UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

24. Tätigkeitsbericht

2011/2012

24. Tätigkeitsbericht

Unabhängiges Datenschutzzentrum Saarland

für die Jahre 2011 und 2012

dem Landtag und der Landesregierung
vorgelegt am 26.06.2013

Unabhängiges Datenschutzzentrum Saarland

Fritz-Dobisch-Straße 12, 66111 Saarbrücken
Postfach 102631, 66026 Saarbrücken
Tel.: 0681/94781-0, Fax: 0681/94781-29
E-Mail: poststelle@datenschutz.saarland.de
Internet: www.datenschutz.saarland.de
www.informationsfreiheit.saarland.de

Vorwort

Die Landesbeauftragte für Datenschutz und Informationsfreiheit hat dem Landtag und der Landesregierung jeweils für zwei Kalenderjahre einen Bericht über ihre Tätigkeit sowohl für den Datenschutz als auch für die Informationsfreiheit vorzulegen.

Der vorliegende Bericht schließt an den mit Datum vom 1. März 2011 vorgelegten 23. Tätigkeitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit für die Jahre 2009/2010 an und deckt den Zeitraum zwischen 1. Januar 2011 und 31. Dezember 2012 für den Datenschutz im öffentlichen Bereich sowie für die Informationsfreiheit ab.

Zugleich schließt er an den im Mai 2011 veröffentlichten 5. Tätigkeitsbericht für den Datenschutz im nicht-öffentlichen Bereich des Ministeriums für Inneres und Europaangelegenheiten an und deckt den Zeitraum vom 2. Juni 2011 bis zum 31. Dezember 2012 für den nicht-öffentlichen Bereich ab.

Mit Gesetz vom 18. Mai 2011 zur Änderung des Saarländischen Datenschutzgesetzes (SDSG), in Kraft getreten am 2. Juni 2011, wurde die Zuständigkeit für die Datenschutzaufsicht im nicht-öffentlichen Bereich, die bislang beim Ministerium für Inneres und Europaangelegenheiten angesiedelt war, auf die Landesbeauftragte für Datenschutz und Informationsfreiheit des Saarlandes übertragen.

Wie bereits im 23. Tätigkeitsbericht dargestellt, basiert diese Zusammenlegung auf einer Entscheidung des Europäischen Gerichtshofes vom 9. März 2010, der auf der Grundlage der Europäischen Richtlinie für Datenschutz die völlige Unabhängigkeit der Datenschutzaufsicht gefordert hat.

Das Unabhängige Datenschutzzentrum Saarland ist seit Inkrafttreten der Änderung des SDSG für den Datenschutz sowohl im öffentlichen als auch im nicht-öffentlichen Bereich zuständig und gewährt mit seinen Mitarbeitern eine einheitliche datenschutzrechtliche Beratung und Kontrolle für alle datenschutzrechtlichen Eingaben und Anfragen der Bürgerinnen und Bürger, der Unternehmen und der öffentlichen Stellen des Saarlandes.

Daher ist dieser 24. Tätigkeitsbericht zugleich auch der erste des Unabhängigen Datenschutzzentrums Saarland.

Durch die Gründung des Unabhängigen Datenschutzzentrums Saarland wurde damit eine Dienststelle geschaffen, die außerhalb der bekannten Behördenstruktur angesiedelt ist, um die Einflussnahme auf Entscheidungen zu vermeiden und den Datenschutz zu stärken.

Die organisatorische Neugestaltung des Datenschutzzentrums und die Öffentlichkeitsarbeit zur Vorstellung dieser neuen Dienststelle als Ansprechpartner für datenschutzrechtliche Belange haben ganz wesentlich die Tätigkeit der Landesbeauftragten für Datenschutz und Informationsfreiheit und ihrer Mitarbeiter in den vergangenen zwei Jahren mitgeprägt.

In verschiedenen Veranstaltungen und Veröffentlichungen wurden aktuelle Themen vorgestellt und auf allgemeine und besondere datenschutzrechtliche Voraussetzungen etwa für die Installation von Kameras im Arbeitsleben, im öffentlichen oder auch im privaten Bereich hingewiesen. Weiterhin fanden Veranstaltungen zum Datenschutz im Internet und in sozialen Netzwerken, aber auch bezüglich der Nutzung von Software-Tools durch Firmen statt.

Das Unabhängige Datenschutzzentrum Saarland wird seine Öffentlichkeitsarbeit fortsetzen, um weiter mehr Sensibilisierung für datenschutzrechtliche Belange zu erreichen und damit neben der Kontroll- und Aufsichtstätigkeit den Datenschutz zu stärken.

So sollen Bürger und Unternehmer, Behördenmitarbeiter und Beschäftigte gleichermaßen durch leicht zugängliche Informationen und Beratung ihre Rechte erkennen und wahrnehmen können. Das Recht auf informationelle Selbstbestimmung kann am besten von demjenigen wahrgenommen werden, der die Gefahren des gläsernen Menschen erkennt.

Das saarländische Informationsfreiheitsgesetz wurde im Jahre 2011 fünf Jahre alt und zum Jubiläum mit unterschiedlichen Fortbildungsveranstaltungen für Mitarbeiter von Kommunen und Behörden beworben. Im Herbst 2012 wurde dann mit Flyern und Plakaten eine Informationskampagne für die Bürgerinnen und Bürger auf den Weg gebracht. Das Recht auf Informationsfreiheit ist notwendiger Bestandteil eines modernen Staates. Ein transparentes Behördenhandeln schafft Vertrauen und ist damit auch ein Motor für ein demokratisches Handeln. Die Gesetzeslage schafft hierfür eine Basis, die sowohl verbreitert als auch öffentlicher gemacht werden sollte.

Die breit gefächerte Tätigkeit der Dienststelle als Beratungs-, Aufsichts- und Kontrollbehörde wird in diesem Bericht ausführlich und anhand einzelner Fälle dargestellt.

Saarbrücken, im Juni 2013

Judith Thieser

Die Landesbeauftragte
für Datenschutz und Informationsfreiheit
im Saarland

Inhaltsverzeichnis

1 Vorbemerkung

Die Tätigkeit aller Mitarbeiter der Dienststelle war im Berichtszeitraum stark geprägt durch die stetig zunehmende Zahl von Videokameras im öffentlichen und privaten Umfeld.

Am Arbeitsplatz, in Restaurants, auf Parkplätzen, auf dem Schulhof, in einem Aufzug eines Mietshauses, im Taxi, im Wald, in Treppenhäusern, auf einem Friedhof, im Außenbereich eines Cafés, in der Toilette einer Kneipe - die Plätze für die Kameras sind so vielfältig wie das Leben, wobei die Voraussetzungen einer Videoüberwachung meist unbekannt sind und daher im konkreten Fall die Kamera oft unzulässig betrieben wird.

Das Beobachten von Personen im öffentlichen oder nicht öffentlichen Raum stellt einen Eingriff in das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung dar. Ein Eingriff in dieses Rechtsgut bedarf daher einer verfassungsmäßigen gesetzlichen Grundlage, damit eines Gesetzes oder einer Einwilligung (§ 4 Abs. 1 Bundesdatenschutzgesetz bzw. § 4 Saarländisches Datenschutzgesetz).

Es gibt auch sehr restriktive gesetzliche Regelungen für Videoüberwachungsmaßnahmen in öffentlich zugänglichen Räumen sowohl im saarländischen Datenschutzgesetz als auch im Bundesdesdatenschutzgesetz. Am Arbeitsplatz ist eine Videoüberwachung zur Verhaltens- und Leistungskontrolle überhaupt nicht zulässig.

Dem Bürger und auch dem Unternehmer fällt es zunehmend schwer, die Grenzen des Zulässigen zu erkennen, wenn die digitale Technik bereits beim Diskounter für wenig Geld zu erwerben, einfach zu bedienen ist und auf den ersten Blick dem Einzelnen Vorteile und Beweisgrundlagen verschaffen kann. Die großen Gefahren des Missbrauchs der persönlichen Daten werden dadurch oft in den Hintergrund gedrängt.

Im Berichtszeitraum haben wir daher neben der Bearbeitung von Eingaben und Beschwerden auch in den Vorträgen und durch Öffentlichkeitsarbeit immer wieder auf die Voraussetzungen für den Einsatz von Videokameras hingewiesen.

Es gibt aber auch Positives zu berichten. Im Bereich der öffentlichen Verwaltung war nach der von meiner Dienststelle initiierten Umfrage zur Videoüberwachung im Jahre 2010 die Aufklärungsarbeit so umfassend, dass gegen Ende des Berichtszeitraumes die Beschwerden zurückgehen und in vielen Fällen im Vorfeld der Installation der Videokameras die Abstimmung mit meiner Dienststelle gesucht wird.

Ein weiterer Schwerpunkt war im Berichtszeitraum der Umgang mit dem Internet. Sei es durch die Nutzung von sozialen Netzwerken oder auch von Diensten im Netz, in vielfältiger Weise kommen Kunden und Anbieter im öffentlichen und nicht öffentlichen Bereich immer wieder an die Grenzen der Privatsphäre, müssen ihre Daten preisgeben, oft ohne zuerkennen, wer diese wo und zu welchem Zweck nutzt.

Auf einer Vielzahl von Homepages von Firmen werden Analysetools genutzt, um Kundeninteressen zu erkennen und die Produkte und Dienstleistungen besser zu bewerben.

Soweit hierzu persönliche Daten des Besuchers der Webseite genutzt werden, ohne dass dieser das überhaupt erkennen kann, verstößt dies gegen die Bestimmungen des Datenschutzrechtes.

Nachdem Google 2011 auf Intervention der Datenschutzbeauftragten des Bundes und der Länder – vertreten durch den hamburgischen Landesbeauftragten sein Analysetool Google Analytics datenschutzkonform gestaltet hat, hat der Düsseldorfer Kreise – als freiwilliger Zusammenschluss der Aufsichtsbehörden - die Voraussetzungen für den datenschutzkonformen Einsatz formuliert und bekannt gemacht.

2012 haben Mitarbeiter meiner Dienststelle eine Prüfsoftware entwickelt und konnten damit feststellen, dass von 4.500 Webseiten saarländischer Unternehmer 840 Seiten Google Analytics einsetzten und über 630 Webseiten nicht die datenschutzkonformen Voraussetzungen einhielten.

Durch Anschreiben, persönliche Unterstützung, einen Aufsatz in der Mitgliederzeitschrift der IHK und eine Informationsveranstaltung bei der IHK Saarland haben wir dann die Firmen informiert und Hilfestellungen gegeben, wie eine datenschutzgerechte Installation erreicht werden kann.

Die Veröffentlichung von persönlichen Daten im Internet kann weitreichende Folgen haben wie ein weiter Fall zeigt.

Eine Feuerwehr hatte auf ihrer Internetseite Einsatzbilder eines Kaminbrandes eingestellt. Die Versicherung des Hauseigentümers wollte den Schaden nicht ersetzen, weil man dem Eigentümer anhand der Einsatzbilder der Feuerwehr zur Last legte, dass Efeu im Außenbereich am Kamin hochgerankt sei, was auf eine fahrlässig Handhabung des Hausbesitzers hindeutete. Aufgrund unserer Intervention hat man sich in der Kommune darauf verständigt, künftig auf die Veröffentlichung von Einsatzbildern zu verzichten.

In einem anderen Fall hat sich ein Bürger an uns gewandt wegen der Veröffentlichung seines Namens, seiner Adresse sowie Bilder seines Baugrundstückes auf einer Webseite. Hier war aufgrund des Sachverhaltes die Veröffentlichung der Bilder, nicht aber die des Namens zulässig.

Ein weiterer Schwerpunkt im öffentlichen Bereich waren die Fragen nach der Zulässigkeit des Einsatzes von Ratsinformationssystemen und Live-Stream Übertragungen aus Stadtrats- und Gemeinderatssitzungen.

Bei den eingesetzten Ratsinformationssystemen der Kommunen geht es um eine internetbasierende Software, die unterschiedliche Module bietet und entweder die Arbeit der Stadt- und Gemeinderäte unterstützt oder darüber hinaus Bürgerinformationen bietet. Je nach Anwendungsbereich sind auch die datenschutzrechtlichen Anforderungen unterschiedlich.

Wenn auch der Einsatz der Systeme, die die Arbeit zwischen Verwaltung und Mandatsträger erleichtern sollen, grundsätzlich zulässig ist, so sind doch jeweils bestimmte technische und organisatorische Maßnahmen zu erfüllen, da etwa die Tagesordnungen der Ratssitzungen umfangreiche sensible Daten enthalten können, die zum einen vor unbefugtem Zugriff geschützt werden müssen, zum anderen auch die technische Sicherheit der Daten auf den einzelnen Rechnern gewährleistet sein muss.

Bei den Bürgerinformationssystemen ist der Maßstab der datenschutzrechtlichen Anforderung an die Weitergabe der personenbezogenen Daten - mangels besonderer Rechtsgrundlage - die Prüfung der Erforderlichkeit zur Aufgabenerfüllung.

Dies stellt sich in der Praxis insbesondere für die Verwaltungen als hoher Aufwand dar, so dass ich ausdrücklich dafür plädiere hier eine gesetzliche Grundlage zu schaffen, die auch den Räten die Möglichkeiten lässt, Einzelheiten in einer Geschäftsordnung zu regeln.

Die an uns herangetragene Frage der Zulässigkeit der Übertragung von Ratssitzungen im Internet bedarf ebenfalls einer umfassenden rechtlichen Bewertung.

Live-Stream Übertragungen von Ratssitzungen sind nicht nur unter dem Wunsch nach mehr Transparenz zu sehen, sondern eben auch wegen der weltweiten Weitergabe von personenbezogenen Daten, die auch nicht mehr gelöscht werden können und unterliegen damit einer datenschutzrechtlichen Prüfung.

Auch nach dem KSVG sind Sitzungen des Gemeinderates nur dann öffentlich, soweit nicht Rücksichten auf das öffentliche Wohl oder berechtige Interessen Einzelner entgegenstehen. Fragen, ob Medienöffentlichkeit gewollt oder aber - wie bei Gerichtsverhandlungen - Saalöffentlichkeit gemeint ist, sind zu prüfen und datenschutzrechtlich auf der Grundlage der allgemeinen Aussagen des SDSG zu bewerten. Des Weiteren ist die Frage zu beantworten, ob alle Anwesenden in die Übertragung freiwillig und umfassend informiert einwilligen müssen oder ein Mehrheitsbeschluss oder gar wie bei der Rundfunkübertragung eine Entscheidung des Vorsitzenden ausreicht.

Auch hier wäre eine gesetzliche Regelung wünschenswert, die in einigen Bundesländern bereits auf den Weg gebracht ist.

Leider ist es heute noch so, dass gewerbliche Streaming Dienstleister ihre Daten überwiegend auf Servern im EU-Ausland - meist in den USA - zumindest zwischenspeichern, so dass dann eine Zulässigkeit nach europäischem Datenschutzrecht in der Regel nicht gegeben ist.

Auf Bundes- und europäischer Ebene war der Entwurf der neuen Datenschutz-Grundverordnung für die Mitgliedsstaaten der Europäischen Gemeinschaft der Themenschwerpunkt schlechthin.

Im Januar 2012 hat die Europäische Kommission den Entwurf einer „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (Datenschutz-Grundverordnung) vorgestellt, die die bisherige EU-Datenschutzrichtlinie vom 24. Oktober 1995 (RL 95/46/EG) ersetzen soll.

Bereits im Jahre 2011 hat sich die Datenschutzkonferenz mit dieser Thematik eingehend befasst und Vorschläge und Stellungnahmen auch zu der Frage abgegeben, ob denn eine in den einzelnen Mitgliedsstaaten umzusetzende Richtlinie oder eine unmittelbar geltende Verordnung den Datenschutz sichert und weiter voranbringt.

Der vorgelegte Verordnungsentwurf hat dann im Jahre 2012 zu umfassenden Stellungnahmen und Anregungen geführt, die im Ansatz in diesem Bericht nachzulesen sind, eine abschließende Vorstellung des neuen europäischen Rechtsrahmens kann nach dem Willen der Kommission frühestens 2014 erfolgen.

2 Änderung des SDSG

Vor dem Hintergrund der Entscheidung des Europäischen Gerichtshofs vom 09.03.2010, wonach die Datenschutzaufsicht über den nicht-öffentlichen Bereich „völlig unabhängig“ sein muss, hat der saarländische Gesetzgeber im Jahre 2011 durch eine Änderung des Saarländischen Datenschutzgesetzes (SDSG) die Datenschutzaufsicht für den nicht-öffentlichen Bereich neu geregelt. Mit der Gründung des Unabhängigen Datenschutzzentrums Saarland ist die bisher vom Ministerium des Innern wahrgenommene Datenschutzaufsicht im nicht-öffentlichen Bereich in die Zuständigkeit der Landesbeauftragten für Datenschutz und Informationsfreiheit übergegangen.

Im Rahmen dieses Gesetzgebungsverfahrens habe ich umfangreiche Änderungen des SDSG vorgeschlagen, die jedoch leider nur teilweise übernommen worden sind.

2.1 Novellierung des Saarländischen Datenschutzgesetzes im Jahre 2011

Durch Artikel 1 des Gesetzes zur Änderung des Saarländischen Datenschutzgesetzes vom 18. Mai 2011 (Amtsbl. I, S. 184) wurden die §§ 8, 25, 26 und 29 des Gesetzes geändert und § 28a neu eingefügt.

Im Wesentlichen wurden folgende Änderungen in Kraft gesetzt:

Durch den neu geschaffenen § 28a SDSG wurde der Landesbeauftragten für Datenschutz die Zuständigkeit für die Kontrolle der Durchführung des Datenschutzes im Aufgabenbereich des dritten Abschnittes des Bundesdatenschutzgesetzes sowie für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 43 des Bundesdatenschutzgesetzes übertragen.

Ebenso wurde der Landesbeauftragten auch die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 36 SDSG übertragen.

Durch die in § 25 SDSG erfolgte die Benennung der nunmehr für den öffentlichen und den nicht-öffentlichen Bereich zuständigen Datenschutzaufsichtsbehörde als „Unabhängiges Datenschutzzentrum Saarland“ soll die vom Europäischen Gerichtshof geforderte Unabhängigkeit der Kontrollstelle hervorgehoben werden.

Um der neuen Bedeutung des Amtes der Landesbeauftragten für Datenschutz gerecht zu werden, wurde das Vorschlagsrecht der Landesregierung hinsichtlich einer Kandidatin bzw. eines Kandidaten für dieses Amt gestrichen.

Zudem wurde § 25 SDSG dahingehend geändert, dass die Zuweisung des Personals und sonstige Personalmaßnahmen im Einvernehmen mit der Landesbeauftragten für Datenschutz erfolgen müssen. Bisher war hierfür nur die Herstellung eines Benehmens erforderlich.

Schließlich wurde den Behörden und öffentlichen Stellen aufgegeben, den behördlichen Datenschutzbeauftragten die Teilnahme an Fort- und Weiterbildungsmaßnahmen zu ermöglich und deren Kosten zu übernehmen.

Infolge der neuen Zuständigkeiten wurde der Stellenplan beim Unabhängigen Datenschutzzentrum um drei Stellen erweitert. Die Personalisierung war am 1. Juni 2012 abgeschlossen. Die Anmietung weiterer Räume erfolgte zu Beginn des Jahres 2012 nach der Wirksamkeit des neuen Haushaltes.

2.2 Änderungsvorschläge der Landesbeauftragten für Datenschutz

Ich stelle hier einige wesentliche Änderungsvorschläge aus dem Gesetzgebungsverfahren 2010/2011 dar, die aber bis heute nicht umgesetzt worden sind. Die Notwendigkeit dieser Änderungen sehe ich nach wie vor als gegeben an.

2.2.1 Datenschutzverordnung für den Landtag

Unter anderem habe ich gefordert, eine eigene Datenschutzverordnung für den Landtag zu schaffen.

Bisher ist das SDSG nur für die dortige Verwaltungstätigkeit anwendbar. Dies wird mit der herausgehobenen verfassungsrechtlichen Stellung des Parlamentes im System der Gewaltenteilung begründet. Gleichwohl sind auch im Rahmen der parlamentarischen Arbeit die grundrechtlich geschützten Persönlichkeitsrechte der Bürger zu beachten. Wie Betroffene ihre Datenschutzrechte gegenüber den Landtagsfraktionen wahrnehmen können, bleibt jedoch offen. Unbestreitbar ist, dass hier kein datenschutzfreier Raum bestehen darf. Durch eine Datenschutzordnung des Landtages, wie diese bereits in anderen Bundesländern existiert, würde daher Klarheit geschaffen.

2.2.2 Datenschutzrechtliche Verantwortlichkeit der Schulen

Nach geltender Rechtslage besteht die unbefriedigende Situation, dass die Gemeinden und Gemeindeverbände verantwortliche Stellen für die Verarbeitung von Schüler- und Lehrerdaten sind, obwohl sie auf die Datenverarbeitung in inneren Schulangelegenheiten nach den schulrechtlichen Regelungen keinen Einfluss nehmen können. Diesen Gegebenheiten der Schulorganisation würde es besser entsprechen, die datenschutzrechtlichen Verpflichtungen insoweit der Schule aufzuerlegen.

2.2.3 Einwilligung in die Datenverarbeitung

Die Freiwilligkeit und Eindeutigkeit der Einwilligung sollten deutlicher im Gesetz herausgestellt werden. In der Praxis ist immer wieder der Fall

anzutreffen, dass sich verantwortliche Stellen auf Einwilligungen berufen, die unter faktischem Zwang abgegeben worden sind.

2.2.4 Auftragsdatenverarbeitung

Bei der Regelung im SDSG zur Auftragsdatenverarbeitung wurden wesentliche Änderungen vorgeschlagen.

Durch das Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009 wurde unter anderem die Vorschrift über die Auftragsdatenverarbeitung im Bundesdatenschutzgesetz geändert.

Die entsprechende Vorschrift im Saarländischen Datenschutzgesetz sollte an die Regelung des Bundesdatenschutzgesetzes angepasst werden, um insoweit ein einheitliches Schutzniveau zu gewährleisten.

Entsprechend der Regelung in § 11 BDSG sollten die gesetzlichen Anforderungen an die Ausgestaltung des Auftrags konkretisiert werden, um mehr Rechtssicherheit für die beteiligten Auftragnehmer und Arbeitgeber sowie die Aufsichtsbehörden zu gewährleisten.

Die Bußgeldvorschriften des SDSG sollten auch für diesen Bereich um einen Bußgeldtatbestand erweitert werden.

2.2.5 Verpflichtung der Behörden zur Bestellung eines Datenschutzbeauftragten

Das Bundesdatenschutzgesetz und die Datenschutzgesetze der meisten Bundesländer sehen (zumindest, wenn Daten in der Behörde automatisiert verarbeitet werden) die Bestellung behördlicher Datenschutzbeauftragter als zwingende Verpflichtung vor. Eine entsprechende Verpflichtung sollte auch in das SDSG aufgenommen werden. Der behördliche Datenschutzbeauftragte ist wegen seiner Präsenz vor Ort in besonderer Weise geeignet, Beratungs- und Kontrollfunktionen wahrzunehmen.

2.2.6 Technischer und organisatorischer Datenschutz

Das Recht auf informationelle Selbstbestimmung kann nur gewährleistet werden, wenn es durch besondere Vorkehrungen für die technische Durchführung und Organisation der Erhebung, Verarbeitung und Nutzung personenbezogener Daten gesichert wird. Angesichts der weit fortgeschrittenen Digitalisierung der automatisierten Datenverarbeitung und ihrer Allgegenwart, angesichts der Verkettbarkeit personenbezogener Daten kommt technischen und organisatorischen Schutzvorkehrungen eine immer größere Bedeutung zu. Die besten rechtlichen Verarbeitungsbeschränkungen sind praktisch wertlos, wenn ihre technische und organisatorische Absicherung fehlt oder mangelhaft ist.

Die Konzeption des Saarländischen Datenschutzgesetzes wird diesen Anforderungen indes nicht mehr gerecht. Die in § 11 SDSG aufgeführten einzelnen Maßnahmen zur Gewährleistung des technischen und

organisatorischen Datenschutzes stammen noch aus der Zeit der Großrechnertechnologie und bilden die Anforderungen, die an heutige IT-Szenarien zu stellen sind, nur unzureichend ab. Sie fußen auf homogenen, zentralen, einheitlich organisierten und von einer Stelle betriebenen IT-Strukturen; einer Situation, wie sie vielfach nicht mehr anzutreffen ist. Heutige IT-Lösungen sind oftmals durch ausgeprägt dezentrale Strukturen, einen hohen Vernetzungsgrad, verteilte Anwendungen und Verantwortlichkeiten und unterschiedliche Betreiber gekennzeichnet (Internet-Portale, Online-Shops, RFID-Anwendungen, ortsbezogene Dienste etc.).

Mit den vorhandenen technisch-organisatorischen Regelungen kann dem nur unzureichend entsprochen werden. Sie lassen sich nur noch mit Mühe auf die heutige Welt vernetzter Systeme übertragen.

Das Bundesverfassungsgericht hat in seinem Urteil zur Online-Durchsuchung (Az.: 1 BvR 370/07, 1 BvR 595/07) bei der Formulierung des neuen „IT-Grundrechts" ebenfalls die Sicherheitsziele „Vertraulichkeit" und „Integrität" aufgegriffen.

Einige Bundesländer haben im Rahmen der Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ihre Datenschutzgesetze bereits entsprechend geändert (Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Sachsen, Thüringen). Die Aufnahme ausdrücklich bezeichneter Datenschutzziele entsprechend der o.g. Nomenklatur ist ein Schritt hin zur Vereinheitlichung der technisch-organisatorischen Regelungen in den einzelnen Datenschutzgesetzen.

Die bisher in § 11 Absatz 2 enthaltenen Kontrollarten („8 Gebote") sollen durch elementare, technologieunabhängige Datenschutzziele ersetzt. Aus den Schutzzielen lassen sich dann konkret in der Praxis zu treffenden Maßnahmen ableiten.

2.2.7 Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Am 1. September 2009 ist ein neuer § 42 a BDSG in Kraft getreten, der Daten verarbeitende Unternehmen in bestimmten Fällen verpflichtet, seine Kunden 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 Schadensersatzansprüche geltend machen. Darüber hinaus kann die Informationspflicht geeignet sein, die Verantwortlichen zu veranlassen, verstärkt präventive Datenschutzmaßnahmen zu ergreifen.

Es ist angesichts der Bedeutung von Datenschutzpannen auch in der öffentlichen Verwaltung nicht nachvollziehbar, dass der Anwendungsbereich in § 42 a BDSG auf nicht-öffentliche Stellen beschränkt ist. Für den Bereich der Sozialleistungsträger hat der Bundesgesetzgeber reagiert und eine entsprechende Vorschrift in das Sozialgesetzbuch X auf-

genommen (§ 83 Abs. 1 SGB X). Auch das Berliner Datenschutzgesetz vom 2. Februar 2011 enthält eine entsprechende Informationspflicht.

Ein Verstoß gegen die Benachrichtigungspflicht sollte durch einen entsprechenden Bußgeldtatbestand sanktioniert werden.

3 Europäischer Datenschutz

3.1 Neuer europäischer Rechtsrahmen

Im Januar 2012 hat die Europäische Kommission den Entwurf einer „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr " (im Folgenden: Datenschutz-Grundverordnung) vorgestellt, die die bisherige EU-Datenschutzrichtlinie vom 24. Oktober 1995 (RL 95/46/EG) ersetzen soll.

Das Revolutionäre an diesem Entwurf ist die Tatsache, dass erstmals in allen 27 EU Staaten ein einheitliches Datenschutzrecht gelten soll. Diese Verordnung ist abschließend, sieht allerdings eine Vielzahl delegierter Rechtsakte für die Kommission vor. Solche Rechtsakte sind nach dem Vertrag über die Europäische Union zulässig, wenn das Parlament der Kommission die Befugnis überträgt, bestimmte nicht wesentliche Vorschriften eines EU-Gesetzes oder Rahmengesetzes zu ergänzen oder zu ändern – mit anderen Worten, darüber zu beschließen.

Neben dem Entwurf für die Datenschutz-Grundverordnung hat die Europäische Kommission auch eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (JI-Richtlinie) vorgestellt.

Bereits 2011 hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (freiwilliger Zusammenschluss des Bundes- und der Landesbeauftragten für Datenschutz mit regelmäßigen Konferenzen) in ersten Konsultationen zu den Positionen der EU-Kommissarin Frau Viviane Reding, Stellung bezogen. Damals ging man aber davon aus, dass erneut eine Richtlinie in Brüssel verabschiedet werden soll, die dann von den einzelnen Mitgliedsländern mit unterschiedlichem Schutzniveau umgesetzt werden soll.

Zwischenzeitlich – Anfang 2013 – ist klar, dass die EU zur Stärkung des freien Datenverkehrs jedenfalls eine unmittelbar geltende Verordnung verabschieden wird; das Maß und die einzelnen Regelungen scheinen aber umstrittener denn je.

