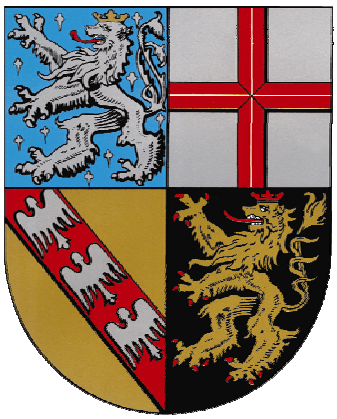
Die Landesbeauftragte
für Datenschutz und Informationsfreiheit
im Saarland



23. Tätigkeitsbericht

2009 / 2010

23. Tätigkeitsbericht
der

Landesbeauftragten
für Datenschutz und Informationsfreiheit

für die Jahre 2009 und 2010

dem Landtag und der Landesregierung
vorgelegt am 13.04.2011

(Landtagsdrucksache 14/425)

Die Landesbeauftragte
für Datenschutz und Informationsfreiheit im Saarland
Judith Thieser

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 März 2011

Vorwort

Sie halten den Tätigkeitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit für die Jahre 2009 und 2010 in Händen.

Da ich selbst dieses Amt im Juni 2010 übernommen habe, ist der Bericht im Wesentlichen geprägt durch die Tätigkeit meines Vorgängers, Herrn Roland Lorenz, und der Arbeit der Mitarbeiterinnen und Mitarbeiter.

Ich habe in den ersten Monaten meiner Tätigkeit erfahren, dass – von wenigen Ausnahmen abgesehen – viele öffentliche Stellen im Lande bereit sind, Hinweise und Vorschläge zum Datenschutz anzunehmen, gleichzeitig aber Unsicherheit und Unkenntnis in der Anwendung des Rechtes bestehen. Dies wird auch durch die in diesem Tätigkeitsbericht geschilderten Vorgänge belegt.

Im Bereich der Videoüberwachung – die ich weder ablehnen noch als das Allheilmittel ansehen will – sind die Vorschriften im saarländischen Datenschutzgesetz aus dem Jahre 2008 bei den Anwendern vielfach unbekannt. Die von meinem Vorgänger, Herrn Roland Lorenz, noch initiierte Umfrage bei den Behörden hat dies bestätigt.

Aufgrund dieser Erfahrungen sehe ich einen starken Schwerpunkt meiner Arbeit in der Information und Beratung öffentlicher Stellen – sei es persönlich, per Internet oder durch Informationsveranstaltungen – um so den Datenschutz zu verbessern.

Natürlich muss auch weiterhin die Einhaltung des Datenschutzes überwacht werden, um den Grundrechtsschutz zu gewährleisten. Ich bin aber der festen Überzeugung, dass bei zunehmenden Informationen der Betroffenen die Sensibilisierung zunimmt und damit der Datenschutz einen immer breiteren Raum einnimmt.
Dies muss das Ziel meiner Tätigkeit sein.

Genauso konsequent muss aber auch die Möglichkeit bestehen Bußgelder anzudrohen und zu verhängen, wenn bewusst und gewollt gegen den Datenschutz verstoßen

wird. Diese Regelungen fehlen in vielen Bereichen und sind im Sinne eines einheitlichen und unabhängigen Datenschutzes unverzichtbar.

Der zweite Bereich meiner Tätigkeit betrifft die Informationsfreiheit und ist ein fast ebenso spannendes Rechtsgebiet.

Nach dem saarländischen Informationsfreiheitsgesetz hat „jeder“ den Zugang zu amtlichen Informationen auf der Grundlage des Informationsfreiheitsgesetzes des Bundes. Dies bedeutet, dass es grundsätzlich – und zwar ohne Grund und Anlass – für jeden Bürger Einsicht in Verwaltungsakten gibt. Die Ablehnungsgründe sind abschließend aufgezählt und werden von den Gerichten zwischenzeitlich sehr restriktiv ausgelegt.

Das Gesetz führt damit zu einer Abkehr vom Aktengeheimnis und stellt jahrzehntelang geübtes Behördenverhalten auf den Kopf. Auch hier ist Information sowohl der Bürger als auch der Verwaltungsmitarbeiter über das inzwischen fünf Jahre alte Gesetz notwendig.

Der Tätigkeitsbericht 2009/2010 zeigt einen kleinen Ausschnitt aus meiner Tätigkeit, der meines Vorgängers und natürlich der Mitarbeiterinnen und Mitarbeiter. Diesen möchte ich hiermit besonders danken, denn der Bericht ist das Ergebnis einer Teamarbeit und wäre ohne deren Einsatz nicht denkbar.

Ich möchte aber auch die Gelegenheit nutzen und den Abgeordneten des saarländischen Landtages für meine Wahl und die Unterstützung danken; ebenso dem Präsidenten des Landtages, der mir den Einstieg in das neue Amt durch seine Unterstützung wesentlich erleichtert hat.

Saarbrücken, den 1. März 2011

Judith Thieser
Die Landesbeauftragte für Datenschutz
und Informationsfreiheit
im Saarland

Inhaltsverzeichnis

1 Vorbemerkung

Darstellung der aktuellen Situation

Die Saarländische Landesregierung hat im Koalitionsvertrag vom November 2009 die Zusammenlegung des Datenschutzes für den privaten und öffentlichen Bereich beschlossen. Es soll ein unabhängiges Landeszentrum für Datenschutz geschaffen werden, um die Bürger im öffentlichen und im nichtöffentlichen Bereich wirksam vor dem Missbrauch ihrer persönlichen Daten zu schützen.

Dieses Unabhängige Zentrum soll nach den Ausführungen im Koalitionsvertrag als niederschwellige und bürgernahe Kontroll- und Beratungsinstanz dienen und die zentrale Anlaufstelle für Bürgerinnen und Bürger in allen Fragen des Datenschutzes sein.

Die Datenschutzkontrolle ist in Deutschland bis dato so geregelt, dass der Bundesbeauftragte für den Datenschutz die Behörden des Bundes und die Landesbeauftragten die Behörden der Länder kontrollieren.

Die privaten Unternehmen und die nicht-öffentlichen Stellen werden von den jeweiligen Aufsichtsbehörden der Länder kontrolliert, die bis 2009 teilweise in den Innenministerien angesiedelt waren, teilweise bei den Landesbeauftragten, wobei eine Einbindung in die staatliche Verwaltung die Regel war.

Die Landesbeauftragte für Datenschutz im Saarland ist für den öffentlichen Bereich zuständig. Die Aufsicht des Datenschutzrechtes im privaten Bereich obliegt derzeit noch der Aufsichtsbehörde im Innenministerium. Das Gesetzgebungsverfahren zur Änderung der Zuständigkeiten ist im März 2011 in der externen Anhörung, so dass mit einer Verabschiedung in 2011 zu rechnen ist.

Der Europäische Gerichtshof hat am 9. März 2010 in einem Verfahren gegen die Bundesrepublik Deutschland festgestellt, dass die Datenschutzaufsicht im privaten Bereich nicht unabhängig ist und damit den Anforderungen der Europäischen Datenschutzrichtlinie nicht genügt.

Die Richtlinie fordert in Artikel 28, dass die Datenschutzbeauftragten ihre Tätigkeit in voller Unabhängigkeit ausüben, wobei die Auslegung in der Praxis uneinheitlich war. Zu der Notwendigkeit und verfassungsmäßigen Zulässigkeit der Zusammenlegung des privaten und öffentlichen Bereichs beim unabhängigen Landesbeauftragten verweise ich im Übrigen auf die Ausführungen meines Vorgängers im letzten Tätigkeitsbericht, dessen Ausführungen ich voll teile.

Durch diese Entscheidung des Europäischen Gerichtshofs sind bis zum März 2011 in 13 von 16 Bundesländern Änderungen auf den Weg gebracht oder bereits umgesetzt worden.

Als Fazit der Entscheidung des Europäischen Gerichtshofs kann man festhalten, dass durch die Unabhängigkeit das Risiko der Einflussnahme auf Entscheidungen der Datenschutzbeauftragten der Länder vermieden und damit der Datenschutz selbst gestärkt wird. Dies ist in einem digitalen Zeitalter von nicht zu unterschätzender Bedeutung.

Das Ausmaß der Datenverarbeitung ist für den Einzelnen kaum noch überschaubar. Internet, E-Mail, soziale Netzwerke, Kundenkarten, Navigationssysteme und Smartphons, ja selbst Videokameras, gehören in unterschiedlicher Fülle zum Alltag eines jeden Bürgers, ohne dass er ausreichend über die Gefahren und Risiken informiert ist, aber auch ohne dass er seine Schutzmöglichkeiten kennt.

Durch diese Entwicklung der digitalen Welt ist sowohl die Erziehung zur Medienkompetenz in den Schulen als auch die Aufklärung der Bürger über die Risiken der Preisgabe der persönlichen Daten von elementarer Bedeutung.

Wer weiß schon was mit seinen Daten in Facebook oder WkW geschieht? Wer kennt die Zugriffe der Unternehmen auf die Daten der Kundenkarten? Wer wird wann an seinem Standort mit dem Handy geortet? Was macht mein Stromversorger mit den Daten meines digitalen Stromzählers? Wissen wir, dass unsere Fotos im Internet unauslöschbar weltweit für immer zu sehen sind? Wer weiß welche Unternehmen die eigenen persönlichen Daten aus dem Internet zusammentragen und zu welchem Zweck? Kennen Sie die Datenschutzerklärungen Ihrer Vertragspartner? Haben sie

schon mal versucht beim Runterladen von Apps in Erfahrung zu bringen wo Ihre Daten in welchem Umfang gespeichert werden? Können wir überhaupt in einer globalisierten Welt unsere Daten schützen?

Die digitale Welt ist wunderbar. Auch für mich ist sie immer noch phantastisch. Wir können uns eine Welt ohne Internet, Smartphone und Navigationsgerät kaum noch vorstellen und wollen das auch nicht.

Dennoch oder besser gerade deshalb ist Aufklärung notwendig.

Nicht das einzelne Datum ist das Problem für den Bürger, sondern das Risiko der Profilbildung. Die Zusammenführung von vielen leicht zugänglichen Daten bedeutet die Gefahr für das Grundrecht auf informationelle Selbstbestimmung. Hier ein Bewusstsein zu schaffen ist eine wichtige Aufgabe der Datenschutzbeauftragten. Erkennt man die Möglichkeiten und Risiken der digitalen Welt, kann man sich viel eher schützen.

Dieses Bewusstsein ist auch im öffentlichen Bereich immer wieder zu wecken und aufrechtzuerhalten. In Zeiten der Diskussionen zu Vorratsdatenspeicherung, Fluggastdaten, ELENA und Beschäftigtendatenschutz sind die unterschiedlichen Interessen immer wieder am Grundgesetz zu messen.

Das Grundrecht auf informationelle Selbstbestimmung ist ein hohes Gut und erfordert ständige Beachtung auch und gerade wenn es unbequem ist.

Nur wenn es ernst genommen und gelebt wird, verhindern wir den gläsernen Menschen und die Anti-Utopie von George Orwells „1984“ kann nicht Wirklichkeit werden.

Die Ziele meiner Tätigkeit richten sich natürlich nach den gesetzlichen Aufgaben, die das SDSG mir stellt, das heißt, die Einhaltung der Datenschutzgesetze zu überwachten und die öffentlichen Stellen zu beraten.

Neben der Kontrolle, die notwendig ist um Verstöße festzustellen, ist die Beratung der Behörden als präventive Tätigkeit von großer Bedeutung. Dies gilt insbesondere auch bei der Beratung bei der Umsetzung von datenschutzfreundlichen Regelungen. Je sensibler Behörden mit den persönlichen Daten umgehen, je mehr Kenntnis über Datenschutz besteht, desto besser kann der Grundrechtsschutz umgesetzt werden.

Damit besteht die Tätigkeit neben der Kontrolle ganz wesentlich in der vorbeugenden Beratung und Unterrichtung der Verantwortlichen.

Das Ergebnis dieser Tätigkeit für die Jahre 2009 und 2010 können sie in diesem Tätigkeitsbericht nachlesen.

2 Technisch-organisatorischer Datenschutz

2.1 Google Analytics

Nachdem eine stichprobenartige Überprüfung überregionaler gesetzlicher Krankenversicherungen zur Verwendung von Webanalysediensten dazu führte, dass der Bundesbeauftragte für Datenschutz und Informationsfreiheit mehr als 100 gesetzliche Krankenkassen aufgefordert hat, den Einsatz von Analysetools bei Internetangeboten einzustellen, wenn die datenschutzrechtlichen Anforderungen nicht erfüllt werden, haben wir dies zum Anlass genommen, auch die saarländische Landesverwaltung und die in unserem Zuständigkeitsbereich liegenden gesetzlichen Krankenversicherungen zu befragen, ob in den jeweiligen Internetangeboten Webanalysetools eingesetzt werden.

Google Analytics hilft Websitebetreibern, mehr über ihre Nutzer zu erfahren. Google kann mit diesem Analysewerkzeug ein umfassendes Profil von den Besuchern einer Website anlegen. Dies geht soweit, dass, falls ein Nutzer ein anmeldepflichtiges Angebot nutzt, dieses Nutzerprofil sogar personalisiert werden kann.

Technisch basiert das System darauf, dass während des Besuches einer Webseite über Cookies oder Skripte Informationen über die Nutzung und den Nutzer dieser Seite einschließlich der vollständigen IP-Adresse erfasst und an Google weitergeleitet und dort gespeichert werden.

Bei einer IP-Adresse handelt es sich um ein personenbezogenes Datum. Mit Hilfe einer kompletten IP-Adresse ist es möglich, den Standort relativ genau zu lokalisieren. Mit Hilfe der genutzten Cookies, die auf dem Computer des Nutzers platziert werden, ist eine Wiedererkennung der jeweiligen Nutzer gegeben. Weiterhin lässt sich erkennen, über welchen Link der Nutzer auf die Webseite gekommen ist und zu welcher anderen Webseite er sie wiederum verlässt. Durch eine Verknüpfung aller sich ergebenden Einzelinformationen ist es somit möglich, ein recht genaues Nutzerprofil zu erstellen.

Einem Einsatz solcher Analyseprogramme steht prinzipiell das Telemediengesetz (§ 12 ff TMG) entgegen. Lediglich nach einer ausdrücklichen Einwilligung durch den Nutzer in die Verarbeitung seiner personenbezogenen Daten wäre ein Einsatz möglich. Eine informierte Einwilligung des jeweiligen Nutzers ist aus unserer Sicht allerdings nicht möglich, da ein Besucher einer Webseite über den Einsatz von Google Analytics nicht informiert wird und somit im Unklaren über die genaue Verarbeitung seiner persönlichen Daten bleibt.

Ebenso bleiben Webseitenbetreiber im Unklaren darüber, in welcher Art und Weise Google die auf der Webseite erworbenen Daten verarbeitet und die daraus gewonnen Erkenntnisse und Profile nutzt. Der Betreiber einer Webseite ist aber für die datenschutzgerechte Ausgestaltung seines Internetauftritts verantwortlich, auch wenn Dienste Dritter eingebunden werden. Somit ist das Einstellen von Internetseiten unter Nutzung von Google Analytics datenschutzrechtlich nicht zulässig.

Hinzu kommt, dass die Datenverarbeitung nicht in Deutschland stattfindet, sondern eine Datenübermittlung in einen Drittstaat erfolgt. Hierdurch wird eine Überprüfung durch deutsche Datenschützer unmöglich. Eine Zustimmung der Betroffenen in die Datenübermittlung liegt im Allgemeinen ebenfalls nicht vor.

Die Erfassung von Daten durch Google Analytics lässt sich für den Besucher einer Webseite verhindern, indem er das Laden und Ausführen des Google-Analytics-Scripts verhindert. Dies ist möglich durch das Blockieren von JavaScript oder durch ein Unterbinden von Zugriffen auf die Domain google-analytics.com. Ebenso sollte das automatische Löschen von Cookies bei Schließen des genutzten Browser aktiviert sein, um eine Wiedererkennung des Rechners zu verhindern. Zur Realisierung dieser Maßnahmen stehen im Internet mehrere Add-Ons für die verschieden Browser zur Verfügung.

Als Ergebnis unserer Umfrage wurde festgestellt, dass bei der saarländischen Landesverwaltung Google Analytics nicht eingesetzt wird. Lediglich bei einer in unserem Zuständigkeitsbereich liegenden gesetzlichen Krankenkasse wurde Google Analytics eingesetzt, die Nutzung des Dienstes auf unser Betreiben hin aber umgehend eingestellt.

2.2 Soziale Netzwerke

In der heutigen Zeit sind soziale Netzwerke und deren Nutzung nicht mehr wegzudenken und ihre Bedeutung steigt stetig. So sind nach einer Emnid-Umfrage aus dem Jahre 2009 etwa 47% der Bevölkerung Mitglied in einem sozialen Netzwerk, in der Altersgruppe der 14- bis 29-jährigen liegt der Anteil der Mitglieder eines sozialen Netzwerkes sogar bei etwa 89%. Aufgrund dieser enormen Verbreitung und Nutzung sozialer Netzwerke ergibt sich eine neue gesellschaftliche Kultur der Kommunikation. Einerseits dienen soziale Netzwerke ihren Mitgliedern unter anderem dazu Beziehungen aufrecht zu erhalten, wiederzubeleben und Informationen auszutauschen. Andererseits sind soziale Netzwerke gerade daher eine willkommene Informationsquelle über das Persönlichkeitsbild von Netzwerkmitgliedern. So nutzt etwa ein Drittel aller Unternehmen das Internet und die sozialen Netzwerke als Informationsquelle im Rahmen einer Bewerbung.

Der Mehrwert eines sozialen Netzwerks für den einzelnen Nutzer hängt neben einer hohen Teilnehmerzahl und einem hohem Aktivitätslevel insbesondere von der Qualität aber auch von der Quantität preisgebender persönlicher Daten ab. Dies wiederum fördert die Bereitschaft persönliche Inhalte einzustellen, die in den meisten Fällen einem sehr großen Teilnehmerkreis zugänglich sind. Eine Kontrolle der weiteren Nutzung dieser eingestellten Daten durch Dritte entzieht sich jedoch meist den Möglichkeiten des Autors.

Weiterhin ist zu erkennen, dass Mitglieder eines sozialen Netzwerkes meist auch gleichzeitig Mitglieder in mehreren Netzwerken sind. Somit steigt auch der Verbreitungsgrad der persönlichen Nutzerdaten und die Möglichkeit der Verknüpfung dieser Daten.

Ein einzelner persönlicher Beitrag gibt meist nur sehr begrenzt Auskunft über die Persönlichkeit seines Erstellers. Allerdings kann sich durch die Verknüpfbarkeit von Einzelbeiträgen auch über Netzwerkgrenzen hinweg ein umfassendes Persönlichkeitsbild offenbaren. Vor diesem Hintergrund und mit dem Wissen, dass einmal im Internet veröffentlichte Daten nur noch sehr schwer zu kontrollieren sind und auch

auf ewige Zeiten recherchierbar bleiben, muss jeder für sich selbst entscheiden, wie viel er über sich selbst und sein Leben preisgeben will. Daher ist es unbedingt erforderlich, dem Schutz der eigenen Privatsphäre eine noch stärkere Bedeutung bei zu messen. Dies setzt allerdings eine Medienkompetenz und die Kenntnis der Bedeutung und Möglichkeiten der „Privatsphäre-Einstellungen“ in sozialen Netzwerken voraus.

Es zeigt sich meinen Mitarbeitern und mir bei vielen Diskussionen und Informationsveranstaltungen, dass bei den Mitgliedern in sozialen Netzwerken, insbesondere aber bei den Jugendlichen, erheblicher Beratungsbedarf im Hinblick auf den Schutz der Privatsphäre in sozialen Netzwerken besteht.

Eine wesentliche Kernaussage meiner Dienstselle ist hierbei immer, den Umfang der bereitgestellten persönlichen Daten in sozialen Netzwerken auf ein Minimum zu beschränken. Weiterhin kann es oftmals schon hilfreich sein, statt des wirklichen Namens ein Pseudonym oder den sogenannten „Spitznamen“ zu verwenden.

Ein Schwerpunkt unserer Arbeit in den kommenden Jahren wird daher sein, die Kompetenz der Bevölkerung bei den Themen Mediennutzung und Datenschutz zu stärken. Denn nur die Kenntnis der Möglichkeiten wie auch der daraus möglicherweise erwachsenden Gefahren ermöglicht einen sorgsamen Umgang mit sozialen Netzen.

Als Einstieg für junge Menschen in diese Thematik bietet es sich an, diese Themen bereits in der Schule in den Unterricht zu integrieren.

Im Rahmen der bereits im 22. Tätigkeitsbericht (Pkt.14.2) erwähnten Arbeitsgruppe Internet für Schüler wird zurzeit eine neue Präsentation zur Erhöhung der Medienkompetenz saarländischer Schüler entwickelt. Neben einem Grundmodul zum richtigen Verhalten im Internet wird auch ein spezielles Datenschutzmodul für den Unterricht entwickelt, welches die Schüler für ein datenschutzbewusstes Verhalten in sozialen Netzwerken sensibilisieren soll.

3 Justiz

3.1 Datenerhebung im Anhörungsbogen bei Verkehrsordnungswidrigkeiten

Eine Petentin bat mich um datenschutzrechtliche Überprüfung eines Anhörungsbogens zu einer Verkehrsordnungswidrigkeit, der von der für die Ahndung und Verfolgung nahezu aller im Saarland begangenen Verkehrsordnungswidrigkeiten zuständigen Zentralen Bußgeldbehörde verwendet wurde. In diesem Anhörungsbogen wurde die betroffene Person darauf hingewiesen, dass sie in jedem Falle verpflichtet sei, die Fragen zur Person vollständig und richtig zu beantworten. Die Verletzung dieser Pflicht sei nach § 111 Ordnungswidrigkeitengesetz (OwiG) mit Geldbuße bedroht. Abgefragt wurde sodann neben dem Vor- und Zunamen, der Anschrift sowie dem Geburtstag und –ort auch die Telefonnummer der Person.

Mit der Übersendung eines Anhörungsbogens wird einem Betroffenen gemäß § 55 OwiG Gelegenheit gegeben, sich gegen den Verdacht einer Ordnungswidrigkeit zu verteidigen. Für den Betroffenen besteht zwar grundsätzlich keine Aussagepflicht zur Sache, allerdings hat er in jedem Falle die zur Identitätsfeststellung notwendigen Angaben zu seiner Person zu machen. Die Regelung des § 111 OwiG enthält eine abschließende Aufzählung der Pflichtangaben, deren Verweigerung bußgeldbewehrt ist. Die im Anhörungsbogen abgefragte Telefonnummer ist in diesem Katalog jedoch nicht vorgesehen.

Meiner Forderung, bei der Erhebung der Telefonnummer, deren Kenntnis für die Behörde bei eventuellen Rückfragen durchaus dienlich sein kann, auf die Freiwilligkeit der Angabe hinzuweisen, ist die Bußgeldbehörde unverzüglich durch eine Änderung der Ausgestaltung des Anhörungsbogens nachgekommen. Dabei wurde eine deutliche Differenzierung zwischen Pflichtangaben, die zur Identifizierung einer Person erforderlich sind und sonstigen, freiwilligen Angaben vorgenommen und die Bitte um Angabe der Telefonnummer wurde dem Bereich der freiwilligen Angaben zugeordnet.

Des Weiteren wurde meiner weiteren Anregung folgend die missverständliche Formulierung bezüglich der Verpflichtung zur vollständigen und richtigen Beantwortung der Fragen zur Person dahingehend überarbeitet, dass nunmehr erkennbar ist, dass die Pflichtangaben zur Person nur dann ausgefüllt werden müssen, wenn die Personalien bislang noch unbekannt oder aber unvollständig sind.

3.2 Formulare im Bereich der Gerichtskasse

Wegen des Umfangs der Datenerhebung durch die Gerichtskasse im Rahmen eines Antrags auf Stundung von Gerichtskosten hat sich ein Gerichtskostenschuldner an meine Dienststelle gewandt.

Unabhängig von der Höhe der jeweiligen Forderung wurde von der Gerichtskasse für diesen Antrag die Verwendung des Vordrucks für die Erklärung über die persönlichen und wirtschaftlichen Verhältnisse bei Prozesskostenhilfe vorgeschrieben. Hierin sind umfassende Angaben über die Familienverhältnisse, den Beruf, das Vermögen, Einkommen und Lasten des Antragstellers unter Beifügung der entsprechenden Belege zu machen.

Mit Blick auf die Unterschiede zwischen dem Verfahren zur Gewährung von Prozesskostenhilfe und der Beitreibung von Gerichtskosten wurden von meiner Dienststelle gegenüber dem zuständigen Ministerium für Justiz Bedenken an der Verhältnismäßigkeit der Datenerhebung im Rahmen eines Antrages auf Stundung von Gerichtskosten geäußert. Nach den Vorschriften über die Gewährung von Prozesskostenhilfe kann einer Partei, die nach ihren persönlichen und wirtschaftlichen Verhältnissen die Kosten der Prozessführung nicht, nur zum Teil oder nur in Raten aufbringen kann, im Falle einer hinreichenden Erfolgsaussicht der Rechtsverfolgung Prozesskostenhilfe gewährt werden, die dann zumindest teilweise von der Staatskasse in einer zum Zeitpunkt der Kostenübernahmezusage der Höhe nach noch nicht feststehenden Forderung getragen wird. Demgegenüber steht im Verfahren zur Beitreibung von Gerichtskosten zum einen die Forderungshöhe eindeutig fest, zum anderen wird, wenn die sofortige Einziehung der Forderung mit besonderen Härten für

den Zahlungspflichtigen verbunden wäre und der Anspruch durch die Stundung nicht gefährdet wird, zunächst allenfalls eine Ratenvereinbarung getroffen, die jedoch bei Nichteinhaltung weitere Beitreibungsvollstreckungsmaßnahmen nach sich ziehen wird. Eine Kostenübernahmezusage durch die Staatskasse wird also nicht gegeben.

Meinen Bedenken folgend hat sodann die Gerichtskasse ein neues Formular für ihren Bereich erstellt, in dem insbesondere die Angaben der Vermögensverhältnisse von Ehegatten und sonstigen Verwandten gegenüber dem bisher verwendeten Vordruck eingeschränkt worden ist. Zudem hat das Ministerium die Gerichtskasse angewiesen, diesen Vordruck nur dann zu verwenden, wenn die zur Entscheidung erforderlichen Erkenntnisse nicht auf andere Art erlangt werden können. Ebenso solle auch die Forderungshöhe und gegebenenfalls das Verhältnis des Stundungs- bzw. Ratenzahlungsbetrages zur Gesamtforderung Berücksichtigung finden.

3.3 Saarländisches Untersuchungshaftvollzugsgesetz

Infolge der Föderalismusreform aus dem Jahre 2006 ist die Gesetzgebungskompetenz für den Vollzug der Untersuchungshaft auf die Länder übergegangen. Von einer Länderarbeitsgruppe, an der sich insgesamt zwölf Bundesländer beteiligt hatten, wurde sodann ein Musterentwurf für ein Untersuchungshaftvollzugsgesetz erarbeitet, der auch als Grundlage für einen Gesetzentwurf im Saarland diente. Ein Referentenentwurf dieses Gesetzes wurde meiner Dienststelle Ende 2008 zur Stellungnahme zugeleitet. Ungeachtet einiger Regelungen, die unter datenschutzrechtlichen Gesichtspunkten bedenklich erschienen, konnte die Schaffung einer gesetzlichen Grundlage für den Vollzug der Untersuchungshaft grundsätzlich begrüßt werden, da bislang wesentliche grundrechtsrelevante Fragen weitgehend ungeregelt bzw. lediglich in Verwaltungsvorschriften niedergelegt waren.

Der von der Regierung schließlich in den Landtag eingebrachte Gesetzentwurf (Drs. 13/2310) trug einigen der im Rahmen der externen Anhörung dargelegten datenschutzrechtlichen Anregungen und Beanstandungen Rechnung. So wurden insbe-

sondere die geäußerten Zweifel an der hinreichenden Normenklarheit und –bestimmtheit der in dem Referentenentwurf enthaltenen pauschaler Bezugnahme auf die Datenschutzvorschriften des Saarländischen Jugendstrafvollzugsgesetzes dadurch ausgeräumt, dass nunmehr in einem umfassenden Abschnitt des Gesetzes Regelungen über den Datenschutz getroffen werden.

Zu begrüßen ist ebenfalls, dass im parlamentarischen Gesetzgebungsverfahren auch eine Passage innerhalb der Vorschrift betreffend die Ablehnung einer Auskunftserteilung an den Betroffenen über die gespeicherten personenbezogenen Daten gestrichen wurde, wonach auch eine Auskunftserteilung an die Landesbeauftragte für Datenschutz und Informationsfreiheit ausgeschlossen sein sollte, sofern dadurch die Sicherheit des Saarlandes, eines anderen Landes oder des Bundes gefährdet würde. Eine solche Gesetzeslage wäre dem § 28 Abs. 2 Saarländisches Datenschutzgesetz (SDSG) zuwidergelaufen, der gerade für derartige Fälle regelt, dass die Auskunfts- und Einsichtsrechte dann von der Landesbeauftragten für Datenschutz und Informationsfreiheit nur *persönlich* ausgeübt werden dürfen.

In einigen anderen Bereichen wurden jedoch leider die aufgezeigten datenschutzrechtlichen Bedenken und Empfehlungen nicht aufgegriffen:

Soweit das Gesetz vorsieht, dass beim Zugangsgespräch andere Gefangene *in der Regel* nicht anwesend sein dürfen, lässt sich dem Gesetz nicht entnehmen, in welchen Fällen und unter welchen Voraussetzungen ein Ausnahmefall anzunehmen ist. Allein die in der Gesetzesbegründung benannten unüberwindbaren sprachlichen Verständigungsschwierigkeiten genügen angesichts des Umstandes, dass in dem Zugangsgespräch sensible personenbezogene Daten des aufzunehmenden Gefangenen erörtert werden und damit in das Recht auf informationelle Selbstbestimmung eingegriffen wird, nicht dem Gesetzesvorbehalt.

Ebenso kann dem Gesetz hinsichtlich der grundsätzlich erlaubten optischen Überwachung von Besuchen nicht entnommen werden, ob und wie die Betroffenen vorher hierauf hingewiesen werden sollen.

Zu beanstanden ist darüber hinaus, dass die Überwachung des Schriftwechsels des Untersuchungsgefangenen nicht dem Richtervorbehalt unterstellt ist.

Auch hinsichtlich der Aufbewahrung bzw. Löschung der durch erkennungsdienstliche Maßnahmen gewonnenen Daten und Unterlagen ist unseren Empfehlungen nicht gefolgt worden. Insoweit wäre es wünschenswert gewesen, die zur Sicherung des Vollzugs erhobenen Daten nicht auch in kriminalpolizeilichen Sammlungen speichern zu dürfen und bei Vorliegen der gesetzlichen Voraussetzungen die Unterlagen nicht erst auf Antrag, sondern von Amts wegen zu löschen.

Schließlich ist auch zu beanstanden, dass das Untersuchungshaftvollzugsgesetz eine anlassunabhängige Übermittlung von personenbezogenen Daten an das Bundeskriminalamt erlaubt, obwohl das Bundeskriminalamtsgesetz eine anlassunabhängige automatisierte Übermittlung gerade nicht vorsieht.

Ungeachtet dieser Bedenken ist die umfassende Regelung des Vollzugs der Untersuchungshaft durch das am 01. Januar 2010 in Kraft getretene Gesetz auch unter datenschutzrechtlichen Gesichtspunkten insgesamt positiv zu betrachten.

4 Polizei

4.1 Datenblatt zur Vorbereitung auf einen Vermisstenfall

Die Zahl der demenzkranken Menschen steigt nicht zuletzt aufgrund der immer älter werdenden Bevölkerung stetig an. Dies führt auch in einem verstärkten Umfang zu Einsätzen der Polizei, bei denen vermisste demenzkranke Personen gesucht oder hilf- und orientierungslose Personen aufgefunden werden. Um bei der Suche und Identifizierung vermisster Personen zu helfen, haben das Ministerium für Inneres und Europaangelegenheiten und die Polizei des Saarlandes das „Datenblatt zur Vorbereitung auf einen Vermisstenfall“ entwickelt. In diesem Datenblatt können an Demenz erkrankte Personen und ihre Angehörigen, Pfleger oder Betreuer persönliche Informationen festhalten, mit deren Hilfe die Polizei in einem Vermisstenfall eine schnelle und zielgerichtete Suche einleiten kann.

