens konnte eruieren, dass das Anwesen unter Zwangsverwaltung stand. Auch war ihm bewusst, dass der Petent sich unter Angabe der neuen Wohnanschrift wieder beim Versorgungsunternehmer angemeldet hatte. Beim Versuch, den neuen Endverbraucher des versteigerten Hauses zu finden, setzte sich der Außendienstmitarbeiter mit der Zwangsverwalterin in Verbindung. Während des Gespräches teilte der Außendienstmitarbeiter der Zwangsverwalterin auf Nachfrage mit, dass der Petent eine neue Verbraucherstelle angemeldet hätte, was die Zwangsverwalterin dazu veranlasste, die Schlüssel im alten Haus austauschen zu lassen und die Familie auszusperren, obwohl die neue Wohnung noch nicht bezugsfertig war, das Mietverhältnis noch nicht begonnen hatte und die Besitztümer der Familie noch im alten Haus aufbewahrt wurden.

Mit der Frage, ob denn der Außendienstmitarbeiter der Zwangsverwalterin die Anmeldung unter der neuen Adresse hätte mitteilen dürfen, wandte sich der Petent an meine Geschäftsstelle.

Da weder ein Gesetz noch eine Einwilligung des Petenten die Datenübermittlung vom Außendienstmitarbeiter an die Zwangsverwalterin legitimierte, handelte es sich hierbei um eine unzulässige Datenübermittlung im Sinne des § 16 SDSG. Das Versorgungsunternehmen wurde darauf hingewiesen, zukünftig darauf zu achten, unter welchen Voraussetzungen sie die Daten ihrer Kunden an Dritte übermitteln darf. Des Weiteren sollten alle Mitarbeiter des Unternehmens nochmals für den datenschutzgerechten Umgang mit Kundendaten sensibilisiert werden.

19.2 Nachweise zur Inanspruchnahme von Ermäßigungen bei Agenturen für haushaltsnahe Arbeiten

Die Nachfrage nach Dienstleistungen in Privathaushalten steigt stetig. Gleichzeitig ist die Hauswirtschaft ein Bereich, in dem das Angebot von Schwarzarbeit weit verbreitet ist. Um die Lücke zwischen Angebot und Nachfrage zu schließen, die Schwarzarbeit zu verringern und zugleich reguläre Arbeitsplätze im hauswirtschaftlichen Bereich zu schaffen, wird das legale Angebot an haushaltsnahen Dienstleistungen von Agenturen für haushaltsnahe Arbeit (AhA) durch die saarländische Regierung gefördert. Senioren ab 60 Jahren und Behinderte ab einem Grad der Behinderung von 50 % erhalten gemäß den Fördergrundsätzen einen höheren Zuschuss als andere Personen.

Als Nachweis für die Berechtigung zur höheren Bezuschussung sollten die Agenturen gemäß den Förderrichtlinien von den Berechtigten eine vollständige Kopie des Personalausweises bzw. des Schwerbehindertenausweises vorhalten.

Wegen dieser Nachweisführung wandte sich eine Agentur an meine Geschäftsstelle mit der Argumentation, dass durch die Kopie des kompletten Personalausweises oder des kompletten Schwerbehindertenausweises Daten der Betroffenen erhoben und gespeichert werden, die für die Aufgabenerfüllung der zuschussgewährenden Stelle nicht erforderlich sind und somit gemäß § 12 Absatz 1 SDSG eine unzulässige Datenerhebung darstellen.

Der Argumentation folgend setzte ich mich mit dem zuständigen Ministerium in Verbindung, um eine datenschutzkonforme Lösung zu finden. Da von Seiten des Rechnungshofes keine rechtliche Möglichkeit besteht, die wahrheitsgemäße Beantragung direkt beim Zuschussempfänger zu kontrollieren, konnten wir uns auf die Möglichkeit des Schwärzens der Angaben, die zur Beantragung nicht erforderlich sind, einigen. Das Ministerium unterrichtete daraufhin umgehend die teilnehmenden Agenturen für haushaltsnahe Arbeiten über die datenschutzkonforme Vorgehensweise bei der Beantragung eines höheren Zuschusses für den oben genannten Personenkreis.