Die Rechtsgrundlage der Verordnung findet sich in Art. 8 der Charta der Grundrechte der europäischen Union, die einen besonderen Schutz der persönlichen Daten seit dem Inkrafttreten des Vertrages von Lissabon am 1. Dezember 2009 erstmals festschreibt. Weitere Ausformulierungen finden sich auch in Art. 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).

Die im Entwurf inzwischen in vielen Konferenzen, aber auch in den Ausschüssen des europäischen Parlamentes diskutierte Verordnung unterscheidet nicht zwischen dem öffentlichen und dem nicht-öffentlichen Bereich. Sie soll daher - unmittelbar - in beiden Bereichen gelten, soweit nicht ausdrücklich eine Ausnahme vorgesehen ist. Die Normen der Mitgliedstaaten treten weitgehend außer Kraft, somit auch das Bundesdatenschutzgesetz, die Landesdatenschutzgesetze und eine Reihe spezialgesetzlicher Rechtsnomen.

Die Verordnung sieht Befugnisse für Regelungen der Mitgliedstaaten „im Rahmen der Verordnung“ nur noch in den Bereichen Presse, Medien, Gesundheitswesen, Beschäftigtendaten sowie Wissenschaft und Forschung vor.

Der Entwurf reformiert aber auch den Datenschutz in der EU und regelt in verschiedenen Punkten eine Verbesserung für den Datenschutz in Europa.

So ist ein Anspruch auf Vergessen im Internet vorgesehen und die Möglichkeit, bisher gespeicherte Daten beim Wechsel zu einem neuen Anbieter mitzunehmen; europaweit tätige Unternehmen sollen nur einen Ansprechpartner bei den Aufsichtsbehörden haben und in großen Unternehmen ist verpflichtend ein Datenschutzbeauftragter zu bestellen. Gleichzeitig gelten diese Datenschutzbestimmungen auch für außereuropäische Firmen, die mit EU-Bürgern Geschäfte machen wollen.

Die 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Stellungnahme zu den beiden Reformvorschlägen verabschiedet, die in der Entschließung "Ein hohes Datenschutzniveau für ganz Europa!" vom 21./22.03.2012 zusammengefasst.

Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22. März 2012 in Potsdam

Ein hohes Datenschutzniveau für ganz Europa!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union zu modernisieren und zu harmonisieren.

Der Entwurf einer Datenschutz-Grundverordnung enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

- *das Prinzip Datenschutz durch Technik,*
- *der Gedanke datenschutzfreundlicher Voreinstellungen,*
- *der Grundsatz der Datenübertragbarkeit,*
- *das Recht auf Vergessen,*
- *die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen und*
- *die verschärften Sanktionen bei Datenschutzverstößen.*

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst hohes Niveau für alle Mitgliedsstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedsstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatli-

che Datenverarbeitungsvorgänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittelbar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutzniveaus den Mitgliedsstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv. Die Konferenz bedauert deshalb, dass die Kommission grundsätzlich nur Unternehmen mit mindestens 250 Beschäftigten zur Bestellung von Datenschutzbeauftragten verpflichten will. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Über die bereits in dem Verordnungsentwurf vorgeschlagenen Modernisierungen hinaus hält die Konferenz weitere Schritte für erforderlich, die sie etwa in ihrem Eckpunktepapier für ein modernes Datenschutzrecht vom 18. März 2010 vorgeschlagen hat:

- *eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,*
- *ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis*
- *eine Anhebung der Altersgrenze,*
- *die Förderung des Selbstdatenschutzes,*
- *pauschalierte Schadensersatzansprüche bei Datenschutzverstößen,*
- *einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,*
- *das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und*
- *die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.*

Die Regelungen zur Risikoanalyse, Vorabkontrolle und zur Zertifizierung bedürfen der weiteren Präzisierung in der Verordnung selbst.

Für besonders problematisch hält die Konferenz die vorgesehenen zahlreichen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte, die dringend auf das unbedingt erforderliche Maß zu reduzieren sind. Alle für den Grundrechtsschutz wesentlichen Regelungen

müssen in der Verordnung selbst bzw. durch Gesetze der Mitgliedsstaaten getroffen werden.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf der Datenschutz-Grundverordnung vorgesehene Kohärenzverfahren, welches die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb vereinfacht und praktikabler gestaltet werden.

Die durch Artikel 8 der EU-Grundrechte-Charta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Europäischen Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter dem deutschen Datenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung). Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

Die Konferenz erklärt, dass sie den Gang des Gesetzgebungsverfahrens konstruktiv und kritisch begleiten wird.

Die Vizepräsidentin der EU-Kommission, auch Kommissarin für das Ressort Justiz, Grundrechte und Bürgerschaft, Viviane Reding, hatte die Konferenz am 21.03.2012 in Potsdam besucht und für ihren Kurs – mehr Datenschutz in ganz Europa - geworben.

Die Landesbeauftragten für den Datenschutz und der Bundesbeauftragten haben am 20.06.2012 in Brüssel ihr Anliegen bei den Vertretern der Kommission, der führenden Ausschüsse und des Rates vorgetragen.

Die 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 7./8. November 2012 nach einem Interparlamentarischen Treffen zum Thema "Datenschutz" am 9./10. Oktober 2012 in Brüssel eine Entschließung mit dem Thema „Europa muss den Datenschutz zügig voranbringen" auf den Weg gebracht.

Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. November 2012 in Frankfurt (Oder)

Europäische Datenschutzreform konstruktiv und zügig voranbringen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies bereits in

ihrer Entschließung vom 21./22. März 2012 verdeutlicht. In zwei umfassenden Stellungnahmen vom 11. Juni 2012 haben die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl einzelner Aspekte der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtssetzungsprozess gegeben.

Angesichts der aktuellen Diskussionen in Deutschland und im Rat der Europäischen Union sowie entsprechender Äußerungen aus der Bundesregierung im Rahmen des Reformprozesses betont die Konferenz folgende Punkte:

- *Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der Datenschutz-Grundverordnung an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall regeln und die so genannte alltägliche Datenverarbeitung weitgehend ungeregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden.*

  Jede Verarbeitung scheinbar „belangloser" Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je.

  Deshalb lehnt es die Konferenz ab, angeblich „belanglose" Daten von einer Regelung auszunehmen.

  Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.

- *Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich beizubehalten und insbesondere für die Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.*

- *Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.*

- *Mit Blick auf die Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.*

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich im Sinne dieser Positionen im Rat der Europäischen Union für die Belange eines harmonisierten Datenschutzrechts auf einem hohen Niveau einzusetzen.

4 Technisch-organisatorischer Datenschutz

4.1 Mobile Endgeräte – Kommunikation, überall!

Noch vor etwa zehn Jahren stand das klassische Mobiltelefon (Handy) im Fokus mobiler Endgeräte. Es konnte neben der Telefonie Kurznachrichten (SMS) senden und empfangen und verfügte über ein integriertes Telefonbuch. Spätere Modelle waren mit einem Terminplaner mit Notiz- und Aufgabenfunktion ausgestattet. Parallel dazu gab es erste Organizer, wie z.B. Handhelds, PDAs oder MDAs, mit denen Adressdaten, Kalendereintragungen oder kleine Notizen erfasst werden konnten. Der Datenaustausch erfolgte mittels Datenkabel zwischen mobilem Gerät und Desktop-PC. Spätere mobile Modelle ermöglichten einen kabellosen Datenaustausch z.B. von E-Mails via ActiveSync zu einem Exchange-Server.

Die fortschreitende Miniaturisierung ermöglichte Ende der 2000er Jahre die Herstellung leistungsfähiger mobiler Endgeräte, deren Nutzungsumfang vergleichbar der damaligen Desktop-PCs war. Die Verschmelzung von Mobiltelefon und Internetzugang zu den heutigen Smartphones und die Weiterentwicklung von Touchscreen-Notebooks zu Tablet-Computern eröffnete den Herstellern neue Märkte und den Endanwendern neue Nutzungsmöglichkeiten. Die Leistungsfähigkeit heutiger mobiler Endgeräte entspricht heutzutage modernen Desktop-PCs. Der Erfolg mobiler Endgeräte geht vor allem auf die permanente Verfügbarkeit der mobilen Internetnutzung zurück.

In einer Mitteilung zur digitalen Agenda für Europa prognostiziert die Europäische Kommission, dass im Jahr 2015 weltweit 25 Milliarden drahtlos vernetzte Geräte eingesetzt würden.[1] Laut Eurostat lag die Nutzung des mobilen Internet mittels Smartphone 2012 bei 24% und mittels Tablet-Computer bzw. Notebook bei 22%. Vor allem junge Menschen nutzen das Internet von mobilen Endgeräten aus.[2] Das Statistische Bundesamt berichtete im Dezember 2012, dass 33% der Unternehmen mobiles Internet einsetzen.[3] Einer Onlinestudie von ARD/ZDF zu Folge umfasste der Anteil der mobilen Internetnutzung im Jahr 2012 23%, bezogen auf die Gesamtinternetnutzung.[4] In dieser Studie sind auch die am meisten mobil genutzten Internetdienste aufgeführt, wie etwa Internetrecherchen über Suchmaschinen, Senden und Empfangen von E-Mails, Surfen im Internet, Abrufen von Online-Nachrichten, Kommunikationsaustausch in sozialen Netzwerken, Onlinebanking, Chatten, oder das Nutzen von Anwendungen (sogenannter Apps).

Der Mehrwert des Einsatzes von mobilen Endgeräten liegt auf der Hand. Diese Geräte ermöglichen den Anwendern, permanent und von

[1] Vgl. Europäische Kommission: Die Digitale Agenda für Europa – digitale Impulse für das Wachstum in Europa, Brüssel 18.12.2012, COM(2012) 784 final, S. 3.
[2] Vgl. Eurostat: Statistics in focus, Industry, trade an services, 50/2012, http://epp.euro-stat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-12-050/EN/KS-SF-12-050-EN.PDF
[3] Vgl. Statistisches Bundesamt: https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2012/12/PD12_447_52911.html
[4] Vgl. van Eimeren, Birgit / Frees, Beate: Mediaperspektiven 7-8/2012, ARD/ZDF-Onlinestudie 2012, http://www.ard-zdf-onlinestudie.de/fileadmin/Online12/0708-2012_Eimeren_Frees.pdf

beliebigen Orten aus über das Internet mit vielen Menschen zu kommunizieren. Sei es per E-Mail oder über soziale Netzwerke. Ebenso sind die Anwender immer auf dem aktuellen Nachrichtenstand. Darüber hinaus bieten mobile Endgeräte unter anderem die Möglichkeit der Anwendung von Office-Anwendungen zum Bearbeiten von Texten oder Tabellen. Auch der mobile Zugriff auf Unternehmens-Infrastrukturen stellt ein Plus mobiler Endgeräte dar. Der Mobilität scheinen keine Grenzen gesetzt zu sein.

Allen Vorteilen zum Trotz, bestehen vor allem im professionellen Einsatz Risiken in der Verwendung mobiler Endgeräte. Auch wenn sie auf den ersten Blick nicht erkennbar sind. So enthalten mobile Endgeräte eine Vielzahl personenbezogener Daten, auch die Daten Dritter, wie z.B. E-Mails, Kontaktdaten, Fotos, Audio- und Videodaten oder Standortdaten. Oftmals werden Daten automatisch gespeichert und unbemerkt an weitere Nutzer verteilt. Diese intransparente Datenweitergabe wird durch unsichere Apps oder durch die Kommunikation in sozialen Netzwerken begünstigt. Dadurch werden beispielsweise Kontaktdaten für andere Anwendungen, sogenannter Apps, zugänglich. Vor allem bergen Apps das Risiko, dass sie während der Installation Zugriff auf geräteinterne Sensoren erhalten und Informationen über den Benutzer, wie z.B. Standort- oder Kontaktdaten, an den Hersteller der App senden.

4.1.1 Risikoanalyse

Den in Verbindung mit dem Einsatz mobiler Endgeräte auftretenden Risiken gilt es im professionellen Einsatz entgegenzuwirken. Deshalb ist es ratsam, dass vor dem Einsatz mobiler Endgeräte eine Risikoanalyse durchgeführt wird. In dieser werden Fragen geklärt, was zu beachten ist wenn zum Beispiel: mobile Geräte verloren gehen, ein Gerät von Viren befallen ist, Daten verloren gehen, ein Gerät zerstört wird, Daten ausspioniert werden oder Daten manipuliert werden. Zum Vermeiden dieser und weiterer Gefahren sollten konkrete Schutzmechanismen erarbeitet werden, die umzusetzen sind.

Neben den Gefahren sollte im Vorfeld über den Umfang (Anzahl der Geräte, Personenkreis?) der einzusetzenden Geräte Klarheit bestehen, ebenso die Gerätearten die zum Einsatz kommen (Smartphones und/oder Tablet-PCs?). Auf Grund der Vielzahl am Markt verfügbarer Gerätetypen, sollte nach Möglichkeit ein einheitliches Betriebssystemkonzept erarbeitet werden, d.h. welche Geräte mit welchen Betriebssystemen (iOS, Android, Windows) werden beschafft. Ein heterogener Geräteeinsatz bringt Sicherheitsrisiken für die IT-Infrastruktur des Unternehmens oder der Behörde mit sich und erhöht den IT-Administrationsaufwand.

Empfehlenswert ist, abhängig von der Anzahl der zu verwendenden Geräte, der Einsatz einer zentralen Geräteverwaltung, eines sogenannten Mobile-Device-Management. Mit einem solchen System können Richtlinien erarbeitet werden, die gewisse Routinen automatisch ausführen, wie z.B. die Betriebssysteme der mobilen Endgeräte auf dem neuesten Stand zu halten, oder die Aktualisierung der Virensoftware.

4.1.2 Klare Regeln

Unabhängig von zentralen Managementsystemen müssen klare Regeln für die Installation und die Nutzung von Apps vereinbart werden, da die Nutzung dieser Anwendungen durchaus, wie oben geschildert, mit Sicherheitsrisiken behaftet sind. Über die Datensicherung und Datenwiederherstellung sind Strategien zu entwerfen, ebenso die Art des Zugriffs auf Unternehmens- bzw. Behördennetzwerke. Eine essentielle Sicherheitsmaßnahme für mobile Endgeräte stellt die PIN-Abfrage dar. Darüber hinaus sollte der Zugang zum Unternehmens- bzw. Behördennetz nur mittels Kennwortabfrage gewährt werden. Der Einsatz mobiler Geräte erfordert das Erarbeiten von Strategien im Umgang mit gestohlenen Geräten. Hierbei stellt sich die Frage, wie solche Geräte gesperrt und bereinigt werden können und ob deren Standort verfolgbar ist.

Für den Fall, dass die mobilen Endgeräte auch privat genutzt werden, ist eine getrennte Datenhaltung, d.h. eine Trennung privater und dienstlicher Daten zu implementieren, z.B. durch sogenannte Containerlösungen. Hier ist vor allem auf die Einhaltung des Fernmeldegeheimnisses hinzuweisen.

Um den sicheren Einsatz mobiler Endgeräte zu gewährleisten, sind weitere technisch-organisatorische Maßnahmen zu ergreifen, wie z.B. Software- und Sicherheits-Updates, die Aktualisierung von Virenscannern, Richtlinien zum sicheren Umgang mit externen Speicherkarten, wie z.B. microSD-Karten, Richtlinien zum Überprüfen der Hardwareschnittstellen (USB-Port, Bluetooth, NFC, WiFi, WLAN), Sicherheitsmaßnahmen zum Verhindern unbeabsichtigter oder unfreiwilliger Datenweitergabe.

4.1.3 Bring-Your-Own-Device

Ein weiterer zu betrachtender Punkt stellen private mobile Endgeräte dar, die dienstlich genutzt werden. (Stichwort: Bring-Your-Own-Device). Hierbei handelt es sich grundsätzlich um Fremdgeräte, die Zugriff auf Unternehmens- bzw. Behördennetze erhalten. Diesbezüglich sind Strategien zu erarbeiten, die festlegen, wie zu handeln ist, wenn solche Geräte beispielsweise verloren gehen.

Für die Unternehmen oder Behörden ist es wichtig, dass alle dienstlichen Daten vom jeweiligen Gerät entfernbar sind, ohne die privaten Daten anzutasten. Auch hier gilt es, eine strikte Trennung der Daten einzuhalten.

4.1.4 Sensibilisierung der Mitarbeiterinnen und Mitarbeiter

Die genannten Maßnahmen dienen als Beispiele, um den Einsatz mobiler Endgeräte sicher zu realisieren. Über die technisch-organisatorischen Maßnahmen hinaus, sind die Mitarbeiterinnen und Mitarbeiter im Hinblick auf Sicherheitsrisiken und Datenschutz zu sensibilisieren und zu schulen. Es ist immens wichtig, dass sie die vom Unternehmen oder der Behörde eingeführten Sicherheitsmaßnahmen nicht umgehen, sondern umsetzen und sparsam mit der Nutzung von Diensten, Apps und Daten umgehen sowie ihr mobiles Endgerät nicht aus der Hand geben oder

liegen lassen. Auch ist Vorsicht im Umgang mit Internetdiensten geboten.

Laut Prognosen steigt die Anzahl mobiler Endgeräte und wird womöglich in Zukunft die Desktop-Computer verdrängen. Mit ihrer Ausstattung und Rechenleistung vereinen sie eine Vielzahl multimedialer Eigenschaften, wie Fotografie, Internet, Video oder Audio in einem Gerät. Die Übertragungsgeschwindigkeit wird durch LTE noch schneller. Mobile Endgeräte können heute schon als Universalgeräte genannt werden. In Verbindung mit der Einhaltung von Sicherheits- und Datenschutzrichtlinien werden sie auch zu sicheren Geräten.

4.2 IPv6 – Ein Mehr an Internet

Das Internet ist mehr als das World Wide Web und mehr als eine bloße Verknüpfung zwischen Rechnern und Netzwerkkomponenten. Das Internet ist vielmehr wie ein lebender Organismus, bestehend aus vielen Gliedern, gebildet durch Netze und Unternetze, an denen die diversesten Endgeräte stationär oder mobil physikalisch angeschlossen sind. Die Menschen, welche diese Endgeräte bedienen, nutzen die unterschiedlichsten Internet-Dienste, wie z.B. das WWW, E-Mail, Chat, Newsgroups, Internet-Telefonie, Internet-Radio oder Internet-TV. Durch das Nutzen des Internets werden unzählige Informationen der unterschiedlichsten Motivationen zwischen den unterschiedlichsten Sendern und Empfängern über unzählige Netzwerke und unterschiedliche Standorte ausgetauscht. Die Übermittlung dieser Informationen erfolgt über eine Einteilung der Daten in Pakete.

Das Internet Protokoll dient hierbei als „Paketvermittler" auf der Netzwerkebene. Vor über 30 Jahren wurde das Internet Protokoll in der Version 4 (IPv4) standardisiert. Dieses, noch heute gängige Protokoll, besitzt eine Länge von 32 Bit, mit der sich 2^{32}, d.h. 4,3 Milliarden Endgeräte adressieren lassen. Diese Adressierungsform galt in der Anfangszeit des Internet als ausreichend. Durch die wachsende Anzahl der mit dem Internet verbundenen Geräte zeigte sich Mitte der 1990er Jahre, dass in absehbarer Zeit die Adressen knapp würden. Um einem möglichen IP-Engpass vorzubeugen entwickelte die ICANN[5] ein Nachfolgeprotokoll, welches von der IETF[6] im Jahr 1998 unter dem Namen IPv6[7] standardisiert wurde. Die Dringlichkeit einer weltweiten Einführung des neuen Internetprotokolls ist erst mit der Vergabe der letzten IPv4-Adressen im Jahr 2011 erkannt worden. Mit dem IPv6 werden die heutigen physikalischen Grenzen des Internets aufgehoben. Theoretisch ergeben sich mit dem neuen Protokoll $3{,}4 * 10^{38}$ Kombinationsmöglichkeiten.[8]

Das Internet Protokoll in der Version 6 steht für ein Mehr an Internet, mit seinen facettenreichen Anwendungen und Verknüpfungen bis hin in das tägliche Leben der Menschen. Der neue IP-Standard führt zu einem weiteren Wachstum, bzw. steht für eine Weiterentwicklung des Internets, mit all seinen Dingen, wie z.B.: Smart Home (selbstständig Waren bestellende Kühlschränke, intelligente Elektroninstallationen, stromspa-

[5] ICANN = Internet Corporation for Assigned Names and Numbers.
[6] IETF = Internet Engineering Task Force.
[7] Vgl. Wikipedia, http://de.wikipedia.org/wiki/IPv6, aufgerufen am 20.02.2013.
[8] Vgl. Beck, Dr. Holger (2012), Doppelpunkt! Das künftige Internetprotokoll verstehen, in: Deutsches Forschungsnetz Mitteilungen, Verein zur Förderung eines Deutschen Forschungsnetzes e.V. (Hrsg.), Ausgabe 83, Berlin, November 2012, S. 14-20.

rende Waschmaschinen, elektronisches Bezahlen an der Haustüre), IP-Telefonie, mobile Endgeräte, Cloud-Computing, Big Data, Logistik, Sensorik, Internet der Dinge, Geolokalisierung (LKW-Maut, intelligente PKWs), Darstellung von Energiekostenmodellen.

Das Internet als große Wolke, in der sich das gesamte Leben abspielt, mit allen positiven wie negativen Elementen

Am 6. Juni 2012, dem sogenannten „World IPv6 Launch Day", startete das neue Internetprotokoll. Geplant ist, die IPv4-Adressen innerhalb einer Dekade auf das neue System umzustellen. Diese Umstellung wirkt sich auch auf Datenschutz und Datensicherheit aus. Aus diesem Grund untersuchen seit geraumer Zeit die deutschen Datenschutzbeauftragten sowie ihre Kollegen weltweit, welche Chancen und Risiken mit dem Umstieg zu IPv6 verbunden sind.

In ihrer Entschließung „Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!" befasste sich die 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, vom 28./29. September 2011 in München, ausführlich mit dieser Thematik.

„Viele Betreiber und Anwender stellen in diesen Monaten ihre Netzwerktechnik auf das Internet-Protokoll Version 6 (IPv6) um. Grundsätzlich darf es mit einer Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung der technischen Rahmenbedingungen zur Ausgestaltung von Privacy kommen. Neuen Herausforderungen muss mit wirksamen Konzepten begegnet werden.

IPv6 stellt eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung, die eine dynamische Vergabe von IP-Adressen, wie sie zur Zeit bei Endkunden gängig ist, aus technischer Sicht nicht mehr erforderlich macht. Aber durch die Vergabe statischer Adressen erhöht sich das Risiko, dass Internetnutzende identifiziert und ihre Aktivitäten auf einfache Weise webseitenübergreifend zu individuellen Profilen zusammen geführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile in den IPv6-Adressen machen eine dauerhafte Identifizierung möglich. Die Zuordnung einer IP-Adresse zu einer bestimmten Person bedarf nicht zwingend einer Beteiligung des Zugangsanbieters. Mit Hilfe von Zusatzinformationen, die dem Betreiber eines Internetangebots vorliegen oder ihm offenstehen, beispielsweise Identifikationskonten von Online-Shops oder Sozialen Netzen, ist eine eindeutige Zuordnung von Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Mit Blick darauf, dass sich ein Identifikationsrisiko aus beiden Teilen der neuen Adressen ergeben kann, sind Maßnahmen in unterschiedlichen Bereichen erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit zu gewährleisten. Anbieter von Internetzugängen und Diensten sowie Hersteller von Hard- und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten (privacy by design) und dementsprechende Voreinstellungen wählen (privacy by default). Internetnutzenden sollten bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

- *Access Provider sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.*

- *Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.*

- *Hard- und Softwarehersteller sollten die „Privacy Extensions" unterstützen und standardmäßig einschalten (privacy by default), um die Wiedererkennung von Nutzenden anhand von Hardwareadressen zu erschweren.*

- *Die Hard- und Softwarehersteller sollten Lösungen für dezentrale Kommunikationsdienste (peer to peer) in Kundensystemen entwickeln, die den Verzicht auf zentrale Plattformen und Portale ermöglichen. Sie sollten interessierten Dritten die Entwicklung solcher Dienste gestatten.*

- *Content Provider dürfen zur Reichweitenmessung nur die ersten 4 Bytes der IPv6-Adresse heranziehen und müssen den Rest der Adresse löschen, denn eine Analyse von Nutzungsdaten ist nach Ansicht der Datenschutzaufsichtsbehörden nur auf der Grundlage anonymisierter IP-Adressen zulässig. Die ersten 4 Bytes sind für eine Geolokalisierung ausreichend.*

- *Zugangsanbieter und Betreiber von Internetangeboten sollten nicht protokollierende Proxy-Server einsetzen und die Voraussetzungen schaffen, dass ein Internetzugang oder die Nutzung von im Internet bereitgestellten Inhalten in anonymer Form möglich ist (Anonymisierungsdienste).*

Hersteller und Anbieter von Betriebssystemen und vorkonfigurierten Geräten (wie PCs, Smartphones und Routern) sollten ihre Anstrengungen bei der Pflege und Weiterentwicklung ihrer Produkte intensivieren und regelmäßig Fehler bereinigte Versionen ihrer IPv6-fähigen Software anbieten.

- *Angesichts häufig mangelnder Reife von IPv6-fähigen Produkten ist Anwendern vom Einsatz von IPv6 innerhalb von lokalen Netzen noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.*

- *Eigentümerinnen und Eigentümer von IP-Adressen dürfen nur auf Wunsch in das weltweite, stark zentralisierte „Internet-Telefonbuch" whois aufgenommen werden. Die Bundesregierung wird aufgefordert, sich für eine datenschutz- freundliche Gestaltung des whois-Dienstes einzusetzen, dahingehend, dass die Internet-Verwaltung ICANN den whois-Dienst künftig als verteilte Datenbank gestaltet, so dass die Daten der Eigentümerinnen und Eigentümer jeweils durch lokale Dienstleister oder Selbstverwaltungsgremien gespeichert, gepflegt und von ihnen nach Maßgabe des lokalen Rechts an Dritte übermittelt werden.*

Die Datenschutzbeauftragten des Bundes und der Länder werden die Einführung von IPv6 wachsam beobachten und bieten allen Akteuren ihre Unterstützung an."

5 Justiz

5.1 Prüfung der Justizvollzugsanstalt Saarbrücken

Im Berichtszeitraum führte ich eine umfassende datenschutzrechtliche Prüfung der für den Vollzug der Freiheitsstrafe und der Untersuchungshaft an männlichen Erwachsenen zuständigen Justizvollzugsanstalt (JVA) Saarbrücken durch.

Da die Gesetzgebungskompetenz für den Strafvollzug durch die Föderalismusreform aus dem Jahre 2006 auf die Länder übergegangen ist, wird – nachdem das Saarland in Ausübung dieser Gesetzgebungskompetenz bislang sowohl für den Jugendstrafvollzug als auch für die Untersuchungshaft entsprechende Vollzugsgesetze erlassen hat – im Jahre 2013 auch ein Erwachsenenstrafvollzugsgesetz für das Saarland erlassen werden.

Dementsprechend diente die nunmehr durchgeführte Prüfung neben der Kontrolle, ob die in den bisher geltenden Vorschriften enthaltenen datenschutzrechtlichen Vorgaben umgesetzt werden, auch dem Zweck, zu prüfen, ob und inwieweit sich die bestehenden Vorschriften bewährt haben und in welchen Bereichen gegebenenfalls bei zukünftigen Vorschriften Änderungen berücksichtigt werden sollten.

5.1.1 Behördlicher Datenschutzbeauftragter

Bei unserem Kontrollbesuch war zwar festzustellen, dass die Anstalt ihrer datenschutzrechtlichen Verantwortung durch die Bestellung eines behördlichen Datenschutzbeauftragten nachgekommen ist. Allerdings war auch zu konstatieren, dass der Funktion des Datenschutzbeauftragten nicht die erforderliche Bedeutung beigemessen wurde.

Dies zeigte sich schon unter dem formalen Aspekt, dass die Funktion des Datenschutzbeauftragten in dem Geschäftsverteilungs- und Organisationsplan der Anstalt nicht ausgewiesen war und auch eine allgemeine Bekanntmachung seiner Berufung in der Anstalt nicht erfolgt ist. Eine ausdrückliche Freistellung für die mit dieser Tätigkeit verbundenen Aufgaben ist ebenfalls nicht erfolgt. Bislang war der behördliche Datenschutzbeauftragte auch nur punktuell mit datenschutzrechtlichen Fragen befasst. Dementsprechend konnten keine Verfahrensbeschreibungen vorgelegt werden und bislang sind durch den Datenschutzbeauftragten in der Anstalt auch noch keine datenschutzrechtlichen Kontrollen durchgeführt worden.