Vor der Einführung dieses Datenblattes wurde meine Dienststelle von dem Ministerium für Inneres und Europaangelegenheiten gebeten, aus datenschutzrechtlicher Sicht zu einem ersten Entwurf Stellung zu nehmen. Das uns übersandte Vermissten-Datenblatt enthielt neben den Personalien eine detaillierte Personenbeschreibung einschließlich Lichtbild sowie die aktuelle und ehemalige Wohnanschriften der vermissten Person. Hinzu kamen Name, Anschrift und Erreichbarkeit von Angehörigen und sonstigen Bezugspersonen einschließlich der Darstellung der Beziehungsverhältnisse zu der Person. In dem Datenblatt enthalten waren des Weiteren Angaben über die Lebensgewohnheiten, zur Mobilität, Kommunikationsfähigkeit, Krankheitsgeschichte sowie den behandelnden Ärzten.

Aus meiner Sicht bestanden keine grundsätzlichen datenschutzrechtlichen Bedenken gegen das Datenblatt, da die abgefragten Daten freiwillig durch die betroffene Person bzw. ihren Betreuer angegeben werden. Aus Gründen der Datensparsamkeit wurde jedoch darum gebeten, die für den Verwendungszweck nicht wesentliche Angabe der Pflegestufe entfallen zu lassen, da diese aufgrund der dezidierten Beschreibung des Gesundheitszustandes für die Suchmaßnahme nicht erforderlich erschien. Diesem Anliegen wurde in der Endfassung des Datenblattes Rechnung ge-

tragen. Ebenso wurde auf meinen Einwand, wonach es sich bei den Daten der Angehörigen und Bezugspersonen um Daten Dritter handele, die grundsätzlich nur mit deren Einwilligung weitergegeben werden dürfen, ein entsprechender Hinweis in dem Datenblatt aufgenommen und diesem ein Formular für eine Einwilligungserklärung beigefügt.

Das Datenblatt steht nunmehr seit Ende 2010 den Pflegeeinrichtungen und pflegenden Angehörigen im Land zur Verfügung.

4.2 Einführung des IT-Verfahrens Führungs- und Lagesystem bei der Führungs- und Lagezentrale der Vollzugspolizei (FLZ)

Das damalige Ministerium für Inneres und Sport übersandte meiner Dienststelle im September 2009 zwecks Freigabe des IT-Verfahrens Führungs- und Lagesystem die entsprechende Verfahrensbeschreibung und die erforderlichen Errichtungsanordnungen zur Wahrnehmung der Beteiligungsrechte nach § 7 Abs. 2 Saarländisches Datenschutzgesetz (SDSG).

Per Erlass des Ministeriums für Inneres und Sport vom 02. Januar 2007 wurde die Führungs- und Lagezentrale (FLZ) eingerichtet. Sie ist neben der Abteilung Bereitschaftspolizei, der Abteilung Dienstleistungen, der Kriminalpolizeiinspektion, den Polizeibezirken sowie der Verkehrspolizeiinspektion eine nachgeordnete Dienststelle der Landespolizeidirektion und gliedert sich in Leitung, Führungsgruppe sowie die ständig besetzten Bereiche Einsatzzentrale und Kommunikationszentrale. Durch die Errichtung der FLZ soll die Effizienz und Effektivität der Führung polizeilicher Lagen, der Koordination von Einsatzmaßnahmen und der Information und Kommunikation im Zusammenhang mit der Bewältigung polizeilicher Einsätze im Saarland nachhaltig gesteigert werden. Als Leitstelle ist die FLZ für die Bearbeitung der innerhalb der Allgemeinen Aufbauorganisation zu bewältigenden Einsätze des täglichen Dienstes zuständig. Sie koordiniert die Maßnahmen bei Sofortlagen bis zur Übernahme durch ein anderes Führungsorgan. Beispielsweise sind landesweit alle Notrufe der Notruf-

nummer 110 und teilweise auch der 112 in der FLZ zur Sicherstellung der Notrufbearbeitung aufgeschaltet. Insbesondere koordiniert die FLZ den Einsatz von Kräften sowie Führungs- und Einsatzmitteln, berät die Kräfte vor Ort und führt im Bedarfsfall weitere Kräfte und Einsatzmittel anderer Dienststellen zu. Darüber hinaus kann sie in zeitlich begrenzten polizeilichen Organisationsformen unterschiedliche Aufgaben wahrnehmen. Mit der Firma Swissphone sollte ein entsprechender Vertrag für die Erstellung eines IT-Systems geschlossen werden.

In einem gemeinsamen Gesprächstermin mit Vertretern des Innenministeriums und der Führungs- und Lagezentrale am 14. Oktober 2009 wurde unsererseits eingefordert, sämtliche Errichtungsanordnungen hinsichtlich der maßgeblichen Rechtsgrundlagen nachzubessern. Insbesondere fehlte es mit Blick auf die Datenübermittlung in Drittländer an den einschlägigen Rechtsgrundlagen, wie beispielsweise § 33 Abs. 2 Saarländisches Polizeigesetz (SpolG) i.V.m. der Verordnung über die Zulassung der Informationsübermittlung von der Polizei an ausländische Polizeibehörden (InfÜVPol) zur Datenübermittlung an die Polizeibehörden in Frankreich und Luxemburg. Es wurde uns mitgeteilt, dass einige Polizeifahrzeuge mit Global Positioning System (GPS) – Sendern ausgestattet werden sollen. Jedoch ist hierdurch keine Routenverfolgung der Einsatzfahrzeuge, sondern lediglich eine momentane Standortwiedergabe möglich. Auch dem Koordinator der FLZ ist die Identität der im Fahrzeug befindlichen Polizeibeamten nicht bekannt, sondern nur die Kennung des Einsatzwagens. Die Erstellung eines Bewegungsprofils der im Dienst befindlichen Polizeibeamten wird dadurch ausgeschlossen. Es wurde zugesichert, die Aufgaben, Zuständigkeiten und Befugnisse der FLZ in einem gesonderten Erlass zu regeln. Meine Dienststelle bat daher zur datenschutzrechtlichen Bewertung neben der überarbeiteten Fassung der Verfahrensbeschreibung sowie den entsprechenden Errichtungsanordnungen, den zuvor erwähnten Erlass, ein Rechte-Rollen-Konzept, ein IT-Sicherheitskonzept und die mit der Firma Swissphone beabsichtigte Vertragsvereinbarung im Entwurf vorzulegen.

Nach eingehender Prüfung dieser Unterlagen war festzustellen, dass in dem mit der Firma Swissphone zu schließenden EVBT-IT Systemvertrag (Ergänzende Vertragsbedingungen für die Erstellung eines IT-Systems) zwar weitere Pflichten des Auftragsnehmers festgelegt wurden, nicht jedoch solche, die zum einen die Pflichten zur Wahrung des Datengeheimnisses nach § 6 SDSG und zum anderen die Pflichten im

Rahmen der Auftragsdatenverarbeitung gemäß § 5 Abs. 3 und 4 SDSG betreffen. Die sich aus den §§ 5 und 6 SDSG ergebenden Pflichten für den Auftragsnehmer sind bei einer etwaigen Leistungserbringung durch Subunternehmer gleichfalls auf diese zu übertragen. Meine Dienststelle hat insoweit konkrete Vorschläge für die Überarbeitung des Systemvertrages unterbreitet.

Gemäß § 31 Abs. 5 SDSG dürfen Daten von Beschäftigten im Rahmen der Durchführung von technischen und organisatorischen Maßnahmen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden. Es wurde daher unsererseits gebeten, in den Erlass über die Aufgaben, Zuständigkeiten und Befugnisse der Führungs- und Lagezentrale der Vollzugspolizei des Saarlandes eine entsprechende Klausel aufzunehmen.

Die Verfahrensbeschreibung wurde, wie von meiner Dienststelle erbeten, ausführlich überarbeitet und die speziellen Rechtsgrundlagen auch nach den jeweiligen EWG-Verordnungen genau dargelegt. Ebenso wurden auch unsere Anregungen hinsichtlich der Vertragsausgestaltung aufgegriffen. Ferner wurde mitgeteilt, dass das jetzige Ministerium für Inneres und Europaangelegenheiten die Kautelen für die Nutzung der angesprochenen GPS-Daten in einer eigenen Dienstvereinbarung zwischen dem Ministerium und dem Polizeihauptpersonalrat regelt und so § 31 Abs. 5 SDSG Rechnung trägt.

Mithin bestanden aus datenschutzrechtlicher Sicht nunmehr gegen die Einführung des IT-Verfahrens „Führungs- und Lagesystem“ keine Bedenken.

4.3 Fallbearbeitungssystem KRISTAL – Kriminalpolizeiliches System zur täterorientierten Analyse und Lagedarstellung

Mit Schreiben vom 03. August 2009 teilte das Landeskriminalamt Saarland mit, dass es beabsichtige, das Kriminalpolizeiliche System zur täter- und tatorientierten Analyse und Lagedarstellung (KRISTAL) einzuführen und lud daher zu einer ersten Informationsveranstaltung ein.

Das Fallbearbeitungssystem dient der Erforschung, Ermittlung und Aufklärung von Verbrechen, Vergehen, die serienmäßig, bandenmäßig, gewerbsmäßig oder organisiert im Saarland begangen werden, und Straftaten von erheblicher Bedeutung sowie Straftaten im Bereich der politisch motivierten Kriminalität. Es unterstützt die Polizei im Rahmen vorbeugender Verbrechensbekämpfung sowie bei der Durchführung spurenintensiver Ermittlungen und bietet so auch die Möglichkeit, Tatzusammenhänge zeitnah zu erkennen und darzustellen.

Oftmals wird bei der Einführung neuer technischer Anwendungen die Frage aufgeworfen, ob die Testverfahren bereits mit Echtdaten durchgeführt werden dürfen. Der Arbeitkreis technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit dieser Fragestellung auseinander gesetzt und eine entsprechende Orientierungshilfe „Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb“ erarbeitet, welche auch in unserem Internetangebot als Download zur Verfügung steht. Hiernach dürfen in einem Test keine personenbezogenen Daten verarbeitet und auch nicht aus anderen Produktivsystemen übernommen werden. Echtdaten sind vor ihrer Übernahme in das Testverfahren zu anonymisieren. Dem Wunsch des Landeskriminalamtes, im Rahmen der Testverfahren mit Echtdaten zu operieren, konnte daher nicht entsprochen werden.

Es wurde eine eigene saarländische Datenbank für die Phänomenbereiche „Organisierte Kriminalität“ (OK) und „Politisch Motivierte Kriminalität“ (PMK) eingerichtet, die mit anderen saarländischen polizeilichen Datenbanken verbunden ist. Dies geschieht über eine sogenannte bidirektionale Schnittstelle, die den Informationsfluss von der

Quelldatei zu einer neuen Datei und umgekehrt ermöglicht. Weitere Schnittstellen zu den Datenbanken, Poladis.net, Analyst-Notebook und Info-Zoom, wurden als Tools integriert. Datenschutzrechtlich von Bedeutung ist dabei, dass verschiedenste Informationen, wie Texte, Bilder und Lebenssachverhalte zügig recherchiert und verknüpft werden können. Auch die grafische Darstellung komplexer Sachverhalte steht systemseitig zur Verfügung. Die Schnittstelle zum Telekommunikations-Modul Digibase, in welchem die für die Telekommunikationsüberwachung erheblichen Daten gespeichert werden, ermöglicht lediglich die Anzeige der Telefonnummern der überwachten Person sowie der Gesprächspartner und der Verkehrsdaten zu den Telefonaten. Tondokumente sind hierbei nicht integriert.

Die Verfahren in den Phänomenbereichen OK und PMK sind intern voneinander abgeschottet. Ein Mitarbeiter eines Bereiches kann beispielsweise bei Eingabe eines Namens lediglich die weiteren Erkenntnisse zu diesem Namen in seinem Bereich und einen eventuellen Hinweis auf weitergehende Erkenntnisse in einem anderen Bereich zu diesem Namen sehen. Die konkreten inhaltlichen Erkenntnisse des anderen Bereiches kann er nur erhalten, wenn über die Fachadministration die Zugriffsberechtigung nach Beantragung mit Zweckangabe für den konkreten Fall beim anderen Bereich und auch nur für die Dauer des konkreten Verfahrens vergeben wurde. Hierbei erfolgt jeweils eine Einzelfallprüfung des Fachbereiches, deren Ergebnis auch zu dokumentieren ist. Durch die Fachadministration wurde unter Beteiligung des behördlichen Datenschutzbeauftragten ein umfassendes Fachkonzept „Rollen und Berechtigungen„ erstellt, welches auch angesichts einer Versionsumstellung unter Berücksichtigung datenschutzrechtlicher Belange überarbeitet und fortgeschrieben wurde.

Die Handhabung der Aussonderungsprüffristen begegnete jedoch datenschutzrechtlichen Bedenken, da systemseitig eine automatisierte Löschung nach Ablauf der Aussonderungsfristen nicht erfolgt. Die Fachadministration druckt zur Prüfung der Aussonderungsfristen monatlich eine entsprechende Liste aus. Die Löschaufträge werden sodann von dort an die einzelnen Dienststellen verteilt. Auf Rückfrage wurde mitgeteilt, dass seitens der Fachadministration auch die tatsächliche, umgehende Löschung durch die Dienstellen überwacht wird. Besonderes Augenmerk wurde hierauf auch in der Pilotphase gerichtet. Unsererseits wurde ausdrücklich darauf hinge-

wiesen, dass programmseitig auf eine automatisierte Löschung hinzuwirken ist. Für die Übergangsphase haben wir empfohlen, bei Fristüberschreitung zumindest die Fertigung von automatisierten „Warnlisten“ zu konzipieren, da eine bloße manuelle Kontrolle ohne technische Unterstützung durch die Sachbearbeitung oder die Fachaufsicht als datenschutzrechtlich nicht ausreichend eingestuft wird. Im weiteren Verlauf der Besprechungen erklärte das Landeskriminalamt, dass es in länderübergreifenden Besprechungsgremien der Polizei mit den Teilnehmern die aus datenschutzrechtlicher Sicht anzustrebende systemimmanente automatisierte Löschung thematisieren wird. Die Software rsCASE der Firma Rola wird für das Fallbearbeitungssystem KRISTAL von Rheinland-Pfalz und dem Saarland genutzt. Das Saarland hat basierend auf einem Kooperationsvertrag mit Rheinland-Pfalz nur eine bestimmte Anzahl von Arbeitsplatzlizenzen. Auch der Landesbeauftragte für den Datenschutz Rheinland-Pfalz hat in seinem 21. Tätigkeitsbericht die Handhabung der Aussonderungsprüffristen durch die rheinlandpfälzische Polizei problematisiert und aus datenschutzrechtlicher Sicht die automatisierte Löschung favorisiert. Nach derzeitigem Kenntnisstand haben sowohl die Polizei Berlin als auch die Bundespolizei und das Bundeskriminalamt die systemseitige automatisierte Löschung bereits technisch umgesetzt.

Die frühzeitige Beteiligung meiner Dienststelle bereits im Testverfahren hat sich aus hiesiger Sicht bewährt, so dass bei der Umsetzung des Fallbearbeitungssystems KRISTAL für die saarländische Polizei die datenschutzrechtlichen Belange hinreichend berücksichtigt wurden. Mithin konnte am 15. Oktober 2009 die erforderliche Freigabe des Verfahrens nach § 7 Abs. 2 SDSG durch das damalige Ministerium für Inneres und Sport erfolgen.

4.4 Rahmenrichtlinie zum Schutz der Bevölkerung vor rückfallgefährdeten Sexualstraftätern im Saarland

Im Oktober 2010 wurde seitens des Ministeriums für Inneres und Europaangelegenheiten angezeigt, dass es in Zusammenarbeit mit dem Ministerium der Justiz eine gemeinsame Rahmenrichtlinie zum Schutz der Bevölkerung vor rückfallgefährdeten Sexualstraftätern im Saarland entwickelt habe. Hintergrund war die Entscheidung des Europäischen Gerichthofes für Menschenrechte vom 17. Dezember 2009, wonach Maßnahmen der nachträglichen Sicherungsverwahrung mit der Europäischen Menschenrechtskonvention nicht vereinbar sind, da die Sicherungsverwahrung als Strafe anzusehen ist und mithin gegen das Rückwirkungsverbot der Konvention verstößt. Weil in der Folge Menschen aus der Sicherungsverwahrung entlassen werden müssen, die als gefährlich gelten, wurde die Erforderlichkeit gesehen, im Rahmen der Gefahrenabwehr entsprechende polizeiliche Maßnahmen durchzuführen. Mit der vorgenannten Rahmenrichtlinie soll daher die Zusammenarbeit von Vollstreckungsbehörde, Straf- oder Maßregelvollzug und Führungsaufsichtsstelle geregelt und der erforderliche Informationsaustausch sichergestellt werden. Meine Dienststelle wurde gebeten zu prüfen, ob aus datenschutzrechtlicher Sicht Einwände oder Bedenken gegen das zuvor beschriebene Vorhaben bestehen.

Zweifelsfrei ist dem Schutz der Bevölkerung und insbesondere dem Schutz von Kindern vor sexuellem Missbrauch mit Blick auf eine durchzuführende Abwägung hochrangiger Rechtsgüter ein sehr hoher Stellenwert beizumessen, weshalb die Schaffung einer Regelung zur Zusammenarbeit der maßgeblichen Stellen als solche grundsätzlich keinen datenschutzrechtlichen Bedenken begegnet.

Nach eingehender Prüfung der Entwurfsfassung der Rahmenrichtlinie bleibt jedoch festzustellen, dass eine Richtlinie Rechtsnormen im materiellen Sinn erfordert, die die Datenübermittlungen zwischen den beteiligten Stellen zulassen. Unter diesem Aspekt ergaben sich daher insoweit datenschutzrechtliche Bedenken, als in dem vorliegenden Entwurf der Richtlinie für einzelne Stellen verpflichtende Datenübermittlungen festgelegt wurden ohne die hierfür einschlägigen Rechtsgrundlagen zu benennen.

Zur konzeptionellen Entwicklung und Abstimmung von Überwachungsmaßnahmen können ressortübergreifende bedarfsorientierte Fallkonferenzen stattfinden, welche von Polizei, Staatsanwaltschaft, Führungsaufsicht und Justizvollzugsanstalt eigenverantwortlich initiiert werden können. Wegen der möglichen Beteiligung von Vertretern weiterer Behörden, Institutionen oder Fachkräften war daher ebenso einzufordern, dass die Voraussetzungen der jeweiligen Datenübermittlungsvorschriften auch bei etwaigen Fallkonferenzen zu beachten sind.

Im November 2010 wurde sodann eine überarbeitete Fassung der Rahmenrichtlinie vorgelegt, in der den Anregungen meiner Dienststelle fast vollumfänglich gefolgt wurde und zur Klarstellung die einschlägigen Rechtsgrundlagen eingearbeitet waren. Lediglich hinsichtlich der vorgesehenen unmittelbaren Unterrichtungspflicht der Bewährungshelfer an die Polizeibehörden konnte kein Konsens erzielt werden, da hierfür keine Rechtsgrundlage besteht. Wie mir das Innenministerium mitteilte, beschäftigt sich deshalb auch eine Arbeitsgruppe des Strafrechtsausschusses der Justizministerkonferenz mit der Angelegenheit und ist bemüht eine entsprechende Rechtsgrundlage zu schaffen. Nach hiesiger Meinung stellt § 34 Strafgesetzbuch (StGB) -Rechtfertigender Notstand- zwar einen Rechtfertigungsgrund, aber nicht die für eine Datenübermittlung der Bewährungshilfe an die Polizei erforderliche Rechtsgrundlage dar. Aus datenschutzrechtlicher Sicht ist daher die Schaffung einer Rechtsgrundlage für die Unterrichtung der Polizeibehörden durch die Bewährungshilfe anzustreben.

Zwischenzeitlich liegt mir ein Gesetzentwurf zur Stärkung der Bewährungshilfe und Straffälligenarbeit, der von der Arbeitsgruppe des Strafrechtsausschusses der Justizministerkonferenz erarbeitet wurde, zur Kenntnis vor. Dieser Gesetzesentwurf soll im achten Buch der Strafprozessordnung (StPO) Niederschlag finden und dem Bewährungshelfer nunmehr in bestimmten Konstellationen die Möglichkeit eröffnen, personenbezogene Daten unmittelbar an die Polizei und an die Vollstreckungsbehörden sowie Einrichtungen des Justiz- und Maßregelvollzuges zu übermitteln.

5 Steuern

5.1 Probleme beim Druck von Steuerbescheiden

Im Jahr 2009 erreichte uns eine Eingabe eines Steuerpflichtigen, der folgendes datenschutzrechtliche Problem schilderte: Im Adressfeld des noch verschlossenen Fensterkuverts waren zwar seitenverkehrt, aber dennoch deutlich erkennbar, das Geburtsdatum seines Kindes, die Einkünfte des Steuerpflichtigen und die Einkünfte des Ehegatten zu lesen. Die Nachfrage beim zuständigen Finanzamt ergab, dass man im Landesamt für Zentrale Dienste (ZDV-Saar), bei dem der Druck der Steuerbescheide erfolgt, bereits über diesen Missstand informiert sei und an einer Lösung arbeite. Das verwendete Papier hatte nicht die notwendige Lichtundurchlässigkeit um ein Durchscheinen der auf der Rückseite aufgedruckten Zeichen zu verhindern.

Zuerst wollte man das Problem durch die Verwendung von Kuverts mit einem sogenannten Zahlenmeer lösen. Es handelt sich hierbei um ein Druckmuster aus dicht nebeneinander stehenden Ziffern oder Buchstaben auf der Innenseite eines Briefumschlages. Allerdings ergab eine Prüfung durch das hiesige Ministerium der Finanzen, dass durch diese Maßnahme nicht der gewünschte Erfolg erzielt werden konnte.

Danach wurden mehrere Papierlieferanten gebeten, ein schwereres und damit lichtundurchlässigeres Papier für Probedrucke zur Verfügung zu stellen. Dabei war zu beachten, dass das Papiergewicht nicht zu sehr stieg um einerseits eine Umrüstung der Kuvertiermaschine möglichst zu vermeiden und um die Gewichtsgrenzen für das Briefporto nicht zu überschreiten.

Nach mehrwöchigem Test konnte eine geeignete Papiersorte gefunden werden und im Rahmen einer Ausschreibung bestellt werden. Das Problem war damit gelöst und auf eine Beanstandung konnte verzichtet werden.

6 Wahlen

6.1 Einsicht in Wählerverzeichnisse

In Wählerverzeichnisse sind alle Personen eingetragen, die wahlberechtigt sind. Gemäß § 12 Landtagswahlgesetz (LWG) führt der Gemeindewahlleiter für jeden Wahlbezirk ein Verzeichnis der Wahlberechtigten. Jeder Wahlberechtigte hat das Recht, an den Werktagen vom 20. bis zum 16. Tag vor der Wahl während der allgemeinen Öffnungszeiten die Richtigkeit oder Vollständigkeit der zu seiner Person im Wählerverzeichnis eingetragenen Daten zu überprüfen. Nach § 11 Landeswahlordnung (LWO) legt der Gemeindewahlleiter für jeden allgemeinen Wahlbezirk ein Verzeichnis aller am Wahltag Wahlberechtigten an, welches nach Familiennamen und Vornamen, Geburtsdatum und Wohnung geführt wird. Die §§ 14 ff LWO beschreiben insofern Bekanntmachung, Einsichtnahme sowie Einspruchsberechtigung und Abschluss des Wählerverzeichnisses. Zur genauen Personifizierung von Personen, bei denen gegebenenfalls Namensgleichheit besteht oder die nicht im Besitz einer Wahlbenachrichtigungskarte sind, muss durch Vorlage eines Personalausweises oder Reisepasses am Wahltag im Wahllokal anhand des Wählerverzeichnisses überprüft werden, ob diese Personen in dem jeweiligen Wahlbezirk wahlberechtigt sind. Diese Überprüfung erfolgt durch den Wahlvorstand des jeweiligen Wahlbezirkes.

Im August 2009 hat sich ein Petent an meine Dienststelle gewandt und vorgetragen, dass er als Wahlberechtigter am Wahltage in dem von ihm aufgesuchten Wahllokal in die Wählerverzeichnisse hätte Einsicht nehmen können. Daraufhin wurde die betreffende Kommune um Stellungnahme gebeten. Der Bürgermeister dieser Kommune erklärte hierauf, dass der zuständige Wahlvorsteher auf Nachfrage die problemlose Einsicht auf personenbezogenen Daten, hier in das Wählerverzeichnis, so nicht bestätigt habe. Vielmehr habe ein Wählerverzeichnis beim Schriftführer zur Registrierung der Stimmabgabe vor Einwurf des Stimmzettels in die Wahlurne und ein zweites Wählerverzeichnis beim Wahlvorstand zur ordnungsgemäßen und rechtmäßigen Stimmzettelausgabe an die Wahlberechtigten vorgelegen. Die zuvor genannten Wählerverzeichnisse haben seitenverkehrt gelegen, so dass eine eigenmächtige Einsichtnahme durch die Wahlberechtigten nicht möglich gewesen sei.

Dennoch wurde durch den Bürgermeister eine Anordnung unter Beteiligung des dortigen behördlichen Datenschutzbeauftragten getroffen, bei künftigen Wahlen den Abstand zwischen den Wahlberechtigten und den Wählerverzeichnissen angemessen zu erhöhen, um eine wenn auch zufällige Einsicht in Wählerverzeichnisse definitiv auszuschließen.

Mit Blick auf diese durch den Bürgermeister bereits angeordneten Maßnahmen zur Verbesserung datenschutzrechtlicher Belange wurde darüber hinaus von meinen Mitarbeitern empfohlen, bei der Vorbereitung anstehender Wahlen die Wahlvorstände nochmals für datenschutzrechtliche Aspekte zu sensibilisieren.

6.2 Erstwählerbriefe an Grundschüler

Gemäß § 35 Abs. 1 des Meldegesetzes (MG) darf die Meldebehörde sechs Monate vor einer Wahl den Parteien Auskunft aus dem Melderegister über die Namen und Anschriften von Gruppen von Wahlberechtigten erteilen, wobei hinsichtlich der Zusammensetzung der der Auskunft unterliegenden Gruppe auf das Lebensalter abgestellt wird. Das jeweilige Geburtsdatum darf den Parteien jedoch nicht übermittelt werden. Eine Auskunft wird darüber hinaus nur erteilt, wenn der Wahlberechtigte der Weitergabe seiner Daten nicht widersprochen hat.

Aufgrund einer Pressemitteilung ist meine Dienststelle darauf aufmerksam geworden, dass in einer saarländischen Stadt auch 1.600 Grundschüler Wahlwerbebriefe einer Partei erhalten haben. Daraufhin wurde zunächst der Oberbürgermeister um Aufklärung gebeten, der diese Datenübermittlung mit einer technischen Panne erklärte und darauf hinwies, dass seitens der Stadt unmittelbar nach Kenntniserlangung von dieser Datenpanne ein Entschuldigungsschreiben an die Erziehungsberechtigten der betroffenen Grundschüler versandt worden sei. Hierin sei auch ausdrücklich darauf hingewiesen worden, dass das Verschulden alleine bei der Stadt gelegen habe und die Partei, die die Erstwählerbriefe verschickt habe, keinerlei Mitverantwortung trage. Bei einem Kontrollbesuch vor Ort wurde uns sodann erläutert,

dass die Datenübermittlung auf einer fehlerhaften Berechnung der erforderlichen Geburtsdaten beruhte. Um solche Fehlauskünfte zukünftig zu vermeiden, griff die Stadtverwaltung unseren Vorschlag auf, bei derartigen Datenübermittlungen zukünftig das Vier-Augen-Prinzip anzuwenden.

6.3 Wahl eines Jugendrates via Internet

Anfang 2010 konnte meine Dienststelle der Presse entnehmen, dass die für den März des Jahres geplante Wahl eines Jugendrates in einer saarländischen Kreisstadt erstmals und ausschließlich über das Internet erfolgen solle. Daraufhin wandte sich mein Amtsvorgänger an den Oberbürgermeister dieser Stadt und wies darauf hin, dass es sich bei der beabsichtigten Internetwahl um den erstmaligen Einsatz eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, handele, vor dessen Freigabe gemäß § 7 Abs. 2 SDSG der Landesbeauftragte für Datenschutz zu hören sei. Des Weiteren wurde die Stadt gebeten, das Konzept des beabsichtigten Wahlverfahrens insbesondere unter datenschutzrechtlichen Gesichtspunkten darzulegen.

In ihrem Antwortschreiben vertrat die Kommune die Auffassung, es sei nicht von einer Verarbeitung personenbezogener Daten in einem automatisierten Verfahren auszugehen, da im Zusammenhang mit der Wahl personenbezogene Daten weder bei der Stadt gespeichert noch an einen Dritten zur weiteren Verarbeitung übermittelt würden. Im Übrigen wurde zu dem beabsichtigten Wahlverfahren ausgeführt, dass im Vorfeld alle wahlberechtigten Jugendlichen und jungen Erwachsenen jeweils unter Mitteilung eines sechsstelligen Codes (TAN) angeschrieben würden. Diese TAN´s würden der Stadtverwaltung losgelöst von den Namen der Wähler von einem Dienstleister zur Verfügung gestellt. Während der Wahlzeit gelangten die Wähler dann über die Homepage der Kreisstadt auf ein auf dem Webserver dieses Dienstleisters installiertes Online-Wahlmodul. Dort könne sich der Wähler mit der TAN einloggen und seine Stimme abgeben. Jede TAN sei nach der Benutzung verbraucht und könne nicht wieder verwendet werden. Eine Verbindung zwischen TAN

und Adressaten gebe es nicht. Die Vergabe der TAN erfolge nach dem Zufallsprinzip. Eine Registrierung, Dokumentation oder Speicherung, welchem Wähler welche TAN zugeordnet werde, erfolge nicht. Rückschlüsse von TAN-Nummern auf den Wähler seien daher nicht möglich.

Da nach diesen Erläuterungen davon auszugehen war, dass weder von Seiten der Kommune noch von Seiten des Dienstleisters eine Zuordnung zwischen Stimmabgabe des Wählers und Personenbezug erfolgen konnte, gab es aus datenschutzrechtlicher Sicht auch keine Bedenken gegen die Durchführung der Wahl des Jugendrates unter Einsatz des dargelegten Verfahrens. Allerdings war die Kommune darauf hinzuweisen, dass auch schon die Erhebung der Daten der wahlberechtigten Jugendlichen und jungen Erwachsenen aus dem Melderegister und die Zuordnung einer TAN eine Datenverarbeitung im Sinne des § 7 Abs. 2 SDSG darstellt, welche durch den Einsatz eines gesteuerten technischen Verfahrens selbständig abläuft und damit als automatisiert anzusehen ist. Daher ist vor einer Freigabe eines solchen Verfahrens ebenso wie bei wesentlichen Änderungen des Verfahrens die Landesbeauftragte für Datenschutz zu hören.

7 Meldewesen

7.1 Änderung der Meldedaten-Übermittlungsverordnung

Im August 2009 übersandte mir das damalige Ministerium für Inneres und Sport den Entwurf einer Verordnung zur Änderung der Meldedaten-Übermittlungsverordnung mit der Gelegenheit zur Stellungnahme. Mit dieser Verordnung sollte die im Jahre 2007 aktualisierte Verordnung über die Zulassung der regelmäßigen Übermittlung von Daten aus dem Melderegister an Behörden und sonstige öffentliche Stellen den Anforderungen der schnell fortschreitenden technischen Entwicklung im Bereich des eGovernments angepasst werden. Insbesondere sollte auch die Zahl derjenigen Behörden erhöht werden, welche die vom Melderecht grundsätzlich zugelassene Melderegisterauskunft künftig elektronisch abwickeln können. Die Änderungsverordnung enthielt Regelungen hinsichtlich der Zuständigkeit der Vermittlungsstelle des Saarlandes und der Datenübermittlung an für Rettungsdienstleistungen zuständige Stellen. Zusätzlich aufgenommen wurde die Regelung der regelmäßigen Übermittlung von Daten aus dem Melderegister in automatisierter Form an weitere Behörden wie z.B. die Standesämter, die Ausländerbehörde, die Einbürgerungsbehörde und die Rettungsleitstelle des Saarlandes.