19.3 Unerlaubte Nutzung der Mitgliederdaten durch die Vereinigung der Jäger des Saarlandes

Ein Diplom-Forstwirt wandte sich mit der Eingabe an meine Geschäftsstelle, er habe Werbepost mit einer Einladung für eine Fußbodenausstellung erhalten, die im Anschriftenfeld seinen Titel als Diplom-Forstwirt beinhaltet. Diesen Titel benutze er lediglich im Zusammenhang mit seiner Mitgliedschaft in der Vereinigung der Jäger des Saarlandes (VJS). Auf seine Nachfrage bei der VJS sei seine Vermutung bestätigt worden, dass die Daten aus dem Mitgliederdatenbestand der Vereinigung stammten. Da es sich bei der VJS um eine Körperschaft des öffentlichen Rechts handelt, ergab sich meine Zuständigkeit.

Mit den Vorwürfen des Diplom-Forstwirtes konfrontiert, erhielt ich von der VJS folgende Begründung:

Die Daten der Mitglieder der VJS seien nicht an die Fußbodenfirma übermittelt worden. Vielmehr habe man sich des Adressmittlungsverfahrens bedient, wonach die Daten der Mitglieder lediglich in die vorgefertigten Anschreiben der Firma eingesetzt worden seien, ohne der Fußbodenfirma die Daten zu offenbaren. Eine andere Information der Mitglieder, beispielsweise über eine Annonce in der quartalsmäßig erscheinenden Zeitschrift „Der Saarjäger“, sei wegen der terminlichen Gestaltung der Veranstaltung nicht mehr möglich gewesen.

Vor dem Hintergrund, dass die Satzung der VJS unter § 2 auch die Pflege der Kameradschaft unter den Mitgliedern und die Fortbildung der Mitglieder auf dem Gebiet des Jagd- und Schießwesens vorsieht, erschien der VJS die Veranstaltung auch diesen Zwecken dienlich, da während der 3-tägigen Fußbodenausstellung unter anderem auch Vorträge mit dem Titel „Wald, Wild, Wohnqualität“ gehalten wurden.

Diesen Ausführungen der VJS konnte ich allerdings nicht folgen, denn wie aus dem Werbeschreiben ersichtlich, war Schwerpunkt der Veranstaltung die Präsentation von Fußbodenbelägen. Somit lag eine unzulässige Datennutzung des Mitgliederdatenbestandes der VJS im Sinne des § 13 Absatz 1 Satz 1 SDSG vor, da die Präsentation von Fußbodenbelägen sicherlich nicht zur Aufgabenerfüllung der VJS erforderlich ist.

Ich habe das Verhalten der VJS gerügt und die VJS gebeten, in zukünftigen Fällen sorgfältiger zu prüfen, ob sich eine Nutzung der Daten ihrer Mitglieder im Rahmen der Aufgabenstellung ihrer Körperschaft bewegt.

19.4 Interessenkollission bei behördlichen Datenschutzbeauftragten

Immer wieder erreichen mich Anfragen im Zusammenhang mit der Bestellung behördlicher Datenschutzbeauftragten.

Behördliche Datenschutzbeauftragte leisten einen wertvollen Beitrag zur Gewährleistung des Anspruchs der Bürger sowie der Behördenmitarbeiter auf Schutz ihres Rechtes auf informationelle Selbstbestimmung, da sie aufgrund ihrer Präsens vor Ort in besonderer Weise geeignet sind, Beratungs- und Kontrollfunktionen wahrzunehmen. Damit dieses Ziel auch erreicht werden kann, muss der Mitarbeiter, der zum Datenschutzbeauftragten bestellt werden soll, bestimmte Voraussetzungen erfüllen. Neben der erforderlichen Sachkunde muss dieser auch zuverlässig sein, wozu neben der charakterlichen Integrität insbesondere gehört, dass der Datenschutzbeauftragte nicht in Interessenkonflikte mit seiner sonstigen Tätigkeit in der Behörde gerät.