Die Anstalt hat unseren Kritikpunkten jedenfalls insoweit schon Rechnung getragen, dass sie Person und Funktion des Datenschutzbeauftragten mittlerweile innerhalb der Anstalt sowohl bei den Bediensteten als auch bei den Gefangenen bekanntgegeben hat und dies auch nach außen durch Aufführung im Geschäftsverteilungsplan wahrnehmbar ist. Wie ich aus datenschutzrelevanten Vorhaben der Justizvollzugsanstalt aus jüngster Zeit aus eigener Anschauung wahrnehmen kann, ist er zwischenzeitlich in die Bearbeitung datenschutzrelevanter Abläufe in der Anstalt eingebunden.

5.1.2 Gefangenenpersonalakten

§ 183 Abs. 1 StVollzG sieht vor, dass sich der einzelne Vollzugsbedienstete von personenbezogenen Daten der Gefangenen, und damit auch von in den Gefangenenpersonalakten enthaltenen Angaben, nur Kenntnis verschaffen darf, soweit dies zur Erfüllung der ihm obliegenden Aufgabe oder für die Zusammenarbeit nach § 154 Abs. 1 StVollzG erforderlich ist. Akten und Dateien sind nach § 183 Abs. 2 Satz 1 StVollzG durch die erforderlichen technischen und organisatorischen Maßnahmen gegen unbefugten Zugang und Gebrauch zu schützen.

Nach der bisher in der Anstalt geübten Praxis hinsichtlich der Einsichtnahme in die Gefangenenpersonalakten kann eine große Anzahl von Beschäftigten auf den vollständigen Inhalt der Akten zugreifen, ohne dass im Einzelfall eine Kontrolle darüber erfolgt, ob ein Einblick im konkreten Fall für die Belange des Vollzugs notwendig ist. Angesichts der Vielzahl der in den Akten enthaltenen, zum Teil auch sehr sensiblen Daten war diese Praxis zu beanstanden, da es der Schutz des informationellen Selbstbestimmungsrechtes des Betroffenen gebietet, seine persönlichen Daten nur in den wirklich notwendigen Fällen zu offenbaren.

Um sicherzustellen, dass tatsächlich diejenigen Mitarbeiter, die die jeweiligen Unterlagen zur konkreten Aufgabenerfüllung benötigen, im erforderlichen Umfang Zugriff auf die Gefangenenpersonalakte erhalten, wurde in meinem Prüfbericht gefordert, entsprechende organisatorische Vorkehrungen zu treffen. Des Weiteren habe ich darauf hingewiesen, dass es auch erforderlich ist, die jeweilige Einsichtnahme in die Gefangenenpersonalakten zu dokumentieren.

Auch hierauf hat die Anstalt umgehend reagiert und mitgeteilt, dass durch eine interne Dienstanweisung und durch entsprechende Aushänge auf der Vollzugsgeschäftsstelle darauf hingewiesen worden ist, dass eine Entnahme einer Akte nur nach Dokumentation des Namen des Mitarbeiters, des Datums der Entnahme sowie des Entnahmegrundes sowie nach Gegenzeichnung eines Mitarbeiters der Vollzugsgeschäftsstelle erfolgen darf. Diese Verfahrensweise soll auch für aus dem Archiv zu entnehmende Akten gelten.

Hinsichtlich der im Archiv aufbewahrten Gefangenenpersonalakten zeigten sich bei der Prüfung deutliche Mängel bei der Vernichtung von Akten nach Ablauf der maximalen Aufbewahrungsfristen. Hier wurde die Anstalt aufgefordert, dafür Sorge zu tragen, die aufgelaufenen Rückstände zeitnah einer Vernichtung zuzuführen, was diese sodann auch zugesichert hat.

5.1.3 Personalabteilung

Gemäß § 95 Abs. 2 Satz 2 1. Halbsatz des Saarländischen Beamtengesetzes (SBG) ist die Führung von Nebenakten (Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden) zulässig, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für den Beamten zuständig sind. Dies ist meiner Auffassung nach bei der Konstellation JVA Saarbrücken - Ministerium der Justiz der Fall. Nebenakten dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde erforderlich ist (§ 95 Abs. 2

Satz 2 2. Halbsatz SBG). Eine Einsichtnahme in verschiedene Personalakten hat jedoch gezeigt, dass die in der Anstalt geführten Akten auch die Unterlagen enthalten, die nur in der Grundakte enthalten sein dürfen.

Nach Auskunft der Justizvollzugsanstalt habe eine im Zusammenhang mit meinem Bericht erfolgte Überprüfung beim Ministerium der Justiz ergeben, dass es sich bei den in der JVA geführten Personalakten um die Grundakten handele, so dass hier beispielsweise auch sämtliche Einstellungsunterlagen enthalten sein müssten.

Hierzu bedarf es von meiner Seite aus noch eines klärenden Gesprächs mit dem Ministerium der Justiz zur Erläuterung der Gründe für diese im Bereich der obersten Landesbehörden ungewöhnliche Personalaktenführung sowie einer Überprüfung des Inhaltes der beim Ministerium vorhandenen Personalakten.

Ungeachtet der Frage, ob es sich bei den in der Justizvollzugsanstalt geführten Personalakten um die Grund- oder Nebenakten handelt, war bei meiner Prüfung festzustellen, dass diese Akten zahlreiche Unterlagen enthielten, die nicht oder jedenfalls nicht mehr dort hinein gehören. Eine zeitnahe, sukzessive Überprüfung des Inhalts der Akten ist daher dringend geboten.

5.1.4 Videoüberwachung

Im Rahmen der datenschutzrechtlichen Prüfung wurde ein besonderes Augenmerk auf die in den verschiedenen Bereichen der Anstalt eingesetzten Videoüberwachungsanlagen gelegt.

Allgemein war festzustellen, dass ein Übersichtsplan, aus dem sowohl die Anzahl als auch die genaue Anbringung der verschiedenen Kameras ersichtlich sind, nicht existiert. Ebenso wenig sind bislang Verfahrensbeschreibungen für die vorhandenen Anlagen erstellt worden, aus denen sich eine Festlegung von Löschfristen und Regelungen über die Zugriffsbefugnisse auf gespeicherte Daten ergeben. Schließlich fehlen – mit Ausnahme vor Betreten des Besucherbereichs - im Inneren der Anstalt jegliche Hinweise auf eine Videoüberwachung.

Innerhalb der Anstalt finden sich sowohl Bereiche, in denen eine reine Videobeobachtung auf einem Monitor (Kamera-Monitoring-Verfahren) erfolgt, als auch solche Bereiche, in denen eine Speicherung der Aufnahmen stattfindet. Die Speicherdauer soll in diesen Fällen nach Angaben der Anstalt 48 Stunden betragen.

Eine Videoüberwachung, insbesondere die damit verbundene Speicherung der Aufnahmen, stellt einen intensiven Eingriff in das aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitete Grundrecht auf informationelle Selbstbestimmung dar, da die Betroffenen - gerade in einer Justizvollzugsanstalt - in der Regel keine Möglichkeit haben, sich der Überwachung zu entziehen. Daher bedarf eine im überwiegenden Allgemeininteresse erfolgende Einschränkung dieses Rechts nach der Rechtsprechung des Bundesverfassungsgerichts einer gesetzlichen Grundlage, die den Anlass, den Zweck und die Grenzen des Eingriffs bereichsspezifisch, präzise und normenklar festlegt (BVerfG, Beschluss vom 23.02.2007 – 1 BvR 2368/06 -).

Das geltende Strafvollzugsgesetz enthält allerdings keine ausdrückliche bereichsspezifische Rechtsgrundlage für eine kameraunterstützte Überwachung.

Ein reines Kamera-Monitoring-Verfahren durch einen Vollzugsbediensteten kann im Wesentlichen einer Beobachtung durch einen anwesenden Beamten gleichgestellt werden, da die Kamera hierbei als „verlängertes Auge" des Beamten dient, können allenfalls die allgemeinen rechtlichen Grundlagen für Überwachungsmaßnahmen durch Bedienstete der Anstalt für ein reines Kamera-Monitoring als gesetzliche Ermächtigung herangezogen werden.

Als spezielle Vorschrift kann daher im Rahmen der Besuchsüberwachung § 27 Abs. 1 Satz 1 StVollzG, der eine optische Überwachung der Besuche erlaubt, eine Echtzeitüberwachung der Besuche der Gefangenen mittels Videokamera rechtfertigen, da die Übergabe unerlaubter Gegenstände durch Besucher die Sicherheit der Anstalt gefährdet.

Die Echtzeitüberwachungsmaßnahmen im Bereich der Freiflächen, den Treppenaufgängen, den besonders gesicherten Hafträumen und den Wartebereichen in der medizinischen Abteilung können auf die allgemeine Datenerhebungsvorschrift des § 179 Abs. 1 StVollzG gestützt werden, wonach die Vollzugsbehörde personenbezogene Daten erheben kann, soweit deren Kenntnis für den ihr nach dem Strafvollzugsgesetz aufgegebenen Vollzug der Freiheitsstrafe erforderlich ist.

Für eine Speicherung von Aufnahmen innerhalb des Anstaltsbereiches fehlt es indes bislang an einer rechtlichen Grundlage, so dass derartige Maßnahmen derzeit unzulässig sind.

Angesichts des Umstandes, dass eine intensive Überwachung verschiedener Bereiche der Anstalt nach den von uns nicht angezweifelten Darstellungen der Justizvollzugsanstalt zur Abwehr von Gefahren für die Sicherheit der Anstalt unerlässlich ist und allein mit dem derzeitigen Personalbestand nicht gewährleistet werden kann, habe ich aber davon abgesehen, eine unverzügliche Einstellung sämtlicher Überwachungsmaßnahmen, für die keine rechtliche Grundlage existiert, zu verlangen. Dies insbesondere deshalb, weil uns seitens des Ministeriums der Justiz zugesichert wurde, dass spätestens bis zum 01.06.2013 ein Landesstrafvollzugsgesetz verabschiedet werden soll, in dem auch bereichsspezifische Regelungen für den Einsatz von Videoüberwachungsanlagen enthalten sein werden.

Um den Eingriff in das informationelle Selbstbestimmungsrecht der Gefangenen nicht weiter zu vertiefen, habe ich die Anstalt aber aufgefordert, kurzfristig u.a. folgende Anforderungen umzusetzen:

In den Bereichen, in denen nicht nur eine Kamera-Monitor-Überwachung stattfindet, ist eine Speicherung der Aufnahmen nur für einen jeweils konkret festgelegten Zweck und nur in einem zwingend erforderlichen Umfang zulässig. Für die Prüfung, ob die gespeicherten Aufnahmen für den festgelegten Beobachtungszweck weiterhin benötigt werden, wird in der Regel ein Zeitraum von maximal 48 Stunden als ausreichend anzusehen sein. Eine längerfristige Speicherung stellt eine unzulässige Datensammlung auf Vorrat dar.

Es müssen geeignete technische Maßnahmen getroffen werden, um zu gewährleisten, dass durch die Videoüberwachungsmaßnahmen keine schutzwürdigen Interessen Dritter beeinträchtigt werden. Soweit im Rahmen der Überwachung der Freiflächen und der Außenmauer – wenn

auch nur durch kurzfristige Einblendungen auf dem Monitor – Einblicke in Fenster von benachbarten Häusern möglich sind, sind hier die Kameraeinstellungen zu verändern oder Verpixelungen vorzunehmen.

Sicherzustellen ist auch, dass die Gefangenen Kenntnis von den Überwachungsmaßnahmen erhalten. Dies gilt auch für Überwachungsmaßnahmen ohne Aufzeichnungen. Insoweit ist es nicht ausreichend, lediglich in dem Besucherbereich auf eine Überwachung hinzuweisen. Auch ansonsten muss den Gefangenen innerhalb der Anstalt erkennbar sein, in welchen Bereichen eine Überwachung stattfindet. Bei den anzubringenden Hinweisen, sollten Schilder mit Piktogrammen gewählt werden, damit die Überwachung auch für solche Gefangene, die der deutschen Sprache nicht oder nicht hinreichend mächtig sind, erkennbar ist.

Schließlich hat die Anstalt für die eingesetzten Videoüberwachungsanlagen Verfahrensbeschreibungen im Sinne des § 9 des Saarländischen Datenschutzgesetzes (SDSG) zu erstellen, aus denen sich insbesondere auch die Zweckbestimmungen der Verfahren, Löschfristen sowie Regelungen über den Zugriff auf gespeicherte Daten ergeben.

Hinsichtlich der – unbeabsichtigt – erfolgten Einsichtsmöglichkeit in Wohnbereiche angrenzender Häuser hat die Anstalt bereits während unserer Prüfung erste technische Maßnahmen getroffen, die eine Erfassung der Privatbereiche unterbinden. Zwischenzeitlich sollen nach Darstellung der Anstalt auch hinsichtlich der noch ausstehenden Bereiche Lösungsmöglichkeiten erarbeitet und überwiegend umgesetzt worden sein.

In Bezug auf meine Forderung, in den kameraüberwachten Bereichen innerhalb der Anstalt durch Schilder auf die durchgeführte Videoüberwachung hinzuweisen, hat die Anstalt erwidert, dies könne aus Sicherheitsgründen nicht geschehen. Auch wenn es die Sicherheitslage der Anstalt gebieten mag, die Gefangenen nicht detailgenau auf die überwachten und damit konkludent auch auf die nicht überwachten Bereiche hinzuweisen, kann eine verdeckte Videoüberwachung nicht zulässig sein. Auch ein pauschaler Hinweis durch Anbringen eines Schildes im Eingangsbereich der Anstalt vermag der Kennzeichnungspflicht nicht zu genügen, zumal zweifelhaft ist, ob für die Gefangenen bei Betreten der Anstalt überhaupt die Gelegenheit besteht, diesen Hinweis zur Kenntnis zu nehmen. Hinsichtlich dieser Problematik werde ich noch einmal mit den Vollzugsbehörden auf eine sachgerechte Lösung hinarbeiten müssen.

5.1.5 Haftraumbeschilderung

Bereits in der Vergangenheit hat sich meine Dienststelle mit der Anbringung von Namensschildern an den Türen der Hafträume befasst. Damals wurde seitens der JVA die Notwendigkeit hierfür im Wesentlichen mit der hohen Belegung der Anstalt sowie der zunehmenden Zahl zu beachtender Trennungen von Gefangenen begründet. Die Haftraumbeschriftung erleichtere die organisatorischen Abläufe erheblich.

Nunmehr habe ich festgestellt, dass neben der Anbringung der Namen der Gefangenen auch der Umstand, ob und ggf. welcher Beschäftigung der jeweilige Gefangene nachgeht, an der Zellentür angebracht ist. Zur Begründung wurde ausgeführt, dass dies in erster Linie der Gewährleistung der Trennung von Gefangenen diene. Durch die Angabe des Be-

schäftigungsverhältnisses sei für die Bediensteten erkennbar, zu welchen Zeiten die Gefangenen in ihren Zellen bzw. an ihren Arbeitsplätzen seien.

Bei der Angabe des Namens handelt es sich ebenso wie bei der Angabe des Beschäftigungsverhältnisses des Gefangenen um personenbezogene Daten. Durch die Angabe dieser Daten an der Zellentür werden diese an andere Gefangene und an eventuelle Besucher der Anstalt übermittelt. Selbst wenn die Anbringung von Namensschildern an dem den Gefangenen zugewiesenen Lebensbereich mit dem Anbringen eines Namensschildes an einer Wohnungstür verglichen und insgesamt zur Gewährleistung eines geordneten Ablaufs in der Anstalt unter gewissen Umständen als erforderlich angesehen werden kann, kann hiervon bei der zusätzlichen Angabe des Bestehens eines Arbeitsverhältnisses nicht mehr ausgegangen werden. Es ist nicht erkennbar, aus welchen Gründen dieser weitergehende Eingriff in das informationelle Selbstbestimmungsrecht erforderlich sein sollte. Um die Trennung der Gefangenen sicherzustellen, bedarf es für die Vollzugsbediensteten zusätzlicher Informationen, nämlich die genaue Angabe der jeweiligen Gefangenen, die nicht zusammentreffen sollen. In diese Aufzeichnungen, die den Beamten zur Verfügung stehen müssen, können dann auch die jeweiligen Anwesenheitszeiten der Gefangenen in ihren Zellen angegeben werden.

In diesem Bereich konnte bislang leider kein Einvernehmen mit der Anstalt erzielt werden, da diese die Auffassung vertritt, aus Gründen der Sicherheit sowie im Interesse eines geordneten und zügigen Ablaufs sei die Beschriftung an den Haftraumtüren geboten.

5.1.6 Fazit

Insgesamt hat die Prüfung gezeigt, dass bei der Anstaltsleitung durchaus eine datenschutzrechtliche Sensibilität vorhanden ist. Im täglichen Arbeitsablauf ist dem Datenschutz allerdings bislang nicht die erforderliche Bedeutung beigemessen worden. Jedoch schon während unserer Prüfung sind Anstrengungen unternommen worden, um den datenschutzrechtlichen Forderungen nachzukommen. Ein nicht unerheblicher Arbeitsaufwand besteht für die Anstalt allerdings noch in Bezug auf die noch ausstehenden Verfahrensbeschreibungen. In ihrer Stellungnahme zu unserem Prüfbericht hat die Justizvollzugsanstalt in zahlreichen weiteren Bereichen Verbesserungen zugesichert und mittlerweile zum Teil auch schon umgesetzt. In einigen Einzelpunkten besteht allerdings noch Gesprächsbedarf.

Es bleibt zu hoffen, dass die Justizvollzugsanstalt den eingeschlagenen Weg der Stärkung des Datenschutzes in der Anstalt, insbesondere durch eine verstärkte Einbindung des behördlichen Datenschutzbeauftragten fortsetzen wird und die zu erwartende gesetzliche Neuregelung die erforderlichen angemessenen Vorschriften im Bereich des Datenschutzes bringen wird.

5.2 Einsichtnahme in das Grundbuch

Sowohl aufgrund einer Eingabe als auch im Rahmen des bundesweiten Austauschs der Datenschutzbeauftragten des Bundes und der Länder war ich im Berichtszeitraum mit der Frage befasst, inwiefern einem Eigentümer ein Anspruch auf Auskunft über Einsichtnahmen ins Grundbuch durch Dritte zusteht.

Die Rechtsposition des im Grundbuch Eingetragenen genießt grundrechtlichen Schutz. Das Grundbuch und die Grundakten enthalten eine Fülle von personenbezogenen Daten aus dem persönlichen, familiären, sozialen und wirtschaftlichen Bereich. Wenn Dritten eine Grundbucheinsicht gewährt wird, liegt darin ein Eingriff in das auf diese Daten bezogene informationelle Selbstbestimmungsrecht des Eingetragenen.

§ 12 Abs. 1 der Grundbuchordnung (GBO) legt fest, unter welchen Voraussetzungen eine Beschränkung dieses Grundrechtes in Betracht kommt und eine Einsichtnahme in das Grundbuch gestattet werden kann.

Bei maschinell geführten Grundbüchern können bestimmte abrufberechtigte Stellen und Personen auch im Wege eines automatisierten Abrufverfahrens Einsicht in das Grundbuch nehmen. Gemäß § 133 GBO muss hierfür aber sichergestellt sein, dass das Grundbuch nur in dem Umfang eingesehen werden kann, wie dies § 12 GBO zulässt. Um die Rechtmäßigkeit einzelner Abrufe prüfen zu können, muss eine Protokollierung der Abrufe erfolgen.

In einem mir geschilderten Fall hatte der Erwerber eines Grundstücks von einem Grundstücksmakler eine Rechnung über eine Vermittlungsprovision erhalten, obwohl seinem Vorbringen nach zum Zeitpunkt des Hauskaufs der Vermittlungsauftrag bereits beendet gewesen sei. Der Petent vermutete, der Grundstücksmakler habe in rechtlich unzulässiger Weise Einsicht in das Grundbuch genommen und hierbei von dem Erwerbsvorgang erfahren.

Da der Grundstücksmakler nicht zu dem Kreis der abrufberechtigten Stellen und Personen nach § 133 Abs. 2 GBO gehört, bestand keine Pflicht zur Protokollierung der Einsichtnahme gemäß § 133 Abs. 1 Nr. 2 GBO. Eine gesetzliche Verpflichtung zur Protokollierung von Einsichtnahmen in die Papierakten enthält die Grundbuchordnung nicht und dementsprechend auch keinen ausdrücklich normierten Auskunftsanspruch für den Eigentümer. Ungeachtet dessen habe ich von dem Grundbuchamt die Auskunft erhalten, dass dort die Einsichtnahmen in die Papierakten nach § 12 GBO in einem Formular vermerkt werden und dieses Formular entsprechend der Regelung für das Abrufverfahren bis zum Ablauf des auf die Erstellung des Protokolls folgenden Kalenderjahres aufbewahrt wird. Da sich meiner Auffassung nach ein Auskunftsanspruch des Eigentümers auch ohne eine spezialgesetzliche Präzisierung bereits aus dem allgemeinen Datenschutzrecht ergibt, ist diese Verfahrensweise des Grundbuchamts ausdrücklich zu begrüßen.

In dem konkreten Fall war der Aufbewahrungszeitraum allerdings bereits überschritten, so dass anhand der Unterlagen des Grundbuchamtes nicht mehr nachvollzogen werden konnte, ob tatsächlich eine Einsichtnahme durch den Grundstücksmakler erfolgt ist. Demzufolge konnte auch nicht geklärt werden, ob die behauptete Einsichtnahme unter Umgehung der Voraussetzungen des § 12 GBO erfolgt ist und

damit ein datenschutzrechtlich relevanter Verstoß gegen die Vorschriften der Grundbuchordnung vorlag.

Obwohl vorliegend die durch das Grundbuchamt erfolgende Protokollierung von Einsichtnahmen in das Grundbuch nicht zur Klärung des Sachverhaltes beitragen konnte, hat sich gezeigt, dass auch außerhalb des Abrufverfahrens nach § 133 GBO zur Gewährleistung des Persönlichkeitsrechts des Grundstückseigentümers grundsätzlich ein Interesse an einer zumindest klarstellenden gesetzlichen Regelung bezüglich einer Protokollierungspflicht des Grundbuchamtes und eines Auskunftsanspruchs des Eigentümers über Einsichtnahmen in das Grundbuch besteht.

Ein Vorschlag für eine entsprechende Ergänzung der Grundbuchordnung findet sich zwischenzeitlich in dem Gesetzentwurf der Bundesregierung zur Einführung eines Datenbankgrundbuchs vom 21.12.2012 (BR-Drs. 794/12).

5.3 Auskunftsverlangen gegenüber Privaten in Ermittlungsverfahren

Im Berichtszeitraum habe ich mehrfach Anfragen von Firmen erhalten, die von der Polizei oder der Staatsanwaltschaft aufgefordert worden sind, in laufenden Ermittlungsverfahren Auskünfte über Adressdaten ihrer Kunden oder über konkret bezeichnete Inhalte der geschäftlichen Beziehungen zu erteilen. Die Betroffenen befürchteten, durch die Übermittlung der gewünschten Daten ihre datenschutzrechtlichen Verpflichtungen gegenüber ihren Kunden zu verletzen. Andererseits wollten sie sich jedoch auch nicht rechtmäßigen Ermittlungshandlungen der Behörden verschließen.

Die geschilderten Maßnahmen der Staatsanwaltschaft – oder der von dieser in rechtmäßiger Weise beauftragten Polizei – beruhten jeweils auf § 161 Abs. 1 Satz 1 Strafprozessordnung (StPO).

§ 161 Abs. 1 Satz 1 StPO

Zu dem in § 160 Abs. 1 bis 3 bezeichneten Zweck ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln.

Diese Vorschrift berechtigt zu Ermittlungsanfragen der Staatsanwaltschaft auch gegenüber privaten Stellen und bildet damit die Rechtsgrundlage für die allgemeine Erhebung personenbezogener Daten zur Aufklärung von Straftaten (vgl. hierzu BVerfG, Beschluss vom 17.02.2009, NJW 2009, 1405). Die Ermittlungsbehörde ist daher grundsätzlich befugt, die gewünschten Daten zu erheben. Allerdings enthält die Vorschrift keine Verpflichtung des Privaten zur Erteilung der Auskunft. Vielmehr handelt es sich um eine formlose Art der Zeugenvernehmung. Weigert sich der Unternehmer die begehrte Auskunft zu erteilen, muss er jedoch damit rechnen, dass eine förmliche Vernehmung erzwungen, eine Herausgabe verlangt oder eine Durchsuchung und Beschlagnahme angeordnet werden.

Die Befugnis des Unternehmers, die auf der Grundlage des § 161 Abs. 1 Satz 1 StPO angeforderten Auskünfte an die Polizei oder Staatsanwaltschaft zu übermitteln, beruht auf § 28 Abs. 2 Nr. 2b Bundesdatenschutzgesetz (BDSG). Hiernach ist die Datenübermittlung zulässig, soweit sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.

Mit Blick auf die Zweckrichtung der Vorschrift, Straftaten zu verhindern oder aufzuklären, kann allein ein zu unterstellendes Interesse des Betroffenen, keinen polizeirechtlichen oder strafprozessualen Maßnahmen ausgesetzt zu werden, nicht schon der Zulässigkeit einer Übermittlung entgegenstehen. Dies könnte allerdings der Fall sein, wenn erhebliche Bedenken an der Rechtmäßigkeit bzw. Verhältnismäßigkeit der beabsichtigten Maßnahmen bestehen.

Diese Prüfung vorzunehmen, ist indes für die betroffenen Unternehmern schwierig bzw. überhaupt nicht zu leisten.

Ich habe den anfragenden Unternehmen daher geraten, grundsätzlich nur auf schriftliche Aufforderungen der Polizei oder Staatsanwaltschaft unter Angabe der zugrundeliegenden Rechtsvorschrift die angeforderten Daten zu übermitteln. Ergeben sich dann keine Anhaltspunkte für ein schutzwürdiges Interesse des Kunden gegen eine Datenübermittlung, wird dem Unternehmer in der Regel wegen der Übermittlung kein Vorwurf gemacht werden können. Einem möglichen Schadensersatzanspruch seines Kunden wegen unzulässiger Datenübermittlung nach § 7 BDSG wird der Unternehmer dann entgegenhalten können, dass er die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

§ 7 BDSG

Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

Bei nicht auszuräumenden Zweifeln an der Übermittlungsbefugnis wird der Unternehmer jedoch gegenüber der Polizei oder Staatsanwaltschaft auf einer förmlichen Anordnung bestehen müssen.

6 Polizei

6.1 Abfragen aus dem Zentralen Verkehrsinformationssystem ZEVIS

Von den nach dem Straßenverkehrsgesetz (StVG) berechtigten Stellen können Daten aus dem Zentralen Fahrzeugregister (ZFZR), dem Verkehrszentralregister (VZR), dem Zentralen Fahrerlaubnisregister (ZFER) und dem Zentralen Kontrollgerätkartenregister (ZKR) über das Zentrale Verkehrsinformationssystem ZEVIS online abgerufen werden.

§ 36 StVG regelt den automatisierten Abruf von Daten aus dem Zentralen Verkehrsregister durch die Polizeien des Bundes und der Länder für in der Vorschrift konkret festgelegte Zwecke. Insbesondere im Rahmen von Fahrzeugkontrollen, zur Verfolgung von Ordnungswidrigkeiten oder Straftaten oder zur Abwehr von Gefahren ist die Polizei abrufbefugt.

Für Auskünfte zur Verfolgung spezifischer Rechtsansprüche an Privatpersonen sind nach § 39 Abs. 1 StVG die Zulassungsstellen und das Kraftfahrt-Bundesamt (KBA) zuständig. Auf der Grundlage von § 39 Abs. 1 und 2 StVG sollen Daten, die im Rahmen der Zulassung zum öffentlichen Straßenverkehr für die Fahrzeugregister erhoben und dort gespeichert werden, später auch nur für Rechtsansprüche im Zusammenhang mit der Teilnahme am Straßenverkehr wieder im Auskunftswege genutzt werden dürfen.

Betroffene können sich daher für die Erteilung einer einfachen Registerauskunft unter Angabe des Kennzeichens oder der Fahrzeugidentifizierungsnummer direkt an die Zulassungsstellen oder das KBA wenden, wenn sie darlegen, dass sie die Daten zur Geltendmachung, Sicherung, Vollstreckung, Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigen. Unter Darlegung ist eine plausible Behauptung, eine annehmbare Erläuterung oder ein schlüssiger, widerspruchsfreier Sachverhaltsvortrag zu verstehen. Für die Darlegung genügt es z.B., wenn der Auskunftsbegehrende erklärt, dass er durch einen mit Zeitpunkt und Unfallort näher zu bezeichnenden Unfall geschädigt wurde und die Fahrzeug- und Halterdaten zur Realisierung von Schadensersatzansprüchen benötigt. In diesem Falle können sie insbesondere Name und Anschrift des Halters, Angaben zum Fahrzeug und der Versicherung erhalten.