In einer ersten Stellungnahme meiner Dienststelle wurde zunächst die beabsichtigte Neuregelung der Abfragebefugnis für Sicherheitsbehörden beanstandet, da hierunter nunmehr auch die jeweils zuständigen Finanzbehörden im Rahmen der Steuerfahndung fallen sollten. Da den Finanzbehörden keine Befugnisse zur Abwehr von Gefahren für die öffentliche Sicherheit im Sinne der in der Begründung der Verordnung geschilderten Gefahrenlagen, wie Feuer, Bombendrohungen und Geiselnahme, zukommt, ließ sich eine Ausweitung der Abrufmöglichkeiten für die Finanzbehörden unter diesem Aspekt nicht rechtfertigen.

Nachdem weitere Behörden und sonstige öffentliche Stellen ihren Bedarf an der Aufnahme in die Meldedaten-Übermittlungsverordnung angezeigt hatten, wurde der Dienststelle im Dezember 2009 ein überarbeiteter Verordnungsentwurf durch das nunmehrige Ministerium für Inneres und Europaangelegenheiten zur datenschutz-

rechtlichen Stellungnahme übersandt. Den bereits geäußerten Bedenken bezüglich der den Finanzbehörden eingeräumten Abrufbefugnis war hierin noch nicht Rechnung getragen. Hinsichtlich der geplanten weiteren Ausweitung des automatisierten Abrufverfahrens für das Statistische Amt, den Entsorgungsverband Saar, die Industrie- und Handelskammer und die Handwerkskammer sowie für saarländische Notare war aus datenschutzrechtlicher Sicht zu kritisieren, dass nicht dargelegt worden ist, aus welchen Gründen für diese Stellen eine einfache Melderegisterauskunft nicht ausreichend sein sollte.

In einer nachfolgenden Besprechung mit Vertretern des Ministeriums konnte schließlich bis auf einen Punkt Konsens hinsichtlich der bislang geäußerten datenschutzrechtlichen Bedenken erzielt werden. So wurde in der zur Auslegung der Verordnung heranzuziehenden Begründung klargestellt, dass die besonderen Steuerbehörden, also die Steuerfahndung und die gemeinsamen Buß- und Strafsachenstelle, entsprechend der Regelung des § 31 Abs. 3 des Meldegesetzes den Polizeidienststellen im Rahmen der Aufgabenzuweisung zur Strafverfolgung und der Staatsanwaltschaft gleichgestellt sind, so dass ihnen insoweit auch die Möglichkeit zum elektronischen Abruf eingeräumt werden kann. Ebenso wurden in die Verordnungsbegründung erläuternde Ausführungen zur jeweiligen Erforderlichkeit der in dem ergänzten Entwurf hinzugekommenen Abrufbefugnisse für weitere öffentliche Stellen aufgenommen. Lediglich unserer Forderung, bei der Befugnis zur Abfrage des Geburtsdatums für die Durchführung des Mikrozensus die Zugriffsmöglichkeit entsprechend den Vorgaben des Mikrozensusgesetzes 2005 auf das Geburtsjahr und den Geburtsmonat zu beschränken und einen Zugriff auf den Tag der Geburt nicht zuzulassen, konnte aus technischen Gründen nicht nachgekommen werden.

Die geänderte Meldedatenübermittlungsverordnung wurde am 20. Mai 2010 im Amtsblatt des Saarlandes veröffentlicht und ist am Tag nach der Veröffentlichung in Kraft getreten.

8 Kommunales

8.1 Erfordernis einer Dienstanweisung für den Einsatz von Finanzsoftware in Kommunen

Im September 2009 zeigte mir eine Kommune durch Übersendung der hierfür erforderlichen Verfahrensbeschreibung an, dass sie beabsichtige, ihr Finanzmanagement künftig mit Hilfe der Finanzsoftware FINANZ+ der Firma DATA-PLAN GmbH zu betreiben. Im konkreten Fall sollten hierdurch Forderungen gegenüber Zahlungspflichtigen und Verbindlichkeiten gegenüber Zahlungsempfängern verwaltet werden sowie Rechnungen, Bescheide und Mahnungen erstellt werden.

Gemäß § 28 Abs. 1 der Kommunalhaushaltsverordnung (KommHVO) des Saarlandes ist von der Bürgermeisterin oder dem Bürgermeister, um die ordnungsgemäße Erledigung der Aufgaben der Finanzbuchhaltung unter besonderer Berücksichtigung des Umgangs mit Zahlungsmitteln sowie der Verwahrung und Verwaltung von Wertgegenständen sicherzustellen, eine Dienstanweisung unter Berücksichtigung der örtlichen Gegebenheiten zu erlassen. Diese Dienstanweisung muss beim Einsatz von automatisierter Datenverarbeitung in der Finanzbuchhaltung die nach § 28 Abs. 2 Nummern 2.1 bis 2.7 KommHVO bestimmten Festlegungen enthalten.

Auf Nachfrage meiner Dienststelle wurde mitgeteilt, dass eine solche Dienstanweisung nicht bestehe. Die betreffende Kommune erkannte aber mit Blick auf § 28 KommHVO die Notwendigkeit einer solchen Regelung und legte alsbald einen ersten Entwurf einer Dienstanweisung für die Finanzbuchhaltung meiner Dienststelle zur Abstimmung vor. Nachdem im Abstimmungsverfahren auch meiner Empfehlung, im Kapitel „Datenschutz“ der Dienstanweisung auf die Vorschriften des Saarländischen Datenschutzgesetzes (SDSG) hinzuweisen, gefolgt wurde, bestanden nunmehr aus datenschutzrechtlicher Sicht keine Bedenken gegen den Einsatz dieser Finanzsoftware.

8.2 Fragebogen zur Bedarfsermittlung Internetversorgung

Im Juli 2010 hat sich ein Petent an meine Dienststelle gewandt und mit der Bitte um datenschutzrechtliche Überprüfung einen Fragebogen zur Bedarfsermittlung der Internetversorgung vorgelegt, welchen eine Kommune dem Amtlichen Bekanntmachungsblatt beigefügt hatte.

Der Zweckverband elektronische Verwaltung für saarländische Kommunen (eGo-Saar) hat zur Breitbandbedarfserhebung in der Gemeinde einen Musterfragebogen nebst Erläuterungen zum Zweck der Datenerhebung und der späteren Datenverwendung durch die Gemeinde entwickelt. Hinsichtlich der Erhebung von personenbezogenen Daten, wie Name und Adresse, wurde ausdrücklich auch auf die Möglichkeit einer anonymisierten Rückmeldung verwiesen.

Weitere Recherchen meiner Dienststelle ergaben, dass der von der Kommune selbst entworfene Fragebogen auch in deren Internetangebot mit der Möglichkeit des Online-Ausfüllens eingestellt war. Der im Internetauftritt zu lesende Erläuterungstext gab jedoch keinerlei Hinweise auf die weitere Datenverwendung. Darüber hinaus enthielt der in Rede stehende Fragebogen gegenüber dem Musterfragebogen des eGo-Saar keinen Hinweis auf die Möglichkeit einer anonymisierten Rückmeldung, jedoch zusätzliche Fragestellungen insbesondere zur Nutzung des Internets und dem Surf-Verhalten der Ausfüllenden.

Ich habe daher die betreffende Kommune um Stellungnahme gebeten und erhielt umgehend Nachricht, dass aufgrund eines Büroversehens dem Amtlichen Bekanntmachungsblatt außer dem Fragebogen leider kein weiterer aufklärender Erläuterungstext beigefügt war. Aufgrund meiner Bitte um Stellungnahme wurde die weitere Vorgehensweise durch den zuständigen Bürgermeister zunächst gestoppt und gleichzeitig angezeigt, dass nunmehr der vom eGo-Saar entwickelte, mit meiner Dienststelle abgestimmte Fragebogen sowie die entsprechenden Erläuterungen zum Zweck der Datenerhebung und der weiteren Verwendung zur Bedarfsermittlung der Internetversorgung eingesetzt werden sollen. Es wurde ferner versichert, dass die

Daten anonym behandelt werden und nur für den erhobenen Zweck ausgewertet werden. Nach dieser internen Auswertung werden die Daten gelöscht bzw. vernichtet.

Aufgrund des von diesem Zeitpunkt an angestrebten Verfahrens ergaben sich aus datenschutzrechtlicher Sicht keinen Bedenken mehr, worüber die betreffende Kommune im August 2010 in Kenntnis gesetzt wurde.

8.3 Landesweite Erhebung zur Videoüberwachung

Durch die bundesweit zunehmende Tendenz, öffentliche Plätze, Gebäude und Einrichtungen mit Videokameras überwachen zu wollen, sah sich mein Amtsvorgänger veranlasst, im Saarland eine Erhebung über die Videoüberwachung im öffentlichen Bereich vorzunehmen, wie diese auch in anderen Bundesländern von den dortigen Datenschutzbehörden bereits durchgeführt wurden.

Wiederkehrende Anfragen hinsichtlich der Zulässigkeit von Videoüberwachungsanlagen sowie der gesetzliche Überwachungsauftrag nach § 26 Abs. 1 SDSG erforderten es, einen aktuellen Überblick hinsichtlich installierter öffentlicher Videoüberwachungsanlagen zu gewinnen. Im Mai 2010 wurden daher die der Kontrolle der Landesbeauftragten für Datenschutz und Informationsfreiheit unterstehenden öffentlichen Stellen gebeten, mittels eines eigens hierfür entwickelten Fragebogens Angaben zu bereits von ihnen durchgeführten Videoüberwachungsmaßnahmen zu machen. Gemäß § 2 Abs. 1 Satz 2 SDSG gelten auch Vereinigungen ungeachtet ihrer Rechtsform als öffentliche Stellen, sofern sie Aufgaben öffentlicher Verwaltung wahrnehmen und eine oder mehrere öffentliche Stellen des Landes, der Gemeinden und Gemeindeverbände mit absoluter Mehrheit der Anteile oder absoluter Mehrheit der Stimmen an diesen beteiligt ist (Gesellschaften, Eigenbetriebe u. ä.). Deshalb waren diese Stellen gleichfalls in die Erhebung mit einzubeziehen. Da nicht alle angeschriebenen Stellen auf die Anfrage meiner Dienststelle antworteten, war es notwendig, in einem weiteren Schreiben erneut um die erforderlichen Angaben zu bitten.

Viele dieser Stellen haben um Fristverlängerung für die Beantwortung ersucht. Schon jetzt kann gesagt werden, dass bislang zahlreiche Antworten eingingen und immer noch eingehen. Für den Berichtszeitraum ist es aber noch nicht möglich, das Gesamtergebnis der Auswertung darzulegen, insoweit muss auf den nächsten Tätigkeitsbericht verwiesen werden, da die vollständige Auswertung erst im laufenden Berichtszeitraum abgeschlossen werden kann. In den nachfolgenden Ausführungen sollen demzufolge nochmals die rechtlichen Parameter für die Installation einer Videoüberwachungsanlage beleuchtet und auf konkrete Fallbeispiele eingegangen werden.

Mit dem am 01. Januar 2008 in Kraft getretenen Gesetz zur Erhöhung der öffentlichen Sicherheit im Saarland wurden neue gesetzliche Grundlagen zur Videoüberwachung sowohl im saarländischen Polizeigesetz (§ 27 Abs. 2 SpolG) als auch im Saarländischen Datenschutzgesetz (§ 34 SDSG) geschaffen. Die Beobachtung öffentlich zugänglicher Bereiche mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist gemäß § 34 Abs. 1 SDSG danach nur zulässig, soweit sie entweder in Wahrnehmung des Hausrechts der verantwortlichen Stelle zum Zweck des Schutzes von Personen, des Eigentums oder des Besitzes oder der Kontrolle von Zugangsberechtigungen, oder zur Aufgabenerfüllung der verantwortlichen Stelle erforderlich ist. Für die Gefährdung der zuvor genannten Rechtsgüter müssen konkrete Anhaltspunkte bestehen. Eine Videoüberwachung im Rahmen der Aufgabenerfüllung der verantwortlichen Stelle ist nur zulässig, wenn Anhaltspunkte für eine konkrete Gefährdung von Gesundheit, Leib oder Leben, Eigentum oder sonstigen hochrangigen Rechtsgütern vorliegen. Es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Videoüberwachung darf nur durch die Leitung der verantwortlichen Stelle angeordnet werden. Zweck, räumliche Ausdehnung und Dauer der Videoüberwachung sind zu dokumentieren.

Nach § 7 Abs. 2 SDSG bedarf der erstmalige Einsatz sowie die wesentliche Änderung von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, der schriftlichen Freigabe durch die oberste Landesbehörde, die federführend für die dem automatisierten Verfahren zugrunde liegende Rechtsmaterie zuständig ist. Vor dieser Entscheidung ist die saarländische Landesbeauftragte für Datenschutz zu hören. Automatisiert ist eine Datenverarbeitung nach § 3 Abs. 6

SDSG dann, wenn sie durch Einsatz eines gesteuerten technischen Verfahrens selbsttätig abläuft. Datenverarbeitung wiederum ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten (§ 3 Abs. 2 Satz 1 SDSG). Die Beobachtung mit „optisch-elektronischen Einrichtungen“ stellt insofern eine Datenerhebung, weitergehende Video-Aufzeichnungen eine Datenspeicherung und beide Vorgänge stellen Datenverarbeitungen i.S.d. § 3 Abs. 2 Satz 1 SDSG dar. Nach § 3 Abs. 1 des SDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffene oder Betroffener). Zweifelsfrei handelt es sich bei Bildaufzeichnungen von Personen, sei es nun, dass sie sich rechtmäßig oder unrechtmäßig an einem Ort aufhalten, beispielsweise bei Betreten einer Anlage außerhalb der Öffnungszeiten, um personenbezogene Daten im Sinne des § 3 Abs. 1 SDSG. Mithin ist die Landesbeauftragte für Datenschutz vor der beabsichtigten Installation einer Videoüberwachungsanlage durch Behörden oder sonstige öffentliche Stellen des Landes zu beteiligen und eine entsprechende Verfahrensbeschreibung mit den nach § 9 Abs. 1 SDSG festzulegenden Angaben zu übersenden.

§ 34 Abs. 1 Satz 1 SDSG manifestiert eine Erforderlichkeitsprüfung, welche sich nicht nur auf den allgemeinen Erforderlichkeitsgrundsatz beziehen darf, sondern auch auf den Einsatz der Videotechnik überhaupt gerichtet sein muss. Können daher weniger einschneidende Mittel für dasselbe Ziel eingesetzt werden, ist die Erforderlichkeit i.S.d. vorgenannten Vorschrift nicht gegeben und die Zulässigkeit einer Videoüberwachung zu verneinen.

Fußt die beabsichtigte Videoüberwachung auf der Rechtsgrundlage von § 34 Abs. 1 Nr. 1 SDSG so sind die „konkreten Anhaltspunkte“ für den erforderlichen Schutz von Personen, Eigentum oder Besitz zu benennen. In der Praxis ist daher der Verfahrensbeschreibung ein gesonderter Vermerk über Vorkommnisse der Vergangenheit, wie beispielsweise Einbruchsdiebstähle, Vandalismusschäden, Beschädigungen an Kassenautomaten und ähnliches sowie sich hieraus ergebende Anzeigen bei der Polizei oder Kostenaufwendungen, beizufügen.

Unter der „Aufgabenerfüllung der verantwortlichen Stelle“ sind alle explizit gesetzlich festgeschriebenen Verwaltungsaufgaben zu verstehen, weshalb diese auch bei einer

nach § 34 Abs. 1 Nr. 2 SDSG beabsichtigten Videoüberwachung konkret zu benennen sind und sich nicht auf eine nur allgemeine Aufgabenerfüllung erstrecken dürfen. Gemäß § 34 Abs. 2 SDSG müssen die Möglichkeit der Beobachtung und die verantwortliche Stelle für Betroffene erkennbar sein. Dies kann durch entsprechende Hinweisschilder mit mindestens Name und Anschrift der verantwortlichen Stelle sichergestellt werden, die im Blickfeld des Betroffenen, jedoch räumlich so angebracht werden, dass dem Betroffenen, bevor er das Erfassungsfeld der Kameras betritt, die Möglichkeit gegeben wird, sich der Erfassung zu entziehen. Meine Dienststelle hat hierfür ein Musterhinweisschild in Form eines Piktogramms erstellt, das bereits zahlreichen anfragenden öffentlichen Stellen zur Verfügung gestellt wurde und in Kürze auch in unserem Internetangebot abgerufen werden kann.

Im Folgenden soll auf einzelne grundsätzliche Gesichtspunkte bei der Videoüberwachung bestimmter Bereiche exemplarisch eingegangen werden.

8.3.1 Videoüberwachung an Schulen

Eine Videoüberwachung zur Wahrnehmung des Hausrechts ist nur für öffentlich zugängliche Bereiche zulässig, was bedeutet, dass einer unbestimmten Vielzahl von Personen der Zutritt grundsätzlich möglich sein muss. In Bezug auf Schulgebäude ist daher eine einzelfallbezogene Prüfung dieser Voraussetzung unumgänglich. Die öffentliche Zugänglichkeit eines Unterrichtsraumes wird daher in der Regel zu verneinen sein.

Im Gegensatz zu anderen Einsatzformen von Videotechnik ist darüber hinaus der Erziehungs- und Bildungsauftrag der Schule in die Erwägungen einzubeziehen. Dabei verträgt sich eine Videoüberwachung grundsätzlich nicht mit dem Auftrag der Schulen, die Entwicklung der Schülerinnen und Schüler zu selbstbestimmten mündigen Persönlichkeiten zu fördern. Hinsichtlich der durchzuführenden Erforderlichkeitsprüfung in Korrelation mit der Interessensabwägung der schutzwürdigen Interessen der Betroffenen wird eine Videoüberwachungsmaßnahme auf Zeiten außerhalb des Schulbetriebs zu beschränken sein, da während des Schulbetriebes die Sicherstel-

lung des Hausrechts den hierfür verantwortlichen Personen zugemutet werden kann und als wesentlich milderes Mittel zur Zielerreichung zu bewerten ist.

8.3.2 Videoüberwachung in Schwimmbädern

Die Überwachung eines Kassenautomaten kann dann nach § 34 Abs. 1 Nr. 1 SDSG zulässig sein, wenn z.B. in der Vergangenheit Kassenautomaten beschädigt wurden und das Eigentum des Hausherrn nunmehr geschützt werden soll. Die Gewährleistung eines reibungslosen Betriebsablaufes, also beispielsweise die ordnungsgemäße Zahlung der Badbesucher, dient jedoch nicht dem Schutz des zuvor erwähnten Rechtsgutes. Ist die Maßnahme zulässig, so ist der Focus der Kamera auf den Kassenautomaten so auszurichten, dass keine weiteren Bereiche, zu nennen wären hier, Durchgänge und Informationsschalter sowie insbesondere solche Bereiche, die zum Verweilen der Badbesucher gedacht sind, wie Wartebänke oder Caféterien, erfasst werden. Von einer Überwachung gänzlich auszuschließen sind in jedem Fall solche Bereiche, die die Intimsphäre der Badegäste berühren (z.B. Umkleiden, Dusch- und Saunabereiche), da hier die berechtigten Interessen der Betroffenen zweifelsfrei überwiegen. Zu berücksichtigen ist ebenso, dass durch Videoüberwachungsmaßnahmen in Bädern auch das dort beschäftige Personal erfasst wird, hier ist § 31 Abs. 5 SDSG zu beachten, wonach diese Daten nicht zur Verhaltens- und Leistungskontrolle der Mitarbeiter herangezogen werden dürfen. Sind Mitarbeiter demnach von einer Videoüberwachungsmaßnahme betroffen, ist ausdrücklich die Einbindung des Personalrates anzuraten.

8.3.3 Videoüberwachung von Außenfassaden

Sehr oft wurde meine Dienststelle bereits zur Frage der Zulässigkeit der Videoüberwachung von Außenfassaden kontaktiert. In vielen Fällen handelte es sich um historische Gebäude, deren Außenwände durch Farbbomben, Graffiti oder Gewalteinwirkung beschädigt wurden, was in der Regel umfassende und kostenintensive Renovierungsmaßnahmen zur Folge hatte. Sicherlich stellt § 34 Abs. 1 Nr. 1 SDSG im Rahmen des Eigentumsschutzes hier eine mögliche Rechtsgrundlage dar. Grenzen

die Außenfassaden jedoch unmittelbar an öffentliche Bereiche, wie Parkanlagen, Fußwege, Fahrradwege oder Straßen, so ist durch den Betreiber sicherzustellen, dass gemessen ab der Hauswand lediglich ein 1 Meter breiter Streifen vom Auge der Kamera erfasst wird. Nach einschlägiger Rechtsprechung wird unter normalen Umständen von einem Passanten so lediglich ein Arm, eine Schulter oder eine Tasche auf den Aufzeichnungen sichtbar sein, nicht jedoch das Gesicht des Betroffenen. Dem Eigentümer wird im Gegenzug durch eine derartige Kameraeinstellung hinreichend ermöglicht, Beschädigungen an der Hauswand festzustellen und den Tatvorgang aufzuzeichnen. Hinsichtlich der erforderlichen täglichen Aufzeichnungsdauer ist zu prüfen, ob eine 24-stündige Überwachung tatsächlich notwendig ist oder vielmehr eine nur auf die Abendstunden begrenzte Überwachung, da die in Rede stehenden Vandalismusschäden in der Regel von den Tätern im vermeintlichen Schutz der Dunkelheit herbeigeführt werden.

8.3.4 Videoüberwachung zur Zufahrtskontrolle

Auch im Rahmen der Zufahrtskontrolle ist zu beachten, dass bei der Einfahrt kein öffentlicher Bereich durch die Kamera erfasst werden darf. Ebenso muss eine Erfassung von Kraftfahrzeugkennzeichen ausgeschlossen werden, da derartige Aufzeichnungen unter Beachtung der gesetzlichen Voraussetzungen des SpolG im Saarland ausschließlich der saarländischen Vollzugspolizei vorbehalten sind. Regelmäßig ist hier auch zu prüfen, ob eine Aufzeichnung zwingend erforderlich ist oder ein reines Kamera-Monitoring-Prinzip, also lediglich eine Beobachtung, für den angestrebten Zweck ausreicht. Je nach Personenkreis der Zufahrtberechtigten wird gleichwohl § 31 Abs. 5 SDSG zu beachten und mithin der Personalrat zu beteiligen sein.

8.3.5 Einsatz von Webcams

Geben die Bilder einer Webcam lediglich Landschaftseindrücke einer Kommune wieder, ohne die Möglichkeit eine Person oder ein Kraftfahrzeugkennzeichen, selbst nur teilweise, erkennen zu können oder eine entsprechende Verbindung herzustellen, so

handelt es sich nicht um die Verarbeitung personenbezogener Daten i.S.d. SDSG. Eine Zoomfunktion einer Kamera hingegen, die die Erkennbarkeit einer Person oder aber ihre Bestimmbarkeit herstellen kann, würde die zuvor gegebene datenschutzrechtliche Bewertung aushebeln.

8.4 Ratsinformationssysteme

Bei vielen Kreis- und Gemeindeverwaltungen wird die Vor- und Nachbereitung der Gemeinderats- oder Kreistagssitzungen durch Sitzungsmanagement-Systeme unterstützt. Hinzu kommt immer mehr der Wunsch nach Anbindung der Systeme an das Internet zur Information und Interaktion mit dem Bürger, jedoch vor allem auch der Wunsch der Ratsmitglieder, Unterlagen von der Verwaltung auch elektronisch zu erhalten sowie auf die Info-Systeme der Verwaltung vom eigenen PC aus zugreifen zu können.

Solche Systeme mit verwaltungsinternem Sitzungsmanagement sind sehr verbreitet. Mit der entsprechenden Vergabe von Nutzungsrechten soll dafür gesorgt werden, dass nur berechtigte Teilnehmer das System im Rahmen der ihnen zustehenden Befugnisse nutzen, sprich die darin enthaltenen Daten bearbeiten bzw. zur Kenntnis nehmen können.

Sowohl bei elektronischer Einladung der Ratsmitglieder zu Sitzungen als auch bei eventueller Veröffentlichung von Niederschriften öffentlicher Sitzungen muss darauf geachtet werden, dass dem Datenschutz Rechnung getragen wird. Insofern dürfen keine personenbezogenen oder –beziehbaren Daten im Internet abrufbar sein, sofern von dem Betroffenen keine Einwilligung vorliegt. Dies betrifft Tagesordnungspunkte aber auch eventuelle Redebeiträge von Mandatsträgern oder sonstigen Sitzungsteilnehmern. Ebenso muss vermieden werden, dass alte Sitzungsniederschriften für ewige Zeiten im Internet verfügbar sind. Von unserer Dienststelle wird daher den Kommunalverwaltungen vorgeschlagen, jeweils nur die letzte Niederschrift bis Verfügbarkeit der darauf folgenden Niederschrift im Internet bereit zu stellen.

Ein weiterer Problembereich stellt die Bereitstellung und Zustellung der Sitzungseinladungen, -unterlagen und –protokolle auf elektronischem Wege an die Ratsmitglieder dar. Bei der Bereitstellung der Unterlagen muss auf eine gesicherte Kommunikation geachtet werden. So muss entweder eine per https-Protokoll abgesicherte Verbindung genutzt oder die Dokumente selbst verschlüsselt werden. Alternativ könnte auch über die Nutzung der virtuellen Poststelle für die Zustellung der Unterlagen nachgedacht werden.

Weiterhin muss darauf hingewiesen werden, dass das Ratsmitglied bei der Nutzung von elektronischen Unterlagen ebenso auf die Verschwiegenheit achtet und somit auch entsprechende Maßnahmen trifft, wie sie bei der Nutzung von Papierunterlagen zu treffen sind.

Ebenso hat das Ratsmitglied nach Ausscheiden aus dem Rat die sichere Löschung aller elektronischen Unterlagen zu gewährleisten.

Auf die umfangreichen Anforderungen ist das Ratsmitglied bei Übernahme seines Mandates – am besten im Zusammenhang mit der Eröffnung des elektronischen Zugangs – durch die Verwaltung hinzuweisen.

9 Soziales

9.1 Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

Am 10. Dezember 2008 hat das Bundessozialgericht, Az: B 6 KA 37/07 R, eine grundlegende Entscheidung zur Reichweite des Schutzes von Patientendaten in der gesetzlichen Krankenversicherung getroffen, die für erhebliches Aufsehen gesorgt hat.

Das Bundessozialgericht hat eine Abrechnungspraxis für rechtswidrig erklärt, die in der Vergangenheit üblich war und nie beanstandet worden ist. Das Gericht hat entschieden, dass Krankenhäuser oder Vertragsärzte keine Patientendaten an private Dienstleistungsunternehmen zur Erstellung der Leistungsabrechnung übermitteln dürfen. Dies gelte auch, wenn die Patienten Einwilligungserklärungen unterzeichnet haben. In dem konkreten Fall ging es darum, dass eine Krankenkasse die Leistungsabrechnung eines Krankenhauses mit der Begründung zurückgewiesen hatte, dass die Abrechnung ambulanter Notfallbehandlungen nicht durch die zuständige Kassenärztliche Vereinigung, sondern eine private Abrechnungsstelle erstellt worden war. Das Gericht hat seine Entscheidung damit begründet, dass der Gesetzgeber im Sozialgesetzbuch V – Gesetzliche Krankenversicherung – detailliert und abschließend die Erfassung, Verwendung und Übermittlung von Leistungs- und Gesundheitsdaten zum Zwecke der Abrechung ärztlicher Leistungen mit den Krankenkassen geregelt habe. Dabei habe der Gesetzgeber die Datenverarbeitung bewusst auf das zu dem erforderlichen Zweck unerlässliche Minimum reduziert, um dem Recht auf informationelle Selbstbestimmung zu genügen. Die Einschaltung privater Abrechnungsstellen in den Abrechnungsweg sei nur für bestimmte Fälle vorgesehen, so etwa für Apotheker und Leistungserbringer im Bereich der Heil- und Hilfsmittel, denen ausdrücklich das Recht eingeräumt ist, externe Rechenzentren einzuschalten.

Bemerkenswert ist, dass das Gericht auch der Einwilligung der Patienten keine die Datenübermittlung rechtfertigende Funktion beigemessen hat, gilt doch gemeinhin die Erteilung einer Einwilligung als Ausdruck der Ausübung des Rechtes auf informa-

tionelle Selbstbestimmung schlechthin. Dem Gericht ist darin zuzustimmen, dass in der vorliegenden Fallkonstellation von einer freien Entscheidung des Betroffenen nicht die Rede sein kann. Beipflichten möchte ich insbesondere der Aussage, dass die meisten Patienten die geforderte Einwilligungserklärung unterschreiben, weil sie den berechtigten Eindruck haben, im Interesse einer schnellen und guten Notfallversorgung die ihnen von dem Leistungserbringer vorgelegte Erklärung unterschreiben zu sollen.

Der Gesetzgeber hat auf dieses Urteil reagiert und eine Abrechnung über private Abrechnungsstellen im Wege der Auftragsdatenverarbeitung zugelassen. Die entsprechenden Regelungen sind nach Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder allerdings nicht geeignet, einen ausreichenden Schutz der Sozialdaten der gesetzlich Krankenversicherten zu garantieren (Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010, Anlage 18.18). Die für die Abrechnung zu verwendenden Daten müssten vielmehr wie bei den herkömmlichen Abrechnungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck begrenzt werden. Insbesondere sei zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten als bei der Abrechnung über die Kassenärztliche Vereinigung erhalten.

9.2 Änderung des Sozialgesetzbuches: Auftragsdatenverarbeitung; Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Am 1. September 2009 sind wichtige Verbesserungen des Bundesdatenschutzgesetzes in Kraft getreten. Dazu gehören insbesondere verschärfte Anforderungen an die Datenverarbeitung im Auftrag und eine Verpflichtung zur Information der Aufsichtsbehörden und der Betroffenen bei unrechtmäßiger Kenntniserlangung personenbezogener Daten. Die Datenschutzbeauftragten des Bundes und der Länder be-

grüßen es, dass die Vorschriften über den Sozialdatenschutz entsprechend geändert wurden (§ 80 SGB X; § 83a SGB X).

Im Einzelnen geht es um folgendes:

Die Vorschriften über die Auftragsdatenverarbeitung regeln den Sachverhalt, dass ein Auftraggeber die Daten durch andere (Auftragnehmer) erheben, verarbeiten oder nutzen lässt. Typischer Fall ist die Datenverarbeitung durch Rechenzentren. Die Regelungen über die Auftragsdatenverarbeitung sollen sicherstellen, dass der Datenschutz- und Datensicherungsstandard durch die Vergabe der Datenverarbeitung außer Haus nicht eingeschränkt wird. Der Auftraggeber ist weiterhin verantwortlich für die ordnungsgemäße Datenverarbeitung; in einem Vertrag sind insbesondere die vom Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen der Datensicherung zu fixieren.

Die Anforderungen an diese schriftlich festzuhaltenden Inhalte bei der Auftragsdatenverarbeitung wurden erweitert. Außerdem wird der Auftraggeber verpflichtet, sich erstmals vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen und das Ergebnis der Prüfungen zu dokumentieren.

Des Weiteren sind die Sozialleistungsträger nunmehr in bestimmten Fällen verpflichtet, die Betroffenen und die Datenschutzaufsichtsbehörden zu informieren, wenn Dritte unrechtmäßig Kenntnis von personenbezogenen Daten genommen haben. Die Betroffenen können so Vorkehrungen gegen die Entstehung und Vertiefung von Schäden ergreifen, sowie ihre datenschutzrechtlichen Betroffenenrechte und etwaige Schadenersatzansprüche geltend machen. Darüber hinaus kann die Informationspflicht geeignet sein, die Verantwortlichen zu veranlassen, verstärkt präventive Datenschutzmaßnahmen zu ergreifen.