In der täglichen Praxis ist oft umstritten, welche Funktionen sich mit der Aufgabenstellung des behördlichen Datenschutzbeauftragten vertragen.

Im Berichtszeitraum hatte mich der Personalrat eines Sozialversicherungsträgers um Unterstützung gebeten, weil er der Auffassung war, dass die Bestellung eines neuen Datenschutzbeauftragten, der gleichzeitig Leiter des Selbstverwaltungsbüros sowie Leiter der Beihilfestelle war, nicht rechtens sei.

Bei meiner datenschutzrechtlichen Bewertung bin ich zu folgendem Ergebnis gekommen: Keine Bedenken habe ich in der gleichzeitigen Wahrnehmung der Aufgaben des behördlichen Datenschutzbeauftragten und des Leiters des Selbstverwaltungsbüros gesehen. Aufgabe des Leiters des Selbstverwaltungsbüros ist die Beratung und Unterstützung der Mitglieder der Selbstverwaltungsorgane und somit auch des Vorstandes des Sozialversicherungsträgers. Durch die Personalunion von behördlichem Datenschutzbeauftragten und Leiter des Selbstverwaltungsbüros ergibt sich nach meiner Ansicht eher ein Synergieeffekt in der Art, dass das Fachwissen als Datenschutzbeauftragter in die unterstützende Tätigkeit des Vorstandes mit eingebracht werden kann und somit das Bewusstsein für den Datenschutz auf der Leitungsebene gestärkt wird.

Als datenschutzrechtlich bedenklich sehe ich hingegen die Personalunion von behördlichem Datenschutzbeauftragten und Leiter der Beihilfestelle an. In der Beihilfestelle werden in erheblichem Umfang personenbezogene Daten sensibler Art verarbeitet, d.h. in diesem Bereich ist eine kritische und unabhängige Datenschutzkontrol-

le besonders wichtig. Nach einstimmiger Auffassung in der datenschutzrechtlichen Kommentarliteratur scheiden Personalleiter als behördliche Datenschutzbeauftragte aus. Die Beihilfesachbearbeitung stellt nun sogar einen besonders sensiblen Teil der Personalsachbearbeitung dar. Die Beschäftigten der Beihilfestelle erhalten regelmäßig personenbezogene Daten über Krankheiten, Diagnosen, Behandlungen und Medikamente der Bedienstete. Die Einhaltung des Datenschutzes in diesem Bereich erfordert deshalb besondere Aufmerksamkeit. Eine „Selbstkontrolle“ wäre hier kontraproduktiv. Um schon im Ansatz die Gefahr eines möglichen Interessenkonfliktes zu vermeiden, sind nach meiner Auffassung die Funktionen des Leiters der Beihilfestelle und des behördlichen Datenschutzbeauftragten nicht miteinander vereinbar.
Leider konnte ich die Behördenleitung nicht von meiner Auffassung überzeugen. Sie hat stattdessen lediglich eine verstärkte Kontrolle der Datenverarbeitung in der Beihilfestelle durch die Innenrevision angekündigt, was das Konfliktpotential zwar verringert, insgesamt aber keine befriedigende Lösung im Sinne des Datenschutzes darstellt.

In diesem Zusammenhang möchte ich noch darauf hinweisen, dass ich eine Broschüre zum behördlichen Datenschutzbeauftragten herausgegeben habe, in der dessen Bestellung sowie seine Aufgaben und Befugnisse erläutert werden. Die Broschüre kann bei meiner Dienststelle unter der Adresse: Der Landesbeauftragte für Datenschutz und Informationsfreiheit, Fritz-Dobisch-Str. 12, 66111 Saarbrücken, Telefon 0681/94781-0, E-Mail: poststelle@lfdi.saarland.de angefordert werden. Sie kann ebenfalls aus meinem Internetangebot www.lfdi.saarland.de ausgedruckt werden.

20 Informationsfreiheitsgesetz

20.1 Saarländisches Informationsfreiheitsgesetz

Am 15. September 2006 trat das Saarländische Informationsfreiheitsgesetz (SIFG) in Kraft. Es lehnt sich größtenteils an das Informationsfreiheitsgesetz des Bundes an. Es soll den Bürgern den Zugang zu amtlichen Informationen erleichtern und zu mehr Behördentransparenz führen und Verwaltungsentscheidungen aus dem Schatten der Amtsverschwiegenheit herausholen.