Eine erweiterte Registerauskunft, nämlich die Erteilung von weiteren Fahrzeug- und Halterdaten, darf hingegen nur erteilt werden, wenn der Auskunftsbegehrende unter Angabe von Fahrzeugdaten oder Personalien des Halters glaubhaft macht, dass die Daten zur Geltendmachung, Sicherung, Vollstreckung, Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr, wegen Diebstahl, dem sonstigen Abhandenkommen des Fahrzeugs oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt werden und die Daten auf andere Weise entweder nicht oder nur mit unverhältnismäßigem Aufwand erlangt werden können.

Für eine Glaubhaftmachung ist die Angabe konkret nachprüfbarer Sachverhalte, wie beispielsweise das Aktenzeichen einer Behörde oder eines Gerichts über ein anhängiges Verfahren, erforderlich.

Der Bürger kann mithin auf der Grundlage von § 39 StVG einen Rechtsanspruch auf Übermittlung von Fahrzeug- und Halterdaten gegenüber der zuständigen Zulassungsstelle oder dem KBA selbst realisieren. Wendet sich der Bürger daher zunächst nicht an die Zulassungsstelle oder das KBA sondern zuvor an die Polizei, so hat diese vor Abruf von Daten aus dem Zentralen Fahrzeugregister zu prüfen, ob die Voraussetzungen des § 36 StVG tatsächlich vorliegen. Ist dies nicht der Fall, ist eine ZEVIS-Abfrage durch die Polizei unzulässig.

Da mehrere Eingaben im Berichtszeitraum aufzeigten, dass ZEVIS-Abfragen durch Polizeibeamte zum Teil vorschnell, nicht sachgerecht oder gar unzulässig durchgeführt wurden, wurde in Zusammenarbeit mit dem behördlichen Datenschutzbeauftragten der Polizei ein Merkblatt „Rechtsgrundlagen polizeilicher Abfragen im automatisierten Verfahren" erstellt, welches künftig via Intranet jedem saarländischen Polizeibeamten zur Verfügung stehen soll. Auf diese Weise sollen die saarländischen Polizeibeamten erneut für datenschutzrechtliche Belange im Zusammenhang mit automatisierten Abrufverfahren sensibilisiert werden.

6.2 Personenauskunftsstelle der Vollzugspolizei

Zu Beginn des Berichtszeitraumes teilte mir das Ministerium für Inneres und Europaangelegenheiten zur Wahrung meiner Beteiligungsrechte nach § 7 Abs. 2 Satz 5 SDSG mit, dass die Landespolizeidirektion beabsichtige, die Datenverarbeitungsverfahren „Größere Schadenslagen" (GSL.net) und „Personenauskunftsstelle – Gesprächsdokumentation" (PAS-Dok) einzuführen.

Das Landespolizeipräsidium führte hierzu aus, dass das damalige Ministerium für Inneres und Sport im April 2009 die Vollzugspolizeibehörden des Saarlandes, unter Federführung der Landespolizeidirektion, beauftragt habe, eine Konzeption zur Einrichtung einer Personenauskunftsstelle (PAS) zu erarbeiten. Hierdurch sei dem Beschluss des Arbeitskreis Innere Sicherheit (AK II) Rechnung getragen worden, wonach in jedem Bundesland eine PAS einzurichten sei. Darüber hinaus sollen im Bedarfsfall die Personenauskunftsstellen der Länder in einer Verbundlösung kommunikationstechnisch und organisatorisch zusammengeschaltet werden können.

Die PAS dient in Großschadenslagen, wie beispielsweise Katastrophen, Amoktaten oder Anschlägen mit terroristischem Hintergrund, der EDV-unterstützten systematischen Erfassung und Bearbeitung von Personendaten, um Angehörigen von Schadensopfern möglichst schnell Auskunft erteilen zu können. Die mit den beschriebenen Einsatzlagen einhergehende Gefährdung oder Schädigung des Lebens oder der körperlichen Unversehrtheit zahlreicher Menschen erfordert besondere Maßnahmen zur schnellen und verlustfreien Abwicklung des regelmäßig hohen Hinweisaufkommens sowie zur Zusammenführung des Spurenaufkommens. Im Rahmen einer Kooperation mit der Vollzugspolizei des Landes Rheinland-Pfalz wurde eine gemeinsame PAS eingerichtet. Der entsprechende Kooperationsvertrag ist seit dem 28.01.2011 in Kraft.

Das Verfahren PAS-Dok dient der Dokumentation des Notfallgeschehens sowie der Beweissicherung und Gefahrenabwehr bei größeren Gefahren- und Schadenslagen/Katastrophen sowie großen Schadenslagen. Anrufer können sich kostenfrei über eine gesondert geschaltete Hotline an die Polizei wenden. Vor Speicherung des Gesprächsinhaltes wird der Anrufer informiert, dass der Inhalt des eingehenden Telefonanrufes aufgezeichnet wird. Datum, Uhrzeit, angerufene Servicenummer, Dauer des Telefonats, die Dateigröße sowie die Telefonnummer des Anrufes werden ebenfalls automatisiert gespeichert. Die letzten drei Stellen der Telefonnummer des Anrufers werden jedoch systemseitig anonymisiert. Die Löschung der aufgezeichneten Gespräche erfolgt automatisiert nach 30 Tagen. Die Speicherdauer kann um weitere 30 Tage im Einzelfall verlängert werden, sofern dies erforderlich ist. Die Entscheidung hierüber trifft die verantwortliche Stelle und dokumentiert schriftlich die Gründe, die zur Verlängerung geführt haben. Für den Aufbau des benötigten Call Centers, die Gesprächsdokumentation sowie auch deren Sicherung wurde zwischen einem saarländischem Unternehmen und der Landespolizeidirektion ein entsprechender Auftragsdatenverarbeitungsvertrag geschlossen.

Bei GSL.net handelt es sich um eine Software, die der Einrichtung einer Personenauskunftsstelle dient und die die Erfassung und Auswertung von Hinweisen und Vermisstenanzeigen ermöglicht. Die Einrichtung erfolgt erst nach Eintritt eines Schadensereignisses. Da hierfür etwa 30 Minuten bis zur Einsatzfähigkeit benötigt werden, kann lageabhängig eine erste dezentrale Hinweisaufnahme auf den polizeilichen Arbeitsplatz-PCs durchgeführt werden (Landesweite Alarmierung Rheinland-Pfalz und Saarland – LARS). Die von den Polizeibediensteten im vorläufigen dezentralen Hinweisaufnahmeverfahren LARS erfassten Daten werden nach Inbetriebnahme der Personenauskunftsstelle über eine technische Schnittstelle in GSL.net exportiert. Anschließend werden die Daten in LARS gelöscht. Die in GSL.net gespeicherten Daten werden in der Regel nach Einsatzende, spätestens jedoch nach 6 Monaten gelöscht. Aus Gründen der Erforderlichkeit kann die Speicherdauer um 12 Monate verlängert werden. Auch hier ist die Begründung für die Erforderlichkeit der verlängerten Speicherdauer von der verantwortlichen Stelle zu dokumentieren.

Die sich nach Prüfung der Unterlagen ergebenden datenschutzrechtlichen Fragestellungen wurden im Rahmen einer Präsentationsveranstaltung bei der Landespolizeidirektion des Saarlandes umfassend beantwortet. Aus hiesiger Sicht ist ausdrücklich zu begrüßen, dass keine Schnittstellen zu anderen polizeilichen Systemen vorhanden sind.

Die einschlägigen Rechtsgrundlagen für die erforderlichen Datenerhebungen und -übermittlungen wurden in den jeweiligen Errichtungsanordnungen dezidiert ausgewiesen. Bis zur Einrichtung und Inbetriebnahme von GSL.net kann lageabhängig eine erste dezentrale Hinweisaufnahme (LARS) auf den im saarländischen Polizeinetz angemeldeten Arbeitsplatz PCs erfolgen. Da dieses Verfahren nur für einen begrenzten Zeitraum als Übergangslösung eingesetzt wird und die in LARS gespeicherten Daten nach GSL.net exportiert werden, konnte im Einvernehmen mit unserer Dienststelle auf die Erstellung einer eigenen Errichtungsanordnung verzichtet werden. Die für LARS erforderlichen Angaben wurden in der Errichtungsanordnung zu GSL.net festgeschrieben.

Auch die uns vorgelegte Vertragsgestaltung zur Auftragsdatenverarbeitung zwischen der Landespolizeidirektion Saarland und einem saarländischen Unternehmen trägt den Vorschriften des Saarländischen Daten-

schutzgesetzes insoweit Rechnung, dass die Kontrollrechte der Landesbeauftragten für Datenschutz und Informationsfreiheit gewahrt werden. Die gewählte 256 Bit-SSL–Verschlüsselung für die elektronische Datenübermittlung zwischen dem Server des Unternehmens und den Arbeitsplatzrechnern innerhalb des SLPOL-Netzes bietet nach heutigem Stand der Technik ausreichende Sicherheit vor unberechtigten Zugriffen Dritter.

6.3 IT-Verfahren Funkzellenauswertung

Im Dezember 2011 erhielt ich den Entwurf der Verfahrensbeschreibung für das automatisierte IT-Verfahren „Funkzellenauswertung – Fukz" zur datenschutzrechtlichen Prüfung. Innerhalb dieses IT-Verfahrens werden die Dateien „Turmdatenbank", „Funky" und „Funkzellen-InfoZoom" betrieben, für welche die entsprechenden Errichtungsanordnungen beigefügt waren.

Die systematische Auswertung von Mobilfunkdaten stellt ein wichtiges kriminalpolizeiliches Ermittlungsinstrument zur Aufklärung von Verbrechen und Straftatenserien dar. Ziel der Auswertungen ist es, Zusammenhänge zwischen den bei den Telekommunikationsanbietern erhobenen Verkehrsdaten und vorliegenden Ermittlungsergebnissen zu erkennen, um so durch strukturierte Datenanalyse neue Ermittlungsansätze zu gewinnen. Für sämtliche Polizeidienststellen des Saarlandes werden die Funkzellenauswertungen von einer Zentralstelle des Landespolizeipräsidiums durchgeführt.

Das Verfahren „Funky" wurde von Rheinland-Pfalz übernommen und beinhaltete bereits eine automatisierte Protokollierung.

Das Verfahren „Turmdatenbank" stammt aus Niedersachsen und enthält keine programmseitig zur Verfügung stehende automatisierte Protokollierung, daher wurde zur Gewährleistung der Kontrollmöglichkeit ein manuelles Protokollierungskonzept entwickelt.

Bei dem Verfahren „Info-Zoom" wurde ebenso keine automatisierte Protokollierung mitgeliefert, deshalb wurde auch hier zunächst ein manuelles Protokollierungskonzept entwickelt. Die technische Abteilung des Landespolizeipräsidiums hatte aber bereits den Auftrag die Möglichkeit einer Programmierung für die automatisierte Protokollierung zu prüfen. Die manuelle Protokollierung könnte sodann durch eine automatisierte Protokollierung abgelöst werden.

Nur manipulationssichere Protokollierungen können ihren Schutzzweck in vollem Umfang erfüllen. Insbesondere bei sensitiven Anwendungen ist die Unveränderbarkeit von Protokolldaten durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten. Dabei richtet sich der zu treibende Aufwand im Wesentlichen nach dem Schutzbedarf der verarbeiteten Daten. Technische Maßnahmen sind organisatorischen vorzuziehen.

Der Einsatz der Dateianwendung „Funky" begegnete insoweit keinen datenschutzrechtlichen Bedenken, da einerseits die zu protokollierenden Ereignisse genau benannt wurden und andererseits die automatisierte Protokollierung dieser Ereignisse eine gewisse Manipulationssicherheit gewährleistet.

Eine nur manuelle Protokollierung kann die bereits zuvor erwähnte Manipulationssicherheit jedoch nicht hinreichend gewährleisten. Da für die Dateianwendung „Info-Zoom“ zum Prüfungszeitpunkt bereits an der Entwicklung eines automatisierten Protokollierungskonzeptes gearbeitet wurde, konnte aus datenschutzrechtlicher Sicht für eine Übergangsphase eine manuelle Protokollierung in den Verfahren „Turmdatenbank“ und „Funkzellen-Info-Zoom“ toleriert werden, mittelfristig sollte jedoch in beiden Verfahren eine automatisierte Protokollierung sichergestellt werden.

7 Steuern

7.1 Auskunftsanspruch in der Abgabenordnung

Schon lange besteht die Forderung der Datenschutzbeauftragten den Auskunftsanspruch in der Abgabenordnung (AO) zu regeln. Die Finanzverwaltung entscheidet bislang nach eigenem Ermessen, ob einem Antrag auf Akteneinsicht entsprochen werden kann.

Ein vielversprechender Entwurf des Bundesministeriums der Finanzen aus dem Jahr 2011 zur Änderung der Abgabenordnung sah vor, eine neue Vorschrift einzuführen, mit der die Auskunft über gespeicherte Daten geregelt werden sollte.

Leider wurde der Gesetzentwurf nicht mit der aus unserer Sicht notwendigen gehobenen Priorität weiterverfolgt. Es gibt derzeit keine Anzeichen auf eine baldige Lösung.

7.2 Versand der elektronischen Lohnsteuerabzugsmerkmale per Infopost

Als im Herbst 2011 der Versand der elektronischen Lohnsteuerabzugsmerkmale anstand, fragte die „WirtschaftsWoche“ bei den Datenschutzbeauftragten von Bund und Ländern an, ob es datenschutzrechtlich zulässig sei, dass die Finanzbehörden die Mitteilungen als „Infopost“ versandten.

Infopost ist ein Angebot der Deutschen Post, standardisierte Massendrucksachen mit gleichartigem Inhalt zu günstigen Tarifen zuzustellen. Zu Kontrollzwecken behält sich die Deutsche Post vor, stichprobenartig einzelne Infobriefe zu öffnen, um zu verhindern, dass die Versender sich einen günstigen Gebührentarif erschleichen.

Der Schutz personenbezogener Daten bestimmt sich im Steuerrecht vorrangig nach dem Steuergeheimnis gemäß § 30 AO und nicht nach den Datenschutzgesetzen. Gegenstand des Steuergeheimnisses sind „Verhältnisse eines anderen“. Diese dürfen gegenüber Dritten nicht unbefugt offenbart werden.

In § 30 Absatz 4 AO ist abschließend geregelt, unter welchen Voraussetzungen eine Offenbarung zulässig ist. Ein Versand von steuerlich relevanten Daten und die damit verbundene Möglichkeit der Kenntnisnahme dieser Daten durch Bedienstete der Deutschen Post ist nicht zulässig.

Meine hierzu durchgeführten Ermittlungen beim saarländischen Ministerium für Finanzen haben ergeben, dass im Saarland der Versand der Lohnsteuerabzugsmerkmale nicht durch die Deutsche Post erfolgt ist, sondern durch den Postdienstleister BS Saar-Mosel GmbH (Saarriva). Nach den allgemeinen Geschäftsbedingungen dieses Dienstleisters ist ein Öffnen von Infopost zu Kontrollzwecken aber nicht vorgesehen. Verantwortlich für Druck und Versand der Mitteilungen war im Saarland

das Landesamt für Zentrale Dienste (LZD). Bereits vor Beginn der Versandaktion hatte „Saarriva“ dem LZD bestätigt, dass Postsendungen mit dem Aufdruck „Infopost“ durch das Unternehmen nicht geöffnet werden. Eine mögliche unbefugte Offenbarung von durch das Steuergeheimnis geschützten Daten war durch die im Saarland gewählte Versandform somit nicht gegeben.

7.3 Datenschutzrechtliche Prüfung des von Finanzämtern durchgeführten Kontenabrufverfahrens

Durch das Gesetz zur Förderung der Steuerehrlichkeit vom 23.12.2003 wurde mit Wirkung zum 1.4.2005 die Möglichkeit des automatisierten Kontenabrufs geschaffen. Die für die Finanzämter verbindlichen gesetzlichen Grundlagen sind § 93 Absätze 7 und 9-10 sowie § 93 b der Abgabenordnung (AO).

Mit meiner datenschutzrechtlichen Kontrolle im Jahr 2012 sollte nachgeprüft werden, ob sich die Finanzbehörden an die Vorgaben des Gesetzes halten:

- Vorliegen eines gesetzlich vorgegebenen Grundes für den Kontenabruf,
- Hinweis an den Steuerpflichtigen, dass ein Kontenabruf durchgeführt werden kann,
- Dokumentationspflicht in den Akten,
- Benachrichtigung des Steuerpflichtigen über den erfolgten Kontenabruf.

Bereits bei der Vorbereitung der Prüfung wurde festgestellt, dass der Kontenabruf nahezu ausschließlich von den Vollstreckungsstellen der Finanzämter durchgeführt wird. Da aufgrund der Größe des Einzugsbereichs die meisten Vorgänge beim Finanzamt Saarbrücken vorzufinden waren, habe ich die Kontrolle auf dieses Finanzamt beschränkt. Aus den vorgelegten Fällen wurden nach dem Zufallsprinzip 19 Kontenabrufe gezogen.

Im Einzelnen ergab meine Kontrolle, dass in allen Fällen der Grund für den Kontenabruf die Erhebung von bundesgesetzlich geregelten Steuern war (§ 93 Absatz 7 Nr. 4 AO).

Mit der Vollstreckungsankündigung wurde regelmäßig auf die Möglichkeit des Kontenabrufverfahrens hingewiesen (§ 93 Absatz 9 AO).

Die Dokumentationspflichten nach § 93 Absatz 10 AO wurden nur teilweise erfüllt. Zwar war aufgrund der Aktenlage in allen Fällen die Notwendigkeit des Kontenabrufs erklärbar, aber eben nicht dokumentiert. Ein Vordruck zur Dokumentierung wurde in drei verschiedenen Versionen vorgefunden. Mal als selbstgefertigter Vordruck, mal als kopierter Vordruckaus Zeiten in denen die Formulare noch nicht im UNIFA-System (Universeller Finanzamts Arbeitsplatz, vormals Unix im Finanzamt) hinterlegt waren sowie der zur Verwendung frei gegebene Vordruck aus dem UNIFA-System. Die Ermessenserwägungen des Finanzamtes zur Durchführung des Kontenabrufverfahrens waren nicht in allen Fällen dargestellt.

Die gesetzlich vorgeschriebene Mitteilung an den Betroffenen über den durchgeführten Kontenabruf wird als Textbaustein in einem Schreiben

eingefügt, mit dem der Steuerschuldner über die Pfändung des Kontos unterrichtet wird. Die Vollstreckungsstelle dieses Finanzamtes ist in zwei Sachgebiete aufgeteilt. In einem Sachgebiet wurde dieser Textbaustein durchgängig verwendet. Darüber hinaus konnte in den dort geprüften Fällen festgestellt werden, dass auch ergebnislose Kontenabrufe mitgeteilt wurden.

Leider war zu verzeichnen, dass im zweiten Sachgebiet durchgängig dieser Textbaustein vergessen wurde und die Mitteilungspflicht nach § 93 Absatz 9 AO somit nicht erfüllt war. Das Finanzamt sagte zu, die Mitteilung in den Fällen, in denen es zeitnah noch sinnvoll erschien, nachzuholen.

Das Prüfungsergebnis wurde dem Ministerium für Finanzen mitgeteilt, verbunden mit der Bitte darauf hinzuwirken, dass den Dokumentationspflichten nachgekommen wird.

8 Meldewesen

Auch in diesem Berichtszeitraum habe ich mich wiederholt mit Fragen im Zusammenhang mit der Weitergabe personenbezogener Daten durch die Meldebehörden an Empfänger aus dem öffentlichen und dem privaten Bereich befasst.

8.1 Auskünfte an politische Parteien im Vorfeld der Wahl eines Bürgermeisters

Durch eine Eingabe bin ich darauf aufmerksam gemacht worden, dass im Vorfeld einer Bürgermeisterwahl auf Antrag einer Partei dieser die Adressen aller von 1985 bis 1993 geborenen Erstwähler, aller vor dem Jahre 1951 geborenen Senioren sowie aller Wähler aus der Altersgruppe 1951 bis 1985, die nach dem Jahre 2003 zugezogen sind, durch die Meldebehörde übermittelt worden sind. Auch anderen Parteien bzw. Wahlkandidaten wurden in nur unwesentlich geringerem Umfang Adressdaten von Einwohnern übermittelt.

Die Kommune wies in ihrer Stellungnahme darauf hin, dass ursprünglich eine vollständige Übermittlung der Adressdaten auch bezüglich der Altersgruppe 1951 bis 1985 beantragt worden sei. Da dies nach Auffassung der Kommune jedoch dazu geführt hätte, dass das komplette Wählerverzeichnis zur Verfügung gestellt worden wäre, seien aus dieser Altersgruppe lediglich die seit 2003 Hinzugezogenen mitgeteilt worden.

Aber auch diese Verfahrensweise stellte einen Verstoß gegen die Regelung des § 35 Abs. 1 des Saarländischen Meldegesetzes (MG) dar. Nach der genannten Vorschrift darf die Meldebehörde u.a. Parteien und Trägern von Wahlvorschlägen im Zusammenhang mit allgemeinen Wahlen in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über die in § 34 Abs. 1 Satz 1 bezeichneten Daten (Familienname, Vorname, Doktorgrad und Anschrift) von Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist und die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben.

Damit dürfen nur die Daten von Personen übermittelt werden, die zu bestimmten altersmäßig zusammengesetzten Gruppen gehören. Diese gesetzliche Beschränkung auf „Gruppen" (wie: Erstwähler, über 65-jährige Wähler) soll verhindern, dass einem Wahlvorschlagsträger die Daten sämtlicher Wahlberechtigter übermittelt werden und er sich damit ein komplettes Register aller Wahlberechtigten anlegen könnte.

Eine Übermittlung der Anschriften aller Wahlberechtigten gestaffelt nach Altersgruppen, wie ursprünglich beantragt worden war, würde diese Regelung insgesamt in Frage stellen und mithin eine – wie die Kommune auch zutreffend erkannt hat - unzulässige Umgehung der Vorschrift bedeuten.

Da die Vorschrift des § 35 Abs. 1 MG jedoch ausschließlich auf das Lebensalter des Betroffenen abstellt, ist es indes auch unzulässig, bei der Zusammensetzung der Personengruppen, über die Auskunft erteilt

werden soll, andere Auswahl- oder Suchkriterien – wie hier das Zuzugsdatum - heranzuziehen.

Die Übermittlung der Daten widersprach dementsprechend der Gesetzeslage und stellte damit auch einen Verstoß gegen das Datenschutzrecht dar. Hierauf wurde die Kommune hingewiesen und sie wurde aufgefordert, bei künftigen Wahlen dafür Sorge zu tragen, dass bei einer Datenübermittlung zu Wahlwerbezwecken allein auf das Lebensalter der Betroffenen abgestellt wird.

Allgemein ist im Zusammenhang mit Werbung im Vorfeld von Wahlen noch darauf hinzuweisen, dass der Gesetzgeber den Betroffenen das Recht einräumt, der Weitergabe der Meldedaten zum Zweck der Wahlwerbung zu widersprechen. Hierauf hat die Meldebehörde die Einwohnerinnen und Einwohner nach § 35 Abs. 4 Nr. 1 MG grundsätzlich acht Monate vor der jeweiligen Wahl durch öffentliche Bekanntmachung hinzuweisen.

§ 35 Abs. 1 MG

Die Meldebehörde darf Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit allgemeinen Wahlen in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über die in § 34 Abs. 1 Satz 1 bezeichneten Daten von Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist und die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Geburtstage der Wahlberechtigten dürfen dabei nicht mitgeteilt werden. …

8.2 Übermittlung von Daten über Alters- und Ehejubiläen

Auch Fragen im Zusammenhang mit der Übermittlung von Daten über Alters- und Ehejubiläen werden immer wieder an mich herangetragen. So habe ich von verschiedenen Kommunen Anfragen erhalten, ob und in welchem Umfang den Ortsvorstehern, einzelnen Parteien oder Wählervereinigungen und Vereinen der Gemeinde Adressdaten mit Geburtsdatum von Gemeindeeinwohnern übermittelt werden können, um diesen zu ihren Alters- oder Ehejubiläen gratulieren zu können.

Nach §§ 33 Abs. 2 und 35 Abs. 2 Saarländisches Meldegesetz (MG) darf die Meldebehörde die begehrte Auskunft sowohl an öffentliche als auch an nicht öffentliche Stellen erteilen. Eine Einschränkung des Kreises der Auskunftsberechtigten sieht das Gesetz nicht vor. Voraussetzung ist aber in jedem Fall, dass der Betroffene dieser Auskunftserteilung nicht widersprochen hat. Über dieses Widerspruchsrecht hat die Meldebehörde die Einwohnerinnen und Einwohner gemäß § 35 Abs. 4 Nr. 2 MG mindestens einmal jährlich durch öffentliche Bekanntmachung hinzuweisen.

Liegt kein Widerspruch des Betroffenen vor, ist die Meldebehörde bei einem entsprechenden Auskunftsbegehren aber nicht verpflichtet, die begehrte Auskunft zu erteilen. Es besteht vielmehr lediglich ein Anspruch darauf, dass die Meldebehörde nach pflichtgemäßem Ermessen über das Begehren entscheidet. Sie kann bei der von ihr zu treffenden Entscheidung darüber, in welchen Fällen Auskunft erteilt werden soll,

Gesichtspunkte des Verwaltungsaufwandes berücksichtigen und auch nach dem mit der Auskunft verfolgten Zweck differenzieren.

Dementsprechend konnte ein Ortsvorsteher gegenüber einer Kommune nicht die Herausgabe der Geburtstage aller Einwohner ab dem vollendeten 80. Lebensjahr beanspruchen, da es geübte Verwaltungspraxis der Kommune war, eine Auskunft ab dem 80. Lebensjahr und danach alle fünf Jahre zu erteilen. Obwohl das Meldegesetz keine Definition des Begriffes „Altersjubiläum" enthält, erscheint es angesichts des demographischen Wandels aus meiner Sicht auch zweifelhaft, bereits ab dem 80. Lebensjahr bei jedem folgenden Lebensjahr von einem Altersjubiläum zu sprechen.

§ 33 Abs. 2 MG

Die Meldebehörde darf zur Vornahme von Ehrungen bei Alters-, Ehe- und Lebenspartnerschaftsjubiläen von Einwohnerinnen und Einwohnern den Tag und die Art des Jubiläums an öffentliche Stellen übermitteln. § 31 Abs. 7 Satz 1 und § 35 Abs. 2 Satz 1 und Abs. 4 Nr. 2 gelten entsprechend.

§ 35 Abs. 2 MG

Begehrt jemand eine Melderegisterauskunft über Alters- oder Ehejubiläen von Einwohnerinnen oder Einwohnern, so darf die Meldebehörde die Auskunft nur dann erteilen, wenn die betroffene Person der Auskunftserteilung nicht widersprochen hat. Wird die Auskunft erteilt, so darf sie nur die in § 34 Abs. 1 Satz 1 genannten Daten der betroffenen Person sowie Tag und Art des Jubiläums umfassen.

8.3 Änderung der Meldedaten-Übermittlungsverordnung

Im Mai 2012 übersandte mir das Ministerium für Inneres und Sport den Entwurf einer Verordnung zur Änderung der Verordnung über die Zulassung der regelmäßigen Übermittlung von Daten aus dem Melderegister an Behörden oder sonstige Stellen (Meldedaten-Übermittlungsverordnung-MeldDÜV), um mir im Rahmen der externen Anhörung Gelegenheit zur Stellungnahme zu geben. Mit dieser Verordnung sollte den von mehreren Behörden vorgetragenen Änderungswünschen bzw. Neuaufnahmen aufgrund spezialgesetzlicher Regelungen Rechnung getragen werden. Die Änderungsverordnung enthielt Regelungen hinsichtlich der regelmäßigen automatisierten Datenübermittlung an die Grundschulen sowie an das Epidemiologische Krebsregister. Zusätzlich aufgenommen wurden automatisierte Datenübermittlungen an die Gesundheitsämter und die Möglichkeit der Einrichtung automatisierter Abrufverfahren für das Epidemiologische Krebsregister Saarland und für die Staatskanzlei.

Bereits durch die im Mai 2010 in Kraft getretene Meldedaten-Übermittlungsverordnung wurde der Katalog sowohl der regelmäßigen Datenübermittlungen als auch der Abrufverfahren erheblich ausgeweitet und sollte nun erneut eine Ergänzung erfahren.

Wiederholt habe ich bereits in der Vergangenheit darauf hingewiesen, dass durch die stetige Aufnahme weiterer Abrufverfahren das kommu-

nale Melderegister zunehmend den Charakter eines öffentlichen Registers erhält, was zu keiner Zeit die Absicht des Verordnungsgebers war.