Ich darf an dieser Stelle bereits ankündigen, dass ich bei einer anstehenden Novellierung des Saarländischen Datenschutzgesetzes die Aufnahme entsprechender Vorschriften auch in dieses Gesetz fordern werde.

9.3 Änderung der datenschutzrechtlichen Kontrollzuständigkeit bei den ARGEn

Seit am 1. Januar 2005 die Arbeitslosenhilfe und die Sozialhilfe für erwerbsfähige Hilfebedürftige zusammengeführt wurden und dieser Personenkreis von den sogenannten Arbeitsgemeinschaften (getragen von der Bundesagentur für Arbeit und den Kommunen) betreut wird, müssen sich die Datenschutzbehörden mit einer Vielzahl von Problemen in diesem Zusammenhang befassen.

Neben Eingaben von Bürgern, bei denen es um konkrete Datenschutzverstöße im jeweiligen Einzelfall geht, sind es auch grundsätzliche Fragestellungen, mit denen sich die Datenschutzaufsichtsbehörden des Bundes und der Länder auseinandersetzen müssen.

Ein solches Thema ist von Anfang an die Frage der Kontrollzuständigkeit über die ARGEn.

So mussten, nachdem die ARGEn ihre Tätigkeit aufgenommen hatten, verschiedene Landesbeauftragte für den Datenschutz erleben, dass ihnen von den zuständigen ARGEn das Recht abgesprochen wurde, ihre Dienststellen zu kontrollieren. Es wurde argumentiert, dass wegen der geteilten Zuständigkeiten innerhalb der ARGEn (die Bundesagentur als Trägerin der Leistungen zur Eingliederung in Arbeit und der Geldleistung zur Sicherung des Lebensunterhaltes; die Kommunen als Leistungsträger für die Kosten der Unterkunft und Heizung) eine geteilte Kontrollkompetenz zwischen dem Bundesbeauftragten für den Datenschutz und den Landesbeauftragten für den Datenschutz bestehe. Schließlich konnten sich alle Beteiligten darauf verständigen, dass die ARGEn von den Landesbeauftragten für den Datenschutz kontrolliert werden. Lediglich soweit es um zentrale IT-Verfahren sowie Vordrucke der Bundesagentur geht, sollte der Bundesbeauftragte für den Datenschutz zuständig sein.
Diese Verfahrensweise hat sich in der Folgezeit bewährt.

Mit Urteil vom 20. Dezember 2007 hat das Bundesverfassungsgericht entschieden, dass die im SGB II getroffene Regelung, wonach die kommunalen Träger und die

Bundesagentur für Arbeit zur einheitlichen Wahrnehmung ihrer Aufgaben Arbeitsgemeinschaften bilden sollen, gegen die Systematik des Grundgesetzes, gegen den Grundsatz der eigenverantwortlichen Aufgabenwahrnehmung sowie gegen den Grundsatz der Verantwortungsklarheit verstoße und damit verfassungswidrig sei. Der Gesetzgeber wurde zu einer verfassungskonformen Neuorganisation der Aufgabenwahrnehmung aufgefordert.

Damit stand auch wieder die Frage der Verteilung der Zuständigkeit für die Datenschutzkontrolle im Raum. Nachdem die Absicht die Bundesregierung bekannt wurde, die Datenschutzkontrolle für die künftigen sogenannten JobCenter zentral auf den Bundesbeauftragten für den Datenschutz zu übertragen, haben sich mehrere Landesbeauftragte für den Datenschutz in einem offenen Brief dafür ausgesprochen, es im Interesse der Bürgernähe bei der bisherigen gemeinsamen Datenschutzkontrolle durch Bundes- und Landesdatenschutzbeauftragte zu belassen. Bei der Bearbeitung von Petitionen werden in vielen Fällen Ortsbesichtigungen oder Einsichtnahmen in die jeweiligen Akten erforderlich; es kommt auch oft vor, dass Bürger persönlich bei den Dienststellen der Landesbeauftragten vorsprechen um ihr Anliegen vorzutragen.
Diese Argumente konnten den Bundesgesetzgeber allerdings nicht überzeugen; mit Wirkung vom 1. Januar 2011 ist der Bundesbeauftragte zuständig für die Kontrolle der JobCenter.

Meine Dienststelle ist allerdings nach wie vor zuständig für die kommunalen Träger für Arbeitsförderung. Dies ist derzeit im Saarland die Kommunale Arbeitsförderung beim Landkreis St. Wendel.

9.4 Datenschutz für Bewohner von Einrichtungen der Alten- und Behindertenhilfe

Auch wenn Menschen in stationären Einrichtungen (z.B. der Alten- oder Behindertenhilfe) betreut werden, bedeutet dies nicht, dass die Einrichtung umfassend über die persönlichen Verhältnisse ihrer Bewohner informiert sein darf.

Anlass zu Irritationen in diesem Zusammenhang gab es im Berichtszeitraum:

In einem Fall hatte der überörtliche Träger der Sozialhilfe solche Einrichtungen angeschrieben und um Mitwirkung bei der Prüfung des einzusetzenden Vermögens der Bewohner gebeten. (Hintergrund ist, dass Sozialhilfe nur insoweit gewährt wird, als kein eigenes Einkommen oder Vermögen vorhanden ist.)

Der überörtliche Träger hatte die entsprechenden Formulare an die jeweiligen Einrichtungen gesandt mit der Bitte, diese an die Bewohner zu verteilen und ausfüllen zu lassen. Bei verschiedenen Einrichtungen ist der Eindruck entstanden, der überörtliche Träger erwarte, dass die Formulare bei den Bewohnern eingesammelt und an den überörtlichen Träger geschickt werden sollen. Eine solche Verfahrensweise wäre nicht zulässig gewesen, da die Vermögensverhältnisse der Bewohner in keiner Weise den entsprechenden Heimen bekannt gegeben werden dürfen.

Der überörtliche Träger hat auf Nachfrage meiner Dienststelle bestätigt, dass dies auch nicht beabsichtigt gewesen sei. Um aber hier in Zukunft solche Missverständnisse von vorn herein zu vermeiden, werde man bei künftigen Überprüfungen der wirtschaftlichen und persönlichen Verhältnisse die Leistungsberechtigten direkt anschreiben.

In einem anderen Fall ging es um die Ausstellung von Ausweisen wegen Befreiung von gesetzlichen Zuzahlungen für Medikamente.

Eine Krankenkasse wollte es für die Bewohner von Altenheimen einfacher machen, in den Besitz der Ausweise zu kommen. Sie hat den Altenheimen die Anträge mit

den Einkommenserklärungen zugeschickt, mit der Bitte, sie an die Bewohner zu verteilen und gesammelt zurückzuschicken.

Das war zwar gut gemeint, hätte aber bedeutet, dass die Bewohner der Einrichtung ihre Einkommens- und Vermögensverhältnisse hätten offenbaren müssen. Meine Dienststelle hat darauf gedrängt, dass das Verfahren so geändert wird, dass jedem Heimbewohner bewusst ist, dass er auch die Möglichkeit hat, seinen Antrag unmittelbar an die betreffende Krankenkasse zu schicken.

9.5 ELENA (Elektronischer Entgeltnachweis)

Seit Jahren ist das Verfahren des elektronischen Entgeltnachweises (ELENA), immer wieder Gegenstand der Tätigkeitsberichte meiner Dienstelle.

Zur Erinnerung: Beantragt heute jemand Sozialleistungen (z.B. bei der Bundesagentur für Arbeit, der Wohngeldstelle usw.), müssen in vielen Fällen Arbeits- oder Verdienstbescheinigungen vorgelegt werden. Diese Daten werden künftig zentral gespeichert und bei Bedarf vom Sozialleistungsträger abgerufen. Dadurch soll ein Beitrag zur Entbürokratisierung der Verwaltung geleistet werden, insbesondere sollen die Arbeitgeber von der Verpflichtung zur Archivierung von Daten und der Ausstellung von Verdienstbescheinigungen entlastet werden.

Am 2. April 2009 ist das ELENA-Verfahrensgesetz in Kraft getreten; seit dem 1. Januar 2010 sind die Arbeitgeber verpflichtet, die Entgeltdaten ihrer Beschäftigten an eine bei der Deutschen Rentenversicherung Bund eingerichtete Speicherstelle zu melden.

Nach Beginn der Meldungen hat sich ein Problem ergeben, an das bisher niemand gedacht hatte: Beim Antrag auf Arbeitslosengeld spielen auch Fehlzeiten des Arbeitnehmers eine Rolle. Dementsprechend sah der zu meldende Datensatz auch Angaben über Krankheits- und Streiktage vor.

Eine Speicherung über die Teilnahme an Streiks in der ELENA-Datenbank wäre verfassungswidrig, denn damit würde die vom Grundgesetz garantierte Koalitionsfreiheit (Artikel 9 Grundgesetz) in Frage gestellt. Auf Intervention des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wurde dieses Feld gestrichen. Angaben über Krankheitstage werden allerdings nach wie vor gespeichert.

Seit Beginn der Meldepflicht haben sich Beschäftigte, aber auch Arbeitgeber an meine Dienststelle mit Fragen zu dem neuen Meldeverfahren gewandt. Hilfreich bei der Beantwortung dieser Fragen war insbesondere auch die Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, www.bfdi.de, in der dieser häufig gestellte Fragen im Zusammenhang mit ELENA beantwortet.

Zur erwähnen ist noch ein Beschluss des Bundesverfassungsgerichtes vom 14. September 2010, in dem das Gericht einen Eilantrag zur Aussetzung des ELENA-Verfahrens abgelehnt hat. Zwischenzeitlich haben mehrere Bürger Verfassungsbeschwerden gegen das ELENA-Verfahrensgesetz eingelegt.

9.6 Hartz-IV; Übermittlung der Diagnosen bei amtsärztlichen Untersuchungen

Eine Frage beschäftigt die Datenschutzbehörden immer wieder: In welchem Umfang dürfen medizinische Informationen bei ärztlichen Begutachtungen an die Verwaltungsbehörden weitergegeben werden? In jüngster Zeit ist dieses Problem wieder aufgetaucht im Zusammenhang mit der amtsärztlichen Begutachtung von Hartz-IV-Beziehern. Da Leistungen nach dem SGB II nur Personen gewährt wird, die erwerbsfähig sind, wird bei Zweifeln an der Erwerbsfähigkeit ein amtsärztliches Gutachten eingeholt.

Im Berichtszeitraum hat sich eine Petentin darüber beschwert, dass das Gesundheitsamt ihre genauen Diagnosen an den Leistungsträger weitergegeben habe. Sie

war der Auffassung, dass diese sensiblen intimen Informationen den Verwaltungsmitarbeiter nichts angingen. Es müsse genügen, dass der Amtsarzt mitteile, ob und in welchem Umfang sie erwerbstätig sein könne; die Diagnosen selbst seien irrelevant, zumal der Mitarbeiter in der Verwaltung nicht in der Lage sei, aus den medizinischen Informationen zutreffende Schlüsse im Hinblick auf ihre Erwerbsfähigkeit zu ziehen.

Der Leistungsträger meinte demgegenüber, dass die Übermittlung der wesentlichen Diagnosen unabdingbarer Bestandteil der in Auftrag gegebenen Begutachtung der Erwerbs- und Arbeitsfähigkeit sei; die Notwendigkeit ihrer Übermittlung an den Fallmanager leite sich aus dessen umfassenden Unterstützungsauftrag nach dem SGB II ab.

Diese Argumentation ist so nicht nachvollziehbar. Es ist zwar zutreffend, dass die Fallmanager die Antragsteller „umfassend zu unterstützen“ haben (§ 4 Abs. 1 Nr. 1 SGB II). Es ginge jedoch zu weit, hieraus den Schluss zu ziehen, der Antragsteller habe sich gegenüber seinem Sachbearbeiter umfassend zu offenbaren. Es ist vielmehr immer zu fragen, ob eine Information für die Aufgabenerfüllung unbedingt erforderlich ist. Dies möchte ich ebenso wie mein Amtsvorgänger für die Angabe der genauen Diagnosen verneinen. Ich halte es vielmehr für ausreichend, dass dem Verwaltungsmitarbeiter lediglich mitgeteilt wird, welche Arbeiten in welchem Umfang von dem Antragsteller verrichtet werden können und welche Arbeiten oder Belastungen auszuschließen sind. Nur dann, wenn in begründeten Einzelfällen die Kenntnis der konkreten Diagnose erforderlich ist, kann diese noch nachträglich durch den Gutachter mitgeteilt werden. Diese Auffassung wird dadurch gestützt, dass das Formular „sozialmedizinische Stellungnahme für den Auftraggeber“, das von der Bundesagentur für Arbeit eingeführt wurde, die Angabe von Befund- oder Diagnosedaten nicht vorsieht.

Der Leistungsträger hat sich schließlich dieser Argumentation angeschlossen und für die Zukunft zugesagt, keine Details zum Gesundheitszustand zu verlangen.

9.7 Überweisung von Beiträgen zur Klassenfahrt durch die ARGE

Hartz-IV-Empfänger können gemäß § 23 Abs. 3 Nr. 3 Zweites Buch Sozialgesetzbuch (SGB II) einen Zuschuss zur Teilnahme ihrer Kinder an einer Klassenfahrt beantragen.

Ein Petent hat sich in diesem Zusammenhang an meine Dienststelle gewandt und bemängelt, dass der ihm bewilligte Betrag direkt von der ARGE auf das zum Zwecke der Klassenfahrt eingerichtete Konto der verantwortlichen Klassenlehrerin überwiesen wurde. So wurde nach Ansicht des Petenten der Klassenlehrerin der Umstand der Bedürftigkeit seiner Familie bekannt. Dies würde einen Verstoß gegen das Sozialgeheimnis nach § 35 Erstes Buch Sozialgesetzbuch (SGB I) darstellen.

Auf Nachfrage teilte die ARGE mit, dass die Überweisung tatsächlich direkt auf das Konto der Klassenfahrt überwiesen wurde, dass die Überweisung jedoch unter Angabe einer Buchungsnummer erfolgte und kein Name des betreffenden Kindes angegeben wurde. Die Klassenlehrerin konnte demnach nicht nachvollziehen, welchem Kind der überwiesene Betrag zuzuordnen ist. Die ARGE hat daraufhin die Klassenlehrerin gebeten, den Betrag zurück zu überweisen und eine Überweisung auf das Konto des Petenten veranlasst.

Weiterhin fühlte sich der Petent durch die Aufforderung der ARGE zur Vorlage eines Nachweises über die Durchführung der Klassenfahrt mit Angaben der entstandenen Kosten und der Mitteilung, dass die schulrechtlichen Bestimmungen eingehalten wurden in seinem Recht auf informationelle Selbstbestimmung derart eingeschränkt, dass durch die Anforderung der Bescheinigung der Schule der Umstand der Bedürftigkeit zur Kenntnis gebracht wird.

Eine solche Datenerhebung ist laut § 67 a Abs. 1 Zehntes Buch Sozialgesetzbuch (SGB X) zulässig, soweit die Erhebung zur Aufgabenerfüllung der erhebenden Stelle erforderlich ist. Zur Aufgabenerfüllung der ARGE gehört unter anderem die Bewilligung von Leistungen für Klassenfahrten nach § 23 Abs. 3 Nr. 3 Zweites Buch Sozialgesetzbuch (SGB II).

Gegenüber der ARGE kann der Nachweis der tatsächlich durchgeführten Klassenfahrt und der tatsächlich entstandenen Kosten nur geführt werden, soweit die Schule die erforderlichen Daten zur Verfügung stellt.

Ein Antragsteller ist gemäß § 60 Abs. 1 Nr. 1 SGB I dazu verpflichtet, alle Tatsachen anzugeben, die für die Leistung erheblich sind. Ebenso ist er verpflichtet, auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen.

Ein datenschutzrechtlich bedenkliches Vorgehen der ARGE konnte in diesem Fall nicht festgestellt werden.

Trotz der ähnlich gelagerten Fallkonstellation führte hier der Grundsatz der Erforderlichkeit zu unterschiedlichen Übermittlungsbefugnissen. Im Falle der Datenübermittlung an die Klassenlehrerin war eine personenbezogene Datenübermittlung der Bedürftigkeit an die Lehrerin durch direkte Überweisung des Betrages auf das Klassenfahrtkonto nicht zulässig.

Im Falle der Datenübermittlung zwecks Ausstellung der Bescheinigung war dies für die Aufgabenerfüllung der ARGE erforderlich und zulässig. Es wurde lediglich das Sekretariat der Schule über die Bedürftigkeit der Familie in Kenntnis gebracht, nicht jedoch das Lehrerkollegium.

9.8 Offenlegung von Kundendaten bei der Einkommensberechnung Selbständiger

Mehrere Selbständige, die Leistungen der Grundsicherung nach dem SGB II beantragt haben, haben bei meiner Dienststelle nachgefragt, ob sie verpflichtet sind, Forderungen der ARGEn nach Vorlage von Kundenrechnungen nachzukommen. Es wurde die Befürchtung geäußert, dass man hierdurch eine Vertragsverletzung begehen oder sich sogar einer Straftat schuldig machen könnte.

Grundsätzlich ist es so, dass derjenige, der Sozialleistungen beantragt oder erhält, alle Tatsachen angeben muss, die für die Leistung erheblich sind, und auf Verlangen des Leistungsträgers auch Beweisurkunden vorzulegen hat (§ 60 SGB I).

Selbstverständlich ist, dass der Leistungsempfänger dem Leistungsträger sein Einkommen nachzuweisen hat. Zu fragen ist allerdings, ob hierfür Kundenrechnungen vorgelegt werden müssen oder ob nicht vielmehr die Vorlage des Einkommensteuerbescheides die geeignete Nachweismöglichkeit wäre. Hierzu haben die ARGEN mitgeteilt, dass nach der „Arbeitslosengeld II/Sozialgeld-Verordnung“ bei der Berechnung nicht das steuerliche Arbeitseinkommen zugrunde zu legen ist, sondern das im Bewilligungsabschnitt – in der Regel sechs Monate – erzielte Einkommen, wobei alle Einnahmen und Ausgaben, die in diesen Zeitraum fallen, bei der Berechnung des zu berücksichtigen Einkommens heranzuziehen sind. Diese Abkehr vom Einkommensteuerrecht hat der Verordnungsgeber unter dem Aspekt vorgenommen, dass das steuerliche Arbeitseinkommen häufig geringer ist als das tatsächlich für den Lebensunterhalt zur Verfügung stehende Einkommen. Beispielhaft sei hier die steuerrechtliche Möglichkeit der Abschreibung genannt.

Grundsätzliche Bedenken gegen die Forderung nach Vorlage von Kundenrechnungen bestehen somit nicht. Dem Datenschutz der Kunden ist allerdings dadurch Rechnung zu tragen, dass dem Selbständigen die Möglichkeit zur Schwärzung der Kundennamen eingeräumt wird.

Im vorliegenden Zusammenhang ist ein Fall zu erwähnen, in dem die zuständige ARGE ausdrücklich auf der Vorlage von ungeschwärzten Kundendaten bestanden hat. Begründet wurde dies damit, dass man sich von den Kunden den genauen Zeitpunkt der Begleichung der Rechnung schriftlich bestätigen lassen wolle.

Ein solches Herantreten an die Kunden hätte bedeutet, dass diese von dem Hartz IV-Bezug des Petenten erfahren hätten und, was noch schwerwiegender wiegt, es hätte der unausgesprochene Vorwurf des Sozialleistungsmissbrauchs durch den Petenten im Raum gestanden.

Die rechtliche Prüfung meiner Dienststelle hat ergeben, dass eine Rechtsvorschrift, die private Dritte verpflichten würde, im vorliegenden Zusammenhang Angaben zu machen, nicht ersichtlich ist. Es hätte sich somit um eine Datenerhebung gehandelt, die zur Erreichung des beabsichtigten Zweckes nicht geeignet gewesen wäre. Eine solche Datenerhebung ist nicht erforderlich und damit unzulässig.

Die betreffende Behörde wurde auf diese Rechtslage hingewiesen und gebeten auf die Forderung nach Vorlage von Kundenrechnungen mit den Namen der betreffenden Kunden zu verzichten. Dem ist die Behörde nachgekommen.

9.9 Wahrung des Sozialgeheimnisses

Gemäß § 35 Erstes Buch Sozialgesetzbuch (SGB I) hat jeder Bürger einen Anspruch darauf, dass die ihn betreffenden Sozialdaten von den verschiedenen Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden. Dies beinhaltet auch die Verpflichtung des Sozialleistungsträgers dafür zu sorgen, dass unbefugte Dritte keine Kenntnis von Sozialdaten erhalten dürfen.

Dieser Verpflichtung kamen im Berichtszeitraum nicht alle Leistungsträger im geforderten Umfang nach, so dass meine Dienststelle gleich mehrere Eingaben zu dieser Thematik erhielt.

So wurde in einem Fall im Rahmen eines Hausbesuches durch Mitarbeiter einer Sozialbehörde laut über die Straße gerufen, man solle die Haustür öffnen, da man wüsste, dass die betroffenen Personen zu Hause seien und man im Auftrage der Sozialbehörde unterwegs sei. Hierdurch wurde der interessierten Nachbarschaft mitgeteilt, dass die Betroffenen eine Sozialleistung beziehen oder zumindest beantragt haben. Auch diese Information fällt unter das Sozialgeheimnis nach § 35 SGB I.

Aufgrund eines Fehlers in der Poststelle einer Sozialbehörde wurde versehentlich ein Schreiben, dass an einen Sozialleistungsbezieher gerichtet war zusammen mit dem Leistungsbescheid eines anderen Leistungsbeziehers einkuvertiert. So wurden diese Daten für einen unbefugten Dritten zugänglich.

Durch einen Zeitungsbericht wurde meine Dienststellestelle darauf aufmerksam gemacht, dass an der Informationstheke eines Sozialleistungsträgers das ungehinderte Mithören der Anliegen anderer Leistungsempfänger möglich wäre. Nach einem Vor-Ort-Termin durch meine Mitarbeiter wurde dieser Mangel bestätigt und aufgrund unserer Intervention durch bauliche Umstrukturierungsmaßnahmen abgestellt.

Im Rahmen der Beratung in einer Sozialleistungsbehörde wurde ein Petent in einem Büro, in dem zwei Sachbearbeiter gleichzeitig Beratungen durchführen, über verschiedene Möglichkeiten, seine Lebenssituation zu verbessern informiert. Während er mit seinem Sachbearbeiter sprach, konnte ein weiterer Leistungsbezieher am Nebentisch ungehindert mithören, was der Petent zu sagen hatte und mischte sich sogar in dieses Gespräch ein. Hier war ein funktionierender Sozialdatenschutz nicht gewährleistet und ein Intervenieren bei meiner Dienststelle mehr als angebracht.

In allen Fällen konnte durch das Handeln meiner Dienststelle wieder die Sicherstellung des Datenschutzes im Sozialbereich herbeigeführt werden. 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.

9.10 Übermittlung von Namen der Berufsbetreuer an eine Berufsgenossenschaft

Im Berichtszeitraum haben mehrere Betreuungsbehörden bei meiner Dienststelle angefragt, ob es zulässig ist, die Namen der bei ihnen gespeicherten Berufsbetreuer an die Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege weiterzugeben.

Die Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege ist der gesetzliche Unfallversicherungsträger für alle Unternehmen im Bereich des Gesundheitswesens und der Wohlfahrtspflege und damit auch für die Berufsgruppe der selbständig tätigen Berufsbetreuer. Die Berufsgenossenschaft hat festgestellt, dass eine große Zahl von Berufsbetreuern ihrer Anmeldepflicht nicht nachkommt und ist deshalb an die Betreuungsbehörden herangetreten, um die Namen der Berufsbetreuer in Erfahrung zu bringen.

Das Anliegen der Berufsgenossenschaft ist zwar nachvollziehbar: Berufsbetreuer, die sich nicht angemeldet haben, zahlen keine Beiträge, erhalten bei Arbeitsunfällen und Berufserkrankungen dennoch Versicherungsleistungen. Im Sinne der Beitragsgerechtigkeit wäre es insofern sicherlich wünschenswert, wenn alle Berufsbetreuer zur Beitragszahlung herangezogen werden könnten.

Gleichwohl bin ich der Auffassung, dass die gewünschte Weitergabe von Namen, Anschriften, Geburtsdaten sowie Tätigkeitsbeginn der selbständig tätigen Berufsbetreuer datenschutzrechtlich nicht zulässig ist. Denn es fehlt an einer Rechtsgrundlage, die es den Betreuungsbehörden erlauben würde, die gewünschten Daten zu übermitteln. Es sollen personenbezogene Daten zu Zwecken verarbeitet werden, für die sie nicht erhoben worden sind. Eine solche zweckändernde Datenverarbeitung ist nach den Vorschriften des Saarländischen Datenschutzgesetzes (§ 13 SDSG) nur unter ganz bestimmten Voraussetzungen zulässig, die meines Erachtens hier nicht vorgelegen haben.

Diese Bewertung hat für viel Unverständnis auf Seiten der Berufsgenossenschaft gesorgt. Dem muss ich entgegen halten, dass Eingriffe in das informationelle Selbstbestimmungsrecht nur auf gesetzlicher Grundlage zulässig sind und es deshalb zu respektieren ist, wenn die gesetzlichen Voraussetzungen für eine Datenübermittlung nicht vorliegen.

9.11 Werbemaßnahmen der Krankenkassen

Seit Einführung des Kassenwahlrechts im Jahre 1992 (§ 173 SGB V) herrscht ein reger Wettbewerb zwischen den Kassen um neue Mitglieder. Auch der Datenschutz kommt hier ins Spiel, weil es um die Erhebung, Speicherung und Nutzung personenbezogener Daten geht. Nachdem jahrelang eine erhebliche Rechtsunsicherheit bestanden hat, hat der Gesetzgeber nunmehr die Verarbeitung personenbezogener Daten durch die Krankenkassen zur Gewinnung von Mitgliedern in § 284 Abs. 4 SGB V geregelt. Nach dieser Vorschrift dürfen die Krankenkassen zur Gewinnung von Mitgliedern Daten erheben, verarbeiten und nutzen, wenn die Daten allgemein zugänglich sind, es sei denn, das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Im Berichtszeitraum haben sich mehrere Bürger bei meiner Dienststelle gegen Werbemaßnahmen von Krankenkassen beschwert.

In einem Fall wurden alle Mitarbeiter einer Klinik, die nicht bei einer bestimmten Krankenkasse versichert waren, von dieser Krankenkasse angeschrieben. Die Petentin wunderte sich darüber, woher die Krankenkasse ihren Namen und ihre Adresse hatte und äußerte den Verdacht, dass möglicherweise ihr Arbeitgeber der Krankenkasse diese Daten zur Verfügung gestellt hat. Auf Nachfrage erklärte die AOK, die Daten der Petentin seien aus dem Bestand der Kasse entnommen, in dem die Petentin als rentenversicherungspflichtige Pflegeperson gespeichert sei. Diese Antwort zur Herkunft der Daten war allerdings nicht überzeugend, insbesondere weil dadurch nicht erklärt ist, wie die Kasse an die Daten der übrigen Mitarbeiter der betreffenden Klinik gelangt ist.

Die Kasse hat den im Raum stehenden Verdacht, sie habe die Daten von dem Arbeitgeber der Petentin erhalten, weiterhin zurückgewiesen und nunmehr erklärt, die Daten über persönliche Beziehungen aus dem Umfeld des Krankenhauses, bei dem die Petentin beschäftigt war, erhalten zu haben. Die genauen Quellen seien nicht bekannt und deshalb nicht zurückverfolgbar.

Die geschilderte Vorgehensweise entsprach nicht der oben erwähnten Vorschrift des § 284 Abs. 4 SGB V und wäre nur bei Vorlage einer schriftlichen Einwilligungserklärung der Mitarbeiter der Klinik zulässig gewesen. Von einer Beanstandung wurde abgesehen, weil die Kasse versichert hat, dass Verstöße dieser Art in Zukunft nicht mehr erfolgen werden und der Vorstand der Kasse seine Geschäftsstellen auf die strikte Einhaltung des Datenschutzes bei Werbemaßnahmen zur Mitgliedergewinnung hingewiesen habe.

In einem anderen Fall hat sich ein ehemaliges Mitglied einer Kasse darüber beschwert, dass es von dieser Kasse Werbepost erhalten hatte.

Der Petent fühlte sich durch dieses Anschreiben belästigt, zumal die Kasse angekündigt hatte, ihn in den nächsten Tagen auch noch telefonisch anzusprechen.

Ich teile die Auffassung meines Vorgängers, dass die Nutzung der Daten ehemaliger Mitglieder einer Krankenkasse zu Werbezwecken nicht zulässig ist. Denn eigentlich müssten die Daten nach Beendigung der Mitgliedschaft gelöscht werden, weil sie zur Aufgabenerfüllung der Krankenkasse nicht mehr erforderlich sind. Zwar hat die Krankenkasse überzeugend dargelegt, dass es eine Vielzahl von Anlässen gibt, die den Zugriff auf die gespeicherten Daten im Interesse der Betroffenen weiterhin erforderlich macht. Allerdings sind die gespeicherten Daten dann zu sperren, was bedeutet, dass die Daten nur noch für bestimmte, im SGB V genau bestimmte Zwecke verwandt werden dürfen. Eine Nutzung zu Werbezwecken erfüllt aber keine der dort genannten Voraussetzungen. Insbesondere ist es nicht aus im überwiegenden Interesse der verantwortlichen Stelle liegenden Gründen unerlässlich, die Daten zu Werbezwecken zu nutzen. Werbemaßnahmen sind auch in anderer Form möglich, z.B. in dem das Mitglied bei seinem Ausscheiden befragt wird, ob eine spätere Kontaktauf-

nahme gewünscht ist. Eine solche Verfahrensweise entspricht am Besten der Interessenlage der Betroffenen; denn grundsätzlich hat der Betroffene durch die Beendigung seiner Mitgliedschaft gerade zum Ausdruck gebracht, dass er kein Interesse mehr an einem Kontakt mit der Kasse hat. Deshalb muss die Kasse das ehemalige Mitglied fragen, ob es weiterhin mit der Zusendung von Informationsmaterialien einverstanden ist.

In einem weiteren Fall wurde von einer Krankenkasse die Frage gestellt, ob es zulässig ist, zur Durchführung einer Werbeaktion Adressdaten potentieller Kassenwechsler von einem Adresshändler zu erwerben. Da die nach bestimmten Selektionskriterien aufbereiteten Datensätze eines Adresshändlers keine „öffentlich zugänglichen Daten“ im Sinne des § 284 Abs. 4 SGB V sind, können solche Daten nicht zu Werbezwecken genutzt werden.

Die betreffende Krankenkasse hat daraufhin von der beabsichtigten Werbeaktion Abstand genommen.

10 Geodaten

10.1 Geodateninfrastrukturgesetz

Im März 2009 wurde der Entwurf eines saarländischen Geodateninfrastrukturgesetzes (SGDIG) vorgelegt. Das Gesetz dient der Umsetzung der Richtlinie 2007/2/EG des Europäischen Parlaments, der INSPIRE-Richtlinie (Infrastructure for Spatial Information in the European Community).

Die rechtlichen Rahmenbedingungen sollen es ermöglichen, Geodienste in allen EU-Mitgliedstaaten zur vereinheitlichen und zu nutzen. Dabei kommt einer Standardisierung der Geodaten selbst und der zugehörigen Datenbankstrukturen eine erhebliche Bedeutung zu.

Die aufzubauende europäische Geodatenstruktur kann dabei die Nutzung dieser Daten über die verschiedenen Verwaltungsebenen hinweg gewährleisten und politische Ziele unterstützen, die mittelbare oder unmittelbare Wirkungen auf die Umwelt haben können.