Die Aufgaben des Landesbeauftragten für Informationsfreiheit wurden dem Landesbeauftragten für Datenschutz übertragen.

Die vergangenen 3 Jahre haben Licht und Schatten im Umgang mit dem Saarländischen Informationsfreiheitsgesetz deutlich werden lassen.

Die erste statistische Erfassung zur Zahl der Anfragen nach dem SIFG wurde durch das damalige Ministerium für Inneres, Familie, Frauen und Sport zum 30.6.2007 erstellt. Daraus ging hervor, dass in den ersten Monaten lediglich 6 Anfragen gestellt wurden. Auch wenn diese Statistik bezüglich ihrer Vollständigkeit angezweifelt werden muss (so ist z.B. eine mir vorliegende Eingabe bzgl. des Landkreises Saarlouis nicht in dieser Statistik ausgewiesen), so lässt sie doch vermuten, dass das SIFG zu selten genutzt wird. Damit ist aber auch die Befürchtung widerlegt, dieses Gesetz würde zu einer Flut nicht zu bewältigender Anfragen führen.

Die Landesbehörden wurden angewiesen, weiterhin statistische Erfassungen zu führen, die in der Evaluationsphase des Gesetzes im Jahr 2010 ausgewertet werden.

Ich selber bin mit meinen Mitarbeitern weiterhin bemüht, das Gesetz mit Leben zu erfüllen.

20.2 Eingaben zum SIFG –allgemein-

Bis zum Ende des Jahres 2008 erreichten mich 20 Eingaben, in denen die Petenten beklagten, dass Ihnen keine bzw. nicht die beantragten Auskünfte nach dem SIFG gegeben wurden.

In den meisten Fällen waren die angefragten Dienststellen durchaus bereit, Auskunft zu gewähren. Die neue Materie, organisatorische Probleme oder Zuständigkeitsfragen führten jedoch allzu oft dazu, dass die gesetzlich festgelegte Frist von einem Monat zur Beantwortung einer Anfrage verstrichen war. Fast ausnahmslos wurde es versäumt, den Antragstellern einen Zwischenbescheid mit dem Grund der Verzögerung zukommen zu lassen.

In einigen Fällen fehlte bei ablehnenden Bescheiden die nach § 3 SIFG vorgeschriebene Rechtsbehelfsbelehrung.

Die betroffenen Ämter wurden von mir über Ihre Pflichten aufgeklärt und erklärten, die gesetzlichen Vorgaben in Zukunft zu beachten. Vorsätzliches Fehlverhalten war in keinem Fall zu erkennen.

Da ich wegen der sehr knappen personellen Ressourcen meiner Geschäftsstelle (derzeit jedenfalls) nicht in der Lage bin, bei den Dienstellen des Landes und der Gemeinden Schulungsmaßnahmen in Sachen Informationsfreiheit durchzuführen, würde ich es begrüßen, wenn die Landesverwaltung und die kommunalen Spitzenverbände in eigener Zuständigkeit die Aufklärung und Schulung der Bediensteten des Landes und der Kommunen betreiben würden.

Alternativ wäre natürlich eine Verstärkung meiner Dienststelle denkbar, da diese seit dem 15.09.2006 ohne jegliche Änderung im Personaleinsatz ihre eigentlich für den Datenschutz veranschlagten Ressourcen auch der Informationsfreiheit widmen muss.

20.3 Sponsoring

Im Februar 2007 erbat ein Antragsteller von einer hervorgehobenen Dienststelle des Landes Auskunft darüber, ob und in welcher Höhe sich Sponsoren am Neujahrsempfang und an weiteren öffentlichkeitswirksamen Kampagnen dieser Dienststelle beteiligt hätten.