In einer ersten Stellungnahme zu dem Verordnungsentwurf habe ich darauf hingewiesen, dass ich es für geboten halte, in einer gesonderten, den automatisierten Abrufverfahren vorangestellten Norm, die Grundvoraussetzungen des Datenabrufs, technisch organisatorische Maßnahmen, die Protokollierung des Datenzugriffs und den Umgang mit den Protokolldaten für datenabrufende Stellen zu regeln.

Zu den geplanten Änderungen und Neuregelungen im Einzelnen habe ich darauf hingewiesen, dass die Datenübermittlung an die Gesundheitsämter zur Umsetzung eines geordneten Einladungs- und korrekten Untersuchungssystems für die Einschulungsuntersuchungen nach § 2 Abs. 1 Schulpflichtgesetz (SchulPflG) grundsätzlich nicht zu beanstanden ist. Hinsichtlich einzelner Datensätze war die Erforderlichkeit der Datenübermittlung jedoch nicht erkennbar. Darüber hinaus habe ich gebeten, zur Klarstellung in der Begründung der Meldedatenübermittlungsverordnung darzulegen, wie seitens des Gesundheitsamtes mit den angelieferten Datenbeständen verfahren werden soll und wie durch weitere technische Maßnahmen gewährleistet werden soll, dass die angelieferten Datenbestände nur für die Zeiträume zugänglich sind, die für die Aufgabenerfüllung der Gesundheitsämter im konkreten Kontext der ärztlichen Untersuchung vor Beginn der Schulpflicht nach § 2 Abs. 1 SchulPlfG erforderlich sind.

Auch die Erforderlichkeit für die Ausweitung des Datenkatalogs der Datenübermittlung an das Epidemiologische Krebsregister vermochte ich nicht zu erkennen. Bereits durch die MeldDÜV 2010 wurde eine Befugnis zur Datenübermittlung zum Zwecke der Durchführung anderer Krebsfrüherkennungsprogramme und weiterer Präventionsmaßnahmen erteilt. Diese Befugnis sollte nun durch die Übermittlung weiterer Datensätze noch erweitert werden. Dies ist insoweit schon nicht nachvollziehbar, weil die Datenübermittlung an eine Stelle erfolgen soll, die erst noch durch eine zu erlassende Verordnung benannt werden muss, so dass der Aufgabenbereich dieser Stelle bisher noch nicht feststeht. Ungeachtet dessen leuchtete mir auch die lediglich pauschale Begründung für das Erfordernis der Datenerweiterung nicht ein.

Schließlich rügte ich in meiner ersten Stellungnahme auch, dass die Begründung für die Notwendigkeit eines Abrufverfahrens für das Epidemiologische Krebsregister Saarland, die sich zunächst nur allgemein auf die Erfüllung von Aufgaben nach dem Saarländischen Krebsregistergesetz bezog, aus sich heraus nicht verständlich ist.

Hinsichtlich der Einrichtung eines Abrufverfahrens für die Staatskanzlei den bloßen Bedarf als Begründung anzuführen, widerspricht sämtlichen Datenschutzgrundsätzen und war daher ebenso zu beanstanden.

Im Juli 2012 wurde meiner Dienststelle sodann ein überarbeiteter Verordnungsentwurf vorgelegt. Die Begründung zur Datenübermittlung an die Gesundheitsämter wurde hierin in ausreichender Weise ergänzt. Nach wie vor ließ sie jedoch vermissen, wie seitens des Gesundheitsamtes mit den angelieferten Datenbeständen verfahren werden soll. Entsprechende Ausführungen wie bei Einführung des § 14 MeldDÜV (Datenübermittlung an die für Früherkennungsuntersuchungen zuständige Zentrale Stelle) wären aus datenschutzrechtlicher Sicht wünschenswert gewesen.

Meine Kritik an der Ausweitung der Datenübermittlung an eine erst noch durch eine Verordnung zu benennende Stelle zur Durchführung anderer Krebsfrüherkennungsprogramme wurde seitens des Ministeriums nicht aufgegriffen. Vielmehr wurde die bereits jetzt getroffene Regelung damit begründet, dass bei einem zukünftigen Erlass der Verordnung keine Änderung bzw. Ergänzung der MeldDÜV vorgenommen werden müsse. Bis zu diesem Zeitpunkt erfolge auf der Grundlage der Vorschrift selbstverständlich keine Datenübermittlung.

Bei allem Verständnis dafür, zukünftig bei Erlass von Verordnungen auf der Grundlage von § 19 Saarländisches Krebsregistergesetz (SKRG) eine erneute Änderung bzw. Ergänzung der MeldDÜV zu vermeiden, halte ich es dennoch unter rechtsstaatlichen Gesichtspunkten für nicht vertretbar, die Übermittlung von Daten zuzulassen, deren Erforderlichkeit sich zum heutigen Zeitpunkt nicht beurteilen lässt. Die Schaffung einer solchen Rechtsgrundlage „auf Vorrat" halte ich für unzulässig.

Aufgrund einer Konkretisierung der Begründung für das Abrufverfahren für das Epidemiologische Krebsregister wird nunmehr deutlich, aus welchem Grund das Epidemiologische Krebsregister den automatisierten Zugriff auf Daten des Melderegisters benötigt. Mit Ausnahme eines Datensatzes, für dessen Übermittlung sich im SKRG keine Rechtsgrundlage findet, sind daher meine Bedenken gegen den automatisierten Zugriff für das Epidemiologische Krebsregister insoweit ausgeräumt worden.

Meine Anregung, in einer gesonderten, den automatisierten Abrufverfahren vorangestellten Norm, Grundvoraussetzungen des Datenabrufs zu regeln, soll entsprechend einer Zusicherung des Ministeriums des Innern mit Blick auf das Bundesmeldegesetz im Rahmen neuerlicher Änderungen der MeldDÜV aufgegriffen werden.

8.4 Ausblick auf die Neuregelung des Meldewesens

Das Meldewesen wurde im Jahre 2006 im Zuge der Föderalismusreform in die ausschließliche Gesetzgebung des Bundes überführt. In Ausübung dieser Gesetzgebungskompetenz wurde dem Bundestag im Jahre 2011 der Gesetzentwurf der Bundesregierung zur Fortentwicklung des Meldewesens vorgelegt. Durch das künftige Bundesmeldegesetz sollen das bisherige Melderechtsrahmengesetz und die Landesmeldegesetze abgelöst werden. Bereits der erste Entwurf dieses Gesetzes enthielt aus datenschutzrechtlicher Sicht einige Defizite. Zu einer weiteren Verschlechterung haben dann aber die abschließenden Beratungen im Bundestag geführt. Während in dem ursprünglichen Gesetzentwurf vorgesehen war, die Verwendung einfacher Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels künftig von der Einwilligung des Betroffenen abhängig zu machen, sah die durch den Bundestag beschlossene Änderung lediglich eine Widerspruchslösung vor. Selbst bei einem erfolgten Widerspruch sollte eine Auskunft möglich sein, soweit die Abfrage der Bestätigung oder Berichtigung vorhandener Datenbestände dient. Diese vom Bundestag beschlossene Änderung hat zu heftigem Widerstand in der Öffentlichkeit geführt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer gemeinsamen Entschließung mit Blick auf die noch ausstehenden Beratungen im Bundesrat ebenfalls eine Rücknahme dieser Regelung sowie weitere datenschutzrechtliche Verbesserungen gefordert.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. August 2012

Melderecht datenschutzkonform gestalten!

Das vom Deutschen Bundestag am 28. Juni 2012 beschlossene neue Melderecht weist erhebliche datenschutzrechtliche Defizite auf. Schon die im Regierungsentwurf enthaltenen Datenschutzbestimmungen blieben zum Teil hinter dem bereits geltenden Recht zurück.

Darüber hinaus wurde der Regierungsentwurf durch das Ergebnis der Ausschussberatungen des Bundestages noch einmal deutlich verschlechtert. Bei den Meldedaten handelt es sich um Pflichtangaben, die die Bürgerinnen und Bürger gegenüber dem Staat machen müssen. Dies verpflichtet zu besonderer Sorgfalt bei der Verwendung, insbesondere wenn die Daten an Dritte weitergegeben werden sollen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher den Bundesrat auf, dem Gesetzentwurf nicht zuzustimmen, damit im Vermittlungsverfahren die erforderlichen datenschutzgerechten Verbesserungen erfolgen können. Dabei geht es nicht nur darum, die im Deutschen Bundestag vorgenommenen Verschlechterungen des Gesetzentwurfs der Bundesregierung rückgängig zu machen, vielmehr muss das Melderecht insgesamt datenschutzkonform ausgestaltet werden. Hierfür müssen auch die Punkte aufgegriffen werden, die von den Datenschutzbeauftragten im Gesetzgebungsverfahren gefordert worden sind, aber unberücksichtigt blieben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere in den folgenden Punkten Korrekturen und Ergänzungen für erforderlich:

- *Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels bedürfen ausnahmslos der Einwilligung des Meldepflichtigen. Dies gilt auch für die Aktualisierung solcher Daten, über die die anfragenden Stellen bereits verfügen und die Weitergabe der Daten an Adressbuchverlage.*

- *Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwerbungszwecken und an Presse oder Rundfunk über Alters- und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.*

- *Der Meldepflichtige muss sonstigen einfachen Melderegisterauskünften widersprechen können. Die Übermittlung hat bei Vorliegen eines Widerspruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.*

- *Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.*

- *Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis*

der einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.

- *Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.*

- *Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.*

- *Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu vernachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür - wie auch bei der Hotelmeldepflicht - außer Verhältnis zum Nutzen.*

Nachdem der Bundesrat den Vermittlungsausschuss angerufen hat, bleibt zu hoffen, dass das endgültig verabschiedete Gesetz datenschutzfreundlicher ausgestaltet sein wird.

Voraussichtlich Anfang 2015 wird das Bundesmeldegesetz in Kraft treten.

9 Kommunales

9.1 Landesweite Erhebung zur Videoüberwachung

Bereits in den vorangehenden Tätigkeitsberichten habe ich über die im Jahr 2010 begonnene landesweite Erhebung meiner Dienststelle zur Videoüberwachung im öffentlichen Bereich berichtet.

Im Wesentlichen war festzustellen, dass zwar von vielen öffentlichen Stellen des Landes bereits Videoüberwachungsmaßnahmen durchgeführt wurden, es jedoch in nahezu allen Fällen an der hierfür erforderlichen Verfahrensbeschreibung nach § 9 Saarländisches Datenschutzgesetz (SDSG) und der damit konkreten Beschreibung der im Einsatz befindlichen Videoüberwachungsmaßnahmen mangelte. Zwischenzeitlich wurden durch die jeweils verantwortlichen Stellen die entsprechenden Verfahrensbeschreibungen unter Beteiligung meiner Dienststelle erstellt sowie weitere Unterlagen wie Lagepläne und Beschreibungen zur eingesetzten Systemarchitektur der Videokameras vorgelegt. In einigen Fällen wurden die Videoüberwachungsanlagen demontiert. Gründe hierfür waren entweder die im Einsatz befindliche veraltete Technik oder zwischenzeitlich defekte Videoanlagen, die noch einen Abschreckungseffekt, ähnlich einer Videoattrappe, erzielen sollten. In einem Fall erfolgte durch die verantwortliche Kommune die umgehende Demontage auf Intervention meiner Dienststelle, da es sich um eine unzulässige verdeckte Videoüberwachungsmaßnahme handelte. Ich werde diese Thematik nachfolgend noch eingehender beleuchten.

Auch Kamerajustierungen waren in manchen Fällen nachträglich rechtskonform auszugestalten. Vornehmlich ging es hierbei darum öffentliche Bereiche oder Privatgrundstücke nicht durch die Kamera zu erfassen.

In einem Großteil der Fälle musste die Aufzeichnungsdauer nachträglich auf die zulässige Höchstdauer von 24 Stunden begrenzt werden. Zuvor wurde meist 72 Stunden bis zu 2 Wochen aufgezeichnet. In wenigen Fällen sogar bis zu 6 Monaten.

Der erforderlichen Hinweispflicht wurde oft nicht oder nur unzureichend nachgekommen, so dass die verantwortlichen Stellen hier nachbessern mussten.

Um den verantwortlichen Stellen Hilfestellung zu geben und auch eine möglichst einheitliche Beschilderung von Videoüberwachungsmaßnahmen zu erreichen, wurde die Internetseite meiner Dienststelle sehr frühzeitig überarbeitet und im Bereich Fachthemen ein eigener Themenkomplex Videoüberwachung eingerichtet, welcher entsprechende Hinweise, Erläuterungen und Muster zum Download bietet.

Auch weiterhin ist meine Dienststelle mit der Prüfung neu eingereichter Unterlagen von beabsichtigten Videoanlagen durch öffentliche Stellen beschäftigt. Ich kann jedoch sagen, dass zum einen die landesweite Erhebung als auch die von mir 2011 initiierte Vorstellung meiner Dienststelle – Der Datenschutz bekommt ein Gesicht – ein Bewusstsein für eine rechtskonforme Videoüberwachung geschaffen haben. Sowohl frühzeitige Anfragen zur Zulässigkeit und Ausgestaltung einer eventuellen Videoüberwachungsmaßnahme, als auch rechtzeitige Beteiligungen

meiner Dienststelle in konkret beabsichtigten Verfahren vor Inbetriebnahme derselben, veranlassen mich zu diesem Schluss.

Nachstehend möchte ich noch einige praktische Anwendungsfälle von Videoüberwachung durch öffentliche Stellen im Saarland erläutern.

§ 34 SDSG Videoüberwachung

(1) Die Beobachtung öffentlich zugänglicher Bereiche mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. *in Wahrnehmung des Hausrechts der verantwortlichen Stelle zum Zweck des Schutzes von Personen, des Eigentums oder des Besitzes oder der Kontrolle von Zugangsberechtigungen, oder*

2. *zur Aufgabenerfüllung der verantwortlichen Stelle*

erforderlich ist. Für die Gefährdung der in Nummer 1 genannten Rechtsgüter müssen konkrete Anhaltspunkte bestehen. Die Videoüberwachung nach Nummer 2 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. Dabei sind der Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung zu dokumentieren.

(2) Die Möglichkeit der Beobachtung und die verantwortliche Stelle müssen für Betroffene erkennbar sein.

(3) Personenbezogene Daten dürfen nur erhoben oder gespeichert werden, wenn dies zum Erreichen der in Absatz 1 genannten Zwecke erforderlich oder unvermeidlich ist. Die Daten dürfen für einen anderen Zweck nur verarbeitet werden, wenn dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Abwehr von Nachteilen für das Wohl des Bundes oder eines Landes oder zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über die Erhebung entsprechend § 12 Abs. 5 Satz 1 zu benachrichtigen. § 12 Abs. 5 Satz 4 gilt entsprechend.

(5) Die Daten sind unverzüglich, spätestens jedoch nach 24 Stunden zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

9.1.1 Verdeckte Videoüberwachung

Gemäß § 28 Abs. 1 und Abs. 2 Nr. 2 Saarländisches Polizeigesetz (SPolG) kann nur die Vollzugspolizei durch den verdeckten Einsatz technischer Mittel, insbesondere zur Anfertigung von Bildaufnahmen oder –aufzeichnungen, auf richterliche Anordnung personenbezogene Informationen über die in § 26 Abs. 2 Nr. 1 und Nr. 2 SPolG genannten Personen erheben, soweit das zur vorbeugenden Bekämpfung

1. von Verbrechen, wenn auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass eine solche Straftat begangen werden soll,

2. anderer Straftaten, wenn auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass die Straftat gewerbsmäßig, gewohnheitsmäßig, von Banden oder von Organisationen begangen werden soll,

erforderlich ist.

In oder aus Wohnungen kann die Vollzugspolizei nach § 28a SPolG personenbezogene Informationen durch den Einsatz verdeckter Bildaufnahmen oder -aufzeichnungen auf richterliche Anordnung nur erheben, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person unerlässlich ist.

§ 34 SDSG eröffnet den öffentlichen Stellen des Landes unter Beachtung weiterer Zulässigkeitsvoraussetzungen grundsätzlich die Möglichkeit der Beobachtung öffentlich zugänglicher Bereiche mit optisch-elektronischen Einrichtungen. Die Möglichkeit der Beobachtung und die verantwortliche Stelle müssen aber für Betroffene erkennbar sein.

Eine verdeckte Maßnahme auf der Grundlage des § 34 SDSG ist mithin ausgeschlossen.

Im konkreten Fall hatte die betroffene Kommune wiederholt auf frei zugänglichem Gelände erhebliche Schadenshöhen aufgrund von Diebstählen hinzunehmen. Sie entschied daher, zu Strafverfolgungszwecken eine verdeckte Videoüberwachungsmaßnahme durchzuführen. Sie selbst zeigte dies meiner Dienststelle - allerdings erst nach erfolgter Umsetzung der Maßnahme - an. Da weder das SPolG, welches ausschließlich die Vollzugspolizei des Saarlandes unter besonderen gesetzlich normierten Voraussetzungen zu verdeckten Videoüberwachungsmaßnahmen berechtigt, noch § 34 SDSG für die Kommune, als verantwortliche Stelle, eine verdeckte Überwachungsmaßnahme gestatten, wurde die Kommune umgehend aufgefordert, den rechtswidrigen Zustand zu beenden und die Videoüberwachungsanlage zu demontieren.

Ich habe mich hiervon zusammen mit den sachlich zuständigen Mitarbeitern meiner Dienststelle in einem gemeinsamen Termin mit dem zuständigen Bürgermeister vor Ort überzeugt. Darüber hinaus wurde ausdrücklich darauf hingewiesen, dass die Landesbeauftragte für Datenschutz und Informationsfreiheit vor der Durchführung einer Videoüberwachungsmaßnahme durch eine Kommune zu beteiligen und eine entsprechende Verfahrensbeschreibung für das beabsichtigte Verfahren durch die Kommune zu erstellen ist. § 34 SDSG eröffne lediglich die Möglichkeit einer offenen Videoüberwachung im Rahmen des Hausrechts zum Schutz von Eigentum. Durch geeignete Hinweisschilder sei der Betroffene vor Betreten des Erfassungsbereiches der Kamera auf die Maßnahme hinzuweisen. Zuvor jedoch sei die Erforderlichkeit unter Einbeziehung der Interessensabwägung, auch mit Blick auf möglicherweise mildere, geeignete Mittel, zu prüfen.

Da die Videoüberwachungsanlage, wie von mir eingefordert, umgehend demontiert wurde, konnte von einer Beanstandung abgesehen werden.

9.1.2 Videoüberwachung auf Wertstoffhöfen

Im Berichtszeitraum erhielt meine Dienststelle von mehreren saarländischen Kommunen Verfahrensbeschreibungen für beabsichtigte Videoüberwachungsmaßnahmen auf Wertstoffhöfen. Sich wiederholende Einbruchsdiebstähle, sei es die Entwendung von Bargeld, Wertstoffen wie beispielsweise Kupfer oder neuwertigen Werkzeugen und Maschinen, veranlassten die jeweiligen Kommunen zu diesem Schritt. Die den Verfahrensbeschreibungen auf Anforderung beigefügten gesonderten Vermerke über die Vorkommnisse der Vergangenheit, hier Einbruchsdiebstähle, zeigten auf, dass konkrete Anhaltspunkte für die Gefährdung der Rechtsgüter Eigentum oder Besitz vorlagen. Mithin war eine Videoüberwachungsmaßnahme auf Grundlage von § 34 Abs. 1 Nr. 1 SDSG in Abwägung mit den schutzwürdigen Interessen der Betroffenen grundsätzlich möglich.

Ebenso war jedoch zu prüfen, ob für den „angestrebten Zweck" tatsächlich eine tägliche Überwachungsdauer von 24 Stunden erforderlich ist, oder ob nicht vielmehr eine Begrenzung, beispielsweise außerhalb der Öffnungszeiten, ausreichend ist. Da die geschilderten Vorkommnisse überwiegend nachts auftraten, war die Überwachungsdauer daher außerhalb der Öffnungszeiten der Wertstoffhöfe zu begrenzen.

In einem Fall wurde zur Durchführung der laufenden Videoüberwachung ein Dienstleistungsvertrag über die Aufschaltung einer Alarmanlage mit einer privaten Werk- und Industrieschutzfirma geschlossen. Es handelt sich hierbei um einen Auftragsdatenverarbeitung nach § 5 SDSG. Die auftraggebende, öffentliche Stelle bleibt dafür verantwortlich, dass die Aufgaben nach Maßgabe der gesetzlichen Vorschriften erledigt werden und das Datenschutzrecht eingehalten wird. Da das SDSG auf private Firmen keine Anwendung findet, hat der Auftraggeber im Rahmen einer vertraglichen Regelung dafür Sorge zu tragen, dass sich der Auftragnehmer verpflichtet, das SDSG zu befolgen und sich insoweit der Kontrolle der Landesbeauftragten für Datenschutz zu unterwerfen.

Auch hierfür wurden entsprechende Musterverträge auf der Internetseite meiner Dienststelle zum Download eingestellt.

9.1.3 Videoüberwachung im Museum

Im Berichtszeitraum erreichten uns mehrere Anfragen zur Zulässigkeit von Videoüberwachung in Museen durch öffentliche Stellen. Gründe hierfür lagen zum einen in der Realisierung einer Zugangskontrolle zum anderen darin, Besitz oder Eigentum zu schützen.

§ 34 Abs. 1 Nr. 1 SDSG eröffnet den öffentlichen Stellen grundsätzlich die Möglichkeit zur Durchführung einer Videoüberwachung aus den zuvor erwähnten Gründen. Zwar fordert § 34 Abs. 1 Satz 2 SDSG für die Gefährdung der dort genannten Rechtsgüter das Bestehen konkreter Anhaltspunkte, unter Berücksichtigung der als besonders wertvoll einzustufenden Ausstellungsobjekte sowie den besonderen Anforderungen an Museen im Umgang mit Ihnen anvertrauten Exponaten, kann im konkreten Fall jedoch auch das Bestehen einer abstrakten Gefahr für das zu schützende Gut als ausreichend angesehen werden. Die weltweit geltenden „Ethischen Richtlinien des International Council of Museums

(ICOM)“ geben den Museumsbetreibern vor, für eine sichere Aufbewahrung der Sammlungen zu sorgen und adäquate Vorkehrungen zum Schutz gegen Gefahren wie Diebstahl und Vandalismus zu treffen. Gleichzeitig haben Museen aber als Bewahrer authentischer Zeugnisse eine besondere Verantwortung, ihre Sammlungen der Öffentlichkeit so frei wie möglich zugänglich zu machen.

Mit Blick auf die Realisierung einer Zugangskontrolle wird jedoch ein reines Kamera-Monitoring-Prinzip, also lediglich eine Beobachtung ohne Aufzeichnung, für den angestrebten Zweck ausreichen. Je nach Personenkreis der Zugangsberechtigten, hier Museumsbesucher aber auch Mitarbeiter, wird gleichwohl § 31 Abs. 5 SDSG zu beachten und mithin der Personalrat zu beteiligen sein.

§ 31 Abs. 5 SDSG

(5) Soweit Daten der Beschäftigten im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 11 Abs. 2 gespeichert werden, dürfen sie nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

Für den angestrebten Zweck, den Besitz oder das Eigentum an den ausgestellten Objekten zu schützen, kann eine Videoüberwachung mit Aufzeichnung, welche mit einem Alarmsicherungssystem verbunden ist, außerhalb der Öffnungszeiten als datenschutzrechtlich unbedenklich eingestuft werden. Eine flächendeckende Videoüberwachung der Museumsräume während der Öffnungszeiten wird jedoch als unzulässig zu bewerten sein, da gerade in Museen der Besucher zum Verweilen vor den Exponaten eingeladen ist, sei es um Informationstäfelchen zu lesen, Audio-Informationen bei gleichzeitiger Betrachtung zu folgen oder einfach nur ein Kunstwerk auf sich wirken zu lassen. Eine Überwachung in solchen Bereichen greift besonders intensiv in das Allgemeine Persönlichkeitsrecht der Betroffenen ein. Die Schutzbedürftigkeit in öffentlichen Räumen, in denen sich Personen zur privaten Lebensgestaltung längere Zeit aufhalten, ist besonders hoch einzustufen, weshalb im konkreten Falle eine Interessensabwägung nur zu Gunsten der Museumsbesucher ausfallen kann.

Zu berücksichtigen ist ebenso, dass durch Videoüberwachungsmaßnahmen in Museen auch das dort beschäftige Personal erfasst werden kann. Auch 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.

9.1.4 Videoüberwachung von Kriegsgräberstätten

Das Ministerium für Soziales, Gesundheit, Frauen und Familie ist für sechs Ehrenfriedhöfe, auf denen ausschließlich Kriegstote bestattet sind, zuständig. Da es sich um Kriegstote verschiedenster Nationalitäten handelt und ausweislich der Besucherbücher Angehörige aus dem Ausland diese Stätten auch weiterhin aufsuchen, sollen alle Ehrenfriedhöfe zu jeder Zeit zugänglich sein. Neben Pflegearbeiten zählen die Renovierung beschädigter Gegenstände sowie auch die Wiederbeschaffung

gestohlener Grabkreuze, Gedenktafeln und Skulpturen zum Aufgabenbereich des Ministeriums.

Im Sommer vergangenen Jahres teilte das Ministerium meiner Dienststelle mit, dass im Rahmen einer landesweiten Serie von verübten Metalldiebstählen auch auf zwei Ehrenfriedhöfen erhebliche Schäden zu verzeichnen waren. Beispielsweise wurden auf einem dieser Friedhöfe 40 bronzene Grabkreuze entwendet. Da auf diesem Friedhof noch 280 Metallkreuze und eine 2,50 Meter hohe Bronzestatue von sehr hohem Wert stehen, bat das Ministerium meine Dienststelle um Prüfung, ob der Einsatz von Kameradummies oder Videoüberwachungsanlagen als Sicherungsmaßnahme zulässig sei.

Sinn und Zweck einer Videoattrappe ist es, bei dem Betroffenen die Vorstellung einer funktionsfähigen Videoüberwachungsanlage zu erzeugen, um auf diese Weise unerwünschte Verhaltensweisen zu unterbinden. Insoweit ist der Betroffene dem gleichen Überwachungsdruck wie durch eine Echtanlage ausgesetzt. Aus diesem Grund sind nach hiesiger Auffassung auch an die Errichtung von Kameradummies die gleichen rechtlichen Zulässigkeitsvoraussetzungen wie bei der Errichtung von Echtanlagen zu stellen.

Aufgrund der Sachdarstellung des Ministeriums für Soziales, Gesundheit, Frauen und Familie ist der Einsatz einer Videoüberwachungsechtanlage im konkreten Fall auf der Grundlage von § 34 Abs. 1 Nr. 1 SDSG zum Schutz des Eigentums oder Besitzes möglich. In der Vergangenheit gab es durch die belegten Diebstähle "konkrete Anhaltspunkte" für eine Gefährdung der Rechtsgüter i.S.d. § 34 Abs. 1 S. 2 SDSG, die eine solche Maßnahme rechtfertigen. Zudem hat das Ministerium dargelegt, weshalb eine Begrenzung der Öffnungszeiten bei Ehrenfriedhöfen nicht opportun ist.

Eine wenn auch vermeintliche Beobachtung ist ebenso durch geeignete Hinweisschilder anzuzeigen.

Bei einer echten Videoüberwachungsmaßnahme handelt es sich um ein automatisiertes Verfahren, weshalb nach § 7 Abs. 2 SDSG die Landesbeauftragte für Datenschutz vor der beabsichtigten Installation einer Videoüberwachungsanlage durch Behörden oder sonstige öffentliche Stellen des Landes zu beteiligen ist. Durch die verantwortliche Stelle ist hierfür eine entsprechende Verfahrensbeschreibung „Videoüberwachung“ mit den nach § 9 Abs. 1 SDSG festzulegenden Angaben zu erstellen. Eine entsprechende Musterverfahrensbeschreibung ist auf unserer Internetseite zum Download eingestellt.

Darüber hinaus ist durch die verantwortliche Stelle das Interesse an der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen gegenüber den „schutzwürdigen Interessen der Betroffenen“ abzuwägen. Schutzwürdige Interessen von Betroffenen überwiegen beispielsweise dort, wo deren Intimsphäre berührt wird. Auf Friedhöfen gilt dies sicher dort, wo Trauernde zum Verweilen in stillem Gedenken oder zum Gebet eingeladen werden.

Ebenso ist zu prüfen, ob für den „angestrebten Zweck“ tatsächlich eine tägliche Überwachungsdauer von 24 Stunden erforderlich ist, oder nicht vielmehr eine Begrenzung beispielsweise auf die Nacht und den Frühmorgen, eben zu jener Zeit, zu welcher die Diebstähle stattfanden, ausreichend ist.

9.2 Anwendungssoftware der Zentralen Bußgeldbehörde

Im Berichtszeitraum bin ich im Rahmen des Freigabeverfahrens gemäß § 7 Abs. 2 Satz 5 Saarländisches Datenschutzgesetz (SDSG) um eine datenschutzrechtliche Stellungnahme zu der von der Zentralen Bußgeldbehörde des Landesverwaltungsamtes eingesetzten Software für die Bearbeitung von Ordnungswidrigkeiten gebeten worden.