Im Bund und den Ländern wurden Festlegungen für die Begrifflichkeiten der INSPIRE-Richtlinie erarbeitet und in den jeweiligen Landesgesetzen aufgenommen. Großer Wert wurde darauf gelegt, dass Geodaten soweit sie personenbezogen sind, geschützt werden. Das SGDIG vom 1. Juli 2009 berücksichtigt dies im § 11: „Soweit durch den Zugang zu Geodaten personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden … ist der Zugang zu beschränken, es sei denn die Betroffenen haben zugestimmt oder das öffentliche Interesse an dem Zugang überwiegt.“ Die Formulierung wurde mit meiner Dienststelle abgestimmt.

10.2 Solarkataster

Bereits Ende 2008 trat der Landkreis Saarlouis an uns heran mit der Bitte um datenschutzrechtliche Prüfung, ob und in welcher Form ein Solarkataster im Internet veröffentlicht werden könne.

Bei der Überfliegung der Gemeinden werden Daten gewonnen, die mittels einer speziellen Software ausgewertet werden und als Ergebnis konkrete Werte liefern, ob das Dach eines Hauses für die Installation einer Photovoltaikanlage geeignet ist. Die erzeugten Daten sind ziemlich präzise und geben die Größe der möglichen Anlage, den Wirkungsgrad, die mögliche Jahresleistung und weitere Daten an. Die Darstellung der Werte sollte im Internet in Satellitenbilddarstellung erfolgen (ähnlich wie in Google-maps) und durch farbliche Kennzeichnung zuerst einmal angeben, ob die Dachfläche eines Hauses vom Nutzungsgrad her überhaupt für eine Installation geeignet ist. Durch Anklicken des Grundstückes sollte sich ein „Fenster“ öffnen, in dem die genauen Werte wiedergegeben werden sollten.

Entsprechende Internetveröffentlichungen seien bereits in Baden-Württemberg und Nordrhein-Westfalen erfolgt. Die Datenschutzbeauftragten dort seien mit der detaillierten Veröffentlichung einverstanden gewesen.

Unsere Recherchen ergaben, dass diese Veröffentlichungen tatsächlich existierten, dass sie aber nicht ohne datenschutzrechtliche Bedenken der zuständigen Datenschutzbeauftragten erfolgten. Bei dem Solarpotenzial von Gebäuden, die im Eigentum von natürlichen Personen stehen, handelt es sich um Angaben über deren sachliche Verhältnisse, mithin um personenbezogene Daten im Sinne des Landesdatenschutzgesetzes für deren Veröffentlichung es keine gesetzliche Grundlage gibt.

Der oftmals von wirtschaftspolitischen Erwägungen getragene Wunsch, Handwerker und potentielle Käufer über das Solarpotential zu informieren, widerspricht dem Recht auf informationelle Selbstbestimmung. Nach Artikel 2 der Saarländischen Verfassung hat jeder Bürger Anspruch auf Schutz seiner personenbezogenen Daten Eingriffe sind nur in überwiegendem Interesse der Allgemeinheit auf Grund eines

Gesetzes zulässig. Es ist nicht nachvollziehbar, inwiefern eine als eher lästig empfundene Werbung durch Handwerker im allgemeinen Interesse liegen soll.

In Gesprächen mit dem saarländischen Umweltministerium konnte eine datenschutzfreundliche Regelung vereinbart werden, die vorsieht, dass die Veröffentlichung des Solarkatasters sich auf eine rechtliche Grundlage stützen kann. Das Saarländische Erneuerbare-Energien-Wärmegesetz soll einen entsprechenden Passus erhalten. Die Absicht der Veröffentlichung ist in der Presse vorab bekannt zu geben, damit die betroffenen Eigentümer von ihrem jederzeitigen Widerspruchsrecht Gebrauch machen können.

Über das Internet werden zunächst nur farblich markierte Dachflächen angezeigt, die Auskunft darüber geben, ob das Dach gut geeignet, geeignet oder nicht geeignet für die Erzeugung von Elektrizität durch Photovoltaikanlagen ist. Die genauen Werte kann der Eigentümer dann bei seiner Gemeinde erfragen.

11 Gesundheit

11.1 Ärztebewertungsportal der AOKen

Die AOKen sind dabei in Zusammenarbeit mit der Bertelsmann-Stiftung ein Ärztebewertungsportal zu errichten.

AOK-Versicherte können in einer Online-Befragung Auskunft zu ihren Erfahrungen beim Arztbesuch geben. Gestartet ist das Bewertungsportal im Juni 2010 zunächst in den Pilotregionen Hamburg, Berlin und Thüringen. Nach und nach soll das Projekt bundesweit ausgedehnt werden.

An der Befragung teilnehmen können lediglich AOK-Mitglieder, die sich unter Angabe ihrer Krankenversichertennummer und der Kassennummer einloggen, darüber als AOK-Mitglied identifiziert werden und über eine E-Mail-Adresse die Zugangsberechtigung auf das Bewertungsportal erhalten. Da in diesem Registrierungsprozess Sozialdaten verarbeitet werden, hat sich die Frage der Zulässigkeit dieser Datenverarbeitung durch die AOKen gestellt. Im SGB V (Sozialgesetzbuch 5. Buch – Gesetzliche Krankenversicherung) sind die Zwecke, für die die Krankenkassen Daten ihrer Versicherten verarbeiten dürfen, abschließend geregelt. Ich meine, dass sich die Befugnis zur Verarbeitung von Sozialdaten im vorliegenden Zusammenhang aus § 305 Abs. 3 Satz 1 SGB V ergibt, wonach die Krankenkassen ihre Versicherten umfassend über in der gesetzlichen Krankenversicherung zugelassene Leistungserbringer zu informieren haben. Hilfsweise kann auf die Einwilligung der Versicherten zurückgegriffen werden, da der Bewertende seine Krankenversichertennummer freiwillig angibt.

Die andere und auch entscheidendere Frage ist, ob die Ärzte die Veröffentlichung der Bewertungen im Internet dulden müssen. Hier stehen sich das informationelle Selbstbestimmungsrecht der betroffenen Ärzte und die öffentliche Aufgabe der Qualitätssicherung im Gesundheitswesen gegenüber.

Die AOKen haben verschiedene Maßnahmen vorgesehen, um eine unangemessene Benachteiligung von Ärzten zu verhindern:

- Wertungen sind nur anhand eines vorgegebenen Fragebogens möglich. Es sind keine Freitextfelder vorgesehen, wodurch Diffamierungen durch Patienten ausgeschlossen sind.

- Ergebnisse zu den jeweiligen Ärzten werden erst veröffentlicht, wenn ein Arzt eine zweistellige Mindestanzahl an Beurteilungen erhalten hat.

- Die beurteilten Ärzte haben die Möglichkeit, ihre Befragungsergebnisse zu kommentieren. Ärzte können die Ergebnisse auch komplett sperren.

- Durch die Registrierung der Bewertenden über die Krankenversichertennummer werden verzerrende Mehrfachbewertungen verhindert.

Im Ergebnis habe ich keine durchgreifenden datenschutzrechtlichen Bedenken gegen die Einführung des Bewertungsportals in der beschriebenen Ausgestaltung.

11.2 COSYCONET-Studie

Im Berichtszeitraum hat meine Dienststelle zusammen mit drei weiteren Landesdatenschutzbeauftragten die Verantwortlichen eines wissenschaftlichen Forschungsvorhabens beraten.

Das Ziel der Studie besteht darin, insgesamt 3.000 Patienten, die an einer chronisch-obstruktiven Lungenerkrankung (COPD) erkrankt sind, darauf zu untersuchen, welche Begleiterkrankungen vorliegen und wie diese sich im Laufe der Zeit entwickeln. Vorgesehen sind umfangreiche körperliche Untersuchungen sowie die Entnahme von Biomaterialien (Blut-, Urin- und Atemwegsprobe).

Die medizinischen Daten mit Angaben über den Gesundheitszustand und die Ergebnisse von Fragebögen und Tests werden an der Medizinischen Hochschule Hannover in einer zentralen Datenbank gespeichert.

In der Biomaterialbank des Universitätsklinikums des Saarlandes werden die probenbezogenen Daten gespeichert. Soweit Computertomographie-Bilder vorliegen, werden diese in einer Bilddatenbank der Universität Heidelberg gespeichert.

Die Speicherung der Daten in den verschiedenen Datenbanken erfolgt unter einem Pseudonym. Die Studienteilnehmer werden in Patienteninformationen über die Durchführung der Studie aufgeklärt.

Die Studienleitung hatte in einem umfangreichen Datenschutzkonzept die Datenverarbeitung im Einzelnen beschrieben sowie Formulare zur Patienteninformation und Einwilligungserklärungen entworfen.

In der Diskussion mit den Forschern konnten noch einige Verbesserungen des ansonsten sorgfältig erarbeiteten Konzeptes erreicht werden:

- Die Verantwortlichkeiten im Rahmen der Studie waren nicht eindeutig geregelt. So war nicht klar, wer für das IT- und Datenschutzkonzept verantwortlich zeichnet. Es erfolgte eine Klarstellung – auch in der Patienteninformation – dass der sogenannte Führungskreis die Grundsatzentscheidungen trifft und dass die einzelnen Kooperationspartner die Verantwortung für die Einhaltung des Datenschutzes vor Ort haben.

- In den Patienteninformationen fehlte ein Hinweis, unter welchen Voraussetzungen die pseudonymisierten Daten wieder entschlüsselt werden. Dies wurde dahingehend klargestellt, dass dies nur dann der Fall ist, wenn man den Probanden die Teilnahme an einer eventuellen neuen Studie anbieten möchte.

- Es wurde in den Patienteninformationen verdeutlicht, gegenüber welcher Stelle der Studienteilnehmer seine Rechte auf Auskunft und Löschung geltend machen kann.

- Die Einwilligungserklärung zur Speicherung der Blutproben in der Biomaterialdatenbank wurde dahingehend präzisiert, dass die Daten allein zu dem Zweck der

Erforschung der COPD und ihrer Ursachen sowie verwandter Störungen verwandt werden dürfen.

Dem daraufhin aktualisierten Datenschutzkonzept konnte bescheinigt werden, dass alle datenschutzrechtlichen Anforderungen erfüllt sind.

11.3 Mammographie-Screening

Im Dezember 2006 wurde im Saarland mit dem Mammographie-Screening begonnen. Mammographie-Screening bedeutet, dass jede Frau im Alter zwischen 50 und 69 Jahren alle zwei Jahre das Recht auf eine kostenlose Brustkrebs-Vorsorgeuntersuchung hat. Im Saarland ist das Mammographie-Screening eine Gemeinschaftsaktion verschiedener Krankenkassen, der Kassenärztlichen Vereinigung Saarland sowie des Ministeriums für Gesundheit und Verbraucherschutz.

Es liegt auf der Hand, dass hier besonders sensible Daten verarbeitet werden. Und manche Frau wird sich fragen, ob ausreichend Vorkehrungen getroffen sind, dass ihre Persönlichkeitsrechte gewahrt sind.

An der Durchführung des Mammographie-Screenings sind verschiedene Stellen beteiligt:

- Die „Zentrale Stelle“ beim Ministerium für Gesundheit und Verbraucherschutz, die aufgrund von Melderegisterdaten die Frauen zur Untersuchung einlädt.

- Die Mammographie-Einheiten, die die eigentliche Untersuchung durchführen.

- Das Referenzzentrum, das unter anderem prüft, ob die mit dem Mammographie-Screening verfolgten Ziele erreicht werden.

- Das Saarländische Krebsregister, das aufgrund der bei diesem gemeldeten Krebsfälle Auskunft darüber geben kann, ob eine Brustkrebserkrankung von den Mammographie-Einheiten möglicherweise nicht entdeckt wurde.

Durch ein ausgeklügeltes System der Bildung von Kontrollnummern, Screening-Identifikationsnummern sowie Kommunikationsnummern ist es gelungen, dass Kenntnis von den medizinischen Daten lediglich die Mammographie-Einheit erhält, die die Untersuchung durchführt. Insofern können wir verunsicherte Frauen beruhigen, was allerdings nicht ausschließt, dass verschiedentlich Fragestellungen auftauchen, die einer Lösung bedürfen.

So wurde im Berichtszeitraum bundesweit diskutiert, ob es hinnehmbar ist, wenn auf dem Briefumschlag für die Einladung zur Mammographie erkennbar ist, dass es sich um eine solche Einladung handelt. Denn immerhin wird damit jedem, der den Briefumschlag sieht, bekannt, dass die Adressatin zwischen 50 und 69 Jahre als ist und einen Termin zum Mammographie-Screening hat.

Erfreulicherweise hatte man im Saarland diese Problematik erkannt und als Absenderangabe die unverfängliche Aufschrift „Gesundheitsberichterstattung Saarland“ gewählt.

11.4 Prüfung eines Krankenhauses

Im Berichtszeitraum wurde eine Datenschutzprüfung bei einem Krankenhaus durchgeführt.

Schwerpunkte waren die Prüfung allgemeiner organisatorischer Maßnahmen zum Datenschutz, die Prüfung der Personalabteilung, der Patientenaufnahme sowie der Wahrung der Vertraulichkeit der Patientenunterlagen in den Stationen.

Insgesamt war der Eindruck positiv, was die Umsetzung datenschutzrechtlicher Maßnahmen in der betreffenden Klinik betrifft. Es waren lediglich kleinere Mängel festzustellen, die mittlerweile behoben bzw. deren Beseitigung angekündigt ist.

Ein Grund für dieses positive Ergebnis liegt u. a. darin, dass die Klinikleitung einen externen Datenschutzbeauftragten bestellt hat, der sich hauptberuflich um die Datenschutzbelange von Krankenhäusern kümmert. Die Klinik, eine Unternehmensgruppe, hat zusätzlich für jedes Haus einen sogenannten Datenschutzkoordinator bestellt. Es sind somit immer ausreichend Personen vorhanden, die die Einhaltung des Datenschutzes in der Klinik überwachen und an die sich Patienten und Mitarbeiter bei datenschutzrechtlichen Anliegen wenden können. Besonders hilfreich ist in diesem Zusammenhang die Erstellung eines Datenschutz-Handbuches, in dem alle wesentlichen Punkte geregelt sind, die beim Umgang mit personenbezogenen Daten im Krankenhaus zu beachten sind (Erhebung und Übermittlung von Daten, Auskunftsrecht der Betroffenen, Aufbewahrungsfristen/Löschung, Auftragsdatenverarbeitung, Maßnahmen gegen unbefugten Zugriff, Entsorgung von Datenträgern, Zugang zu Archivräumen).

Bei dem Datenschutzbeauftragten waren Verfahrensübersichten über alle im Klinikum eingesetzten Verfahren zur Verarbeitung personenbezogener Daten vorhanden. Der Datenschutzbeauftragte führt regelmäßig Kontrollen der Datenverarbeitung in der Verwaltung und den Stationen durch. Es wurde festgestellt, dass alle Mitarbeiter, die bei ihrer Tätigkeit Umgang mit personenbezogenen Daten haben, auf das Datengeheimnis verpflichtet wurden.

Insgesamt ist festzustellen, dass die Klinik ausreichende organisatorische Maßnahmen getroffen hat, um einen effektiven Patientendatenschutz zu gewährleisten. So wurden keine Patientenakten oder sonstige schriftliche Aufzeichnungen von Patientendaten vorgefunden, die für Unbefugte zugänglich gewesen wären. Die Türen der Patientenzimmer sind nicht mit den Namen der Patienten beschriftet. Die Wartebereiche sind so gestaltet, dass andere Patienten Gespräche nicht mithören können.

Im Rahmen der Prüfung der Personalabteilung wurde Einsicht in eine Stichprobe von Personalakten genommen und das eingesetzte Gehaltsabrechnungsprogramm überprüft.

Die Führung der Personalakten ergab keinen Anlass zu Beanstandungen. Insbesondere wurden in den Personalakten keine Eintragungen festgestellt, die nicht Inhalt einer Personalakte sein dürfen.

Keinen Anlass zur Kritik gab auch die Aufbewahrung der Personalakten. Diese waren vor einem Zugriff Unbefugter gesichert aufbewahrt.

Lediglich bei dem eingesetzten Gehaltsabrechnungsprogramm gab es einige kleinere Mängel:

- In dem Programm waren Felder vorgegeben, die für die Zwecke der Klinik nicht erforderlich sind und dementsprechend auch nicht ausgefüllt werden (z.B. „Berufskrankheit“, „Schuhgröße“). Um auszuschließen, dass hier nicht erforderliche, und damit datenschutzrechtlich unzulässige Eintragungen vorgenommen werden, müssen die entsprechenden Felder für eine Eintragung gesperrt werden.

- Das Programm verlangt zwingend die Eingabe des Prozentsatzes der Behinderung. Da die Angabe des genauen Grades der Behinderung nicht erforderlich ist, darf in dem Programm nur die Schwerbehinderteneigenschaft, nicht aber der genaue Prozentsatz erfasst werden.

- Es waren noch keine Festlegungen getroffen worden, wann die einzelnen Daten zu löschen sind. Nach den datenschutzrechtlichen Vorschriften sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgabe nicht mehr erforderlich ist.

Die Klinikleitung hat mittlerweile das Programm entsprechend geändert bzw. die Festlegung von Löschungsfristen zugesagt.

11.5 Zugriff auf Patientendaten im Krankenhaus

Im Krankenhaus sind an der Behandlung eines Patienten eine Vielzahl von Personen beteiligt (Ärzte, Pflegekräfte, Physiotherapeuten, Röntgenfachkräfte usw.). Dennoch bildet das Krankenhaus keine informationelle Einheit, bei der alle an der Behandlung Beteiligten auf alle Daten aller Patienten zugreifen dürfen. Dieser Grundsatz ist ausdrücklich in den Vorschriften des Saarländischen Krankenhausgesetzes zum Patientendatenschutz niedergelegt. Es heißt dort in § 12 Abs. 3: „Die Weitergabe von Patientendaten an andere Fachabteilungen innerhalb des Krankenhauses oder an den Sozialdienst im Krankenhaus ist nur zulässig, soweit sie für die Behandlung oder soziale Betreuung von Patientinnen oder Patienten erforderlich sind. Im Rahmen der Aus-, Weiter- und Fortbildung von Ärztinnen und Ärzten, Zahnärztinnen und Zahnärzten, Apothekerinnen und Apothekern, Psychologischen Psychotherapeutinnen und Psychotherapeuten, Kinder- und Jugendlichen-Psychotherapeutinnen und –therapeuten und Angehörigen der Gesundheitsfachberufe ist zu gewährleisten, dass auf Patientendaten nur insoweit zugegriffen wird, als dies für die dem Berufsbild entsprechenden Funktionen erforderlich ist und diese Zwecke nicht mit anonymisierten Daten erreicht werden können. Die Nutzung der Patientendaten durch die Krankenhausverwaltung darf nur in dem Maß erfolgen, wie dies für die Abwicklung des Behandlungsfalles erforderlich ist.“

In der Praxis sind diese Grundsätze allerdings vielfach nicht umgesetzt, was seine Ursache u. a. darin hat, dass die Krankenhäuser von den Herstellern der Krankenhausinformationssysteme abhängig sind und die gängigen Krankenhausinformationssysteme nur eine Zuordnung nach Rollen (Fachrichtungen, Stationen usw.) vornehmen. So kommt es vor, dass – wie ein Kollege aus einem anderen Bundesland in einem konkreten Fall festgestellt hat – ca. 100 Mitarbeiter auf die Daten eines konkreten Patienten zugreifen könnten, obwohl allenfalls ca. 20 Mitarbeiter tatsächlich mit diesem Patienten zu tun gehabt hatten.

Erwähnenswert ist in diesem Zusammenhang ein Urteil des Europäischen Gerichtshofes für Menschenrechte vom 17. Juli 2008, in dem ein Krankenhaus zu Schadensersatz verurteilt worden ist, weil dieses in seinem Informationssystem keine Protokol-

lierung der Zugriffe auf Patientendaten vorgesehen hatte. Eine an AIDS erkrankte Mitarbeiterin des Krankenhauses hatte sich dort behandeln lassen. Ein anderer Krankenhausmitarbeiter hat dies der Krankenhausverwaltung mitgeteilt, worauf der Mitarbeiterin gekündigt worden war.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich auf ihrer Konferenz am 8. und 9. Oktober 2009 mit der Thematik befasst und fordert in einer Entschließung (Anlage 18.10) die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten einschließlich einer ordnungsgemäßen Protokollierung in der Informationstechnik von Krankenhäusern.

Es wurde eine Arbeitsgruppe mit Experten aus den Datenschutzaufsichtsbehörden des Bundes und der Länder gebildet, die zu dieser schwierigen Thematik eine Orientierungshilfe erarbeitet, in der sowohl die normativen Eckpunkte als auch die technischen Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen dargestellt werden sollen.

12 Schule und Bildung

12.1 Aufzeichnung von Drohanrufen in saarländischen Schulen

Im Rahmen der Errichtung von Notfallplänen an Schulen wurde im Kreise der Datenschutzbeauftragten diskutiert, ob der Mitschnitt von Telefongesprächen an Schulen im Falle der telefonischen Androhung einer Straftat gegen die Schule zulässig ist.

Entgegen anderslautender Meinungen diverser Bundesländer, die einen Mitschnitt als Verstoß gegen das verfassungsrechtlich verankerte Recht am gesprochenen Wort werten und keine gesetzliche Grundlage für diese Art der Datenverarbeitung sehen, vertreten wir die Auffassung, dass eine Datenverarbeitung in oben genannter Fallkonstellation im Saarland durchaus rechtmäßig ist.

Gemäß § 2 Abs. 3 der Verordnung über die Verarbeitung personenbezogener Daten in saarländischen Schulen gelten, soweit in dieser Verordnung nichts Näheres bestimmt ist, die Bestimmungen des Saarländischen Datenschutzgesetzes. Da die Aufzeichnung von Telefonaten in Notfällen an Schulen in dieser Verordnung nicht näher ausgeführt wird, ist die Regelung des § 4 Abs. 2 Nr. 6 SDSG als legitimierend anzusehen. Demnach ist die Verarbeitung selbst besonders schützenswerter personenbezogener Daten zulässig, soweit die Datenverarbeitung zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Strafverfolgung erforderlich ist. Sowohl die Datenerhebung gemäß § 12 Abs. 2 SDSG als auch das Speichern der Telefongespräche gemäß § 13 Abs. 2 Satz 1 Buchstabe e SDSG ist zum Schutz von Leben und Gesundheit legitim.

Die Aufzeichnung der Telefongespräche darf jedoch nur unter bestimmten Rahmenbedingungen erfolgen. So muss eine genaue Festlegung der Voraussetzungen erfolgen, unter denen die Gespräche aufgezeichnet werden dürfen. Eine pauschale Aufzeichnung aller bei einer Schule eingehenden Telefonate wäre unzulässig. Des Weiteren muss die Dauer der Speicherung solcher Aufzeichnungen derart geregelt werden, dass die Telefonate unverzüglich zu löschen sind, sobald sie für den Zweck der Strafverfolgung oder zur Abwehr von Gefahren nicht mehr erforderlich sind.

12.2 Behördliche Datenschutzbeauftragte an Schulen

In einer Umfrage an die Datenschutzbeauftragten der Länder wurde aus Baden-Württemberg die Frage gestellt, in welchen Bundesländern eine Verpflichtung zur Bestellung behördlicher Datenschutzbeauftragter im Schulbereich besteht und inwieweit datenschutzrechtlichen Defiziten durch die Bestellung eines Datenschutzbeauftragten entgegengewirkt werden kann.

Für das Saarland können allgemein gemäß § 8 Abs. 1 SDSG behördliche Datenschutzbeauftragte schriftlich bestellt werden, eine Verpflichtung dazu besteht jedoch nicht. Speziell im Schulbereich wird gemäß § 3 Abs. 11 der Verordnung über die Verarbeitung personenbezogener Daten in Schulen geregelt, dass die Schule in Abstimmung mit der Schulaufsichtsbehörde einen behördlichen Datenschutzbeauftragten bestellen kann. Auch die Bestellung eines gemeinsamen Datenschutzbeauftragten für mehrere Schulen ist nach dieser Vorschrift möglich.

Bei der Anfrage im federführenden Ministerium für Bildung, ob im Schulbereich von der Möglichkeit zur Bestellung eines Datenschutzbeauftragten nach § 3 Abs. 11 der Verordnung über die Verarbeitung personenbezogener Daten in Schulen Gebrauch gemacht wurde, konnte uns keine einzige Schule benannt werden, die zur Verbesserung datenschutzrechtlicher Defizite an Schulen einen Datenschutzbeauftragten bestellt hat.

In Zeiten immer umfassender werdender Datenverarbeitung durch Schulen, sei es durch automatisierte Erfassung von Schulnoten und Schülerdaten, durch e-Learning-Programme oder Fehlzeitenerfassung der Lehrer, stellt die Berufung eines schulinternen Datenschutzbeauftragten ein probates Mittel dar, die datenschutzrechtlichen Defizite bei der Umsetzung solcher Projekte vor Ort zu minimieren. Es wäre auch begrüßenswert, wenn bei der Erstellung einer Schulhomepage der Datenschutzbeauftragte einer Schule involviert werden könnte und vor der Veröffentlichung unzulässiger Daten einschreiten könnte.

12.3 Online Noten- und Klassenbuch

Immer wieder werden wir von Seiten des Ministeriums für Bildung oder den Herstellern selbst gefragt, ob serverbasierte Dienstleistungen für Lehrer zur Verwaltung von Noten, Fehlzeiten, Klassenbucheintragungen oder Stundenplänen aus datenschutzrechtlicher Sicht zulässig sind.

Die Freigabe solcher Programme obliegt der obersten Dienstbehörde, hier dem Ministerium für Bildung. Im Vorfeld der Freigabe ist gemäß § 7 Abs. 2 SDSG der oder die Landesbeauftragte für Datenschutz zu hören.

Gemäß § 20 b Abs. 5 des saarländischen Schulordnungsgesetzes (SchoG) wird die Schulaufsichtsbehörde ermächtigt, für personenbezogene Daten unter anderem den zulässigen Umfang der Erhebung, Verarbeitung und sonstige Nutzung von Daten durch Rechtsverordnung im Einzelnen zu regeln. Dies wurde mit der Verordnung über die Verarbeitung personenbezogener Daten in Schulen umgesetzt.

Gemäß § 2 Abs. 4 der Verordnung ist den Lehrkräften zur Erfüllung ihrer Dienstpflichten gestattet, dass sie folgende Daten der Schülerinnen und Schüler auf Datenverarbeitungsgeräten außerhalb der Schulgebäude verarbeiten dürfen:

Name, Vorname, Geburtsdatum, Anschrift, Anschrift der Erziehungsberechtigten, Kommunikationsverbindungen, Klassen-/ Jahrgangsstufe, Klassen-/ Kurs-/ Lerngruppenbezeichnung, Unterrichtsfächer, Leistungsdaten.

Es handelt sich hierbei um eine abschließende Aufzählung der zulässigen Daten, die Lehrer auf Ihrem Heim-PC verarbeiten dürfen. Die Dokumentation von Fehlverhalten der Schülern während des Unterrichtes sowie die Datenverarbeitung, die über den in der Verordnung vorgegebenen Rahmen hinausgehen, ist laut Gesetzestext nicht legitim. Der Abruf dieser Daten über das Internet vom Heim-PC eines Lehrers ist unzulässig, da es sich auch hierbei um eine Datenverarbeitung handelt.

Gemäß § 4 Abs. 4 SDSG hat sich bei der Verarbeitung personenbezogener Daten die Art der Datenverarbeitung sowie die Auswahl und Gestaltung hierzu bestimmter technischer Einrichtungen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten (Grundsatz der Datenvermeidung und Datensparsamkeit).

Eine webbasierte Version des elektronischen Klassen- oder Notenbuches hat zur Folge, dass auf dem, unter Umständen im Ausland stationierten Webserver der Firma die Daten sämtlicher Schüler, Erziehungsberechtigten und Lehrer gespeichert werden. Es stellt sich die Frage, ob die mit der Führung eines elektronischen Klassen- oder Notenbuches verbundenen Vorteile eine solche Datenspeicherung auf einem im Ausland befindlichen Server rechtfertigen, zumal die Möglichkeit einer effektiven Datenschutzkontrolle sowohl durch die Schule als Auftraggeber, als auch durch unsere Dienststelle mehr als zweifelhaft erscheint.

Unseren Ausführungen folgend hat sich das Ministerium für Bildung dazu entschlossen, keine Freigabe für webbasierte Dienstleistungen zur Verarbeitung von Schülerdaten durch Lehrer zu genehmigen.

Für die Zukunft bleibt abzuwarten, wie sich der Umgang mit technischen Hilfsmitteln für Lehrer aber auch für Schüler und Eltern, mit denen personenbezogene Daten verarbeitet werden können, in der Praxis entwickelt. Eine ständige Modifizierung der Verordnung über die Verarbeitung personenbezogener Daten in Schulen wird erforderlich sein, um der praxisorientierten Anpassung an den technischen Fortschritt Stand zu halten.

12.4 Einführung der Schulbuchausleihe im Saarland

Die Saarländische Landesregierung hat beschlossen, zum Schuljahresbeginn 2009/2010 ein Schulbuchausleihsystem einzuführen, das die Familien finanziell entlasten soll.

Im Rahmen der organisatorischen Umsetzung wurde meine Dienststelle beratend hinzugezogen, um den datenschutzrechtlichen Aspekt des Vorhabens zu begleiten. Die Teilnahme an dem Ausleihverfahren ist zwar freiwillig, hat man sich allerdings für eine Teilnahme entschieden, müssen aus organisatorischen Gründen viele Daten der Schüler und Eltern erhoben und in einer Schulbuchverwaltungssoftware verarbeitet werden. Schüler und Eltern, die im Rahmen des Schülerförderungsgesetz förderberechtigt sind, werden vom Leihentgelt befreit.

Sowohl die Schulbuchverwaltungssoftware als auch die Befreiung von der Zahlung des Leihentgeltes stellten aus datenschutzrechtlicher Sicht Probleme dar. So wurde die Forderung erhoben, dass im Rahmen der Schulbuchausleihe der Kreis der Personen, die auf die Verwaltungssoftware zugreifen dürfen, so klein wie möglich gehalten wird. Außerdem sollten die förderberechtigten Personen einen Berechtigungsschein erhalten, aus dem der Grund der Befreiung nicht hervorgeht. Dieser Berechtigungsschein darf nur einer zuvor bestimmten Person an der jeweiligen Schule, dem sogenannten Schulbuchkoordinator, aushändigt werden, der im Vorfeld auf den Datenschutz verpflichtet wurde. Die Aufbewahrung der Berechtigungsscheine zur Befreiung vom Leihentgelt in den Schulen darf nur in einem abschließbaren Stahlschrank erfolgen, zu dem lediglich der Schulbuchkoordinator Zugang hat.

Durch diese Maßnahmen soll sichergestellt werden, dass nur der Schulbuchkoordinator, nicht jedoch weitere Personen, die mit der Ausgabe der Schulbücher betraut sind, erkennen können, ob der Ausleihbetrag aufgrund der Einzahlung der Eltern oder aufgrund der Befreiung im Rahmen des Schülerförderungsgesetztes ausgeglichen wurde.

12.5 Vergleichsstudien an saarländischen Schulen

Auch im letzten Berichtszeitraum gab es im Saarland eine Menge Schultests, wie NEPS, PISA, „Bildungsstandards“ und ADDITION sowie Forschungsprojekte, wie „Kinder- und Jugendarmut im Saarland“, an denen sich Schüler, Lehrer und Eltern beteiligen sollten und die vom Ministerium für Bildung in Zusammenarbeit mit mir und meinen Mitarbeitern datenschutzrechtlich begleitet wurden.