Da der Antragsteller zuerst keine Auskunft erhielt, wandte er sich an mich. Ich musste feststellen, dass auch in diesem Fall die Antwort an den Antragsteller erst sieben Wochen und damit verspätet erteilt wurde. Zudem waren die Antworten unbefriedigend, da unter Hinweis auf „schutzwürdige Interessen Dritter“ die Namen der Sponsoren sowie die Höhe der Sach- oder Geldleistungen nicht benannt wurden.

Der Antragsteller hat es versäumt, gegen diese Auskunft fristgerecht Rechtsmittel einzulegen. Möglicherweise hoffte er, dass eine ähnlich lautende parlamentarische Anfrage eines Mitglieds des Landtages die begehrten Auskünfte liefern würde. Aber auch hier wurde die Auskunft unter Hinweis auf „schutzwürdige Interessen Dritter“ verweigert.

Die Haltung besagter Dienststelle lässt sich nachvollziehen, soweit natürliche Personen als Sponsoren auftreten. In diesem Fall greift § 5 SIFG und eine Veröffentlichung des Namens ist nur zulässig, wenn der Sponsor einwilligt.

Treten hingegen Firmen als Sponsoren auf, lässt das SIFG keine Begründung erkennen aus der sich die Weigerung zur Namensnennung ableiten lässt. Der oft bemühte § 6 SIFG „Schutz des geistigen Eigentums und von Betriebs- und Geschäftsgeheimnissen“ kann hier nicht herangezogen werden. Ein Betriebs- oder Geschäftsgeheimnis setzt ein berechtigtes wirtschaftliches Geheimhaltungsinteresse voraus. Die Aufdeckung eines Geheimnisses müsste geeignet sein, dem Betrieb wirtschaftlichen Schaden zuzufügen.

Da es beim Sponsoring aber regelmäßig gerade darum geht, publikums- und werbewirksam aufzutreten, zahlreiche Banner mit Firmennamen sprechen hier für sich,

kann ich nicht erkennen, dass das Bekanntwerden von Sponsoring zu wirtschaftlichen Nachteilen führen kann.

Um Spekulationen über Einflussnahmen der Wirtschaft auf die Politik zuvorzukommen, halte ich es für wünschenswert und notwendig, dass die Regierung des Saarlandes einen Sponsoringbericht veröffentlicht, der sich in der Form an dem „Zweijahresbericht des Bundesministeriums des Innern über die Sponsoringleistungen an die Bundesverwaltung“ orientieren könnte.

20.4 G8/G9-Notenvergleich

Eine Anfrage nach dem SIFG ist durch zahlreiche Medienveröffentlichungen während des Berichtszeitraums ins Blickfeld der Öffentlichkeit gelangt: die Forderung nach Veröffentlichung des sog. G8/G9 Notenvergleichs.

Die Behandlung dieser Anfrage durch das Ministerium für Bildung, Familie, Frauen und Kultur lässt erkennen, dass dem Auskunftsbegehren der Bürgerinnen und Bürger in manchen Behörden, sei es aus Rechtsunsicherheit oder aber aus anderen Gründen, nur ungern und unzureichend Rechnung getragen wird.

In diesem Fall war festzustellen, dass der Antrag erst nach mehr als 6 Wochen abschlägig beschieden wurde, obwohl der der Anfrage zu Grunde liegende Sachverhalt eine rechtliche und tatsächliche aktuelle Bearbeitung aus meiner Sicht durchaus möglich machte. Eine Rechtsbehelfsbelehrung fehlte vollständig. Neben diesen formalen Fehlern muss aber auch die Begründung der Ablehnung durchaus hinterfragt werden. Zum einen wurden datenschutzrechtliche Bedenken vorgetragen: Aus dem Notenvergleich könnten Rückschlüsse auf einzelne Personen (Schüler oder Lehrer) gezogen werden. Außerdem sei durch eine Auswertung ein Ranking der Schulen möglich. Die datenschutzrechtliche Begründung vermag ich in dieser Absolutheit nicht nachzuvollziehen. Im Übrigen stellt sich für mich die Frage, ob die theoretische Möglichkeit eines Schulrankings einer ansonsten zu beantwortenden Informations-

freiheitsanfrage im Wege stehen kann. Da die Ablehnungsgründe im SIFG abschließend geregelt sind, ist das aus meiner Sicht nicht der Fall.