Das Verfahren zur Bearbeitung von Verkehrsordnungswidrigkeiten dient der Vorgangsverwaltung und ersetzt zudem im Wesentlichen die bisher geführte Papierakte. Lediglich Unfallakten, Akten von Alkohol-Verkehrsordnungswidrigkeiten und von Gefahrgutverfahren werden nicht in elektronischer Form geführt. Da das Saarland bislang allerdings noch nicht von seiner Ermächtigung zum Erlass der erforderlichen Rechtsverordnung für die elektronische Aktenführung nach § 110b Abs. 1 S. 2 Ordnungswidrigkeitengesetz (OWiG) Gebrauch gemacht hat, werden sämtliche Urschriften weiterhin noch in Papierform aufbewahrt. Auch erfolgt bei Abgabe an die Justiz keine elektronische Übermittlung der Akte, sondern es wird eine Papierakte ausgedruckt und versendet. Das Verfahren veranlasst automatisiert verschiedene Arbeitsschritte wie Halteranfragen, Verkehrszentralregisteranfragen und den Ausdruck von Bußgeldbescheiden.

Nach den Planungen des Landesverwaltungsamtes soll das vorhandene Programm in naher Zukunft um weitere Module erweitert werden. Die in dem Programm vorgehaltenen Daten sollen dann nach Erledigung der jeweiligen Verfahren zunächst in ein Archivierungsmodul und nach Ablauf der Aufbewahrungsfristen in anonymisierter Form in ein Statistikmodul überführt werden. Bis das Archivierungsmodul eingesetzt werden kann, werden alle Verfahren bis zum Ablauf der Aufbewahrungsfristen in dem aktiven Modul gespeichert. Die Löschung der Daten erfolge derzeit noch von Hand, solle aber nach Einsatz der weiteren Module automatisch erfolgen.

Bei der datenschutzrechtlichen Betrachtung des Verfahrens lag ein besonderes Augenmerk auf den Aufbewahrungsfristen. Die Aufbewahrung von Bußgeldakten erfolgt bislang auf der Grundlage eines Erlasses des damaligen Ministeriums des Innern aus dem Jahre 1990. Die dort aufgeführten Aufbewahrungsfristen sollten nach den Vorstellungen des Landesverwaltungsamtes – vorläufig bis zum Inkrafttreten einer Rechtsverordnung zur elektronischen Aktenführung - im Wesentlichen auch für die elektronische Sachbearbeitung übernommen werden. Eine Ausnahme sollte jedoch hinsichtlich solcher Verfahren gelten, bei denen der Erlass eine Aufbewahrungsfrist von einem Jahr bzw. 6 Monaten vorsieht. Hier beabsichtigte das Landesverwaltungsamt eine Verlängerung der Aufbewahrungsdauer auf zwei Jahre. Grund hierfür war, dass die Verfahren zur Verfolgung und Ahndung von Ordnungswidrigkeiten von den Kommunen auf das Landesverwaltungsamt abgegeben worden sind. Für diese Verfahren erhalten die Kommunen zur Kompensation der im Rahmen der Verkehrsüberwachung entstandenen Aufwendungen eine vertraglich vereinbarte Fallkostenpauschale, die im ersten Quartal eines Jahres für das vorausgegangene Jahr errechnet werde. Für eventuelle Rückfragen durch die Kommunen sei es erforderlich, dass die Verfahrensdaten noch bis zum Abschluss dieses Abrechnungsverfahrens vorgehalten werden. Die noch parallel vorhandenen Papierakten sollen hingegen bereits vorher vernichtet werden.

Da ausdrückliche Fristen für die Dauer der Aufbewahrung elektronisch geführter Akten nicht existieren, gilt, dass eine Löschung personenbezogener Daten zu erfolgen hat, wenn diese zur Aufgabenerfüllung nicht mehr erforderlich sind.

Die Daten, die über den in dem Erlass vorgesehenen Zeitraum hinaus gespeichert werden sollen, werden zwar zu Abrechnungszwecken weiterhin benötigt, für die Bearbeitung der jeweiligen Verkehrsordnungswidrigkeitenverfahren sind sie jedoch nicht mehr erforderlich.

Daher wurde mit dem Landesverwaltungsamt die Vereinbarung getroffen, dass – bis zum Einsatz eines entsprechenden Erweiterungsmoduls - hinsichtlich der Daten, die nach Ablauf der in dem Erlass aufgeführten Fristen zu verfahrensfremden Zwecken noch zur Verfügung stehen sollen, besondere Vorkehrungen zum Schutz des informationellen Selbstbestimmungsrechts der Betroffenen zu treffen sind. Diese Daten werden für die generelle Sachbearbeitung gesperrt und sind nur noch einem begrenzten, für die abschließende Bearbeitung der Verfahren zuständigen Bearbeiterkreis zugänglich.

Des Weiteren habe ich darauf hingewiesen, dass eine automatische Löschung der Daten der bislang erfolgenden Löschung von Hand vorzuziehen ist, da hierdurch die Einhaltung der geltenden Aufbewahrungsfristen besser zu gewährleisten ist. Insofern sollte das Verfahren baldmöglichst die automatische Löschung ermöglichen.

Da aufgrund des Fehlens der erforderlichen rechtlichen Grundlage für die ausschließliche elektronische Aktenführung derzeit parallel neben der Speicherung in dem automatisierten Verfahren auch noch sämtliche Urschriften in Papierform über einen längeren Zeitraum vorgehalten werden müssen, wurde von unserer Seite der Erlass einer gemäß § 110b Abs. 1 Satz 2 und 3 OWiG erforderlichen Rechtsverordnung für die elektronische Aktenführung angemahnt. Nach Inkrafttreten dieser Rechtsgrundlage werden auch die dann festzulegenden Aufbewahrungsfristen am Maßstab der Erforderlichkeit erneut zu überprüfen sein.

9.3 Einwohnerbefragungen

Um kommunale Planungen nach den Bedürfnissen und Erwartungen der Einwohner ausrichten zu können, führen Kommunen verschiedentlich Befragungen ihrer Einwohner durch.

Im Berichtszeitraum wurde ich um eine datenschutzrechtliche Bewertung einer von einer Kommune in Zusammenarbeit mit einem Institut der Universität des Saarlandes beabsichtigten Befragung der Einwohner gebeten. Hierdurch versprach sich die Kommune Hinweise für ihre künftige Arbeit im Bereich des Sports. Zur Durchführung der Befragung wurden die Adressdaten von in einem mehrstufigen Quotenverfahren zufällig ausgewählten Personen durch die Meldebehörde der Kommune an die Universität übermittelt, die mit der Versendung der Fragebögen an den ausgewählten Personenkreis beauftragt war. Der Rücklauf der Fragebögen erfolgte sodann unmittelbar an das mit der Durchführung des Projekts beauftragte Institut. Sofort nach Versendung der Fragebögen löschte die Universität sämtliche Adressdaten, so dass im weiteren Verlauf der Befragung eine Zusammenführung dieser Daten mit den an das Institut rücklaufenden Fragebögen nicht mehr möglich war. In ei-

nem dem Fragebogen beigefügten separaten Hinweisblatt wurden die angeschriebenen Bürger in datenschutzrechtlich ausreichender Weise über die Herkunft ihrer Adressdaten sowie deren unverzüglichen Löschung und damit über die anonymisierte Durchführung der Befragung informiert. Darüber hinaus wurde in dem Anschreiben in dem gebotenen Umfang auf die Freiwilligkeit der Teilnahme an der Befragung hingewiesen. Durch die frühzeitige Einbindung meiner Dienststelle konnten bereits im Vorfeld auftretende Fragen geklärt und eine datenschutzgerechte Durchführung der Befragung erreicht werden.

Dass hingegen eine fehlende Transparenz bei der Durchführung einer Einwohnerbefragung bei den betroffenen Bürgern Bedenken hinsichtlich des Umgangs mit ihren personenbezogenen Daten hervorrufen, zeigt das Beispiel einer Gemeinde, die ebenfalls in Zusammenarbeit mit einem Institut eine Seniorenbefragung durchgeführt hatte. Ein Bürger hat sich unter Vorlage des von dem Bürgermeister der Gemeinde versandten Anschreibens einschließlich des Fragebogens an meine Dienststelle gewandt, da er Zweifel an der datenschutzgerechten Durchführung des Projekts hatte. Diese Bedenken waren auch nicht unberechtigt. Meine Recherchen ergaben, dass der Einwohnerbefragung ein Beschluss des Gemeinderates zugrunde lag und die Durchführung anonym erfolgen sollte. Von einer vollständigen Anonymität konnte in dem geschilderten Fall indes nicht ausgegangen werden, da in dem Fragebogen zahlreiche, teils sehr individuelle Einzelangaben von den Befragten erhoben worden sind, die Rückschlüsse auf bestimmte Personen zuließen. Von den über 55-jährigen Einwohnern der Kommune, die alle im Rahmen der Befragung angeschrieben worden sind, wurden Angaben zu ihrem Alter, Geschlecht, Familienstand, Bildungsabschluss, derzeitiger Berufstätigkeit und der Höhe ihres Haushaltsnettoeinkommens erbeten. Darüber hinaus wurde erfragt, in welchem Ortsteil sie leben. Hinzu kamen weitere Fragen zur derzeitigen Wohnsituation, zur Mobilität und zur Inanspruchnahme haushaltsnaher Dienstleistungen. Die von den Befragten zu erteilenden Auskünfte sind personenbeziehbar und lassen jedenfalls bei Vorliegen von Zusatzwissen einen Rückschluss auf die befragte Person zu. Dabei kommt es nicht darauf an, ob im konkreten Fall die Absicht besteht, sich das Zusatzwissen zu besorgen, um die jeweiligen Personen zu identifizieren.

Handelt es sich bei den zu erhebenden Daten mithin um personenbezogene Daten, so sind die Betroffenen gemäß § 12 Abs. 1 des Saarländischen Datenschutzgesetzes (SDSG) - sofern nicht schon auf Grund einer Rechtsvorschrift eine Auskunftspflicht besteht - zwingend auf die Freiwilligkeit ihrer Angaben hinzuweisen. Dieser Hinweis auf die Freiwilligkeit ist so zu gestalten, dass dem Betroffenen hinreichend deutlich wird, dass er die Teilnahme insgesamt oder hinsichtlich einzelner Fragen verweigern kann und ihm aus der Weigerung der Teilnahme keinerlei Nachteile entstehen. Ein solcher, ausdrücklicher Hinweis auf die Freiwilligkeit ist umso wichtiger, wenn ein Schreiben, wie hier, von dem Bürgermeister versandt wird und dieses daher bei dem Empfänger einen amtlichen Eindruck hinterlässt. Das Schreiben des Bürgermeisters enthielt hier lediglich eine allgemein gehaltene Bitte, das Projekt zu unterstützen, ein ausdrücklicher Hinweis auf die Freiwilligkeit fehlte hingegen völlig.

Da jedoch bereits alle Fragebögen verschickt worden waren, blieb mir nichts anderes übrig, als die Gemeinde aufzufordern, nachträglich in Form einer öffentlichen Bekanntmachung auf die Freiwilligkeit der Teilnahme an der Befragung hinzuweisen. In gleicher Weise sollten die Bürger darüber informiert werden, dass die Fragebögen nur zu dem

angegebenen Zweck verwendet und unverzüglich nach der Auswertung vernichtet werden. Diesen Forderungen kam die Gemeinde durch Veröffentlichung der geforderten Angaben im Nachrichtenblatt und auf der Homepage der Gemeinde sowie in regionalen Zeitungen nach.

Da die Kommune auf meine Hinweise und Forderungen zur datenschutzgerechten Ausgestaltung der Befragung mit großem Unverständnis reagierte und hierin eine Abwertung ihres Projekts sah, musste ich nachdrücklich darauf hinweisen, dass ich keine inhaltliche Bewertung des Projekts vorgenommen habe, sondern entsprechend meiner Zuständigkeit lediglich die Einhaltung der Vorschriften über den Datenschutz überwache. Des Weiteren habe ich angeregt, meine Dienststelle zukünftig bereits frühzeitig in die Planung solcher Vorhaben einzubeziehen, damit bereits vor der Durchführung von konkreten Maßnahmen Empfehlungen zur Einhaltung der datenschutzrechtlichen Vorschriften gegeben werden können.

9.4 Übertragung von Gemeinderatssitzungen im Internet

Um zu einer größeren Transparenz von Entscheidungen der Gemeinden beizutragen und den Bürgern die Mitwirkung und Teilhabe an der Gestaltung ihrer Gemeinde zu erleichtern, möchten immer mehr Kommunen ihre Gemeinde- bzw. Stadtratssitzungen über das Internet übertragen. Neben einer Kommune, die im Berichtszeitraum bei meiner Dienststelle nach den Zulässigkeitsvoraussetzungen für ein solches Live-Streaming-Angebot anfragte, informierte sich auch der Ausschuss für Datenschutz und Informationsfreiheit des Landtages darüber, wie ein solches Angebot datenschutzgerecht umgesetzt werden kann.

Da bislang keine speziellen Regelungen dazu existieren, unter welchen Voraussetzungen Ratssitzungen im Internet übertragen werden können, gibt es in diesem Bereich nach wie vor zahlreiche rechtliche Unsicherheiten.

Nach § 40 Abs. 1 Kommunalselbstverwaltungsgesetz (KSVG) sind die Sitzungen des Gemeinderats öffentlich, soweit nicht Rücksichten auf das öffentliche Wohl oder berechtigte Interessen Einzelner entgegenstehen. Auszugehen ist davon, dass der Begriff der „Öffentlichkeit" i.S.d. § 40 KSVG nicht nur eine ausschließliche Saalöffentlichkeit in dem Sinne einer Begrenzung auf die im Sitzungssaal Anwesenden bedeutet, sondern auch den medienspezifischen Einsatz von Aufnahme- und Übertragungsgeräten mit dem Ziel der entsprechenden Verbreitung der Aufnahmen erlaubt.

§ 40 KSVG enthält allerdings keine Regelung darüber, unter welchen Bedingungen die Öffentlichkeit hergestellt werden kann.

Da bei der Übertragung von Ratssitzungen im Internet personenbezogene Daten im Sinne des Saarländischen Datenschutzgesetzes (SDSG) übermittelt werden, kann eine Übertragung – mangels Vorliegens einer gesetzlichen Befugnis – gemäß § 4 Abs. 1 b SDSG grundsätzlich nur dann zulässig sein, wenn die Betroffenen, von denen Bild- oder Tonaufnahmen übertragen werden sollen, zuvor hierin eingewilligt haben.

Dies gilt zunächst für die an der Sitzung teilnehmenden Ratsmitglieder, da diesen auch im Rahmen von öffentlichen Ratssitzungen das Recht zusteht, über die Nutzung ihrer Daten selbst zu entscheiden. Liegt eine

solche Einwilligung des Ratsmitgliedes nicht vor, ist die Internetübertragung seines Redebeitrages unzulässig. Daher müssen bei der Übertragung der Sitzung die Bild- und Tonaufnahmen des Redebeitrages dieses Ratsmitgliedes ausgeblendet werden.

In diesem Zusammenhang ist allerdings auch anzumerken, dass die Frage, ob Ratsmitglieder als Inhaber eines öffentlichen Amtes überhaupt unter den Schutzbereich des SDSG fallen, nicht unumstritten ist (vgl. hierzu OVG des Saarlandes, Beschluss vom 30.08.2010 – 3 B 203/10 -, VG des Saarlandes, Urteil vom 25.03.2011 – 3 K 501/10 – jeweils m.w.N.). Unterfallen sie entsprechend den Ausführungen in den genannten Entscheidungen nicht oder nur eingeschränkt dem Schutz des SDSG hätte dies zur Folge, dass nicht zwingend eine explizite Einwilligung der Ratsmitglieder einzuholen wäre, sondern der Ratsvorsitzende im Rahmen seiner Sitzungsgewalt lediglich sorgfältig zu prüfen hätte, ob ein aus dem allgemeinen Persönlichkeitsrecht eines Ratsmitgliedes hergeleitetes Widerspruchsrecht besteht.

Hinsichtlich der im Sitzungssaal anwesenden Zuschauer bedarf es vor einer Übertragung von Bild- oder Tonaufnahmen in jedem Falle einer informierten Einwilligung. Da die Einwilligung gemäß § 4 Abs. 1 Satz 2 SDSG schriftlich zu erteilen ist, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist, und diese schriftliche Einwilligung vermutlich nicht von allen im Zuschauerraum anwesenden Personen erteilt wird, ist von einer bildlichen Erfassung des Zuschauerraums grundsätzlich abzusehen.

Bezüglich der im Sitzungssaal anwesenden Verwaltungsmitarbeiter kann von einer freiwilligen Erteilung der Einwilligung nicht ausgegangen werden, da diese in einem Beschäftigungsverhältnis mit der Gemeinde und damit in einer besonderen Abhängigkeit zu dieser stehen. Daher können diese im Regelfall nicht wirksam in die Übertragung einwilligen.

Schließlich ist bei der Übertragung der Sitzungen im Internet zu beachten, dass die Anbieter solcher Streaming-Dienste die Daten häufig auf Servern in Staaten speichern, in denen kein angemessenes Datenschutzniveau gewährleistet ist.

Angesichts der zahlreichen rechtlich nicht eindeutig geklärten Fragen im Zusammenhang mit der Übertragung von Gemeinderatssitzungen im Internet ist anzuregen, dass der Gesetzgeber hierzu klare Regelungen erlässt.

9.5 Rats- und Bürgerinformationssysteme

Immer mehr Gemeinde- und Kreisverwaltungen führen zur Unterstützung der Mandatsarbeit und zur Vor- und Nachbereitung der Gemeinderats- oder Kreistagssitzungen sogenannte Sitzungsmanagement-Systeme ein. Diese bestehen regelmäßig aus einem verwaltungsinternen Modul, das alleine den Mandatsträgern zur Verfügung steht und aus einem öffentlich zugänglichen Bürgerinformationssystem, mit dessen Hilfe dem Bürger Informationen aus der Ratsarbeit zum Abruf über Internet zur Verfügung gestellt werden können.

Gerade was das Bürgerinformationssystem betrifft, sind im Berichtszeitraum immer wieder einzelne Bürger und Gemeinde- bzw. Kreisverwal-

tungen mit der Frage an uns herangetreten, welche Informationen überhaupt im Internet durch die Verwaltungen veröffentlicht werden dürfen.

Die Tagesordnung und auch Sitzungsvorlagen dürfen nur veröffentlicht werden, wenn sie keine personenbezogenen Daten von Bürgern enthalten oder der Bürger in die Veröffentlichung im Rahmen des Bürgerinformationssystems ausdrücklich eingewilligt hat.

Die Sitzungsniederschriften dürfen personenbezogene Daten der Mandatsträger enthalten. Im Hinblick darauf, dass diese eine Funktion wahrnehmen, die einer verstärkten öffentlichen Wahrnehmung unterliegt ist es zulässig, dass die Sitzungsniederschrift die Namen der an der Sitzung teilnehmenden Mandatsträger sowie deren inhaltliche Beiträge wiedergibt. Auf eine wortwörtliche Wiedergabe der Beiträge sollte dabei jedoch verzichtet werden. Von Bürgern oder anderen Beteiligten ist es in der Regel unzulässig personenbezogene Daten in die Sitzungsniederschrift aufzunehmen.

Auch das Veröffentlichen von personenbezogenen Daten über die Mandatsträger ist zulässig, soweit es sich hierbei um den Namen und die Parteizugehörigkeit handelt. Die Aufnahme von Bildern, der Adresse oder von privaten Kontaktmöglichkeiten (Telefonnummer, E-Mail) der Mandatsträger ist ohne deren ausdrückliche Einwilligung unzulässig.

Darüber hinaus ist die Veröffentlichung von personenbezogenen Daten von Bürgern oder Verwaltungsmitarbeitern, die in der Ratssitzung zu Wort kommen im Regelfall unzulässig.

9.6 Zugriff auf Ratsinformationssysteme durch Nicht-Mandatsträger

Wir wurden durch den Landrat eines saarländischen Landkreises gebeten, zu der Frage Stellung zu nehmen, inwiefern der Zugriff von Nicht-Mandatsträgern auf den nicht öffentlichen Teil des kommunalen Ratsinformationssystems zulässig sei. Hintergrund war, dass eine Fraktion darum gebeten hatte, dem Fraktionsgeschäftsführer, der selbst nicht Mitglied des Kreistags war, einen uneingeschränkten Zugang auf die im Ratsinformationssystem eingestellten Sitzungsunterlagen zu eröffnen, damit dieser die Sitzungen entsprechend seiner Funktion vorbereiten könne.

Nach unserer Auffassung gibt es für derartige Zugriffe durch Nicht-Mandatsträger keine rechtliche Grundlage.

Datenschutzrechtlich ist der Landkreis im Hinblick auf das Ratsinformationssystem als verantwortliche Stelle im Sinne des § 3 Abs. 3 Saarländisches Datenschutzgesetz (SDSG) zu qualifizieren. Zum einen dient das Ratsinformationssystem der Arbeit und Unterstützung des Kreistags. Zum anderen hat der Landkreis als technischer Betreiber des Systems aber auch die physische Herrschaft über den Verarbeitungsprozess.

Demgegenüber ist der Fraktionsgeschäftsführer als Dritter im Sinne des § 3 Abs. 5 SDSG anzusehen. Er steht in einem privat-rechtlichen Anstellungsverhältnis zur Fraktion. Er ist weder Angestellter des Landkreises noch des Kreistags.

Damit ist der Zugriff des Fraktionsgeschäftsführers als Abruf aus einem automatisierten Verfahren (Übermittlung, § 3 Abs. 2 Nr. 4 SDSG) zu werten, für den es jedoch an einer rechtlichen Grundlage fehlt.

Die Voraussetzungen des einzig in Betracht kommenden § 16 Abs. 1 Satz 1 Buchstabe a SDSG sind nicht erfüllt. Nach unserer Auffassung fehlt es am Merkmal der Erforderlichkeit zur Aufgabenerfüllung. Im Rahmen der Aufgabenerfüllung ist allein auf die Aufgaben des Landkreises als verantwortliche Stelle abzustellen. Danach existiert aber keine Aufgabenzuweisung, die eine Bereitstellung der Sitzungsunterlagen als erforderlich erscheinen ließe. Anders als in den Kommunalgesetzen einiger anderer Bundesländer enthält das Kommunale Selbstverwaltungsgesetz (KSVG) keine ausdrückliche Berechtigung zur Beschäftigung eigenen Personals von Fraktionen oder Mandatsträgern. Im KSVG sind solche externen Mitarbeiter weder erwähnt, geschweige denn mit eigenen Rechten und Pflichten ausgestattet. Am Prozess der Meinungsbildung und Beschlussfassung des Kreistags wirken sie daher nicht mit. Eine Kenntnis der Inhalte der Sitzungsunterlagen ist daher nicht erforderlich.

Auch andere Rechtsvorschriften, die eine Übermittlung gestatten würden, existieren nicht. In der Geschäftsordnung des Kreistags ließen sich keine derartigen Erlaubnistatbestände regeln. Zwar bestimmt § 4 Abs. 1a SDSG, dass auch andere Rechtsvorschriften grundsätzlich in Betracht kommen. Verlangt wird aber eine Außenwirkung des entsprechenden Regelungswerkes. Der Geschäftsordnung des Kreistags fehlt diese Außenwirkung. Sie wird nicht von einem Gesetz-, Verordnungs- oder Satzungsgeber mit Wirkung für nachgeordnete Dritte, sondern von den Mandatsträgern des Kreistags zur Regelung der inneren Ordnung sowie des Ablaufs der Meinungs- und Willensbildung ihres Kollegialorgans beschlossen. Sie regelt ausschließlich ihre eigenen organinternen Rechtsbeziehungen im Kreistag und nicht das Verhältnis zwischen Staat und Bürger.

9.7 Versteigerungen von Handys und Smartphones durch Fundbüros und Staatsanwaltschaft

Im Berichtszeitraum hat ein Petent gegenüber hiesiger Dienststelle vorgetragen, dass er des Öfteren gebrauchte Handys und Smartphones teils von Fundbüros teils auch von Staatsanwaltschaften ersteigert. Nicht selten seien auf dem internen Speicher noch persönliche Daten und Fotos zu finden.

Meine Dienststelle hat daher das hiesige Innenministerium und auch das Justizministerium um Mitteilung gebeten, ob gebrauchte Handys und Smartphones überhaupt in Versteigerungen angeboten werden können und ob gegebenenfalls hierzu eine entsprechende Anweisung zum Löschen etwaiger noch vorhandener personenbezogener Daten erlassen worden sei.

Soweit in Mobiltelefonen, Smartphones oder ähnlichen mobilen Geräten personenbezogene Daten gespeichert sind, kommt es nach Auffassung des Innenministeriums im Falle der Versteigerung zu einer Übermittlung personenbezogener Daten in Form der körperlichen Weitergabe des Datenträgers. Da es dem Fundbüro jedoch an einer entsprechenden Datenübermittlungsbefugnis fehlt, sind personenbezogene

Daten vor der Verwertung zu löschen. Kann dies nicht oder nicht mit vertretbarem Aufwand erfolgen, hat die Versteigerung zu unterbleiben. Ich teile die Auffassung des Ministeriums.

Das Ministerium der Justiz führte auf meine Anfrage Nachstehendes aus: „Die Staatsanwaltschaft Saarbrücken bietet aus datenschutzrechtlichen Gründen keine gebrauchten Handys oder Smartphones in Versteigerungen an. Darüber hinaus stünden der Aufwand für eine ordnungsgemäße Datenlöschung und der weitere Versteigerungsaufwand in der Regel nicht in einem angemessenen Verhältnis zum zu erwartenden Versteigerungserlös. Gebrauchte Handys werden grundsätzlich an das Landeskriminalamt zum internen dienstlichen Gebrauch bzw. zur Nutzung von Akkus oder sonstigen Ersatzteilen übergeben.

Auch die saarländische Justiz nutzt die Internetversteigerungsplattform http://www.justiz-auktion.de. Grundlage ist die Saarländische Verordnung zur Regelungen der Versteigerungen im Internet – Internetversteigerungsverordnung –. Gemäß § 2 dieser Verordnung ist für Versteigerungen durch Gerichtsvollzieher im Internet gemäß § 814 Abs. 3 S. 1 Zivilprozessordnung (ZPO) sowie für Versteigerungen von an Justizbehörden abgelieferten Fundsachen und im Besitz von Justizbehörden befindlicher unanbringbarer Sachen gemäß § 979 Abs. 1 b S. 2 Bürgerliches Gesetzbuch (BGB) die genannte Versteigerungsplattform zu nutzen, des Weiteren zur Versteigerung eingezogener Gegenstände sowie ausgesonderter Sachen des Verwaltungsgebrauchs.

Nach Nr. 11.7 des Leitfadens für die Nutzung der Internetplattform Justiz-Auktion für die Gerichtsvollzieher/innen ist bei der Versteigerung von Gegenständen mit Speicherkapazität (z. B. Festplatten aus PCs, Laptops, Druckern oder Kopierern, Navigationsgeräten, Digitalkameras, Spielekonsolen etc.) sicherzustellen, dass sich keine dienstlichen oder privaten Daten auf dem Medium befinden. Zwar sind in der beispielhaften Aufzählung Handys und Smartphones nicht genannt, aber auf Grund der Definition dennoch von der genannten Regelung umfasst, so dass insoweit die Voraussetzungen für eine sichere Versteigerung im Sinne des Datenschutzes geschaffen sind.

Sowohl die Verfahrensweise der Staatsanwaltschaft Saarbrücken, als auch die Nutzung der Internetversteigerungsplattform der saarländischen Justiz begegnen keinen datenschutzrechtlichen Bedenken.

10 Abfallentsorgung

10.1 Datenschutzrechtliche Fragen bei der Abfallentsorgung

Immer wieder wenden sich Bürger oder auch Stellen, die die Abfallentsorgung durchführen, mit Fragen zum Datenschutz an meine Dienststelle. So auch im Berichtszeitraum:

10.1.1 Müllverwiegung im Testbetrieb

Einer Petentin war aufgefallen, dass eine Kommune mit der Verwiegung des Haus- und Biomülls begonnen hatte, obwohl ihr auf ausdrückliche Nachfrage mitgeteilt worden war, dass damit erst zu einem späteren Zeitpunkt, wie er in der entsprechenden Satzung festgelegt war, begonnen werden sollten.