Grundlage für die Datenerhebungen ist § 20 e Abs. 1 Saarländisches Schulordnungsgesetz (SchoG), wonach Schüler und Lehrer dazu verpflichtet sind, an den von der Schulaufsichtsbehörde oder in deren Auftrag durchgeführten Vergleichsuntersuchungen sowie an sonstigen von der Schulaufsichtsbehörde vorgesehenen Maßnahmen zur Qualitätssicherung und zur Qualitätsentwicklung teilzunehmen. Für Forschungsvorhaben gelten die Regelungen des § 20 c SchoG. Immer öfter ist festzustellen, dass das private und soziale Umfeld der Schüler ins Visier der Tester fällt. Auskünfte aus diesem Umfeld sind jedoch nicht durch die Regelungen im Schulordnungsgesetz abgedeckt und dürfen nur auf freiwilliger Basis erhoben werden. Auf freiwilliger Basis heißt in diesem Zusammenhang, dass Schüler unter 18 Jahren nur unter Einwilligung ihrer Eltern, Lehrer und Eltern nur unter der eigenen Einwilligung Auskünfte aus dem nicht schulischen Bereich geben dürfen. Vor der Erhebung der Daten müssen alle Beteiligten genau über den Verwendungszweck der Daten und über die Tatsache, dass bei Nichtbeteiligung keine Nachteile für Schüler und Eltern zu erwarten sind, aufgeklärt werden.

Um die datenschutzrechtlichen Belange bei Forschungsvorhaben an saarländischen Schule umzusetzen, wurde ergänzend zur Vorschrift des § 20 c SchoG die Verordnung über die Durchführung von Erhebungen zum Zwecke wissenschaftlicher Forschung in Schulen erlassen. Das Ministerium für Bildung, das in eigener Zuständigkeit die Zulässigkeit der Forschungsmaßnahmen prüft, hat in der Verordnung eine Art Leitfaden, wann ein Forschungsprojekt datenschutzgerecht gestaltet ist, zur Hand. Darüber hinaus stehen ich und meine Mitarbeiter dem Ministerium für Bildung jederzeit für weitergehende datenschutzrechtliche Fragen zur Verfügung.

12.6 Videokamera im Warteraum des schulpsychologischen Dienstes

Ein schulpsychologischer Dienst überlegte, in seinem Warteraum eine Videokamera zu installieren. Dies vor dem Hintergrund, dass im Rahmen schulpsychologischer Untersuchungen Elterngespräche ohne Anwesenheit der Kinder geführt werden und dass diese sich in dieser Zeit allein im Wartezimmer aufhalten. Besonders unruhige oder verhaltensauffällige Kinder benötigten hierbei Beaufsichtigung. Da eine Beaufsichtigung durch die Mitarbeiterin des Geschäftszimmers nicht immer sichergestellt werden könne, halte man die Anbringung einer Videokamera für eine gute Lösung.

Mein Vorgänger hat demgegenüber darauf hingewiesen, dass jede Form der Videoüberwachung einen Eingriff in das Persönlichkeitsrecht der davon betroffenen Personen darstellt, der nur zulässig ist, wenn es hierfür eine gesetzliche Grundlage gibt. Vorliegend sollte eine Videoüberwachung in nicht öffentlich zugänglichen Räumen erfolgen, so dass die Zulässigkeit der Maßnahme nach allgemeinem Datenschutzrecht zu beurteilen war. Die Zulässigkeit der Videoüberwachung hängt nach dessen Vorschriften von der Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit der Maßnahme ab.

Dem schulpsychologischen Dienst wurde mitgeteilt, dass unter Zugrundelegung dieser Maßstäbe eine Überwachung des Warteraumes datenschutzrechtlich bedenklich ist.

Unverhältnismäßig ist eine Überwachung auf jeden Fall, wenn sich auch Erwachsene in dem Raum aufhalten. Abgesehen davon, dass es in diesem Fall keinen Grund für eine Überwachung gibt, würden die Betroffenen unverhältnismäßig belastet, indem sie sich einer ständigen Überwachungssituation ausgesetzt sehen.

Keine praktikable Lösung wäre es, die Mitarbeiterin der Geschäftsstelle anzuweisen, die Videokamera nur einzuschalten, wenn sich unruhige oder verhaltensauffällige Kinder allein in dem Raum aufhalten. Denn einerseits besteht die Gefahr, dass die Kamera doch permanent eingeschaltet bleibt. Zu berücksichtigen ist aber vor allem,

dass die Videokamera sichtbar ist und ein entsprechendes Schild auf die Videoüberwachung hinweist, so dass für einen wartenden Erwachsenen nicht erkennbar wäre, ob die Anlage eingeschaltet ist oder nicht.

Zweifel sind auch angebracht, ob eine Videokamera überhaupt geeignet ist, den mit ihr verfolgten Zweck zu erreichen. So ist fraglich, ob die Mitarbeiterin des Geschäftszimmers den Bildschirm neben ihren sonstigen Arbeiten permanent so im Blick haben kann, dass sie im Ernstfall schnell genug reagieren kann, um einen Schaden abzuwenden.

Überlegenswert ist, ob es nicht andere Maßnahmen gibt, um eine effektive Aufsicht zu gewährleisten. Zu denken wäre hier an eine Gestaltung der Räumlichkeiten, die es der Mitarbeiterin in der Geschäftsstelle ermöglicht, wartende Kinder im Auge zu behalten. Eine andere Möglichkeit wäre auch, die Kinder im Geschäftszimmer warten zu lassen, zumal es wohl nicht sinnvoll ist, verhaltensauffällige Kinder längere Zeit in einem separaten Warteraum alleine zu lassen.

Der schulpsychologische Dienst hat daraufhin mitgeteilt, dass er aufgrund der von mir vorgebrachten Bedenken auf die Installation einer Videokamera in seinem Warteraum verzichtet.

13 Öffentlicher Dienst

13.1 Beihilfebearbeitung der bei der Beihilfestelle beschäftigten Beamten

Ein Mitarbeiter der Zentralen Beihilfestelle für saarländische Landesbedienstete informierte meine Dienststelle darüber, dass die Beihilfeanträge der in der Beihilfestelle beschäftigten Beamten durch den Sachgebietsleiter der Beihilfestelle beschieden werden. Zudem hatten durch verschiedene Zugriffsberechtigungen in der Beihilfebearbeitung der jeweils zuständige Mitarbeiter, Sachbearbeiter, Sachgebietsleiter, die Innenrevision und deren Vertreter Zugang zu den Beihilfedaten der Beihilfemitarbeiter. Nachdem wir die Beihilfestelle um Stellungnahme gebeten haben, konnten wir uns auf folgende Vorgehensweisen bei der Beihilfebearbeitung von Beihilfeanträgen der Mitarbeiter der Beihilfestelle einigen:

Da die Bearbeitung der Beihilfeanträge auf den Sachgebietsleiter und damit dem direkten Vorgesetzten der betreffenden Beamten übertragen wurde, bestand die Gefahr, dass medizinische Daten aus der Beihilfebearbeitung in Personalentscheidungen einfließen könnten. Der Bundesgesetzgeber hat diese Problematik erkannt und für Sozialleistungsträger die Vorschrift des § 35 Abs. 1 Satz 3 Erstes Buch Sozialgesetzbuch (SGB I) eingeführt, wonach Sozialdaten der Mitarbeiter von Sozialleistungsträgern Personen nicht zugänglich sein dürfen, die an Personalentscheidungen mitwirken. Nach Rücksprache mit der Beihilfestelle wurde die Beihilfebearbeitung auf einen Mitarbeiter des Landesamtes für Zentrale Dienste außerhalb der Organisation der Beihilfestelle übertragen.

Die Zugriffsberechtigung der Mitarbeiter der Beihilfestelle wurde im Vorfeld der Einführung des Beihilfebearbeitungsprogramms mit meiner Dienststelle abgestimmt und für zulässig erachtet. Dennoch muss im Rahmen der Beihilfebearbeitung der Beihilfemitarbeiter darauf geachtet werden, dass ein noch enger umfasster Kreis von Personen eine Zugriffsberechtigung auf diese Daten hat, da man beispielsweise durch die Bewilligung einer psychotherapeutischen Maßnahme auch auf die Erkrankung des Kollegen schließen kann. Als Lösung werden die Daten der Beihilfemitarbeiter

nicht mehr automatisiert erfasst, sondern in Papierform bearbeitet und anschließend unter Verschluss gehalten.

So konnte eine datenschutzgerechte Lösung der Beihilfebearbeitung von Mitarbeiteranträgen herbeigeführt werden.

13.2 Gesetz zum Beschäftigtendatenschutz

Ein wichtiger Bereich des Umgangs mit personenbezogenen Daten, von denen fast alle Menschen im Laufe ihres Lebens betroffen sind, ist die Erhebung und Nutzung von persönlichen Daten im Zusammenhang mit der Eingehung und Durchführung eines Beschäftigungsverhältnisses. Seit Jahrzehnten fordern die Datenschutzbeauftragten des Bundes und der Länder vergeblich, die damit im Zusammenhang stehenden Fragen in einem speziellen Gesetz zu regeln. Umso mehr ist es zu begrüßen, dass – wohl ausgelöst durch die Datenschutzskandale der letzten Jahre – die Bundesregierung nunmehr erstmals den Entwurf eines Beschäftigtendatenschutzgesetzes vorgelegt hat. Es geht darum, Rechtssicherheit herzustellen, Regelungslücken zu schließen und bereits vorhandene Regelungsaspekte sowie Vorgaben der Rechtsprechung in einem Spezialgesetz zusammenzufassen.

Das Thema war im Berichtszeitraum zweimal Gegenstand von Erörterungen auf der Konferenz der Datenschutzbeauftragten des Bundes und Länder. Auf ihrer Konferenz am 26. und 27. März 2009 haben die Datenschutzbeauftragten die unverzichtbaren Eckpunkte für einen Beschäftigtendatenschutz dargelegt (Anlage 18.5) In ihrer Entschließung vom 22. Juni 2010 (Anlage 18.20) haben sie ihre Kritikpunkte an dem vorgelegten Entwurf des Bundesministers des Innern zusammengefasst.

Der Gesetzentwurf befindet sich gegenwärtig in der parlamentarischen Beratung. Hinzuweisen ist auf zahlreiche konkrete Änderungsvorschläge des Bundesrates (Brat-Drs. 535/10).

Die Datenschutzbeauftragten des Bundes und der Länder werden sich weiterhin in die Diskussion einbringen, um einen angemessenen Ausgleich zwischen den Belangen der Arbeitgeber und den schutzwürdigen Rechtsgütern der Beschäftigten herzustellen.

13.3 Webcam an einer Abfall-Verwertungs-Anlage

Einen besonderen Service bieten Abfall-Verwertungs-Anlagen im Saarland ihren Kunden an: Es werden Bilder von der Zufahrt zur Verwertungsanlage ins Internet übertragen; potentielle Kunden können sich so einen Eindruck von dem Andrang an den Anlagen verschaffen.

Gegen den Einsatz von Netzwerkkameras zu diesem Zweck bestehen aus datenschutzrechtlicher Sicht grundsätzlich keine Bedenken. Es muss nur sichergestellt sein, dass auf den übertragenen Bildern weder Personen noch Autokennzeichen zu erkennen sind.

Dieser Problematik war man sich bewusst und hatte deshalb eine Verpixelung der Bilder vorgenommen. Allerdings war diese Verpixelung nicht ausreichend, wie uns durch den zuständigen Betriebsrat mitgeteilt wurde.

Der Betriebsrat hat uns Bilder vorgelegt, auf denen eindeutig Personen, in diesem Fall Mitarbeiter der Abfallverwertungsanlage, erkennbar waren.

Die von uns daraufhin angeschriebene Geschäftsleitung meinte, die Veröffentlichung von Daten von Mitarbeitern im Internet sei in diesem speziellen Fall zulässig und berief sich zur Begründung auf die Vorschrift des § 23 des Kunsturhebergesetzes, wonach Bilder veröffentlicht werden dürfen, auf denen Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen.

Dieser Rechtsauffassung konnte sich mein Vorgänger nicht anschließen. Er hat auf die Vorschrift des § 31 SDSG hingewiesen, der die Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen regelt. Nach dieser Vorschrift dürfen Daten von Beschäftigten nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Da offensichtlich keine dieser Voraussetzungen für eine Veröffentlichung von Bildern von Mitarbeitern im Internet vorlag, insbesondere die Durchführung des Arbeitsverhältnisses eine solche Übertragung nicht erfordert, wurde die Geschäftsführung der Abfallverwertungsanlage aufgefordert, durch technische Maßnahmen sicherzustellen, dass die Mitarbeiter im Internet nicht erkennbar sind.

Die Geschäftsleitung ist schließlich der Auffassung meines Vorgängers, die auch von mir geteilt wird, gefolgt und hat eine noch weitergehende Verpixelung vorgenommen, sodass nunmehr keine Personen, die sich im Übertragungsbereich der Kamera befinden, erkennbar sind.

14 Rundfunk und Medien, Telekommunikation

14.1 Änderung des Rundfunkstaatsvertrages – geräteunabhängiger Haushaltsbeitrag

Am 15. Dezember 2010 haben die Ministerpräsidenten der Bundesländer den 15. Rundfunkstaatsvertrag unterzeichnet.

Der Vertrag beinhaltet einen Systemwechsel in der Rundfunkfinanzierung: War bisher die Beitragspflicht an das Bereithalten eines Empfangsgerätes geknüpft, soll zukünftig jeder Haushalt eine Rundfunkgebühr bezahlen, unabhängig davon, ob und wie viele Empfangsgeräte betrieben werden.

Es ist zu begrüßen, dass die unter Datenschutzgesichtspunkten problematischen Ermittlungstätigkeiten der GEZ damit der Vergangenheit angehören sollen. Anlass zur Zufriedenheit gibt der geänderte Staatsvertrag allerdings nicht. Auf ihrer Datenschutzkonferenz am 11. Oktober 2010 haben sich die Datenschutzbeauftragten des Bundes und der Länder mit dem Entwurf befasst und ihre wesentlichen Kritikpunkte in einer Entschließung (Anlage 18.22) wie folgt zusammengefasst:

- Die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern sind auf das erforderliche Maß zu beschränken, der Direkterhebungsgrundsatz ist zu beachten und vor allem ist auf die Datenerhebung beim Adresshandel zu verzichten.

- Bei Befreiungsanträgen von Wohnungsinhabern aus sozialen Gründen wie Armut oder Behinderung soll nur die Vorlage einer Bestätigung des Leistungsträgers zulässig sein, auf die Vorlage der vollständigen Leistungsbescheide ist zu verzichten.

- Auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren sollte verzichtet werden, statt dessen sollte die Daten-

übermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht beschränkt werden.

Leider wurde diesen Kritikpunkten bei der Unterzeichnung des Staatsvertrages nicht Rechnung getragen. Falls der Vertrag wirksam wird, wurde die Chance, den Wechsel in der Rundfunkfinanzierung für ein Mehr an Datenschutz zu nutzen, vertan.

Bei Redaktionsschluss stand noch nicht fest, ob der Vertrag die erforderliche Zustimmung aller 16 Länderparlamente erhält.

15 Wirtschaft

15.1 Einheitlicher Ansprechpartner

Die EU-Dienstleitungsrichtlinie (2006/123/EG) hat zum Ziel, rechtliche und administrative Hindernisse für die grenzüberschreitende Erbringung von Dienstleistungen zu beseitigen. In vielen Bereichen werden für die Ausführung von Dienstleistungen Sach- und Fachkundenachweise verlangt, so zum Beispiel im Schornsteinfegerhandwerk. Damit in naher Zukunft ein reibungsloser Dienstleistungsverkehr im Binnenmarkt trotz unterschiedlicher bürokratischer Regelungen möglich ist, wurde es für notwendig erachtet, sogenannte einheitliche Ansprechpartner in den Ländern zu installieren, die bei der Abwicklung bürokratischer Formalitäten Hilfestellung leisten.

Die nationale Umsetzung der Dienstleitungsrichtlinie musste bis zum 28. Dezember 2009 erfolgen.

Im Kern bedeutete das für das Saarland den „einheitlichen Ansprechpartner“ zu benennen, der für Dienstleistungserbringer aus der EU das bürokratische Verfahren abwickelt und an ihn und die Dienstleistungsempfänger Auskünfte erteilt.

Die rechtlichen Voraussetzungen wurden durch das Gesetz über den einheitlichen Ansprechpartner (EA) für das Saarland vom 10. Februar 2010 geregelt. Der EA ist örtlich bei der IHK angesiedelt und wird von verschiedenen Kammern getragen.

Die Gesetzgebung und die dv-technische Umsetzung wurden durch die Dienststelle der LFDI begleitet.

15.2 Veröffentlichung von Subventionsempfängern im Agrarbereich

Die rechtliche Grundlage für die Veröffentlichung von Subventionsempfängern im Agrarbereich sind die Verordnungen EG Nr. 1290/2005 und 259/2008. Damit sollte Verwaltungshandeln nachvollziehbar und die notwendige Transparenz geschaffen werden. Bei Subventionen im Bereich des Europäischen Garantiefonds für die Landwirtschaft (EGFL) und dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) waren insbesondere zu veröffentlichen: Name, Vorname (bzw. juristische Person), Postleitzahl und Gemeinde sowie die Förderungsbeträge.

Im Berichtszeitraum erreichten uns zahlreiche telefonische Anfragen betroffener Personen, die ihr Recht auf informationelle Selbstbestimmung verletzt sahen. Die Veröffentlichungspraxis wurde von uns durchaus kritisch gesehen, da durch die Veröffentlichung der Schutz personenbezogener Daten (im Saarland werden landwirtschaftliche Betriebe in überwiegender Zahl von Einzelpersonen geführt) dem Informationsinteresse der Öffentlichkeit pauschal untergeordnet wurde.

Den Betroffenen konnte nur die für sie nicht zufriedenstellende Mitteilung gegeben werden, dass es sich um eine per Gesetz erlaubte und damit rechtlich zulässige Veröffentlichung handele, die allerdings durch anhängige Klagen beim Europäischen Gerichtshof überprüft werde.

Der Europäische Gerichtshof hat am 9. November 2010 entschieden, dass die Veröffentlichungen von EU-Subventionsempfängern im Agrarbereich in der durchgeführten Form nicht dem Gemeinschaftsrecht entsprechen.

16 Statistik

16.1 Zensus 2011 – Volkszählung

Im Berichtszeitraum wurden die rechtlichen Grundlagen für die Volkszählung des Jahres 2011 festgelegt und die für die Durchführung erforderlichen Gesetze erlassen. Hierzu zählen das Zensusgesetz 2011 vom 16. Juli 2009, die Stichprobenverordnung Zensusgesetz 2011 vom 25. Juni 2010 und die landesspezifischen Gesetze zur Ausführung des Zensusgesetzes 2011 (im Saarland vom 16. Juni 2010).

Die Volkszählung 2011 besteht im Wesentlichen aus der Auswertung von Registerdaten, der Haushaltsbefragung, der Gebäude- und Wohnungszählung, sowie der Befragung in Wohnheimen und Gemeinschaftsunterkünften.

Zur Vorbereitung der Gebäude- und Wohnungszählung wurden im November 2010 Fragebögen verschickt, die in erster Linie dazu dienten, Eigentumsverhältnisse auf einen aktuellen Stand zu bringen und dadurch einen reibungslosen Ablauf der eigentlichen Befragung im Mai 2011 zu gewährleisten.

Im Rahmen der ebenfalls im Mai stattfindenden Haushaltsbefragung werden im Saarland rund 130.000 Personen in ca. 30.000 Haushalten um Auskunft gebeten. Die Haushalte wurden unter Berücksichtigung methodisch-statistischer Verfahren durch das Bundesamt für Statistik ermittelt. Die jeweiligen Adressdaten werden den Statistischen Landesämtern übermittelt. Im Saarland wird die Volkszählung durch das Statistische Amt ausgeführt. Hierzu werden bei den Landkreisen und dem Regionalverband Erhebungsstellen eingerichtet.

Beim Gesetzgebungsverfahren und dem technisch-organisatorischen Aufbau der Datenverarbeitungs-Infrastruktur wurde die Landesbeauftragte für Datenschutz und Informationsfreiheit zeitnah unterrichtet.

Eine im Juli eingereichte Klage beim Bundesverfassungsgericht gegen den Zensus 2011 wurde nicht zur Entscheidung angenommen, weil die Annahmevoraussetzun-

gen nicht vorlagen. Im Kern mangelte es der Klageschrift an der exakten Bezeichnung der Rechtsvorschrift, die möglicherweise eine Grundrechtsverletzung darstellt, sowie der entsprechenden substantiierten Begründung, welches Gewicht dem Eingriff in das Recht auf informationelle Selbstbestimmung beizumessen ist (1 BvR 1865/10).

17 Sonstiges

17.1 Datenmigration von den Kommunen zum Entsorgungsverband Saar

Der Entsorgungsverband Saar (EVS) ist ein solidarischer Zweckverband, der im Gesetz über den Entsorgungsverband Saar (EVSG) verankert ist, um allen saarländischen Kommunen eine moderne Infrastruktur für die Abwasserreinigung und die Abfallentsorgung zu ermöglichen.

Wurden die anfallenden Gebühren bisher von den zuständigen Kommunen erhoben und an den EVS abgeführt, läuft die Gebührenabrechnung ab 1. Januar 2011 direkt zwischen Gebührenschuldner und dem EVS ab. Die zur Festsetzung der Gebühren erforderlichen Daten, haben die im EVS organisierten Kommunen gemäß § 8 Abs. 5 Saarländisches Abfallwirtschaftsgesetz (SAWG) dem EVS zur Verfügung zu stellen. Näheres über Art und Umfang der dem EVS zur Verfügung zu stellenden und von diesem zu speichernden Daten regelt die Gebührensatzung des Verbandes.

Bei der Erstellung eines Entwurfes zur Gebührensatzung des Verbandes wurden wir beratend zur Datenmigration vom EVS hinzugezogen.

Die Datensätze von circa 400.000 saarländischen Haushalten mussten datenschutzkonform von den Kommunen an den EVS übermittelt werden. Dabei wurden insbesondere die technisch-organisatorische Umsetzung aber auch die fachliche Zulässigkeit der zu übermittelnden Datensätze geprüft.

Zur Übermittlung der Daten von der Kommune zum EVS wird das kommunale Netz genutzt. Es handelt sich dabei um ein datenschutzrechtlich sicheres Netz, das vom eGo-Saar betrieben wird und an das alle saarländischen Kommunen und Landkreise sowie der EVS angeschlossen sind.

Diskussionsbedarf in fachlicher Sicht gab es insbesondere bei der Übermittlung der Bankdaten der Gebührenschuldner an den EVS. Sah der EVS die Übermittlung der

Bankdaten als zulässig an, wurde von unserer Seite die Unzulässigkeit der Datenübermittlung mit der Formulierung des § 8 Abs. 5 SAWG begründet, wonach lediglich für die Festsetzung der Gebühren erforderliche Daten übermittelt werden dürfen. Die Bankdaten sind jedoch für die reine Festsetzung der Gebühren nicht relevant. Letztendlich folgte der EVS unseren Ausführungen und stellte eine datenschutzkonforme Lösung zur Migration der Daten von den Kommunen an den EVS sicher.

17.2 Beteiligung bei der Freigabe automatisierter Verfahren

Auch in diesem Berichtszeitraum haben wir automatisierte Verfahren zur datenschutzrechtlichen Beurteilung erhalten. Gemäß § 7 Abs. 2 SDSG ist vor dem erstmaligen Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, die Landesbeauftragte für Datenschutz zu hören.

Gerade aus dem Bereich der Personalverwaltung mussten wir des Öfteren zu den Themen Zeiterfassung, Beschäftigtendatenbank oder Lohnabrechnungsprogramm unsere Stellungnahme abgeben. Das Spektrum der vorgelegten Verfahren reichte von Programmsystemen zur kommunalen Datenverwaltung im Bereich des Jagd-Fischerei- oder Waffenwesens bis hin zum Abrechnungsprogramm einer Musikschule.

Durch die Vorlage der automatisierten Verfahren mittels einer in meinem Internetangebot abrufbaren Verfahrensbeschreibung gemäß § 9 SDSG ergaben sich häufig ähnliche Kritikpunkte an der Art und Weise, wie uns das Programm zur datenschutzrechtlichen Bewertung vorgelegt wurde. So fehlten des Öfteren die Rechtsgrundlagen zur Datenerhebung sowie Löschkonzepte, die eine datenschutzgerechte Löschung gemäß § 21 Abs. 3 SDSG vorsehen, sobald die Daten für die Aufgabenerfüllung der verantwortlichen Stelle nicht mehr erforderlich sind.

Bei Zeiterfassungsprogrammen ist darauf zu achten, dass die An- und Abwesenheitszeiten der Mitarbeiter lediglich für das laufende und das vorhergehende Kalen-

derjahr vorzuhalten sind. Nach Ablauf der oben genannten Frist sind diese Daten für die Aufgabenerfüllung der Personalverwaltung in der Regel nicht mehr erforderlich. Die Zugriffsberechtigung auf diese Daten muss auf einen möglichst kleinen Kreis an Mitarbeitern beschränkt werden, der diese Informationen zur eigenen Aufgabenerfüllung benötigt.

Lohnabrechnungsprogramme beinhalten meistens ein Datenfeld zur Eingabe der Schwerbehinderteneigenschaft. Liegt eine solche Eigenschaft vor, wird meist nach dem Grad der Behinderung gefragt. Da die Schwerbehinderteneigenschaft arbeitsrechtliche Folgen wie Zusatzurlaubsansprüche beinhaltet, ist die Angabe der Schwerbehinderteneigenschaft an sich für die Aufgabenerfüllung der Personalverwaltung zulässig. Der genaue Grad der Behinderung spielt aber rechtlich keine weitere Rolle, soweit der Tatbestand der Schwerbehinderung nachgewiesen wurde. Eine Erhebung des Grades der Behinderung ist somit unzulässig.

17.3 Ausblick zum Gesamtkonzept für den Datenschutz in der Europäischen Union

Am 4. November 2010 hat die Europäische Kommission ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vorgestellt. Ziel des Konzeptes ist es, eine Modernisierung des europäischen Datenschutzrechts durchzuführen und somit vor allem auf technische Entwicklungen zu reagieren. Das Konzept ist Bestandteil der für das Jahr 2011 von der Europäischen Kommission angekündigten Überarbeitung der EU-Datenschutzrichtlinie 95/46/EG aus dem Jahre 1995 und dient als Grundlage für die momentan noch laufenden Diskussionen mit anderen EU-Organen und interessierten Kreisen, damit konkrete Vorschläge und Maßnahmen EU-weiten Gesetzescharakter erreichen können.

Kernpunkte des Konzeptes sind:

- Stärkung der Rechte des Einzelnen, damit die Sammlung und Nutzung personenbezogener Daten auf das erforderliche Mindestmaß beschränkt wird.
- Stärkung der Binnenmarktdimension durch Verringerung des Verwaltungsaufwands für Unternehmen und die Gewährleistung gleicher Rahmenbedingungen.
- Überarbeitung der Datenschutzbestimmungen im Bereich der Zusammenarbeit der Polizei- und Strafjustizbehörden, damit personenbezogene Daten Einzelner auch hier geschützt werden.
- Gewährleistung eines hohen Schutzniveaus bei außerhalb der EU übermittelten Daten durch die Verbesserung und Erleichterung von Verfahren für den internationalen Datentransfer.
- Wirksamere Durchsetzung der Vorschriften durch die Stärkung und weitere Harmonisierung der Aufgaben und Befugnisse der Datenschutzbehörden.

Die Einführung eines einheitlichen Datenschutzniveaus in der Europäischen Union darf allerdings nach Forderung der deutschen Datenschutzbeauftragten nicht dazu führen, dass der derzeit gültige Rechtsrahmen für Datenschutz in Deutschland unterschritten wird. Es bleibt abzuwarten, welche konkrete Vorschläge der Europäischen Kommission zur Verbesserung des Datenschutzes dem Europäischen Rat und dem Europäischen Parlament zur Entscheidung unterbreitet werden.

17.4 Ein modernes Datenschutzrecht für das 21. Jahrhundert

Die Datenschutzbeauftragten des Bundes und der Länder haben anlässlich der Frühjahrskonferenz 2010 ein Eckpunktepapier zur Modernisierung des Datenschutzrechtes entwickelt. Die dort gemachten Feststellungen beruhen auf der Tatsache, dass Computer, Smartphones, Videokameras, Navigationshilfen, elektronische Sensoren, Kundenkarten und soziale Netzwerke im Internet nicht mehr aus dem Alltag des Otto-Normalverbrauchers wegzudenken sind.

Die Datenschutzgesetze stammen im Wesentlichen aus den siebziger Jahren des vorigen Jahrhunderts, als Datenverarbeitung im Vergleich zu heute nur eine geringe Bedeutung hatte. Unsere vernetzte Welt ist gekennzeichnet durch die oft unbemerkte Verarbeitung von Daten. Daher ist es heute umso notwendiger, dass der Bürger wieder weiß, wer was von ihm wo gespeichert hat, um überhaupt sein Grundrecht auf informationelle Selbstbestimmung ausüben zu können.

Die wesentlichen Forderungen der Datenschutzbeauftragten lassen sich wie folgt zusammenfassen:

1. Konkrete Schutzziele des Datenschutzes sind als Grundlage aller Regelungen und Maßnahmen zu verankern: Spezialgesetzliche Regelungen sollen nur noch ausnahmsweise vorgehen. Für öffentliche und nichtöffentliche Stellen sind gleiche Regeln zu schaffen. Datenschutz ist technisch in Produkte und Verfahren zu integrieren. Die Bildung von Profilen ist grundsätzlich strikt zu reglementieren.

2. Im Interesse der Betroffenen ist die Datenerhebung, -verarbeitung und –nutzung möglichst transparent zu gestalten: Eine vom Betroffenen unbemerkte Datenerhebung soll grundsätzlich unzulässig sein; umgekehrt muss der Betroffene eindeutig und verständlich über die Art und Weise des Umgangs mit seinen Daten und seine Rechte aufgeklärt werden. Unvermeidliche Datenerhebungen sind auch hinsichtlich der weiteren Verwendung der gewonnenen Daten eng zu begrenzen. Verstöße sind wirksam zu ahnden.

3. Die Beteiligung mehrerer Stellen an der Datenverarbeitung ist durch entsprechende datenschutzrechtliche Vorschriften rechtskonform zu gestalten: Die vielfach praktizierte arbeitsteilige Datenverarbeitung von öffentlichen und privaten Stellen, teilweise sogar mit Auslandsbezug, ist mit dem geltenden Recht nicht befriedigend in Einklang zu bringen. Die datenschutzrechtliche Verantwortung sollte unter Berücksichtigung der tatsächlichen Einflussmöglichkeiten und der Interessenlage der Betroffenen neu geregelt werden.

4. Die Regeln zum technischen und organisatorischen Datenschutz sind grundlegend zu reformieren: Die bisher geltenden technikabhängigen Maßnahmen sind durch elementare, technikunabhängige und praxistaugliche Schutzziele zu ersetzen, aus denen sich konkrete Maßnahmen nach dem jeweiligen Stand der Technik ableiten lassen. Vor der Freigabe von EDV-Verfahren sind die Risiken für das Recht auf informationelle Selbstbestimmung zu dokumentieren und ein entsprechendes Schutzkonzept zu schaffen. Den Betroffenen müssen verstärkt Methoden und Mittel des Selbstdatenschutzes zur Verfügung gestellt werden.

5. Die Rechte der Betroffenen sind nachhaltig zu stärken: Die Informationspflichten der Datenverarbeiter sind zu erweitern. Herkunft und Empfänger von Daten sowie Datenbankzugriffe sind zu protokollieren. Betroffene müssen verbesserte Auskunftsrechte erhalten. Über Datenpannen ist auch im öffentlichen Bereich zu informieren. Die informierte Einwilligung als zentrale Ermächtigungsgrundlage für die Datenverarbeitung in der Privatwirtschaft ist verbraucherfreundlich auszugestalten; statt einer formularmäßigen Erklärung soll ein aktives Tun (Ankreuzen, Haken setzen usw.) Voraussetzung sein. Einwilligungen sind zeitlich zu begrenzen. Aus einer Verweigerung dürfen keine Nachteile erwachsen.