Um jedenfalls den vorhandenen und berechtigten datenschutzrechtlichen Einwand zu würdigen, unterbreitete ich den Vorschlag, bestimmte Lehrfächer, in denen die Schüler- oder Lehrerzahl sehr gering ist, von der Veröffentlichung auszunehmen. Dieses Vorgehen ist üblich und insbesondere in den Obersten Landesbehörden bei der Veröffentlichung statistischer Auswertungen gängige Praxis. Ein Personenbezug wäre auch in dieser Auswertung nicht mehr herstellbar.

Bis heute verweigert das Bildungsministerium die Herausgabe des G8/G9-Notenvergleichs. Der Antragsteller hat mittlerweise Klage beim Verwaltungsgericht eingereicht.

21 Entschließungen

21.1 GUTE ARBEIT in Europa nur mit gutem Datenschutz

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007 in Erfurt

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19. Januar 2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen.
Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, zum Beispiel durch

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

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen

21.2 Anonyme Nutzung des Fernsehens erhalten!

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007 in Erfurt

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Vermarktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrie-

ren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der Abrechnung – beispielsweise durch den Einsatz von vorbezahlten Karten – ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen, und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

21.3 Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben!

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007 in Erfurt

Mit dem Verfahren ELENA (elektronische Einkommensnachweise) sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Dieses Verfahren ist angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass ein derartiges Register nur dann eingerichtet werden darf, wenn die verfassungsrechtlichen Voraussetzungen erfüllt und die gesetzlichen und technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten getroffen werden.

Zu den wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers gehören der Nachweis der Erforderlichkeit und die Verhältnismäßigkeit. Angesichts bestehender Zweifel daran, dass diese Voraussetzungen gegeben sind, muss belastbar dargelegt werden, dass die Daten für die jeweiligen Zwecke tatsächlich benötigt werden und dass der angestrebte Zweck nicht mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung erreicht werden kann.

Im Hinblick auf den vom Bundesministerium für Wirtschaft und Arbeit erarbeiteten Referentenentwurf sieht die Konferenz darüber hinaus in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens zu entschlüsseln sind.
- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.
- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.
- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

21.4 Keine heimliche Online-Durchsuchung privater Computer

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007 in Erfurt

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. „Trojaner“ heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31. Januar 2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzgeber, es beim bisherigen Rechtszustand des „offenen Visiers“ zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie z. B. die Strafverfolgung, betroffen sind. Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszu-

spähen. Dies gilt umso mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungsmaßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betroffen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Software-Updates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

21.5 Pläne für eine öffentlich zugängliche Sexualstraftäterdatei

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007 in Erfurt

In der aktuellen Diskussion um einen verbesserten Schutz von Kindern vor Sexualstraftätern wird u.a. die Einrichtung einer öffentlich zugänglichen Sexualstraftäterdatei mit Wohnsitzangaben gefordert. Es wird vorgeschlagen, die Namen und Adressen von verurteilten Sexualstraftätern z.B. über das Internet zu veröffentlichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zusteht.

Der Vorschlag ist lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern. Die Betroffenen könnten damit eher zu einem erhöhten Gefahrenpotenzial werden. Er sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht weiter verfolgt werden.

21.6 Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007 in Erfurt

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden

zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.

- Für Angehörige i.S.v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i.S.v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht - wie im Entwurf vorgesehen - auf Beweiszwecke begrenzt werden.

- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraum-

überwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.

- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.

- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

21.7 Entschließung der Datenschutzbeauftragten des Bundes und der Länder Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung – ob via Telefon oder Internet – pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.
Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen – bis zum Erfordernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

21.8 Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 in Saalfeld

Die fortschreitende technologische Entwicklung führt zu immer weitreichenderer Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung

für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürgern berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass letztlich bei allen vertraglichen Beziehungen – also auch bei Versicherungs- und Arbeitsverträgen – vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematisch-statistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich der Scorewert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Betroffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Scorewert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug. Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

21.9 Nein zur Online-Durchsuchung

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 in Saalfeld

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.

Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um „Online-Durchsicht“ als einmalige Durchsuchung und die damit verbun-

dene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen andere Kommunikations- und Datenverarbeitungssysteme, wie Computernetze, Mobiltelefone, PDA usw. in die heimliche Durchsuchung einbezogen werden. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von – auch unverdächtigen – Nutzerinnen und Nutzern betroffen sein werden.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit – jedenfalls bei der Verfolgung von Straftaten – die Geeignetheit der Online-Durchsuchung in Frage stellt.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden. So begründen z.B. die drohende Aufweichung der Zweckbindung der Mautdaten und die Entwicklung der Telekommunikationsüberwachung die Befürchtung, dass Online-Durchsuchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung eingesetzt werden. Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregie-

rung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

Sie halten es für zwingend notwendig, dass das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abgewartet wird.

21.10 Zentrale Steuerdatei droht zum Datenmoloch zu werden

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 in Saalfeld

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche - teilweise sensible - Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 9. November 2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/Arbeitnehmerinnen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

- Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitserwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.
- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.
- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87a Abs. 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform „Elster“ für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuer*fremden* Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139b Abs. 5 Abgabenordnung zu rein

steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139b Abs. 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsaufträge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BaföG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z.B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

21.11 Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 in Saalfeld

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können – auch wenn die Betroffenen über die Umstände informiert wurden – diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen – zusätzlich – zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem u.a. die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

21.12 Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

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

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 Steuer-Identifikationsnummer (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.

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

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

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 Datenübermittlungsbefugnisse 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.

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

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

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 Scoringverfahren 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.

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

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

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 Dammbruch 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.

21.16 Keine Vorratsspeicherung von Flugpassagierdaten

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

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[1], 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.

21.17 Medienkompetenz und Datenschutzbewusstsein in der jungen „online-Generation“

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

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-

[1] 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

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 sorgsamen 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.

21.18 Mehr Augenmaß bei der Novellierung des BKA-Gesetzes

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

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 diente 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 Terrorismus 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.

21.19 Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten

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

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.

21.20 Entschlossenes Handeln ist das Gebot der Stunde (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 diese 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 endlich 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 der 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 sollten 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 Aufsichtsbehörden 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."

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

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

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.

21.22 Mehr Transparenz durch Informationspflichten bei Datenschutzpannen

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

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.

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

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

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.

21.24 Elektronische Steuererklärung sicher und datenschutzgerecht gestalten

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

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 Authentisierungs- 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.
3) 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.

21.25 Datenschutzgerechter Zugang zu Geoinformationen

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

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 INSPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

21.26 Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren

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

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 Löschungskonzept 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.

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

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

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 Belastungen 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.

21.28 Beschluss zu länderübergreifenden gemeinsamen Datenverarbeitungen

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

Der *Arbeitskreis Grundsatzfragen der Verwaltungsmodernisierung* (AK GdV) hat auf Basis einer Erhebung der vorhandenen und geplanten Verfahren in Bund und Ländern mit länderübergreifender gemeinsamer Datenverarbeitung in einem ersten Schritt generell zu beachtende Eckpunkte erarbeitet (vgl. 2.1 des Papiers „Länderübergreifende gemeinsame Datenverarbeitungen“ vom 30.10.2008). Er empfiehlt der *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, diese beim Einsatz solcher Verfahren zu berücksichtigen.

Die Aufarbeitung der Thematik hat gezeigt, dass die bestehenden Regelungen unzulänglich sind, weil sie nicht die Bandbreite der Fälle abdecken, oftmals keine praxisgerechten Lösungen ermöglichen und die Regelungen in den Ländergesetzen sich teilweise widersprechen. Der AK GdV empfiehlt eine Modernisierung und Anpassung der Regelungen in den Datenschutzgesetzen und bittet die Konferenz um Diskussion, ob ein Mustervorschlag hierzu entwickelt werden soll.

21.29 Adress- und Datenhandel nur mit Einwilligung der Betroffenen

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

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 machten.

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 wirksameres 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.

21.30 Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten

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

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.