Die Petentin war empört darüber, dass hinter dem Rücken der Bürger bereits Daten gesammelt würden, über deren Verwendung Unklarheit bestehe. Auf Nachfrage hat der Entsorgungsverband Saar (EVS) mitgeteilt, dass in einem Zeitraum von 5 Monaten tatsächlich eine Verwiegung stattgefunden habe. Dies sei geschehen, um das neue Verwiegesystem zu testen, damit ab Echtbetrieb die Abfallgebühren korrekt abgerechnet werden können. Eine Auswertung der Verwiegeergebnisse in Bezug zu einem bestimmten Anwesen sei nie beabsichtigt gewesen und auch nicht erfolgt. Im Übrigen seien die Testdaten mittlerweile durch Echtdaten überschrieben.

Bei dieser Sachlage haben wir keinen Anlass zur Beanstandung der mit der Müllverwiegung verbunden Datenspeicherung gesehen, weil die Datenspeicherung zur Aufgabenerfüllung des EVS im Sinne des Saarländischen Datenschutzgesetzes erforderlich und somit zulässig war. Zu bemängeln war allerdings die fehlende Information der Betroffenen durch den EVS oder die betreffende Kommune. Ich bin sicher, dass durch eine entsprechende Aufklärung die Irritationen im vorliegenden Fall hätten vermieden werden können.

10.1.2 Angaben bei der Ausgabe der „Gelben Säcke“

Ein Petent wandte sich mit einer Frage im Zusammenhang mit der Ausgabe der „Gelben Säcken“ an meine Dienststelle. Er habe kürzlich in einem Drogeriegeschäft eine Rolle mit Gelben Säcken abgeholt. In eine frei ausliegende Liste habe er Name, Anschrift und Unterschrift eintragen müssen. Den Petenten stört es, dass die Liste für jeden Kunden, der eine Rolle beziehen will, voll umfänglich einsehbar ist. So sei ihm aufgefallen, dass ein Kunde nach ihm aufmerksam die Liste studiert habe. Ihm sei überhaupt nicht klar, wofür die Daten notwendig seien und hat deshalb unsere Dienststelle um Prüfung der datenschutzrechtlichen Zulässigkeit gebeten.

Auf Nachfrage hat mir die Entsorgungsfirma (die im Auftrag der Kommunen die Gelben Säcke einsammelt) mitgeteilt, dass die Angabe von Namen und Adressen zu Abrechnungszwecken mit den Ausgabenstellen diene, da deren Bezahlung sich nach der Anzahl der ausgegebenen Rollen mit „Gelben Säcke" richte. Der Eintrag in die Listen stelle eine Art Quittung dar, mit der nachvollzogen werden könne, ob die Ausgabestellen tatsächlich die in Rechnung gestellten Rollen ausgegeben haben. Die Listen würden monatlich eingesammelt und nach 6 Monaten vernichtet. Eine Speicherung oder automatisierte Verarbeitung erfolge nicht.

Vom Grundsatz her ist ein berechtigtes Interesse der Entsorgungsfirma an der Erhebung der fraglichen Daten anzuerkennen. Für problematisch halte ich allerdings die Form der Datenerhebung mittels einer Liste, weil jeder Bürger, der die Abholung einer Rolle bestätigt, die Daten der vorhergehenden Personen mit Name und Anschrift sehen kann. Eine Erörterung der Problematik mit der Entsorgungsfirma hat im Ergebnis dazu geführt, dass zukünftig nur noch die Unterschrift zwingend verlangt wird.

Ich habe mich mit dieser Verfahrensweise einverstanden erklärt und die Entsorgungsfirma gebeten, alle Ausgabestellen der Gelben Säcken entsprechend zu informieren.

10.1.3 Internetabfrage der eigenen „Abfalldaten"

Nicht nur Bürger, sondern auch die mit der Abfallentsorgung befassten Stellen wenden sich immer wieder zur Klärung datenschutzrechtlicher Fragen an meine Dienststelle. Dies begrüße ich ausdrücklich, da unzulässige Datenverarbeitungen so von vorneherein vermieden werden und nicht im Nachhinein mit eventuell erheblichem Aufwand datenschutzgerechte Verfahren installiert werden müssen.

Ein Beispiel möchte ich hier wiedergeben:

Im Zuge eines Mehr an Bürgerinformation wollte der EVS die Möglichkeit schaffen, dass sich der Kunde über die Anzahl der durchgeführten Leerungen seiner Müllbehälter und das eingesammelte Gewicht über das Internet informiert. Die Informationen, die angefragt werden können, sind zweifellos personenbeziehbar, sodass sich für den EVS die Frage stellte, wie sichergestellt werden kann, dass nur der Berechtigte auf seine Daten im Internet zugreifen kann.

Der EVS plante von Anfang an, ein Anmeldesystem zu etablieren, bei dem der EVS-Kunde mittels Benutzername und Passwort an seine Daten gelangt. Da dies wegen Zeitknappheit aber erst zu einem späteren Zeitpunkt realisierbar sei, fragte der EVS, ob vorübergehend die Eingabe der sogenannten Debitorennummer, das ist die Nummer, die im Gebührenbescheid des Kunden abgedruckt ist, sicher genug sei, um auszuschließen, dass Unberechtigte Daten auslesen können. Die Debitorennummer besteht aus zwei führenden Ziffern, die stets identisch sind, der Kundennummer und einer Prüfziffer, wobei die Nummern in den Straßenzügen selbst nicht fortlaufend vergeben werden. Die Eingabe der Debitorennummer zur Erlangung der Kenntnis von der Leerungszahl eines fremden Anschließers auf gut Glück sei ohne Kenntnis

des Algorithmus zur Berechnung der Prüfziffer und ohne Kenntnis der Lage des zur Debitorennummer geführten Grundstücks nicht möglich. Damit sei nahezu ausgeschlossen, dass ein Dritter ohne konkrete Kenntnis der Debitorennummer sowie des dazu geführten Grundstücks an fremde Informationen gelangen könne.

Dieser Einschätzung haben wir uns angeschlossen und die Nutzung der Debitorennummer statt Benutzername und Passwort für eine Übergangszeit als vertretbar angesehen.

11 Soziales

11.1 Datenverarbeitung im Jobcenter

Der datenschutzkonforme Umgang mit Sozialdaten im Jobcenter ist immer wieder Gegenstand von Anfragen bei meiner Dienststelle. Auf zwei typische Fragestellungen möchte ich im Folgenden eingehen:

11.1.1 Vorlage von Kundenrechnungen

Wenn Selbständigen Leistungen zur Sicherung des Lebensunterhaltes nach dem Sozialgesetzbuch II -Grundsicherung für Arbeitsuchende- bewilligt werden, wird ihnen zur Auflage gemacht, als Leistungsberechtigungsnachweis die unternehmerische Buchführung, einschließlich der Ausgangsrechnungen an die Kunden, der Sozialbehörde vorzulegen.

Ich vertrete hierzu die Auffassung, dass im Grundsatz die Forderung nach Vorlage von Kundenrechnungen datenschutzrechtlich nicht zu beanstanden ist. Denn der Leistungsträger muss in die Lage versetzt werden, das nach § 11 SGB II maßgebliche Erwerbseinkommen zu ermitteln. Die Vorlage der Kundenrechnungen ist ein geeignetes Mittel, um das Einkommen nachzuweisen.

Allerdings ist in diesem Zusammenhang regelmäßig ohne Belang, welcher Person ein Betrag in Rechnung gestellt worden ist. Die Namen der Kunden sind insofern regelmäßig nicht erforderlich und dürfen deshalb grundsätzlich nicht erhoben werden. Das ergibt sich aus § 67a SGB X, wonach das Erheben von Sozialdaten durch Sozialleistungsträger nur zulässig ist, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle erforderlich ist. Ich empfehle deshalb regelmäßig, auf den Rechnungen den Namen und die Adressen der Kunden zu schwärzen.

11.1.2 Weitergabe von Bewerberdaten an potenzielle Arbeitgeber

Bei den Jobcentern ist es Praxis, Arbeitgebern, die eine Stelle zu vergeben haben, die Namen von als geeignet angesehenen Bewerbern mitzuteilen, ohne die Betreffenden vorher um ihr Einverständnis zu bitten. Manche Bewerber meinen, diese Vorgehensweise widerspreche dem Datenschutz.

Diese sehe ich nicht so. Ausgangspunkt meiner Überlegungen ist, dass jede Datenübermittlung einer Rechtsgrundlage bedarf und diese Rechtsgrundlage ist in der vorliegenden Fallkonstellation § 69 Abs. 1 Satz 1 Nr. 10 SGB X. Nach dieser Vorschrift ist eine Übermittlung von Sozialdaten zulässig, soweit sie erforderlich ist für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle.

Eine Aufgabe der Jobcenter ist die Arbeitsvermittlung (§ 16 Abs. 1 Satz 1 SGB II in Verbindung mit § 35 SGB III). Die Arbeitsvermittlung umfasst alle Tätigkeiten, die darauf gerichtet sind, Arbeitssuchende mit Arbeitgebern zur Begründung eines Beschäftigungsverhältnisses zusammen zuführen. Insoweit ist neben der Übersendung des Stellenangebotes mit den erforderlichen Arbeitgeberdaten an den Bewerber die Übermittlung des Bewerberangebotes an den Arbeitgeber zur problemlosen Kontaktaufnahme erforderlich. Darüber hinaus muss zur Prüfung der Einhaltung von Mitwirkungspflichten und eventuellen Sanktionsmöglichkeiten die tatsächliche Teilnahme an Bewerbungsterminen geklärt werden, was nur möglich ist, wenn dem Arbeitgeber der Name des Arbeitssuchenden zuvor mitgeteilt worden ist. Auch ist es für die Vermittler der Jobcenter von Interesse zu erfahren, weshalb die für geeignet erachteten Bewerber sich letztlich nicht haben durchsetzen können.

Wichtig ist allerdings, dass für den Bewerber transparent ist, an welche Arbeitgeber seine Daten weitergegeben worden sind. Für gut geeignet diese Transparenz herzustellen, halte ich einen Hinweis in dem Vermittlungsvorschlag, dass dem Arbeitgeber der Name und die Adresse des Bewerbers genannt wurde.

12 Gesundheit

12.1 Patientenrechtegesetz

Am 26.02.2013 ist das Patientenrechtegesetz in Kraft getreten. Auf dem Gebiet des Behandlungs- und Arzthaftungsrechts war vieles nicht im Gesetz geregelt, sondern war Richterrecht. Wesentliches Ziel des Patientenrechtegesetzes war, mehr Transparenz und Rechtssicherheit für Patienten und Ärzte zu schaffen.

Schwerpunkt des Gesetzes ist die Kodifizierung des Behandlungs- und Arzthaftungsrecht im Bürgerlichen Gesetzbuch. Wichtige Regelungen betreffen etwa die Informations- und Aufklärungspflichten des Behandelnden, die Einholung der Einwilligung des Patienten vor Durchführung einer medizinischen Maßnahme oder die Beweislast bei Haftung für Behandlungs- und Aufklärungsfehler.

Aus datenschutzrechtlicher Sicht besonders erwähnenswert ist die neue Vorschrift des § 630f BGB, der konkrete Vorgaben zum Inhalt der Behandlungsdokumentation sowie zur Dauer der Aufbewahrung der Patientenakte enthält.

§ 630f BGB hat folgenden Wortlaut:

„Dokumentation der Behandlung

(1) Der Behandelnde ist verpflichtet, zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen. Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind. Dies ist auch für elektronisch geführte Patientenakten sicherzustellen.

(2) Der Behandelnde ist verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen. Arztbriefe sind in die Patientenakte aufzunehmen.

(3) Der Behandelnde hat die Patientenakte für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen."

Eine ganz zentrale Vorschrift aus datenschutzrechtlicher Sicht ist auch der neue § 630g, der die Voraussetzungen der Einsichtnahme in die Patientenakte regelt.

Im Folgenden die Regelung im Wortlaut:

„Einsichtnahme in die Patientenakte

(1) Dem Patienten ist auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische oder sonstige erhebliche Rechte Dritter entgegenstehen. Die Ablehnung der Einsichtnahme ist zu begründen. § 811 ist entsprechend anzuwenden.

(2) Der Patient kann auch elektronische Abschriften von der Patientenakte verlangen. Er hat dem Behandelnden die entstandenen Kosten zu erstatten.

(3) Im Fall des Todes des Patienten stehen die Rechte aus den Absätzen 1 und 2 zur Wahrnehmung der vermögensrechtlichen Interessen seinen Erben zu. Gleiches gilt für die nächsten Angehörigen des Patienten, soweit sie immaterielle Interessen geltend machen. Die Rechte sind ausgeschlossen, soweit der Einsichtnahme der ausdrückliche oder mutmaßliche Wille des Patienten entgegensteht."

Im Rahmen der Beratungen des Gesetzesentwurfs haben die Datenschutzbeauftragten des Bundes und der Länder deutlich gemacht, dass für eine umfassende Sicherstellung der Patientenrechte noch weiterer gesetzgeberischer Handlungsbedarf besteht. Dies betrifft beispielsweise die Datenverarbeitung im Auftrag.

Nach wie vor ist im Gesundheitsbereich bei der Einbeziehung Dritter in Form einer Auftragsdatenverarbeitung (z.B. Systemadministration, Fernwartung) die Frage ungelöst, unter welchen Voraussetzungen diese zulässig ist, wenn die zu verarbeitenden Daten bei dem Auftraggeber durch ein Berufsgeheimnis im Sinne von § 203 Abs. 1 StGB geschützt sind. Da die Weitergabe der Daten an den Auftragnehmer eine Offenbarung nach § 203 Abs. 1 StGB darstellt, fehlt es hierfür – bis auf wenige Ausnahmen in einigen Krankenhausgesetzen der Länder- bislang an einer Rechtsgrundlage, insbesondere für den Bereich der niedergelassenen Ärzte. Die Datenschutzbeauftragten haben deshalb gefordert, bereichsspezifische Vorgaben zur Auftragsdatenverarbeitung im Zusammenhang mit Behandlungsverträgen vorzusehen.

Schließlich wäre das Patientenrechtengesetz eine gute Gelegenheit gewesen, den Umgang mit der Behandlungsdokumentation im Falle eines vorübergehenden Ausfalls, des Todes oder Insolvenz des Behandelnden zu regeln. Ein bundesweit einheitlicher rechtlicher Rahmen fehlt hier. So ist beispielsweise fraglich, ob und gegebenenfalls unter welchen Voraussetzungen im Falle einer Praxisinsolvenz oder einer für den Nachlass eines Praxisinhabers bestellten Nachlasspflegschaft die von der ärztlichen Schweigepflicht umfassten Patientendaten von Dritten zur Kenntnis genommen werden dürfen. Klärungsbedürftig ist weiterhin, ob und gegebenenfalls welche Stellen neben den Rechtsnachfolgern für eine weitere Aufbewahrung der Behandlungsdokumentationen im Falle einer Insolvenz oder des Todes des Praxisinhabers verantwortlich sind.

Leider hat der Gesetzentwurf diese Forderungen der Datenschutzbeauftragten des Bundes und der Länder nicht berücksichtigt.

13 Schule und Bildung

13.1 Datenschutzrechtliche Aktivitäten im Bildungssektor

Neben der Bearbeitung datenschutzrechtlicher Eingaben und der datenschutzrechtlichen Begleitung diverser Projekte im Bildungssektor lag im Berichtszeitraum ein besonderer Schwerpunkt meiner Tätigkeit auf der Publikation von Chancen und Risiken im Internet. In mehreren Veranstaltungen wurden Vorträge und Workshops zur Problematik Soziale Netzwerke und Medienkompetenz durch meine Dienststelle gehalten. Hier ein kurzer Überblick über die wichtigsten Aktivitäten:

13.1.1 Power-Point-Präsentation der Arbeitsgemeinschaft Medienkompetenz auf dem Bildungsserver Saar

Schon im Jahre 2008 haben sich im Saarland verschiedene Institutionen vernetzt, die auf dem Gebiet der Förderung der Medienkompetenz tätig sind. Sie gründeten die Arbeitsgemeinschaft Medienkompetenz, in der sich in regelmäßigen Abständen über Aktivitäten und Optimierungsmöglichkeiten auf dem Bereich der Medienkompetenz ausgetauscht wird. Das Unabhängige Datenschutzzentrum war von Anfang an Teil der Arbeitsgemeinschaft und hat sich im Berichtszeitraum an der Erstellung einer Lehrpräsentation zur Medienkompetenz beteiligt. Die Präsentation ist für Lehrkräfte gedacht, die ihren Schülern im Unterricht Medienkompetenz vermitteln möchten. Die Präsentation besteht aus einem Grundmodul und fünf möglichen Erweiterungsmodulen. Eines der Module befasst sich mit den datenschutzrechtlichen Aspekten bei der Nutzung Sozialer Netzwerke im Internet. Die Module stehen auf dem Bildungsserver Saar unter http://www.saarland.de/17931.htm zum Abruf bereit.

13.1.2 Vortrag zur Themenreihe „Eltern und Medien“ im Elternfortbildungsprogramm

Die Landesmedienanstalt Saar bietet in Zusammenarbeit mit dem Landesinstitut für Pädagogik und Medien Vorträge zur Themenreihe „Eltern und Medien“ an. Soziale Netzwerke sind Bestandteil der Lebenswelt junger Menschen und werden von ihnen zur Kommunikation und zur Selbstdarstellung genutzt. Allerdings bergen sie auch Gefahren, da sie eine Informationsquelle über den Nutzer, sein Verhalten und seine Lebensweise darstellen. Daher gilt es, Jugendliche für den Datenschutz zu sensibilisieren und sie zu dem entsprechenden Verhalten anzuleiten. Was das Elternhaus dazu beitragen kann war Gegenstand einer Veranstaltung, die von einem Mitarbeiter meiner Dienststelle gestaltet wurde.

13.1.3 Vortrag „Facebook & Co. / Soziale Netzwerke im Alltag von Kindern und Jugendlichen“

Die Christliche Erwachsenenbildung sowie die Gemeinde Weiskirchen luden zu einem Vortrag ein, der durch meine Dienststelle gestaltet wurde. Gegenstand waren unter anderem eine interaktive Präsentation, wie man einen Facebook-Account sicher einstellt, welche Chancen und Gefahren in sozialen Netzwerken zu finden sind und was man als Betroffener gegen Cybermobbing tun kann.

13.1.4 1. P@d-Day des Landesinstituts für Pädagogik und Medien

Das Landesinstitut für Pädagogik und Medien verfügt über ein Kontingent an Tablet-PCs, die sich Schulen ausleihen können. Den Schülern sollen die Möglichkeiten des Lernens mit einem solch modernen Medium näher gebracht werden. Anlässlich dieser Möglichkeiten bot das Landesinstitut einen Workshop für interessierte Lehrkräfte an, in dem verschiedene Referenten zu diesem Thema eingeladen wurden.

Mobile Endgeräte und die entsprechenden Softwareprogramme erhalten einen zunehmenden Stellenwert bei der Verarbeitung personenbezogener Daten an Schulen. Dabei werden sowohl Schüler-, Eltern- als auch Lehrerdaten genutzt, um den Unterricht oder die Schulverwaltung effizienter zu gestalten. Durch den rasanten technischen Fortschritt bedingt, kann die rechtliche Gestaltung der Zulässigkeit solcher Datenverarbeitungen nur schwerlich mithalten. Welche rechtlichen Hürden beim Einsatz mobiler Endgeräte beachten werden müssen, wie eine rechtssichere Lösung für die Zukunft aussehen könnte und welche Konsequenzen bei Datenverlusten oder Datenmissbrauchsskandalen drohen, diese Fragen wurden durch einen Mitarbeiter meiner Dienststelle beantwortet.

14 Forschung

14.1 Forschungsprojekt motorisierte Zweiradunfälle

Im Auftrag der Landespolizeidirektion Saarland wurde ein interdisziplinäres Forschungsprojekt über Unfälle mit motorisierten Zweirädern durchgeführt. Im Vordergrund des Projekts stand das Ziel zu überprüfen, inwieweit zeitnahe Erkenntnisse des Unfallablaufs die ärztliche Versorgung der verletzten Zweiradfahrer optimieren können. Bei einem entsprechenden Verkehrsunfall soll die Polizei unverzüglich ein Unfallforschungsteam bestehend aus einem Mediziner und einem technischen Sachverständigen informieren, damit diese noch an der Unfallstelle genauere Informationen über die Unfallursachen bekommen. Neben den technischen Daten mit Informationen zur Unfallursache, zum Unfallhergang und zu den Beschädigungen an den unfallbeteiligten Fahrzeugen interessieren aus medizinischer Sicht vor allem die Verletzungen der Zweiradfahrer sowie die Beschädigungen an deren Bekleidung. In einem weiteren Schritt sollen die Unfallbeteiligten von Ärzten zu den Verletzungsfolgen befragt werden.

Vor Beginn des Projekts wurde meine Dienststelle von dem damaligen Ministerium für Inneres und Europaangelegenheiten um eine datenschutzrechtliche Bewertung gebeten.

Maßgebliche rechtliche Grundlage für die Beurteilung des Forschungsvorhabens war vorliegend die Vorschrift des § 30 Saarländisches Datenschutzgesetz (SDSG).

§ 30 Datenverarbeitung zum Zweck wissenschaftlicher Forschung

(1) Öffentliche Stellen dürfen personenbezogene Daten zu wissenschaftlichen Zwecken verarbeiten, wenn die oder der Betroffene eingewilligt hat.

(2) Öffentliche Stellen dürfen personenbezogene Daten ohne Einwilligung der oder des Betroffenen für ein bestimmtes Forschungsvorhaben verarbeiten, wenn deren oder dessen schutzwürdige Belange wegen der Art der Daten und ihrer Verwendung oder wegen ihrer Offenkundigkeit nicht beeinträchtigt werden. Der Einwilligung der oder des Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

....

(7) Soweit die Vorschriften dieses Gesetzes auf die Empfängerin oder den Empfänger keine Anwendung finden, dürfen dieser oder diesem personenbezogene Daten nur übermittelt werden, wenn sie oder er sich verpflichtet, die Vorschriften der Absätze 4 bis 6 einzuhalten und sich der Kontrolle der oder des Landesbeauftragten für Datenschutz unterwirft. Die übermittelnde Stelle unterrichtet die Landesbeauftragte oder den Landesbeauftragten für Datenschutz.

Nach einer gemeinsamen Besprechung mit an dem Projekt beteiligten Polizeibeamten und Medizinern konnten bestehende Unklarheiten ausgeräumt und schließlich eine datenschutzgerechte Konzeption erreicht werden.

Da die von dem Forschungsteam an der Unfallörtlichkeit erhobenen medizinischen, biologischen sowie technischen Spuren keinen unmittelbaren Bezug zur Person des Betroffenen herstellen lassen, sofern nicht zugleich Namen, Fahrzeugkennzeichen oder ähnliche personenbezogene Daten aufgenommen werden, bestanden gegen die Erhebung dieser Spuren ohne Einwilligung des jeweils Betroffenen keine datenschutzrechtlichen Bedenken.

Die vorgesehene Übermittlung von Namen und Anschriften der bei einem Zweiradunfall verletzten Personen durch die Polizei an die am Projekt beteiligten Mediziner zum Zwecke der Kontaktaufnahme mit dem Unfallopfer konnte auf der Grundlage des § 30 Abs. 2 Satz 2 SDSG auch ohne Einwilligung der Betroffenen zugelassen werden, da der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand hätte erreicht werden können.

Dagegen bedarf die weitere Verarbeitung von personenbezogenen Daten der verletzten Zweiradfahrer durch die medizinischen Projektteilnehmer entsprechend § 30 Abs. 1 SDSG der ausdrücklichen und informierten Einwilligung der betroffenen Personen.

Die Probandeninformation, die es den betroffenen Personen ermöglichen soll, die Aufgaben und Belange des Forschungsprojekts zu verstehen und den Umfang der hierfür erforderlichen Datenerhebung zu erkennen, wurde überarbeitet. Das überarbeitete Formular setzt die Probanden in dem gebotenen Umfang über die Modalitäten des Forschungsprojekts, die Nutzung der erhobenen Daten sowie ihre Rechte im Rahmen des Projekts in Kenntnis. Auch die von dem Probanden zu unterzeichnende Einwilligungserklärung sowie das Formular über die Entbindung von der ärztlichen Schweigepflicht enthalten nunmehr die erforderlichen Informationen für die Probanden.

Um die erforderliche Trennung der Polizeiarbeit von der Forschungstätigkeit bei der Durchführung des Projekts zu gewährleisten, wurden von mir gegen das ursprüngliche Vorhaben, alle im Rahmen der Unfallforschung erhobenen Spuren der Polizei zur Verfügung zu stellen, damit diese Daten der Ermittlungsakte beigefügt werden können, Einwände erhoben. Ohne eine ausdrückliche vorherige informierte Einwilligung der betroffenen Personen ist eine solche Datenübermittlung unzulässig. Gleiches gilt auch für die zunächst beabsichtigte Übermittlung von polizeilicherseits gefertigten Unterlagen an die Forschungsstelle.

Nachdem die Landespolizeidirektion auch diesen Bedenken Rechnung getragen hatte, bestanden aus meiner Sicht keine Bedenken gegen die Durchführung dieses Forschungsprojekts.

15 Medien und Telekommunikation

15.1 Soziale Netzwerke und Facebook

Moderne digitale Kommunikationsgeräte und -medien sind heutzutage aus unserer Lebenswelt nicht mehr wegzudenken. So besitzen 2011 nach Erhebungen des Statistischen Bundesamtes etwa 75% aller Deutschen mindestens ein Mobiltelefon und ebenso viele Deutsche nutzen das Internet.

Mit immer vielfältigeren Möglichkeiten, die die digitale Welt bietet, ändert sich auch die Nutzung dieser elektronischen Medien. Insgesamt gaben nach einer Erhebung des Statistischen Bundesamtes im ersten Quartal 2009 82% der jungen Erwachsenen an, täglich im Internet zu surfen. Die 65-jährigen und älteren Internetbenutzer waren mit 57% täglich online[9]. Bis zum heutigen Tage dürfte die Anzahl der Internetnutzer nochmals angestiegen sein. Im Jahre 2011 waren 74% aller Internetnutzer in sozialen Netzwerken angemeldet und ca. 66% aller Internetnutzer auch in sozialen Netzwerken aktiv[10]. Auch diese Zahlen dürften sich im letzten Jahr nach oben hin verändert haben.

Einhergehend mit der steigenden Vernetzung, dem gestiegenen Angebot im Internet und einem sich veränderten Nutzerverhalten ist aber auch ein wachsender Verlust der Privatsphäre und Privatheit zu erkennen.

Im Folgenden soll der Bereich der sozialen Netzwerke und im speziellen Facebook näher dargestellt werden. Facebook wird hier zum Teil nur exemplarisch für alle sozialen Netzwerke angesprochen, da die genutzten Mechanismen und Techniken sowie die daraus folgenden Gefahren für den Verlust der Privatsphäre bei allen sozialen Netzwerken identisch sind.

Soziale Netzwerke stehen für eine Form von Netzgemeinschaften (Online-Communitys), die technisch durch Webanwendungen oder Portale abgebildet werden. Die bekanntesten Dienste in Deutschland sind Facebook, StayFriends, wer-kennt-wen, studiVZ, XING, meinVZ, Google+, Twitter, schülerVZ und Jappy. Das weltweit größte soziale Netzwerk mit über einer Milliarde Mitgliedern weltweit ist Facebook.

Trotz all der unbestreitbar hilfreichen und positiven Möglichkeiten in sozialen Netzwerken sollte man sich darüber bewusst sein, dass man auf Schritt und Tritt „verfolgt“ wird. Wir hinterlassen überall eine Unmenge an digitalen Spuren, die von den Anbietern der Internetangebote gesammelt und ausgewertet werden.

Der Mehrwert der Vernetzung von Menschen kann sich aber auch ins Gegenteil verkehren. Er birgt somit ein großes Risiko durch den Missbrauch der dabei anfallenden Datenbestände. So wurden noch nie

[9] Vgl. Statistisches Bundesamt „Wirtschaft und Statistik 8/2010“ im Internet zu finden unter: http://www.destatis.de/jetspeed/portal/cms/

[10] Vgl. BITKOM „Soziale Netzwerke 2. Auflage“ im Internet zu finden unter: http://www.bitkom.org/de/publikationen/38338_70897.aspx

zuvor so detaillierte und kategorisierte persönliche Daten von Nutzerinnen und Nutzern abgefragt und veröffentlich, wie dies bei den umfangreichen Nutzerprofilen der sozialen Netzwerke üblich ist. Die automatische Analyse dieser Daten und die daraus resultierende Schaffung eines Mehrwerts wurde dadurch enorm vereinfacht und das damit einhergehende Risiko für die Persönlichkeitsrechte der Nutzerinnen und Nutzer potenziert.

Die Währung mit der heute im Internet bezahlt wird, sind neben dem Verlust der Privatheit und Anonymität im Internet Daten und Personenprofile.

Im Folgenden werden zwei Thematiken näher betrachtet, die aus datenschutzrechtlicher Sicht gravierende rechtliche Mängel aufweisen.