6. Das Datenschutzrecht ist internetfähig zu machen: Grundsätzlich ist die unbeobachtete Kommunikation und Nutzung des Internets zu gewährleisten. Zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen sind besondere Schutzmechanismen zu entwickeln. So müssen die Grundeinstellungen von Internetdiensten ein Optimum an Datenschutz bieten; Abweichungen hiervon können vom informierten Nutzer eigenverantwortlich im Sinne einer Opt-In-Lösung gewählt werden. Betroffene sollen die von ihnen ins Internet eingestellten Daten mit einem „Verfallsdatum“ versehen können. Die Bundesregierung wird aufgefordert, sich auf internationaler Ebene für ein möglichst hohes Datenschutzniveau im Internet einzusetzen.

7. Die Eigenkontrolle der verantwortlichen Stellen ist zu verbessern: Ein freiwilliges Audit für EDV-Verfahren und –Produkte kann Datenschutz zum Wettbewerbsvorteil machen. Datenschutzkonzepte sind verbindlich aufzustellen und zu dokumentieren. Die behördlichen und betrieblichen Datenschutzbeauftragten sind in ihrer Funktion zu stärken.

8. Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar.

9. Ein wirksamer Datenschutz braucht effektive Sanktionen: Auch für nichtöffentliche Stellen sollte eine Gefährdungshaftung (entsprechend § 8 Abs. 1 des Bundesdatenschutzgesetzes) eingeführt werden. Bei Datenschutzverstößen sollte ein pauschalierter Schadensersatz greifen. Zudem sollten die Betroffenen einen Folgenbeseitigungsanspruch erhalten, wenn unrichtige oder unrechtmäßige Datenübermittlungen zu negativen Folgen führen. Die Bußgeldtatbestände, insbesondere für das unbefugte Nutzen von Daten, die unzulässige Beobachtung durch automatisierte Verfahren (z.B. Videoüberwachung) sowie das Unterlassen technisch-organisatorischer Maßnahmen, sind zu erweitern. Die Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten sollte konzentriert werden. Bei besonderem öffentlichem Interesse sind datenschutzrechtliche Straftaten auch von Amts wegen zu verfolgen. Durch die erweiterten Sanktionsmöglichkeiten können zugleich vorhandene Vollzugsdefizite abgebaut werden, wie sie aufgrund der unzureichenden Kontrollmöglichkeiten heute leider unvermeidlich sind.

Die Broschüre der Datenschutzbeauftragten des Bundes und der Länder mit dem Titel „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ kann bei unserer Dienststelle angefordert werden.

Das Dokument ist auch von der Internetseite www.lfdi.saarland.de herunterzuladen.

17.5 Datenschutz bei der Alarmierung von Feuerwehr und Rettungsdienst

Der Zweckverband für Rettungsdienste und Feuerwehralarmierung Saar ist zurzeit in den Planungen, eine neue, landesweit einheitliche Infrastruktur für die Alarmierung des Rettungsdienstes, der Feuerwehren und Katastrophenschutzeinheiten zu errichten. Aus synergetischen Gründen hat man sich dazu entschlossen, aufbauend auf einem digitalen Alarmierungssystem, das sich bereits in einigen saarländischen Landkreisen im Einsatz befindet, eine einheitliche landesweite Lösung zu finden.

Es wurde in diesem Zusammenhang die Frage an uns herangetragen, welche datenschutzrechtlichen Vorgaben, insbesondere im technisch-organisatorischen Bereich bei der Umsetzung des Projektes und zum Schutze des Fernmeldegeheimnisses zu beachten sind.

Welche technischen Vorkehrungen oder sonstige Maßnahmen zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten getroffen werden müssen, dass auch ein unerlaubter Zugriff auf diese Daten verhindert werden soll, wird in den §§ 109 des Telekommunikationsgesetzes (TKG) sowie 11 SDSG geregelt. So sind technische Vorkehrungen und sonstige Schutzmaßnahmen angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtung für die Allgemeinheit steht.

Da bei der Alarmierung der vom Zweckverband betreuten Organisationen nicht auszuschließen ist, dass auch Gesundheitsdaten und somit besonders sensible Daten im Sinne des § 4 Abs. 2 SDSG übermittelt werden, ist von einem hohen Schutzbedarf im Sinne des Gesetzes auszugehen. Um dem festgestellten Schutzbedarf der Daten gerecht zu werden, halten wir aus technisch-organisatorischer Sicht eine Ende-zu-Ende Verschlüsselung der digitalen Alarmierung für erforderlich und angemessen.

Für die zukünftige Beschaffung von digitalen Alarmierungssystemen im Saarland ist somit eine datenschutzkonforme Vorgabe geschaffen worden.

18 Entschließungen

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

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. Februar 2009

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

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

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

1. die Ermächtigung des BSI, die gesamte Sprach- und Datenkommunikation aller Unternehmen, Bürgerinnen und Bürger mit Bundesbehörden ohne Anonymisierung bzw. Pseudonymisierung zu überwachen und auszuwerten (§ 5),

2. die vorgesehene Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen werden (§ 5 Abs. 4) und

3. die fehlende Verpflichtung des BSI, Informationen über ihm bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Unternehmen, Bürgerinnen und Bürger vor (zu erwartenden) Angriffen (Spionage und Sabotage) zu warnen (§ 7).

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

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

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

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

18.2 Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten!

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

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

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

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

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich

aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

18.3 Defizite beim Datenschutz jetzt beseitigen!

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

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

1. Der Deutsche Bundestag wird aufgefordert, noch in dieser Legislaturperiode die von der Bundesregierung vorgelegten Gesetzentwürfe für erste notwendige Korrekturen des Bundesdatenschutzgesetzes im Bereich der Auskunfteien und des Adresshandels zu verabschieden. Ansonsten verlieren die Bürgerinnen und Bürger das Vertrauen in die Zusagen der Bundesregierung nach den Skandalen des Jahres 2008. Insbesondere mit Adressen darf nur noch mit ausdrücklicher Einwilligung der Betroffenen Handel getrieben werden. Der Entwurf für ein Datenschutzauditgesetz muss gründlich überarbeitet werden, damit dieser notwendige Schritt hin zu einem modernen Datenschutzrecht von der Praxis auch umgesetzt werden kann.

2. Mit Beginn der nächsten Legislaturperiode muss endlich eine grundlegende Modernisierung des Datenschutzrechts in Angriff genommen werden, die bereits zu lange aufgeschoben wurde. Nur so kann das Datenschutzrecht den

Herausforderungen der Informationsgesellschaft zu Beginn des 21. Jahrhunderts gerecht werden.

3. Der Einsatz datenschutzfreundlicher Technik muss vorangetrieben und rechtlich verpflichtend vorgeschrieben werden. Darin liegt auch eine Chance für den Wirtschaftsstandort Deutschland in Zeiten der Krise.

18.4 Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage

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

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

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

Ohne eine derartige Rechtsverordnung ist die Gesamtheit der in Verbunddateien stattfindenden polizeilichen Datenverarbeitungen rechtswidrig. Die Datenschutzbeauftragten von Bund und Länder fordern das Bundesministerium des Innern und die Landesregierungen auf, unverzüglich daraus Konsequenzen zu ziehen und die polizeiliche Datenverarbeitung auf den Prüfstand zu stellen.

18.5 Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz

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

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

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

- Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.

- Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festle-

gungen im Hinblick auf Gesundheitsdaten (u. a. zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen, etc.)

- Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z. B. der Innenrevision auf erhobene Personaldaten bedarf enger gesetzlicher Vorgaben.

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

- Der Einsatz von Überwachungssystemen, wie z.B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.

- Es bedarf der Festlegung der Rechte der Beschäftigten, z.B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.

- Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.

- Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.

- Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch gewonnenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

18.6 Datenschutz beim vorgesehenen Bürgerportal unzureichend

Entschließung der Konferenz der Datenschutzschutzbeauftragten des Bundes und der Länder vom 16. April 2009

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

- Der Entwurf sieht vor, dass nur akkreditierte Anbieter Portale betreiben dürfen. Voraussetzung für die Akkreditierung darf nicht allein der Nachweis der technischen und administrativen Sicherheit, sondern muss auch die tatsächliche Einhaltung datenschutzrechtlicher Standards sein. Die dabei zu erfüllenden

Mindestanforderungen müssen verbindlich im Gesetz vorgegeben werden. Portalbetreiber sollten zudem erst dann die Akkreditierung erhalten, wenn die Umsetzung dieser Anforderungen durch unabhängige Prüfstellen bescheinigt wurde.

- Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Diensteanbietern und durch die Sicherung des Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte gelesen oder verändert werden können. Deshalb muss die Kommunikation standardmäßig durch eine Ende-zu-Ende-Verschlüsselung zwischen Absendenden und Empfangenden nach dem Stand der Technik gesichert und nicht nur als Option angeboten werden.

- Das Bürgerportal soll gerade zwischen Bürgerinnen und Bürgern und Verwaltung eine rechtlich gesicherte Kommunikation ermöglichen. Insbesondere sind über das Bürgerportal förmliche Zustellungen mit den entsprechenden Rechtsfolgen beabsichtigt. Dies darf nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort wird abgelehnt.

- Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. Das ermöglicht Angriffe durch Schadsoftware auf dem Rechner der Nutzenden. So könnten Zugangsdaten beschafft und widerrechtlich dazu verwendet werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern oder unberechtigt auf Daten im De-Safe zuzugreifen. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen.

- Die Möglichkeit, eine pseudonyme Bürgerportaladresse zu nutzen, muss – entgegen der Stellungnahme des Bundesrates vom 3. April 2009 – erhalten bleiben. Denn die pseudonyme Nutzung ermöglicht gerade einen sinnvollen Kompromiss zwischen hinreichender Identifizierbarkeit im Rechtsverkehr und Datenschutz für die Nutzerinnen und Nutzer.

- Die Nutzerinnen und Nutzer müssen bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen – etwa zur verbindlichen Kommunikation mit staatlichen Stellen – hingewiesen werden. Die Aufklärungs- und Informationspflichten müssen im Gesetzestext klarer als bislang geschehen gefasst werden. Gleiches gilt für die Feststellung von Identitätsdaten und der Aufdeckung von Pseudonymen.

- Eine Benachteiligung von Bürgerinnen und Bürgern, die über kein Bürgerportalkonto verfügen, muss ausgeschlossen werden. Auch dürfen Bürgerportale nicht dazu führen, dass staatliche Stellen dazu übergehen, bei jeder Inanspruchnahme einer E-Government-Anwendung eine persönliche Identifizierung zu verlangen, selbst wenn dies für die konkrete Dienstleistung nicht erforderlich ist.

- Der Entwurf sieht vor, dass grundsätzliche Fragen der technischen Ausgestaltung der Bürgerportale und der darüber angebotenen Dienste in einer Rechtsverordnung geregelt werden sollen. Dies widerspricht der Rahmenkonzeption des Art. 80 GG und dient auch sonst nicht der Normenklarheit des Gesetzes. Zumindest die grundsätzlichen technisch-organisatorischen Anforderungen an die Eröffnung des Kontos, den Postfach- und Versanddienst, den Speicherplatz, den Identitätsbescheinigungsdienst und das Akkreditierungsverfahren sollten in das Gesetz selbst aufgenommen werden.

- Der Entwurf des Bürgerportalgesetzes sieht jetzt auch vor, dass nicht nur die Datenerhebung, sondern auch die Verarbeitung und Nutzung der erhobenen Daten durch den akkreditierten Dienstanbieter an eine enge Zweckbestimmung gebunden ist. Allerdings ist der pauschale Verweis auf die Regelungen des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes in diesem Zusammenhang zu weitgehend, da so für die Diensteanbieter die Möglichkeit eröffnet wird, die personenbezogenen Daten für Werbung oder Marktforschungszwecke zu nutzen. Die Bürgerinnen und Bürger müssen jedoch sicher sein können, dass ihre Daten ausschließlich zur Teilnahme am Bürgerportal genutzt werden.

18.7 Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur

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

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

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

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

Die Konferenz hält es insbesondere für erforderlich:

- Das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z.B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;

- die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;

- ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;

- die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;

- die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;

- auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z. B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;

- im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;

- die Videoüberwachung in Staat und Gesellschaft einzuschränken;

- den Schutz der Meldedaten zu verbessern;

- ein praktikables Datenschutzaudit zu schaffen;

- die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

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

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Ju-

gendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

18.8 Datenschutzdefizite in Europa auch nach Stockholmer Programm

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

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

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

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

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

- Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.

- Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.

- Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.

- Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.

- Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

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

18.9 Kein Ausverkauf von europäischen Finanzdaten an die USA!

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

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

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

Im Übrigen bestehen bereits an der Notwendigkeit eines so weit reichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebliche Zweifel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

18.10 Krankenhausinformationssysteme datenschutzgerecht gestalten!

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

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

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

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

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

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

18.11 „Reality-TV“ – keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

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

„Reality-TV“-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige „Lieferanten“ für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen

Haftbefehl gegen einen Schuldner zu vollziehen – wobei auch schon einmal eine Wohnung zwangsgeöffnet wird – oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mitverfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleibt oder gar ausfällig werden. Aufgrund des Erfolgs derartiger „Unterhaltungssendungen“ ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

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

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

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

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

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

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

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

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

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

18.13 Datenschutz am Scheideweg – Datenschützer fordern Neuorientierung für einen besseren Datenschutz

Ergebnisse der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17. und 18. März 2010 in Stuttgart

Zum Abschluss der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Stuttgart hat der diesjährige Konferenzvorsitzende, der baden-württembergische Datenschutzbeauftragte Jörg Klingbeil, gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit, Dr. Alexander Dix, die Konferenzergebnisse vorgestellt. Beide vertreten den deutschen Datenschutz auch auf europäischer Ebene.

Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch das Urteil des Europäischen Gerichtshofs vom 9. März 2010 bestätigt, nach dem auch die deutschen Datenschutzaufsichtsbehörden von jeder Weisung durch Regierungsstellen völlig frei sein müssen, soweit sie private Datenverarbeiter kontrollieren. Sie halten daher eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland für geboten und fordern von den Gesetzgebern in Bund und Ländern eine europarechtlich einwandfreie Regelung, die für die Tätigkeit der unabhängigen Datenschutzbeauftragten im öffentlichen Bereich ebenfalls Folgen haben dürfte. Die in den Ländern und beim Bund bisher bestehenden Regelungen und Strukturen müssen im Einzelnen daraufhin überprüft werden, wie die Unabhängigkeit im Sinne des Urteils realisiert und im Interesse der Bürgerinnen und Bürger auch wirksam ausgestaltet werden kann. Eine Fach- und Rechtsaufsicht darf es nicht geben.

Die Konferenz hat sich erneut mit der Modernisierung des Datenschutzrechts befasst. „Unser Recht passt nicht mehr ins Internetzeitalter“, so Jörg Klingbeil. Oft sei es schwer zu klären, wer in den Welten des Internets jeweils für den Datenschutz zuständig ist. Als Grundlage für eine Diskussion über eine grundlegende Reform des Datenschutzrechts haben die Datenschutzbeauftragten ein Eckpunktepapier vorge-

legt; unter anderem werden darin ein technikneutraler Ansatz, die Stärkung der Betroffenenrechte und wirksamere Sanktionen gefordert.

Das Bundesverfassungsgericht hat durch Urteil vom 2. März 2010 die Vorratsdatenspeicherung in der aktuellen Form für verfassungswidrig erklärt. Die Datenschutzbeauftragten sehen sich durch die Entscheidung des höchsten deutschen Gerichts in ihrer Auffassung bestärkt. Jörg Klingbeil: „Der Gesetzgeber hätte sich die erneute Blamage ersparen können. Bereits 2007 hatte die Konferenz der Datenschutzbeauftragten auf die Unverhältnismäßigkeit dieses Eingriffs in die Kommunikationsfreiheit hingewiesen. Ebenso wurde von uns damals deutlich gemacht, dass das in Kraft gesetzte Regelwerk weit über die Vorgaben der Europäischen Union hinausging.“ Die Konferenz lehnt die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehöre zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland. Die Datenschutzbeauftragten fordern die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen. Nach Ansicht der Konferenz müsse die Entscheidung des Bundesverfassungsgerichts auch über die Kommunikationsdaten hinaus Beachtung finden, etwa bei Flugpassagierdaten oder bei der Konzeption von Mautsystemen. Auch die zentrale ELENA-Datenbank müsse auf den Prüfstand.

Beim Einsatz von Ganzkörperscannern sieht die Konferenz der Datenschutzbeauftragten noch viele offene Fragen. Es müsse noch geklärt werden, was die Geräte technisch leisten können, ob damit ein nennenswerter Sicherheitsgewinn erzielbar ist und inwieweit Gesundheitsschäden entstehen können. Der Gesetzgeber habe nun über den Einsatz der Scanner zu entscheiden. Die Grundrechte der Betroffenen müssten dabei geschützt werden. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel dürften nicht angezeigt werden.

Für einige Sicherheitsgesetze der letzten Jahre ist eine Evaluierung vom Gesetzgeber vorgesehen worden. Allerdings ist eine wirksame Erfolgskontrolle entscheidend davon abhängig, unter welchen Vorgaben und von wem sie durchgeführt wird. Die Datenschutzbeauftragten des Bundes und der Länder sehen mit Sorge, dass bei der derzeit vorgesehenen Evaluierung des Gemeinsame-Dateien-Gesetzes externer wissenschaftlicher Sachverstand nur eine Alibifunktion haben könnte. Es sollte eigent-

lich eine Selbstverständlichkeit sein, dass der Gesetzgeber diese Erfolgskontrolle von unabhängigen Experten, die nicht der die Sicherheitsgesetze vollziehenden Gewalt angehören, durchführen lässt. Dies gilt auch für die von der Bundesregierung vorgesehene Evaluierung der Kooperationszentren von Polizei und Nachrichtendiensten.

Das Bundesgesundheitsministerium plant, die bisherige Regelung zur Abrechnung hausärztlicher Leistungen und ambulanter Notfallbehandlungen im Krankenhaus durch private Abrechnungsstellen in der gesetzlichen Krankenversicherung um ein Jahr zu verlängern. Damit setzt sich der Bundesgesundheitsminister nicht nur über ein Urteil des Bundessozialgerichts hinweg. Auch die Datenschutzbeauftragten halten die derzeitigen Regelungen zur Datenverarbeitung höchst sensibler Daten durch private Stellen für völlig unzureichend. Sie fordern daher vom Gesetzgeber, schnell präzise Vorgaben für die Einschaltung privater Stellen bei der Abrechnung von Kassenleistungen im Sozialgesetzbuch zu verankern.

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 20. Dezember 2007 eine unzulässige Mischverwaltung bei den JobCentern festgestellt. Dies führte zu unklaren Zuordnungen von Verantwortlichkeiten in den Arbeitsgemeinschaften beim sozialrechtlichen Datenschutz im Bereich des Arbeitslosengelds 2. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb für die anstehende Neuorganisation der Arbeitsgemeinschaften/JobCenter eindeutige gesetzliche Regelungen für die datenschutzrechtlichen Aufgaben und Kontrollzuständigkeiten, um die bisher bestehenden Unsicherheiten bei der Datenschutzkontrolle zu beseitigen. Keinesfalls dürfe es zu einer voraussetzungslosen Mehrfachspeicherung sensibler personenbezogener Daten bei den Leistungsträgern kommen, denn damit würden unvertretbare datenschutzrechtliche Risiken verbunden sein.

Zu folgenden Themen sind jeweils nähere Informationen abgeschlossen:

- Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

- Ein modernes Datenschutzrecht für das 21. Jahrhundert – Zusammenfassung zum Eckpunktepapier

- Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

- Keine Vorratsdatenspeicherung!

- Klare gesetzliche Regelungen zur Abrechnung bei privaten Stellen in der gesetzlichen Krankenversicherung

- Körperscanner – viele offene Fragen

18.14 Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Art. 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.

- Es darf keine Fach- und Rechtsaufsicht geben.

- Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.

- Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.

- Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.

- Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

18.15 Ein modernes Datenschutzrecht für das 21. Jahrhundert

79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010

Zusammenfassung

Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Doch wie soll dieses Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung gewährleistet werden? Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Eckpunkte formuliert, die Grundlage einer Diskussion über eine Reform des Datenschutzrechts sein sollen.

1. Konkrete Schutzziele und Grundsätze verankern

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nichtöffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten. Dies betrifft etwa den Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Die Vorgaben des allgemeinen Datenschutzrechts können – soweit erforderlich – in Bezug auf bestimmte Anwendungsgebiete weiter konkretisiert werden.

2. Technikneutralen Ansatz schaffen

Den aus der technologischen Entwicklung resultierenden Gefährdungen sollte durch technikneutrale Vorgaben begegnet werden, die auf konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible, und praxistaugliche gesetzliche

Bedingungen geschaffen werden, die das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch technischen und organisatorischen Datenschutz sichern.

3. B**etroffenenrechte stärken**

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Die Datenverarbeitung muss für die Betroffenen transparenter werden, etwa indem die Wahrnehmung des Auskunftsanspruchs erleichtert wird. Die Freiwilligkeit der Einwilligung in eine Datenverarbeitung muss gestärkt werden.

4. Datenschutzrecht internetfähig machen

Ein modernes Datenschutzrecht muss internetfähig sein. Grundsätzlich muss eine unbeobachtete Kommunikation und Nutzung des Internets gewährleistet werden. Auch sind besondere Schutzmechanismen zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz zu schaffen. Nationale Regelungen sollten durch internationale Vereinbarungen flankiert werden.

5. Mehr Eigenkontrolle statt Zwang

Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden. Dies kann etwa durch Einführung eines freiwilligen Auditverfahrens befördert werden. Daneben müssen die verantwortlichen Stellen dazu verpflichtet werden, durch interne Mechanismen die Einhaltung des Datenschutzes sicherzustellen, etwa durch verbindliche Datenschutzkonzepte.

6. Stärkung der unabhängigen Datenschutzaufsicht

Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-

Datenschutzrichtlinie nicht vereinbar. Erforderlich sind auch verstärkte Mitwirkungspflichten der kontrollierten Stellen bei Datenschutzkontrollen.

7. Wirksamere Sanktionen

Die immer noch vorhandenen Lücken im datenschutzrechtlichen Sanktionssystem müssen endlich geschlossen werden. Sie sollten ergänzt werden um für die Betroffenen einfach zu handhabende Haftungsansprüche, etwa einen pauschalierten Schadenersatzanspruch. Die Zuständigkeiten für die Verfolgung von Ordnungswidrigkeiten sollten bei den jeweiligen Datenschutzbehörden liegen. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit braucht insoweit wirksame Sanktionsbefugnisse.

8. Gesetz einfacher und besser lesbar machen

Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf auch insoweit der Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen.

18.16 Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene „Evaluierung“ des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

Dazu muss insbesondere Folgendes dargelegt und bewertet werden:

- die mit der zu evaluierenden Norm intendierten Ziele,

- die tatsächlich erzielten Wirkungen (beabsichtigte und unbeabsichtigte) sowie die Wirkungszusammenhänge,

- die Auswirkungen auf die Grundrechte von Betroffenen und unbeteiligten Dritten (Eingriffsbreite und –tiefe),

- die Gewährleistung eines effektiven Grundrechtsschutzes, insbesondere im Hinblick auf den absolut geschützten Kernbereich der privaten Lebensgestaltung, sowie die Wahrung des Verhältnismäßigkeitsgebots,

- die Umsetzung von organisations-, verfahrens- und technikorientierten Schutz-vorkehrungen (z.B. von Kennzeichnungspflichten, differenzierten Zugriffsberechtigungen, Verwertungsverboten, Prüf- und Löschungspflichten, Richtervorbehalten, Benachrichtigungspflichten),

- die Leistung, Wirkung sowie der Erfolg und die Effizienz,

- die Stellung der zu evaluierenden Norm im Gesamtrechtsgefüge sowie ihre Wechselwirkung mit anderen Normen.

Die Evaluierung ist kein statischer, sondern ein dynamischer, entwicklungsoffener Prozess, der einer ständigen Optimierung bedarf.

18.17 Keine Vorratsdatenspeicherung!

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“. Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grund-

sätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

18.18 Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010

In seinem Urteil vom 10. Dezember 2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften. Infolge des Urteils

war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17. Juli 2009 vorläufige Rechtsgrundlagen in den §§ 120 Abs. 6 und 295 Abs. 1b SGB V geschaffen, die bis zum 30. Juni 2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder öffentlichrechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Abrechungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.

18.19 Körperscanner – viele offene Fragen

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18. März 2010

Der Anschlagsversuch von Detroit am 23. Dezember 2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.

2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.

3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften z.B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.

4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

18.20 Beschäftigtendatenschutz stärken statt abbauen

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. Juni 2010

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz „Qualität vor übereilten Regelungen“ gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zu Gunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinte-

ressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substantielle Verbesserungen an dem Entwurf eines Beschäftigtendatenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

- Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst werden und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.

- Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur „Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten“ würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss vielmehr klarstellen, dass Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln – etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen -, weiterhin zu unterbleiben haben.

- Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn – wie im Entwurf vorgesehen – Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber

werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv – und nicht erst auf Nachfrage – darüber aufzuklären, woher die verwendeten Daten stammen.

- Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.

- Die im Gesetzentwurf an mehreren Stellen vorgesehene „Einwilligung“ der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-)Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

18.21 Erweiterung der Steuerdatenbank enthält große Risiken

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Erweiterung der zentralen Steuerdatenbank um elektronische Lohnsteuerabzugsmerkmale (ELStAM) vom 24. Juni 2010

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie z.B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

- Vorherige Information der Arbeitnehmer
  Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

- Keine Speicherung auf Vorrat
  In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

- Verhindern des unzulässigen Datenabrufs

  Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

- Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept

  Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

18.22 Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz!

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2010

Die Staatskanzleien der Länder bereiten zurzeit den auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderten Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vor. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Größe bezahlen sollen. Der Modellwechsel eröffnet die Möglichkeit, sowohl Finanzierungssicherheit für den öffentlich-rechtlichen Rundfunk zuschaffen, als auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und –vermeidung bei der Beitragserhebung umzusetzen.

Der Staat ist gehalten, gesetzlich dafür zu sorgen, dass die Datenverarbeitung auf ein Maß beschränkt wird, das für den Zweck der Rundfunkfinanzierung unerlässlich ist. Der zur Anhörung zu dem Modellwechsel vorgelegte Entwurf des 15. Rundfunkänderungsstaatsvertrages (Rundfunkbeitragsstaatsvertrages – RBStV-E) entspricht dem nicht, sondern schafft statt dessen eine Vielzahl von Datenerhebungsbefugnissen für die Beitragserhebungsstelle, die diese nach dem Modellwechsel von der Gebühr zur Wohnungsabgabe nicht mehr benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Staatskanzleien daher auf, den vorgelegten Entwurf noch einmal unter Beachtung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nachzubessern und dabei insbesondere die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern auf das erforderliche Maß zu beschränken, den Direkterhebungsgrundsatz zu beachten und vor allem auf Datenerhebung beim Adresshandel zu verzichten, bei Befreiungsanträgen von Wohnungsin-

habern aus sozialen Gründen wie Armut oder Behinderung nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen, auf die Vorlage der vollständigen Leistungsbescheide aber zu verzichten und auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren zu verzichten, stattdessen die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auch auf die Stellungnahme hin, die sie zur Anhörung zum 15. Rundfunkänderungsstaatsvertrag abgegeben hat.

18.23 Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

Entschließung der 80. Konferenz der der Datenschutzbeauftragten des Bundes und der Länder vom 3. und 4. November 2010

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z. B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch ein-

zelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und Energienutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

18.24 Förderung des Datenschutzes durch Bundesstiftung

Entschließung der 80. Konferenz der der Datenschutzbeauftragten des Bundes und der Länder vom 3. und 4. November 2010

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mit Hilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass

- die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,
- die größtmögliche Transparenz der Tätigkeit garantiert ist und
- die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. Dies gilt insbesondere für die Kontrolle, ob gesetzliche Anforderungen eingehalten werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

18.25 Keine Volltextsuche in Dateien der Sicherheitsbehörden

Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. und 4. November 2010

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei-

und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die – ggf. gänzlich unverdächtigen – Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

19 Informationsfreiheitsgesetz

19.1 Saarländisches Informationsfreiheitsgesetz weiterhin in Kraft

Das erste Saarländische Informationsfreiheitsgesetz (SIFG), das am 15. September 2006 in Kraft getreten ist, war befristet auf den 31. Dezember 2010. Mit dem Einführungserlass war dem Ministerium für Inneres aufgegeben worden, vor Ablauf der Frist eine Evaluation durchzuführen.

Die Evaluation wurde in Form einer statistischen Auswertung (Stichtag 31. März 2010) durch das Ministerium für Inneres durchgeführt, in der die Gesamtzahl der Anträge, die Ablehnungen und Erledigungen aufgeführt sind. Insgesamt waren seit Bestehen des SIFG 52 Anträge eingegangen. In 38 Fällen wurde der Informationszugang gewährt, es gab sieben Ablehnungen und fünf sonstige Erledigungen. Zahlen über die Anträge, die bei den Kommunen eingegangen sind, wurden leider nicht erhoben, insofern ist eine Aussage über die Nutzung des SIFG nicht möglich.

Bereits im Koalitionsvertrag des Jahres 2009 hatten sich die an der Regierung beteiligten Parteien darauf verständigt, das Recht auf Informationsfreiheit zu stärken und den Informationszugang zu erleichtern.

Insofern war es nicht überraschend, dass das Saarländische Informationsfreiheitsgesetz weiterhin Bestand haben wird. Es wurde allerdings inhaltlich nicht verändert und gilt somit nahezu unverändert bis zum 31. Dezember 2020.

19.2 Gebührenordnung zum SIFG

Mit der Einführung des SIFG wurde das Ministerium der Finanzen gebeten, eine neue Gebührenstelle für Amtshandlungen nach dem SIFG zu schaffen Die Anwendung der Gebührenordnung stößt in der Praxis aber immer wieder auf Schwierigkeiten.

Ein Antragsteller wollte beispielsweise bei einer Behörde aus einer Datenbank nur bestimmte abgrenzbare Datenfelder als Auszug haben. Die Daten waren in dieser Auswertung natürlich nicht verfügbar. Statt dies dem Antragsteller mitzuteilen, programmierte die Behörde eine Datenbankauswertung und druckte die Daten aus. Sie schrieb dem Antragsteller, dass er die gewünschten Daten gegen Zahlung des entstandenen Programmieraufwandes und weiterer Gebühren in Höhe von 60,- € abholen könne. Dem Antragsteller waren die Daten diesen Betrag nicht Wert und er hat von der Entgegennahme der Daten Abstand genommen.

Die Gebühren müssen sich in dem vom Gesetzgeber vorgegebenen Rahmen bewegen. Sie sind abzustellen auf den Vorgang der Erteilung von Auskünften zu vorhandenen Informationen. Die Behörde muss keine weitergehenden Recherchen anstellen.

In der Praxis hat es sich bewährt, den Antragsteller aufzufordern, seinen Antrag möglichst präzise zu formulieren und ihm bei erkennbar hohem Aufwand, die zu erwartende Höhe der Gebühren vorab mitzuteilen.

19.3 Eigenbetriebe unterliegen dem Saarländischen Informationsfreiheitsgesetz

Aus telefonischen Anfragen ist uns bekannt, dass eine Unsicherheit in der Frage besteht, ob das Saarländische Informationsfreiheitsgesetz auch für die Eigenbetriebe der Kommunen oder des Landes gilt.

Grundsätzlich besteht der Auskunftsanspruch gegenüber allen Behörden des Landes der Gemeinden und Gemeindeverbände. Maßgeblich ist der Behördenbegriff des § 1 des Saarländischen Verwaltungsverfahrensgesetzes.

Es gilt der funktionelle Behördenbegriff - d.h.: jede Stelle, die öffentliche Aufgaben wahrnimmt – neben Behörden im organisatorischen Sinne – ist von dem Auskunftsanspruch betroffen.

Der Eigenbetrieb stellt lediglich eine Gestaltungsmöglichkeit eines kommunalen Unternehmens auf der Grundlage der Gemeindeordnung dar. Er hat keine eigene Rechtspersönlichkeit und ist lediglich organisatorisch und finanzwirtschaftlich aus der Gemeindeverwaltung ausgegliedert. Somit unterliegt er, wie die Kommune selbst, dem Anwendungsbereich des Saarländischen Informationsfreiheitsgesetzes.