22 Sachverzeichnis

23 Abkürzungsverzeichnis

AO	Abgabenordnung
AhA	Agenturen haushaltsnaher Arbeiten
ALG	Arbeitslosengeld
ARGE	Arbeitsgemeinschaft
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMF	Bundesministerium der Finanzen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
DMS	Dokumentenmanagementsystem
Ed	erkennungsdienstlich
EG	Europäische Gemeinschaft
EU	Europäische Union
EGMR	Europäischer Gerichtshof für Menschenrechte
eGo-Saar	Zweckverband elektronische Verwaltung für saarländische Kommunen
eGovernment	Electronic Government, elektronische Verwaltung
eMail	Elektronisch versandte Post
EUREKA	EDV-Unterstützung für Rechtsgeschäftstellen und Kanzleien
GSM	Global system for mobile communication - Standard für Mobilfunknetze
GPRS	General packet radio service - paketorientierter Dienst zur Datenübertragung, welcher in GSM-Netzen verwendet wird
GZPZ	Gemeinsames Zentrum für landesübergreifende Polizei- und Zollzusammenarbeit
ID	Identifikator, Kennung
INSPIRE	Infrastructure for spatial information in the European Community
IP	Internetprotokoll

IT	Informationstechnik
IPSec	Internetprotokollsecurity
KaInDÜV	Katasterinhalts- und Datenübermittlungsverordnung
KAN	Kriminalaktennachweis
KPS	Kriminalpolizeiliche Sammlung
KWG	Kommunalwahlgesetz
JVA	Justizvollzugsanstalt
KSVG	Kommunalselbstverwaltungsgesetz
LfDI	Landesbeauftragter für Datenschutz und Informationsfreiheit
LWG	Landtagswahlgesetz
MBFFK	Ministerium für Bildung, Familie, Frauen und Kultur
MeldDÜV	Meldedatenübermittlungsverordnung
MG	Meldegesetz
OSCI	Name eines Protokollstandards für die deutsche öffentliche Verwaltung (engl. für Online Services Computer Interface)
OwiG	Ordnungswidrigkeitengesetz
PKS	Polizeiliche Kriminalstatistik
POLADIS	Polizeiliches anwendungsorientiertes dezentrales Informationssystem
RFID	Radio frequency identification, Identifikation mit Hilfe elektromagnetischer Wellen
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SGB I	Sozialgesetzbuch – Allgemeiner Teil (Erstes Buch)
SGB II	Sozialgesetzbuch – Grundsicherung für Arbeitssuchende (Zweites Buch)
SGB III	Sozialgesetzbuch – Arbeitsförderung (Drittes Buch)
SGB IV	Sozialgesetzbuch – Gemeinsame Vorschriften für die Sozialversicherung (Viertes Buch)
SGB V	Sozialgesetzbuch – Gesetzliche Krankenversicherung (Fünftes Buch)
SGB VI	Sozialgesetzbuch VI – Gesetzliche Rentenversicherung (Sechstes Buch)

SGB X	Sozialgesetzbuch X – Verwaltungsverfahren, Schutz der Sozialdaten, Zusammenarbeit der Leistungsträger und ihre Beziehungen zu Dritten (Zehntes Buch)
SIFG	Saarländisches Informationsfreiheitsgesetz
SJStVollzG	Saarländisches Jugendstrafvollzugsgesetz
SPolG	Saarländisches Polizeigesetz
SSL	Secure Socket Layer: durch Verschlüsselung gesichertes Übertragungsverfahren im Internet
StA	Staatsanwaltschaft
StGB	Strafgesetzbuch
Steuer-ID	Steueridentifikationsnummer
StPO	Strafprozessordnung
SVerfSchG	Saarländisches Verfassungsschutzgesetz
StVollzG	Strafvollzugsgesetz
TESTA	Trans-European Services for telematics between Administrations, Internes Netzwerk von europäischen Verwaltungen
TKG	Telekommunikationsgesetz
TVL	Tarifvertrag für der öffentlichen Dienst der Länder
URL	Uniform resource locator, Adresse im Internet
VPN	Virtuelles privates Netzwerk
VSRG	Verwaltungsstrukturreformgesetz