19.4 G8/G9-Notenvergleich

In meinem letzten Tätigkeitsbericht hatte ich berichtet, dass das Ministerium für Bildung, Familie Frauen und Kultur sich weigerte, den Notenvergleich der G8- und der G9-Abiturienten des Abiturientenjahrgangs 2009 zugänglich zu machen.

Der Antragsteller wollte mit dieser Information hinterfragen, ob das sogenannte Turbo-Abi insbesondere vor der Problematik neu entwickelter Lehrpläne und Stundentafeln für die betroffenen Schüler Vor- oder Nachteile aufzeigen würde. Die Ablehnung wurde mit der nicht substantiierten Behauptung begründet, es könnten Rückschlüsse auf Einzelkurse, Lehrer und Schüler gezogen werden. Außerdem sei durch eine Auswertung ein Ranking der Schulen möglich. Ob die theoretische Möglichkeit eines Schulrankings einer ansonsten zu beantwortenden Informationsfreiheitsanfrage im Wege stehen kann, ist fraglich. Da die Ablehnungsgründe im SIFG abschließend geregelt sind, ist das aus unserer Sicht nicht der Fall. Dem datenschutzrechtlichen Einwand könnte begegnet werden, indem Lehrfächer mit geringer Schüler- oder Lehrerzahl von der Veröffentlichung ausgenommen werden.

Gegen den ablehnenden Bescheid hatte der Antragsteller Klage beim Verwaltungsgericht erhoben.

Im März 2010 hat das Bildungsministerium die Informationen herausgegeben.

Die vom Antragsteller weiter verfolgte Feststellungsklage, dass sein Recht auf Informationszugang nach dem SIFG verletzt wurde, wurde nicht entschieden, sondern das Verfahren wurde nach mündlicher Verhandlung übereinstimmend für erledigt erklärt.

20 Entschließungen der Konferenzen der Informatonsfreiheitsbeauftragten

20.1 Informationszugang für Bürgerinnen und Bürger verbessern

Entschließung der 18. Konferenz der Informationsfreiheitsbeauftragten in Deutschland am 24. Juni 2009 in Magdeburg

Die Anwendung der Informationsfreiheitsgesetze in Bund und Ländern hat bewiesen: Der freie Zugang von Bürgerinnen und Bürgern zu Informationen öffentlicher Stellen ist auch in Deutschland fester Bestandteil der Demokratie. Seit 1998 haben nun schon elf Länder und der Bund ein allgemeines Informationsfreiheitsgesetz erlassen. Umweltinformationsgesetze und das Verbraucherinformationsgesetz ergänzen und erweitern den freien Zugang zu Informationen in spezifischen Bereichen.

In einer Vielzahl von Fällen haben die Bürgerinnen und Bürger Zugang zu amtlichen Informationen erhalten. Die Erfahrungen zeigen aber auch, dass sie immer wieder auf unnötige Hindernisse stoßen, wenn sie ihre Informationsrechte geltend machen wollen. So ist es für alle Beteiligten, auch für die Behörden, immer wieder schwer zu bestimmen, welches Informationszugangsrecht gilt. Zudem mindern teilweise ausufernde Ablehnungsgründe die Erfolgsaussichten von Zugangsanträgen.

Die Informationsfreiheitsbeauftragten halten es deshalb zugunsten einer größeren Transparenz des Verwaltungshandelns für geboten, einen unkomplizierten und umfassenden Zugang zu amtlichen Informationen zu ermöglichen Ausnahmen vom Informationszugang auf das unabdingbar notwendige Maß zu beschränken den Informationszugang grundsätzlich kostenfrei zu gewähren:

- die Verfahren zur Rechtsdurchsetzung des Informationsanspruchs zu beschleunigen

- Veröffentlichungspflichten als zweite Säule des Informationszugangs im Sinne einer aktiven Informationspolitik zu stärken.

Die Konferenz der Informationsfreiheitsbeauftragten Deutschlands sieht darüber hinaus die Notwendigkeit, die Bewertung des Informationsfreiheitsgesetzes des Bundes auf unabhängiger wissenschaftlicher Grundlage anzugehen.

20.2 Mehr Transparenz durch gesetzlichen Schutz von Whistleblowern

Entschließung der 18. Konferenz der Informationsfreiheitsbeauftragten in Deutschland am 24. Juni 2009 in Magdeburg

Beschäftigte, die Missstände und Rechtsverstöße in Behörden oder Unternehmen aufdecken (Whistleblower), sorgen dort für mehr Transparenz. Beispiele wie die Aufdeckung der sog. Gammelfleischskandale, der heimlichen Überwachung von Mitarbeiterinnen und Mitarbeitern, der Ausspähung von Telefonverbindungsdaten und der übermäßigen Erfassung von Gesundheitsdaten belegen das. Nur weil Beschäftigte betriebsinterne Vorgänge offenbarten, gelangten die Rechtsverstöße überhaupt ans Licht.

Das öffentliche Interesse an der Offenlegung von Missständen muss mit den zivil- und arbeitsrechtlichen Loyalitätspflichten der Beschäftigten gegenüber den Arbeitgeberinnen und Arbeitgebern in einen angemessenen Ausgleich gebracht werden. Transparenz kann nur erreicht und gefördert werden, wenn die Hinweisgeberinnen und Hinweisgeber keine Repressalien durch Arbeitgeberinnen und Arbeitgeber und die Kollegenschaft befürchten müssen.

Die Konferenz der Informationsfreiheitsbeauftragten fordert den Deutschen Bundestag auf, für mehr Informationsfreiheit einzutreten, indem endlich der Schutz von Whistleblowern gesetzlich festgeschrieben wird. Beschäftigte sollen keine arbeitsrechtlichen Konsequenzen befürchten müssen, nur weil sie Rechtsverstöße im Arbeitsumfeld anzeigen. Die Konferenz bedauert, dass ein erster Schritt hierzu, näm-

lich mit einem neuen § 612a BGB den Informantenschutz für Beschäftigte durch ein Anzeigerecht zu regeln, nicht weiterverfolgt wurde.

Der Gesetzgeber ist auch gehalten, den Transparenzgedanken und die datenschutzrechtlichen Belange der meldenden sowie der gemeldeten Person in ein ausgewogenes Verhältnis zu bringen. Hierfür hält die Konferenz folgende Erwägungen für maßgeblich:

Zur Wahrung der schutzwürdigen Belange der Beteiligten sind verbindliche Verfahrensregeln in Behörden und Unternehmen unerlässlich.

Whistleblowern muss die vertrauliche Behandlung des Hinweises zugesagt werden können.

Auch die Rechte der belasteten Person, z.B. auf Benachrichtigung, Auskunft über sowie Berichtigung und Löschung von Daten, müssen berücksichtigt werden.

Zum Schutz der Vertraulichkeit können Beschwerden an unabhängige ggf. externe Stellen (Ombudsleute) geschickt werden, die sie nur anonymisiert weitergeben dürfen.

20.3 Regelungen zum Informationszugang der Bürgerinnen und Bürger vereinheitlichen

Entschließung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) vom 16. Dezember 2009

Die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder begrüßt die Ankündigung in der Koalitionsvereinbarung der neuen Bundesregierung, die Ansprüche der Verbraucherinnen und Verbraucher auf Information in einem ein-

heitlichen Gesetz zur Regelung der Informationsansprüche der Bürgerinnen und Bürger zusammenzufassen.

Die Ansprüche auf Einsicht in Verwaltungsakten und auf Zugang zu sonstigen Informationen öffentlicher Stellen sind derzeit auf eine Vielzahl von Einzelvorschriften verteilt: Sie finden sich insbesondere im Informationsfreiheitsgesetz, im Umweltinformationsgesetz und im Verbraucherinformationsgesetz. Dabei werden vergleichbare Sachverhalte unterschiedlich geregelt, etwa die Voraussetzungen für den Informationszugang, die Fristen zur Beantwortung von Anfragen, die Gebühren, welche für den Informationszugang zu entrichten sind, und die Rechte auf Anrufung der Informationsfreiheitsbeauftragten. Diese Zersplitterung erschwert die Wahrnehmung der Rechte der Bürgerinnen und Bürger und trägt zu Unsicherheiten bei der Rechtsanwendung durch die Behörden bei.

Bei der anstehenden Überarbeitung sollten die Vorschriften so gestaltet werden, dass ein Höchstmaß an Transparenz und Bürgerfreundlichkeit erreicht wird. Die vielfältigen gesetzlichen Ausnahmetatbestände, wegen derer ein Informationszugang verweigert werden kann, gehören auf den Prüfstand.

20.4 Informationsfreiheit bei öffentlich-rechtlichen Rundfunkanstalten

Entschließung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) vom 24. Juni 2010

Die Informationsfreiheit erfasst grundsätzlich alle Formen und Bereiche öffentlich-rechtlichen Handelns. Ihr Ziel ist es, Verwaltungsvorgänge transparenter zu gestalten und den Menschen die politische Mitgestaltung zu erleichtern. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland weist deshalb darauf hin, dass das Recht auf Informationszugang auch gegenüber den öffentlich-rechtlichen Rundfunk-

anstalten als Trägern mittelbarer Staatsverwaltung gilt, sofern nicht deren grundrechtlich geschützte journalistisch-redaktionelle Tätigkeit berührt ist.

Die Rundfunkfreiheit garantiert den Schutz vor staatlicher Kontrolle und Beeinflussung. Eine Öffnung aller Sendeanstalten außerhalb dieses geschützten Kernbereichs für die Informationsbelange der Bürgerinnen und Bürger gefährdet diese Freiheit nicht. Offenheit und Transparenz sind keine Bedrohungen, sondern schaffen Vertrauen in der Bevölkerung. Die Geltung der Informationsfreiheitsgesetze wird die Rundfunkanstalten daher in ihrem demokratischen Auftrag und Selbstverständnis nachhaltig stärken.

Die derzeitige Rechtslage ist aufgrund unterschiedlicher Landesgesetze uneinheitlich. Während in einigen Bundesländern die Anwendbarkeit des Informationsfreiheitsgesetzes ausdrücklich festgeschrieben oder ausgeschlossen ist, ergibt sie sich in anderen Bundesländern nur aus allgemeinen Regeln. Einige Sendeanstalten der ARD sind zudem in Ländern ansässig, in denen noch immer kein Informationsfreiheitsgesetz gilt.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert deshalb die Schaffung ausdrücklicher Rechtsvorschriften, sofern nicht schon vorhanden, nach denen die jeweiligen Informationsfreiheitsgesetze auch auf die öffentlich-rechtlichen Rundfunkanstalten außerhalb der grundrechtlich garantierten Rundfunkfreiheit anzuwenden sind.

20.5 Open Data: Mehr statt weniger Transparenz

Entschließung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) vom 13. Dezember 2010

Die WikiLeaks-Debatte zeigt beispielhaft sowohl ein wachsendes Bedürfnis der internationalen Öffentlichkeit nach verbesserter Information und mehr Transparenz staatlichen Handelns als auch nach einem wirksamen rechtsstaatlichen Rahmen für den Zugang zu öffentlichen Informationen. Auch in Deutschland muss die Transparenz des politischen Handelns einen deutlich höheren Stellenwert bekommen, indem die rechtlichen und tatsächlichen Möglichkeiten zum Zugang zu staatlichen Informationen verbessert werden.

Die Informationsfreiheitsbeauftragten haben bereits vor vier Jahren die Verwaltungen aufgefordert, Informationen nicht erst auf Anfrage zu gewähren, sondern auch aus eigener Initiative im Internet zu veröffentlichen. Den Bürgerinnen und Bürgern soll damit der Zugang erleichtert und gleichzeitig der Aufwand für die öffentlichen Stellen mit der Bearbeitung von individuellen Anträgen auf Informationszugang reduziert werden.

Inzwischen ist einiges geschehen: Immer mehr Informationen, zum Beispiel über die Umwelt, Gerichtsentscheidungen, Parlamentsdokumente, amtliche Statistiken oder Vorlagen kommunaler Vertretungen, sind im Internet frei zugänglich. Aber immer noch fehlt ein Wegweiser durch die meist dezentral veröffentlichten Informationen ebenso wie ein einheitlicher technischer Standard, der die Weiterverwendung der Informationen erleichtern würde.

Beispiele aus dem In- und Ausland zeigen bereits heute, dass es möglich ist, eine Vielzahl von Informationen übersichtlich und über eine einheitliche Plattform zur Verfügung zu stellen. So kann Transparenz gleichermaßen einen Beitrag zur Stärkung der Demokratie und auch zur effizienten Aufgabenwahrnehmung der Verwaltung leisten.

20.6 Verträge zwischen Staat und Unternehmen offen legen!

Entschließung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) vom 13. Dezember 2010

Öffentliche Stellen des Bundes, der Länder und der Kommunen bedienen sich bei der Wahrnehmung ihrer Aufgaben vielfach privater Unternehmen: von großen Firmen, die öffentliche Infrastrukturprojekte verwirklichen, bis hin zu kleinen Betrieben, die für eine Gemeinde das Dorffest arrangieren. Dabei nimmt der Umfang des Outsourcing ständig zu und umfasst auch zentrale Felder der staatlichen Daseinsvorsorge. Die wesentlichen Inhalte und Konditionen werden dabei vertraglich fixiert.

Das Interesse der Öffentlichkeit an den Inhalten solcher Verträge ist groß, die Bereitschaft der Vertragspartner, sie offen zu legen, meist gering. Bisweilen wird privaten Geschäftspartnern sogar die Vertraulichkeit der Vertragsbestimmungen ausdrücklich zugesichert, um deren Offenbarung zu vermeiden.

Von besonderem öffentlichem Interesse sind aussagekräftige Informationen über öffentliche Gelder, die für bestimmte Leistungen bezahlt wurden, ob die Leistungen mit den zuvor ausgeschriebenen Anforderungen übereinstimmen und in welcher Höhe Steuermittel dafür aufgewendet werden. Diese Angaben dienen der Haushaltstransparenz und der Verhinderung von Korruption. Transparenz bei derartigen Verträgen ist auch deshalb besonders wichtig, weil hier nicht selten langfristige Weichenstellungen getroffen werden, die auch Parlamente späterer Legislaturperioden nicht mehr ändern können. Angaben hierüber dürfen der politischen Diskussion nicht vorenthalten werden.

Die Informationsfreiheitsbeauftragten fordern deshalb, die Verträge zwischen Staat und Unternehmen grundsätzlich offen zu legen. Die pauschale Zurückweisung von auf solche Verträge gerichteten Auskunftsbegehren unter Hinweis auf Vertraulichkeitsabreden und Betriebs- und Geschäftsgeheimnisse ist nicht länger hinnehmbar. Die Konferenz hält es deshalb für zwingend geboten, den Zugang zu entsprechen-

den Verträgen in den Informationsfreiheitsgesetzen sicherzustellen, wie dies jüngst im Berliner Informationsfreiheitsgesetz (GVBl. Berlin 2010, Seite 358) geschehen ist.

21 Orientierungshilfe zur Informationsfreiheit

Stellen Sie sich vor, ein Bürger sieht, dass in seiner Straße der Bagger anrollt und Bauarbeiten beginnen, ohne dass er weiß, was dort gebaut wird. Er ruft auf dem Bauamt der Gemeinde an und will Auskunft. Dort wird er mit einem Mitarbeiter verbunden, der ihm berichtet, dass dort ein Einfamilienhaus gebaut wird. Eine ganz einfache Auskunft, die die meisten Kommunen auch gerne erteilen, unabhängig davon, ob das Gesetz bekannt ist oder nicht.

Wenn der Bürger aber dann Akteinsicht fordert, werden sicher viele schon Bedenken haben. Dabei macht das Informationsfreiheitsgesetz keinen Unterschied zwischen Auskunft, Akteneinsicht und die Aushändigung von Kopien. Der Bürger selbst entscheidet, was er haben möchte, nicht die Verwaltung. Wenn personenbezogene Daten nicht herausgegeben werden dürfen, sind diese zu schwärzen.

Ein kleiner Fall zeigt aber auch, wo die Grenzen der Informationsfreiheit sein können:

Wenn ein Bürger Akteneinsicht in den Terminkalender des Bürgermeisters haben will, dann kann dies nach herrschender Meinung abgelehnt werden, weil es sich nicht um eine Akte im Sinne des Gesetzes handelt. Entscheidend ist immer, ob das Handeln einem Verwaltungsvorgang zuzuordnen ist oder nicht. Allerdings ist ein förmliches Verwaltungsverfahren nicht erforderlich.

Ein Wort noch zu den Ablehnungsgründen:

Das Gesetz – hier das IFG des Bundes, auf das das saarländische Gesetz verweist – hat eine abschließende Anzahl von Ablehnungsgründen, die von den Gerichten zudem noch sehr zurückhaltend angewandt werden.

Die Frage der Geheimhaltung gem. § 3 IFG ist etwa jeweils fallbezogen zu prüfen. So kann etwa die Akteneinsicht in eine Verschlusssache nicht mit dem Hinweis auf diese abgelehnt werden. Die formale Einstufung als Verschlusssache reicht nicht

aus. Vielmehr kommt es darauf an, ob die materiellen Gründe für eine solche Einstufung vorliegen.

Auch zu der Frage der ablehnenden Entscheidung wegen Berufs- und Geschäftsgeheimnissen gibt es gerichtliche Entscheidungen, die diese Möglichkeit sehr einengen. Die allgemeine Verschwiegenheitspflicht soll nämlich gerade durch das IFG geöffnet werden. Nur die besondere Verschwiegenheitspflicht ist geschützt. Hierzu zählen etwa das Sozialgeheimnis, das Meldegeheimnis und das richterliche Beratungsgeheimnis. Dort besteht kein Informationsanspruch.

Das Betriebs- und Geschäftsgeheimnis wurde vom Bundesverfassungsgericht in einem Beschluss vom 14. März 2006 – 1 BvR 2087/03 = NVwZ 2006, 1041 dahingehend formuliert, dass hierzu „alle auf ein Unternehmen bezogenen Tatsachen, Umstände und Vorgänge verstanden werden, die nicht offenkundig, sondern nur einem begrenzten Personengkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat.“ Hierzu gehören Umsätze, Geschäftsbücher, Kundenlisten, aber auch Unterlagen zur Kreditwürdigkeit Kalkulationsunterlagen. Ein solches berechtigtes Interesse fehlt, wenn die Offenlegung nicht geeignet ist, exklusives technisches oder kaufmännisches Wissen den Marktkonkurrenten zugänglich zu machen und so die Wettbewerbsposition des Unternehmens nachteilig beeinflussen.

Soweit es um urheberrechtliche Fragen – etwa in einem Gutachten – geht, wird in der Rechtsprechung vertreten, dass dem Bürger keine Kopien ausgehändigt werden dürfen, er aber das Gutachten abschreiben kann.

Auf unserem Internetangebot www.lfdi.saarland.de finden Sie die im Anschluss abgedruckten Fragen und Antworten, die als Orientierungshilfe dienen sollen.

Die Antworten beziehen sich ausschließlich auf allgemeine, häufig gestellte Fragen (Frequently Asked Questions) zur Informationsfreiheit. Einzelheiten zur Rechtslage im Saarland sind auf der Internetseite dem Menüpunkt „Informationsfreiheitsrecht“ zu entnehmen.

Natürlich können sich Bürger und Mitarbeiter von Verwaltungen gleichermaßen an uns zur Klärung von weitergehenden Fragen wenden.

Was ist ein Informationsfreiheitsgesetz?

Ein Informationsfreiheitsgesetz gewährt in seinem Geltungsbereich den Bürgern einen grundsätzlich freien Zugang zu allen bei den öffentlichen Stellen existierenden Informationen und ist somit Voraussetzung des umfassenden Informationszugangs der Bürger. Es regelt die entsprechenden Rechte und legt das nähere Verfahren fest.

Wo gibt es solche Gesetze?

In der Bundesrepublik Deutschland haben bisher lediglich die Länder Brandenburg, Berlin, Bremen, Hamburg, Saarland, Schleswig-Holstein, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Sachsen-Anhalt und Rheinland-Pfalz ein solches Gesetz verabschiedet. Das Informationsfreiheitsgesetz für Bundesbehörden ist am 1. Januar 2006 in Kraft getreten. Ähnliche Gesetze gibt es schon lange in den USA und Kanada, aber auch in den meisten europäischen Ländern.

Was soll damit erreicht werden?

Die Bürger sollen wissen, wie die öffentliche Verwaltung arbeitet, wie ihre Entscheidungen zu Stande kommen und welche Absichten und Intentionen dahinter stehen. Auf diese Weise wird die öffentliche Verwaltung transparent und zu einem von der Öffentlichkeit nachvollziehbaren Handeln angehalten. Informationsfreiheit ist überdies ein wirksames Mittel der Korruptionsbekämpfung. Den Bürgern werden bessere Möglichkeiten eröffnet, den politischen Prozess mitzugestalten und staatliche Entscheidungen zu kontrollieren.

Wer muss die Informationen herausgeben?

Dem Zweck der jeweiligen Gesetze entsprechend besteht der Informationsanspruch der Bürger grundsätzlich gegenüber sämtlichen Stellen der Exekutive, also Behörden auf kommunaler-, Bezirks- Landes- oder Bundesebene, teilweise auch gegenüber

Einrichtungen der Judikative und Legislative. Ausgenommen sind in der Regel das Parlament in seiner Funktion als Legislativorgan und die Organe der Rechtspflege, also Gerichte und die Staatsanwaltschaft, soweit sie im Rahmen der Rechtsprechung und Strafverfolgung tätig werden.

Bin ich gegenüber Verwaltungen in Bundesländern ohne ein solches Gesetz rechtlos?

Der Zugang zu den Akten und Informationen der Behörden ist in Ländern ohne ein Informationsfreiheitsgesetz nicht generell eröffnet, sondern an bestimmte Verfahrensgestaltungen gebunden oder von der Darlegung eines besonderen Interesses abhängig. Akteneinsicht oder –auskunft wird beispielsweise dann gewährt, wenn man Beteiligter eines Verfahrens ist, wenn es nur um die eigenen Daten geht oder wenn man aus wirtschaftlich motivierten Gründen Auskünfte aus öffentlichen Registern wie z.B. aus dem Grundbuch, dem Gewerberegister oder auch aus dem Kfz-Halterverzeichnis der Straßenverkehrsbehörde benötigt. Ein vergleichbarer allgemeiner Anspruch auf Einsichtnahme in Behördenakten, wie er sich aus den Informationsfreiheitsgesetzen ergibt, besteht sonst nur im Umweltbereich auf der Grundlage des Umweltinformationsgesetzes. Weitere Einsichtsrechte, die von jedermann ohne den Nachweis eines bestimmten Interesses wahrgenommen werden können, existieren sonst nur als Ausnahme (Einsicht in das Handelsregister oder in einigen Ländern in Wasserbücher).

Wer hat Anspruch auf Informationszugang?

Die Informationsfreiheitsgesetze eröffnen jeder natürlichen und juristischen Person, also einzelnen Bürgern, aber auch Vereinen, Gesellschaften und Stiftungen sowie Wirtschaftsunternehmen einen Informationszugang.

Welche Voraussetzungen hat der Anspruch auf Herausgabe von Informationen?

Keine, außer dass Sie einen Antrag stellen. Dies kann – je nach Gesetz – mündlich, schriftlich oder elektronisch (per E-Mail) geschehen. Was habe ich als Bürger konkret

von diesem Recht? Gibt es praktische Beispiele? Vielleicht interessieren Sie sich für die Haushaltslage Ihres Landkreises, Ihrer Gemeinde oder Ihres Bundeslandes oder für die jüngsten Planungsvorhaben in Ihrer Umgebung. Sie möchten wissen, nach welchen Kriterien der Auftrag zur Planung und Errichtung eines Schulneubaus vergeben wurde, wie die letzte Bürgerversammlung gelaufen ist oder was bei der jüngst durchgeführten Verkehrszählung herausgekommen ist. Oder Sie sind umgezogen und möchten wissen, wie „streng“ in der neuen Heimatgemeinde bestimmte Gesetze oder Verordnungen umgesetzt werden.

Ist der Antrag auf Information zu begründen?

Nein! Da die Informationsfreiheit gerade das Ziel verfolgt, wirklich allen einen freien Zugang zu Informationen zu ermöglichen, kann es nicht darauf ankommen, warum Sie sich für bestimmte Fragen interessieren oder was Sie in Ihrer Position „damit anfangen können“.

In welcher Form werden die Informationen zugänglich gemacht?

Maßgebend ist grundsätzlich der Antrag des Informationssuchenden. In Frage kommen z.B. die Gewährung von Akteneinsicht, die Erteilung von Auskünften oder die Anfertigung von Kopien.

Welche Auskünfte dürfen verlangt werden?

Um den Aufwand bei den Behörden in einem zumutbaren Rahmen zu halten, ist der Informationsanspruch auf die bei den Behörden vorhandenen Informationen beschränkt. Sind die Informationen tatsächlich nicht vorhanden, geht der Antrag ins Leere. Es kommt nicht darauf an, ob die Behörde die Information aufgrund ihrer Aufgaben eigentlich haben sollte. Es kann auch nicht verlangt werden, dass die Informationen erst mit viel Aufwand neu zusammengestellt werden. Ist der Antrag bei einer öffentlichen Stelle gestellt worden, die über die gewünschten Informationen nicht verfügt, so hat sie den Antrag an die zuständige Stelle weiterzuleiten bzw. den Antragsteller über den richtigen Adressaten des Antrags zu unterrichten.

Dürfen die Behörden auch Informationen über meine Person an Andere herausgeben? Kann ich mich dagegen schützen?

Der Umgang mit Informationen über einzelne Bürgerinnen und Bürger ist unter Berücksichtigung der datenschutzrechtlichen Vorgaben festgelegt. Der prinzipielle Schutz dieser Daten kann aber ausnahmsweise zurücktreten, wenn beispielsweise das Informationsinteresse der Allgemeinheit oder auch eines Einzelnen für gewichtiger befunden wird. Bevor aber personenbezogene Daten an einen Dritten herausgegeben werden, sehen die existierenden Informationsfreiheitsgesetze vor, dass der Betroffene hierüber grundsätzlich zu informieren ist und die Gelegenheit erhält, sich hierzu zu äußern. Werden seine Daten gegen seinen Willen offenbart und hält er dies für rechtswidrig, kann er dagegen auch juristisch vorgehen.

Welche Informationen dürfen oder müssen allgemein verweigert werden?

Ausdrücklich ausgenommen sind in der Regel bestimmte öffentliche und private Belange. So wäre es beispielsweise gegenüber dem öffentlichen Interesse nicht zu vertreten, durch die Offenbarung von bestimmten Informationen eine wirksame Rechtsdurchsetzung zu vereiteln oder den behördlichen Entscheidungsprozess zu beeinträchtigen. Auch bleiben sicherheitsrelevante Daten nicht zugänglich. Als private Belange sind die Betriebs- und Geschäftsgeheimnisse von Unternehmen und personenbezogene Daten einzelner Bürger geschützt. Ebenfalls sind private Daten geschützt, soweit das geistige Eigentum (Urheber-, Marken-, Patent-, Gebrauchs-, Geschmacks-Muster-rechtlich geschützte Rechte) einer Offenbarung entgegen stehen.

Kostet das etwas?

Ja! Die bestehenden Informationsfreiheitsgesetze sehen für die Erteilung von Auskünften, für die Gewährung der Akteneinsicht oder auch für die Anfertigung von Kopien die Erhebung von Verwaltungsgebühren oder die Erstattung von Auslagen in einem angemessenen Rahmen vor, da die Bearbeitung der Anträge häufig mit einem erheblichen Verwaltungs- und Personalaufwand verbunden ist.

Was kann ich tun, wenn ich mich individuell beraten lassen möchte oder mir Auskünfte verweigert werden?

In den Ländern, die über ein Informationsfreiheitsgesetz verfügen, können Sie sich an den bzw. die Landesbeauftragte/n für den Datenschutz und Informationsfreiheit wenden, dem/der auch die Wahrung des Rechts auf Informationszugang obliegt. Auf der Bundesebene ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig. Nach den bestehenden Informationsfreiheitsgesetzen ist diesen Stellen die Aufgabe übertragen worden, die Bürger bei der Wahrnehmung ihrer Informationszugangsrechte zu unterstützen. Sie beraten sowohl die Bürger als auch anfragende Behörden und fungieren im Streitfall quasi als außergerichtliche Schiedsstelle. Dies gilt allerdings nicht für Hamburg. Unabhängig davon können Sie natürlich auch die ihnen zustehenden Rechtsmittel gegen behördliche Entscheidungen einlegen (Widerspruch, Klage zum Verwaltungsgericht).

22 Sachverzeichnis

F

G

H

I

S

T

U

V

W

Z

23 Abkürzungsverzeichnis

ALG	Arbeitslosengeld
Add-On	Ein Add-On ist ein Erweiterungspaket für Anwendungen
AO	Abgabenordnung
App	Ein App ist z.B. eine Anwendung für Smartphones
ARGE	Arbeitsgemeinschaft
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMF	Bundesministerium der Finanzen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BverfG	Bundesverfassungsgericht
Drs	Drucksache
EA	Einheitlicher Ansprechpartner
ed	erkennungsdienstlich
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
eGo-Saar	Zweckverband elektronische Verwaltung für saarländische Kommunen
eGovernment	Electronic Government, elektronische Verwaltung
ELENA	Elektronisches Entgeltnachweisverfahren
ELStAM	Elektronische Lohnsteuer-Abzugs-Merkmale
EU	Europäische Union
EUREKA	EDV-Unterstützung für Rechtsgeschäftstellen und Kanzleien
EUROPOL	Europäisches Polizeiamt
EUROJUST	Einheit für justizielle Zusammenarbeit der Europäischen Union
EVB-IT	Ergänzende Vertragsbedingungen für die Erstellung eines IT-Systems
EVS	Entsorgungsverband Saar
EVSG	Gesetz über den Entsorgungsverband Saar
EWG	Europäische Wirtschaftsgemeinschaft

FLZ	Führungs- und Lagezentrale
GEZ	Gebühreneinzugszentrale
GPS	Global Positioning System
GZPZ	Gemeinsames Zentrum für landesübergreifende Polizei- und Zollzusammenarbeit
ID	Identifikator, Kennung
IFG	Informationsfreiheitsgesetz
IFK	Konferenz der Informationsfreiheitsbeauftragten in Deutschland
InfÜVPol	Informationsübermittlungsverordnung Polizei
INPOL	Informationssystem der Polizei des Bundes und der Länder
INSPIRE	Infrastructure for spatial information in the European Community
IP	Internetprotokoll
IPSec	Internetprotokollsecurity
IT	Informationstechnik
JVA	Justizvollzugsanstalt
K A N	Kriminalaktennachweis
KaInDÜV	Katasterinhalts- und Datenübermittlungsverordnung
KommHVO	Kommunalhaushaltsverordnung
KPS	Kriminalpolizeiliche Sammlung
KRISTAL	Kriminalpolizeiliches System zur täter- und tatorientierten Analyse und Lagedarstellung
KSVG	Kommunalselbstverwaltungsgesetz
KWG	Kommunalwahlgesetz
LfDI	Die Landesbeauftragte für Datenschutz und Informationsfreiheit
LWG	Landtagswahlgesetz
LWO	Landeswahlordnung
MeldDÜV	Meldedatenübermittlungsverordnung
MG	Meldegesetz
OK	Organisierte Kriminalität
OWiG	Ordnungswidrigkeitengesetz
PKS	Polizeiliche Kriminalstatistik
PMK	Politisch motivierte Kriminalitäten

POLADIS	Polizeiliches anwendungsorientiertes dezentrales Informationssystem
SAWG	Saarländisches Abfallwirtschaftsgesetz
SchoG	Schulordnungsgesetz
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SIFG	Saarländisches Informationsfreiheitsgesetz
SJStVollzG	Saarländisches Jugendstrafvollzugsgesetz
SpolG	Saarländisches Polizeigesetz
StA	Staatsanwaltschaft
Steuer-ID	Steueridentifikationsnummer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVollzG	Strafvollzugsgesetz
SverfSchG	Saarländisches Verfassungsschutzgesetz
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAN	Transaktionsnummer
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TVL	Tarifvertrag für der öffentlichen Dienst der Länder
WkW	Soziales Netzwerk „wer kennt wen?“