15.1.1 „Gefällt mir"-Button

Bei Einbinden des „Gefällt mir"-Buttons in eine Webseite erlangt Facebook Kenntnis über das Aufrufen dieser Seite. Bei einem Aufruf werden – auch ohne dass der „Gefällt mir"-Button betätigt wird - personenbezogene Daten zu Facebook übermittelt. Auch ist es hierbei unerheblich, ob der Nutzer bei Facebook registriert ist oder nicht. Ist der Nutzer bei Facebook registriert, werden diese Informationen mit Hilfe eines auf dem Rechner platzierten Cookies dem Facebook-Mitglied zugeordnet. Somit ist es Facebook ebenso wie anderen sozialen Netzwerken möglich, recht genaue Bewegungsprofile von Internetnutzern zu erstellen.

Bei der Übermittlung von Daten im Internet muss das Telemediengesetz (TMG), hier der § 15 Abs. 3 TMG, beachtet werden. Darin wird festgelegt, dass der Diensteanbieter und somit der Betreiber einer Internetseite Daten der Nutzerinnen und Nutzer zum Zwecke der Profilbildung erheben darf. Dies allerdings nur in pseudonymisierter Form und mit der Möglichkeit des Widerspruchs gegen die Datenerhebung. Die Widerspruchsmöglichkeit setzt allerdings das Wissen der Nutzerinnen oder Nutzer um die Datenerhebung als solche und den Umfang der erhobenen Daten voraus. Da die Datenerhebung und Datenübermittlung alleine schon beim Webseitenaufruf ohne die Betätigung des „Gefällt mir"-Buttons erfolgt, ist eine Information des Nutzers hierüber vorab auch nicht möglich. Somit werden die rechtlichen Anforderungen nicht erfüllt und stellt das Einbinden des Gefällt mir Button ein Verstoß gegen § 15 Abs. 3 TMG dar. Von der Nutzung des „Gefällt mir"-Buttons muss daher abgesehen werden.

§ 15 Abs. 3 TMG

Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

Um die rechtskonforme Nutzung des „Gefällt mir"-Buttons zu ermöglichen, weisen wir auf die Nutzung der sog. „Zwei-Klick-Lösung" hin.

Hierbei erscheint, sobald man den Cursor über den Button bewegt ein Hinweisfenster mit Informationen über die Funktionsweise des „Gefällt mir"-Buttons. Erst wenn die Nutzerinnen oder Nutzer in der Folge den vorgeschalteten Button betätigen, erscheint der eigentliche „Gefällt mir"-Button. Allerdings muss dennoch darauf hingewiesen werden, dass eine umfängliche Information des Nutzers, die laut Gesetz erforderlich ist, kaum stattfinden kann, da von Facebook die hierzu erforderlichen Angaben über die Datenverarbeitung nicht zur Verfügung gestellt werden.

15.1.2 Fanpages bei Behörden und Unternehmen

Es ist mittlerweile festzustellen, dass kaum mehr ein Unternehmen auf die Nutzung eine Facebook-Fanpage verzichtet. Im Bereich der Behörden ist dieser Trend ebenso zu erkennen, die sich bietenden Möglichkeiten der Fanpages immer stärker zu nutzen.

Bei einer Fanpage handelt es sich um eine Webseite auf der Facebook-Plattform. Somit stehen alle Informationen, besonders aber Daten über das Nutzerverhalten, Facebook zur Verfügung und werden durch Facebook verarbeitet. Facebook erstellt aus den bei der Nutzung der Fanpages gewonnenen Daten Nutzungsstatistiken. Mit Hilfe der auf dem Computer der Nutzerinnen und Nutzer installierten Cookies, kann bei Facebook-Mitgliedern ein ausgesprochen detailliertes Nutzungsprofil erstellt werden. Dem Anbieter der Fanpage wird ein Report zur Verfügung gestellt, der Angaben wie z.B. Alter, Geschlecht und auch lokale Herkunft der Nutzerinnen und Nutzer beinhaltet. Der Dienst, der hierzu genutzt wird, heißt Facebook Insight. Darüber hinaus ist der „Gefällt mir"-Button integraler Bestandteil aller Fanpages.

Die rechtliche Grundlage, die für das Bereitstellen von Fanpages betrachtet werden muss, ist wiederum das Telemediengesetz (TMG). Wie bereits vorne beschrieben, ist für die Erstellung von Nutzerprofilen § 15 Abs. 3 TMG maßgeblich. Es muss daher eine umfassende Information über die Datenverarbeitung ebenso wie eine Widerspruchsmöglichkeit bereitgestellt werden.

2011 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sich mit der Thematik der sozialen Netzwerke befasst und die Ergebnisse in einer Entschließung zusammengefasst:

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München

„Datenschutz bei sozialen Netzwerken jetzt verwirklichen!"

Anlässlich der aktuellen Diskussionen um den Datenschutz bei sozialen Netzwerken, wie beispielsweise Facebook, stellt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass sich die Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben.

Die Konferenz stellt insbesondere fest, dass die direkte Einbindung von Social-Plugins beispielsweise von Facebook, Google+, Twitter und anderen Plattformbetreibern in die Webseiten deutscher Anbieter

ohne hinreichende Information der Internet-Nutzenden und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang steht. Die aktuelle von Social-Plugin-Anbietern vorgesehene Funktionsweise ist unzulässig, wenn bereits durch den Besuch einer Webseite und auch ohne Klick auf beispielsweise den „Gefällt-mir"-Knopf eine Übermittlung von Nutzendendaten in die USA ausgelöst wird, auch wenn die Nutzenden gar nicht bei der entsprechenden Plattform registriert sind.

Die Social-Plugins sind nur ein Beispiel dafür, wie unzureichend einige große Betreiber sozialer Plattformen den Datenschutz handhaben. So verwendet Facebook mittlerweile Gesichtserkennungs-Technik, um Bilder im Internet bestimmten Personen zuzuordnen; Betroffene können sich dem nur mit erheblichem Aufwand entziehen. Sowohl Facebook als auch Google+ verlangen, dass die Nutzenden sich identifizieren, obwohl nach deutschem Recht aus guten Gründen die Möglichkeit zumindest einer pseudonymen Nutzung solcher Dienste eröffnet werden muss.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher alle öffentlichen Stellen auf, von der Nutzung von Social-Plugins abzusehen, die den geltenden Standards nicht genügen. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Unbeschadet der rechtlichen Verantwortung sollten die öffentlichen Stellen auf solchen Plattformen keine Profilseiten oder Fanpages einrichten.

Die Obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich haben bereits 2008 und zuletzt 2010 in Beschlüssen Anforderungen an die datenschutzkonforme Gestaltung sozialer Netzwerke formuliert. Die Konferenz der Datenschutzbeauftragten fordert die Anbieter sozialer Netzwerke auf, diese Beschlüsse umzusetzen, soweit dies noch nicht geschehen ist. In diesem Zusammenhang unterstützen die Datenschutzbeauftragten Bestrebungen zur Entwicklung von technischen Lösungen zur datenschutzkonformen Gestaltung von Webangeboten.

Bedauerlicherweise hat die Bundesregierung ihrer schon im letzten Jahr gemachten Ankündigung, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Verweis darauf, dass die Diensteanbieter Selbstverpflichtungen eingehen sollten, wird dem akuten Schutzbedarf der immer zahlreicher werdenden Nutzerinnen und Nutzer nicht gerecht. Die Konferenz der Datenschutzbeauftragten unterstützt den Gesetzentwurf des Bundesrates zur Änderung des Telemediengesetzes (BT-Drs. 17/6765) als einen Schritt in die richtige Richtung.

Zurzeit informiert meine Dienststelle über die datenschutzrechtlichen Probleme im Umfeld der sozialen Netzwerke. Hierzu wurden und werden auch weiterhin vielfältige Informationsveranstaltungen durchgeführt, die die unterschiedlichsten Nutzergruppen ansprechen, auf die existierenden Gefahren hin sensibilisieren und zu einer datenschutzgerechten Nutzung von sozialen Netzwerken führen sollen.

15.2 Prüfung des Einsatzes von Google Analytics im Internetauftritt saarländischer Unternehmen

Bereits im 5. Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Saarlandes für den Berichtszeitraum 2009/2010 wurde über den Beschluss des Düsseldorfer Kreises vom 26./27. November 2009 zur datenschutzkonformen Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten berichtet.

Als Ergebnis von Verhandlungen, die der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit federführend für die Datenschutzaufsichtsbehörden in Deutschland mit der Firma Google geführt hatte, wurde der Einsatz des Google Analytics-Verfahrens derart geändert, dass ein beanstandungsfreier Betrieb möglich ist. Webseitenbetreiber haben daher folgende Anforderungen zu beachten, wenn sie Google Analytics auf ihren Seiten eingebunden haben:

- Jedem Nutzer muss die Möglichkeit des Widerspruchs gegen die Erfassung von Nutzungsdaten eingeräumt werden. Die Firma Google stellt dafür ein sog. Deaktivierungs-Add-On für den Browser zur Verfügung.

- Der Nutzer ist in einer Datenschutzerklärung über die Einbindung von Google Analytics und über die Art und Weise wie der Widerspruch gegen die Erfassung von Nutzungsdaten ausgeübt werden kann, zu unterrichten.

- Auf Anforderung des Webseitenbetreibers löscht Google innerhalb von Europa das letzte Oktett der IP-Adresse vor der systematischen Verarbeitung, so dass darüber keine Identifizierung des Nutzers mehr möglich ist. Konkret bedeutet dies, dass der Webseitenbetreiber (und nicht der Nutzer) im Programmcode auf seiner Webseite die Anonymisierung der IP-Adressen der Webseitenbesucher durch Google konfigurieren muss.

- Der Webseitenbetreiber hat einen Vertrag zur Auftragsdatenverarbeitung mit der Firma Google nach den Vorschriften des § 11 Bundesdatenschutzgesetzes abzuschließen.

Im Oktober 2012 haben wir uns dazu entschlossen, die Umsetzung der oben genannten Punkte auf Webseiten saarländischer Unternehmen zu überprüfen. Hierzu haben wir eine Prüfsoftware entwickelt, die automatisiert eine eingegebene URL auf die Verwendung von Google Analytics untersucht, indem die von der Seite initiierten Aufrufe abgefangen werden. Handelt es sich bei dem Ziel des Aufrufs um die Google-Analytics-Server wird der Datenstrom auf eine etwaige Anonymisierung hin untersucht.

Eine Überprüfung von 4.500 Webseiten saarländischer Unternehmen ergab, dass von 840 Seiten auf denen Google Analytics zum Einsatz kam, etwa 74 % nicht den Vorgaben des Düsseldorfer Kreises entsprachen.

Wir haben daraufhin alle 630 Webseitenbetreiber angeschrieben, ihnen das Ergebnis unserer Überprüfung mitgeteilt und Hilfestellung gegeben, wie die Anforderungen aus dem Beschluss des Düsseldorfer Kreises bei der Nutzung von Google Analytics erfüllt werden können. Begleitet wurde das Schreiben durch eine Informationsveranstaltung bei der IHK des Saarlandes, zu der alle interessierten Unternehmen eingeladen waren und in der wir nochmals die rechtlichen Rahmenbedingungen beim Einsatz von Reichweitenanalysetool dargelegt haben.

15.3 Veröffentlichung personenbezogener Daten auf Internetseiten

Wir hatten die Eingabe eines Bürgers zu beurteilen, der sich an uns gewendet hatte wegen der Veröffentlichung seines Namens, seiner Adresse sowie Bilder seines Baugrundstücks auf einer Webseite. Der Petent war der Schwiegersohn des Bürgermeisters einer saarländischen Gemeinde. Die Webseite beschäftigte sich mit der Frage, ob der Bürgermeister bei der Erteilung der Baugenehmigung an seinen Schwiegersohn, insbesondere im Hinblick auf Befreiung von den Festsetzungen des Bebauungsplanes, und bei der Rodung des hinter dem Baugrundstücks liegenden Stadtwaldes, sich hat von sachfremden Motiven leiten lassen.

Inhaltlich verantwortlich für die Webseite war ein Bürger der Gemeinde, der den entsprechenden Vorgang in Form einer Chronik mit Hilfe von Bildern, Berichten aus Funk und Fernsehen, Presseartikeln sowie Dokumenten und Schriftstücken dokumentierte.

Da es sich bei der Veröffentlichung von personenbezogenen Daten im Internet um eine Übermittlung durch den Webseitenbetreiber gem. § 3 Abs. 4 Nr. 3 b Bundesdatenschutzgesetz (BDSG) handelt, bedarf es dafür grundsätzlich einer datenschutzrechtlichen Erlaubnis (§ 4 Abs. 1 BDSG). Diese kann entweder in einer Einwilligung oder einer Erlaubnisnorm liegen. Eine Einwilligung des Petenten in die Veröffentlichung der personenbezogenen Daten lag hier nicht vor. Als Erlaubnisnorm kam hier lediglich § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Hiernach sind die Interessen der veröffentlichenden Stelle, insbesondere deren Recht auf Meinungsfreiheit gemäß Art. 5 Abs. 1 GG mit den schutzwürdigen Interessen des Betroffenen und dessen Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abzuwägen.

Die Veröffentlichung der Bilder und der Adresse des Baugrundstücks war hier zulässig. Unzulässig war hingegen die Veröffentlichung des Namens des Schwiegersohnes.

- Ausweislich der Startseite diente das Internetangebot der Aufarbeitung des Verwaltungshandelns des Bürgermeisters bei der Befreiung von den Festsetzungen des Bebauungsplanes und um die Maßnahmen im Stadtwald, soweit er an das Baugrundstück grenzt. Zweck der Seite war es, dass sich der Besucher ein eigenes Bild von den durch den Bürgermeister getroffenen Maßnahmen machen konnte, um dann selbst einschätzen zu können, ob sich der Verwaltungschef von sach-

fremden Erwägungen hat leiten lassen. Hierbei handelte es sich um Werturteile, die grundsätzlich von Art. 5 Abs. 1 GG gedeckt sind. Von der Meinungsäußerungsfreiheit umfasst sind aber auch Tatsachenbehauptungen, soweit sie Voraussetzung für eine bestimmte Meinung sind.

Unter Berücksichtigung dieser Kriterien stellte sich die Veröffentlichung der Adresse sowie der Bilder des Grundstücks aus datenschutzrechtlicher Sicht als zulässig dar. Die veröffentlichten Informationen sollten den Ort und Zustand des Grundstücks vor den Rodungsmaßnahmen dokumentieren, sowie die Maße des bebaubaren Bereichs im Verhältnis zur gerodeten Fläche aufzeigen und befriedigten damit ein öffentliches Informationsinteresse. Diese Informationen waren erforderlich um sich ein eigenes Bild davon machen zu können, ob das Ausmaß der angeordneten Rodungsmaßnahmen hier verhältnismäßig war, und ob die von der Stadtverwaltung als Begründung vorgebrachten Argumente nachvollziehbar sind. Hierbei war zu berücksichtigen, dass es sich lediglich um Informationen handelte, die für jedermann öffentlich wahrnehmbar waren und angesichts der politischen Auseinandersetzung musste hier das Interesse des Grundstückeigentümers zurücktreten.

- Anders beurteilten wird die Veröffentlichung des Namens des Schwiegersohnes des Bürgermeisters. Nach unserer Auffassung überwog im konkreten Fall das informationelle Selbstbestimmungsrecht des Petenten, sodass eine Namensnennung im Rahmen des oben genannten Webangebotes unzulässig war. Das Webangebot sollte lediglich das Verwaltungshandeln des Bürgermeisters kritisch beleuchten. Hierfür spielte der Name des Schwiegersohnes keine Rolle. Dem Informationsinteresse der Öffentlichkeit konnte hier auch mittels der Veröffentlichung von anonymisierten Schriftstücken entsprochen werden.

- Das Medienprivileg des § 41 Abs. 1 BDSG hielten wir im konkreten Fall für nicht anwendbar. Danach finden die Regelungen des BDSG nur eingeschränkt Anwendung, wenn es sich bei der veröffentlichenden Stelle um ein Presseunternehmen handelt, das ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken personenbezogene Daten erhebt, verarbeitet oder nutzt. Nach unserer Auffassung handelte es sich hier nicht um ein journalistisch-redaktionelles Angebot. Ein solches liegt nur vor, wenn die „meinungsbildende Wirkung für die Allgemeinheit prägender Bestandteil des Angebots und nicht nur schmückendes Beiwerk ist“[11]. Das Angebot stellte lediglich in chronologischer Reihenfolge den Vorgang in Bezug auf das Baugrundstück und die umgebende Waldfläche dar.

§ 41 Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu ei-

[11] BGH, Urteil vom 23.06.2009, Az.: VI ZR 196/08.

genen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

16 Beschäftigtendatenschutz

16.1 Beschäftigtendatenschutz im öffentlichen Bereich

16.1.1 Veröffentlichung von Personaldaten und Mitarbeiterfotos im Internet

Für viele saarländische Behörden ist es selbstverständlich, sich im Internet zu präsentieren. Dabei werden beispielsweise in Kommunen touristische Aspekte ebenso präsentiert wie das Verwaltungsangebot. In diesem Zusammenhang erreichen uns immer wieder Eingaben von Behördenbeschäftigten, deren Namen als Ansprechpartner der einzelnen Fachbereiche im Internet veröffentlicht werden. Oft werden sogar Fotos der Beschäftigten ins Netz gestellt.

Das Internet bietet vielfältige Möglichkeiten, durch einfache Suchkriterien und Verknüpfungsmöglichkeiten ein genaues Persönlichkeitsprofil auch von Behördenbeschäftigten zu konstruieren. Schnell wird die Wohnadresse oder der Verein ausfindig gemacht, in dem sich der oder die Sachbearbeiter(in) aufhalten, die einen negativen Bescheid erlassen haben. Der Presse ist hierzu immer wieder zu entnehmen, dass es zu Belästigungen und Bedrohungen gerade auch im privaten Umfeld von Behördenmitarbeiter gekommen ist.

Bei der Entscheidung, ob und wie die Beschäftigtendaten im Internetangebot einer öffentlichen Stelle veröffentlicht werden, sollte beachtet werden, dass ratsuchende Bürger zunächst darauf bedacht sind, einen kompetenten Ansprechpartner für ihr Anliegen zu erreichen. Dabei kommt es nicht darauf an, ob hier ein Herr Meyer oder eine Frau Müller am Telefon erreicht wird, sondern der für das Anliegen zuständige Sachbearbeiter. Erst nach Begründung der individuellen Kommunikation kommt die individuelle Ansprache zum Tragen.

Die Fürsorgepflicht des Dienstherrn gebietet es in jedem Fall, vor einer Veröffentlichung eine Interessenabwägung zwischen der Sicherheit der Bediensteten und einem Interesse der Öffentlichkeit an der namentlichen Nennung der Bediensteten zu treffen.

Bei Personen, deren Tätigkeit nach außen wirkt, ist die Nennung der Namen im Internetangebot im Zuge einer Interessenabwägung höher einzustufen als bei einem Hausmeister. Auch das mögliche Gefahrenpotential ist bei der Interessenabwägung zu beachten. Mitarbeiter eines Ordnungsamtes sind aufgrund ihrer Tätigkeit einem höheren Risiko ausgesetzt, Opfer von Gewalttätigkeiten zu werden als beispielsweise Mitarbeiter der Tourismuszentrale.

Die Einstellung von Mitarbeiterfotos im Internet ist aufgrund der rechtlichen Vorgaben des Rechtes am eigenen Bild, das in den § 22 und 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) fixiert wird, nur dann zulässig, wenn der Bedienstete in die Veröffentlichung der Fotografie eingewilligt hat. Die Einwilligung kann aber jederzeit durch den Betroffenen widerrufen werden.

16.1.2 Bewerbungen und Nebentätigkeitsanzeigen über den Dienstweg

Bewerbungen

In manchen saarländischen Behörden muss ein Beamter, der sich auf eine behördeninterne oder externe Stellenausschreibung bewirbt den sogenannten „Dienstweg" einhalten. Das heißt, alle unmittelbaren Vorgesetzten des Beamten müssen die Bewerbung zur Kenntnis nehmen, bis sie beim zuständigen Personalamt eingereicht werden kann. Dies hat zur Folge, dass einige Beamten befürchten, durch Bewerbungen bei ihren Vorgesetzten einen schlechten Eindruck zu hinterlassen und ihnen ihr Anliegen nach einem Arbeitsplatzwechsel zukünftig negativ ausgelegt werden kann. Genau mit diesem Anliegen hat sich ein Petent an meine Dienststelle gewandt und die Praxis der Bewerbungsvorlage über den Dienstweg datenschutzrechtlich hinterfragt.

Im Saarländischen Beamtengesetz (SBG) ist die Vorgabe „auf dem Dienstweg" lediglich für Anträge und Beschwerden des Beamten im Sinne des § 116 SBG vorgesehen. Nach Auffassung meiner Dienststelle fällt eine Bewerbung nicht unter die im § 116 SBG genannten Tatbestandsmerkmale.

Schon im Jahre 1995 war die Bewerbung auf dem Dienstweg Gegenstand datenschutzrechtlicher Überlegungen auf Bundesebene. Das Bundesministerium des Inneren teilte die Bedenken der Datenschutzbehörden und stellte fest: „Eine Bewerbung eines Beamten auf eine behördeninterne oder externe Stellenausschreibung stellt von ihrem Sinn und Zweck her keinen Antrag im Sinne der Dienstpetition dar. Vielmehr haben die Bewerbung und das der Bewerbung zugrundeliegende Ausschreibungs- und Ausleseverfahren eine eigenständige Bedeutung, die die Einhaltung des Dienstweges nicht voraussetzt."

Weiterhin führte das Bundesministerium für Inneres aus: „Die Pflicht des Beamten, seine Vorgesetzten rechtzeitig über einen von ihm angestrebten Wechsel zu unterrichten, wird dem Informationsbedürfnis des Dienstherrn voll gerecht, so dass auch aus diesem Grunde eine Vorlage der Bewerbung auf dem Dienstweg nicht erforderlich ist".

Ich habe die Petition zum Anlass genommen, alle saarländischen Ministerien auf die Unzulässigkeit der Vorlage von Bewerbungen auf dem Dienstweg hinzuweisen. Es ist ausreichend, wenn der Beamte den Vorgesetzten erst bei einer konkreten Wechselmöglichkeit über einen von ihm angestrebten Wechsel informiert.

Anzeige der Nebentätigkeiten

Eine andere Petition bezog sich auf die Vorlage der Nebentätigkeitsanzeige über den Dienstweg in einer saarländischen Kommune. Der Petent empfand es als datenschutzrechtlich nicht hinnehmbar, dass alle Vorgesetzten über seine Nebentätigkeit und die daraus resultierenden Einnahmen informiert werden, wenn die Anzeige über den Dienstweg vorgelegt werden muss.

Gemäß § 31 Absatz 1 Saarländisches Datenschutzgesetz (SDSG) ist die Verarbeitung personenbezogener Daten der Beschäftigten unter anderem dann zulässig, wenn dies zur Durchführung des Dienstverhält-

nisses oder zur Durchführung organisatorischer Maßnahmen erforderlich ist. Die Verarbeitung personenbezogener Daten beinhaltet gemäß § 3 Absatz 2 SDSG auch die Datenübermittlung und Datenerhebung.

Für organisatorische Zwecke des Personalamtes ist es unzweifelhaft erforderlich, die für eine Entscheidung zur Nebentätigkeit erforderlichen Daten beim jeweiligen Beschäftigten zu erheben. Die Erhebung der für die Entscheidung erforderlichen Daten hat gemäß § 12 Absatz 1 SDSG grundsätzlich beim Betroffenen zu erfolgen.

Dabei dürfte es regelmäßig der Fall sein, dass aus der Nebentätigkeitsanzeige der Beschäftigten alle für die Entscheidung relevante Daten ersichtlich sind. Schließlich hat der Beamte gemäß § 89 Saarländisches Beamtengesetz (SBG) die Pflicht, alle für eine Entscheidung erforderlichen Nachweise, insbesondere über Art und Umfang der Nebentätigkeit sowie die Entgelte hieraus zu führen und jede Änderung unverzüglich anzuzeigen.

Eine pauschale Weitergabe der Nebentätigkeitsanzeige auf dem Dienstweg bis hin zum zuständigen Personalamt und die damit verbundene Kenntnisnahme aller Vorgesetzten über Höhe und Art der ausgeübten Nebentätigkeit stellt aus datenschutzrechtlicher Sicht jedenfalls eine unzulässige Verarbeitung personenbezogener Daten der Beschäftigten dar, weil es in den meisten Fällen nicht erforderlich sein dürfte, dass zusätzlich zu den durch den Beschäftigten bereits bekannt gegebenen Daten auch die Stellungnahme aller Dienstvorgesetzten eingeholt werden muss.

Sollten sich im Einzelfall Tatsachen ergeben, die eine Rückfrage bei direkten Vorgesetzten der Beschäftigten erforderlich erscheinen lassen, so würde dies eine zulässige Datenerhebung im Sinne des § 12 Absatz 1 Satz 1 SDSG darstellen.

Ich habe die Kommune gebeten, von ihrer Praxis der Weitergabe der Nebentätigkeitsanzeige über den Dienstweg zum Personalamt Abstand zu nehmen und eine direkte Übermittlung der Nebentätigkeitsanzeige an das Personalamt zu verfügen.

Die Kommune kam meiner Bitte unmittelbar nach und hat das Anzeigeformular derart modifiziert, dass die Vorlage über den Dienstweg herausgenommen wurde.

16.1.3 Angabe des Arbeitgebers des Ehegatten beim Familienzuschlag

Eine Fragebogenaktion der Zentralen Besoldungs- und Versorgungsstelle (ZBS) hat im Berichtszeitraum für erhebliche Aufregung gesorgt. Etliche Beamte haben sich bei meiner Dienststelle darüber beschwert, dass sie der ZBS angeben sollten, bei welchem Arbeitgeber ihr Ehegatte beschäftigt ist. Es sei doch egal, ob der Ehepartner bei einem Discounter, an einer Frittenbude oder als Reinigungskraft arbeite, das gehe den Dienstherrn gar nichts an. Was man abfragen könne sei lediglich die Tatsache, ob der Ehepartner im öffentlichen Dienst beschäftigt sei oder nicht. Hierzu hätten zwei Kästchen zum Ankreuzen genügt.

Auf meine Anfrage hin hat mir die ZBS den Hintergrund für ihre Frage erläutert:

Den Beamten steht der Familienzuschlag nur zur Hälfte zu, wenn sein Ehegatte ebenfalls im öffentlichen Dienst steht (§ 40 Abs. 4 Bundesbesoldungsgesetz –BBesG-). Die Entscheidung, ob öffentlicher Dienst (§ 40 Abs. 6 BBesG) vorliege, sei in vielen Fällen zweifelhaft und könne von den Beamten nicht verbindlich beantwortet werden.

Nach Lektüre des § 40 Abs. 6 BBesG, in dem definiert ist, was unter öffentlichem Dienst im Zusammenhang mit der Zahlung des Familienzuschlages zu verstehen ist, konnten wir die Argumentation der ZBS nachvollziehen, dass es sich hier um eine schwierige Frage handelt, die von dem einzelnen Beamten häufig nicht verbindlich entschieden werden kann. Wir haben den Vorschlag gemacht, eine Positivliste zu entwickeln, aus der alle Arbeitgeber ersichtlich sind, die dem „öffentlicher Dienst" zuzurechnen sind und diese Liste dem Beamten zur Verfügung zu stellen. Dem wurde allerdings entgegen gehalten, dass diese Liste nie abschließend sein könne und auch nicht aktualisiert vorgehalten werden könne.

Im Ergebnis hat unsere Prüfung ergeben, dass die Abfrage des Arbeitgebers des Ehegatten zulässig ist, weil sie zur Erfüllung der Aufgaben der ZBS erforderlich ist. Die ZBS hat zugesagt, zukünftige Fragebogenaktionen im Vorfeld mit unserer Dienststelle abzustimmen. Wenn den Beamten die Hintergründe erklärt werden, können Irritationen wie in diesem Fall von vorne herein vermieden werden.

16.2 Beschäftigtendatenschutz im privaten Bereich

16.2.1 Videoüberwachung im Beschäftigungsverhältnis

Videoüberwachung am Arbeitsplatz ist allgegenwärtig. Dieser Eindruck bestätigte sich auch durch die vielen Eingaben, die wir zu dieser Thematik erhalten haben. Ob im Baugewerbe, im produzierenden Gewerbe, der Gastronomie oder im Museum, überall werden Videomaßnahmen eingesetzt, die auch zur Überwachung der Beschäftigten genutzt werden können. Die Beschäftigten bemängeln in ihren Eingaben, dass sie einem permanenten Überwachungsdruck durch ihre Vorgesetzten ausgesetzt sind und regelmäßig für Sachverhalte gerügt werden, die nur durch die Videoüberwachungsmaßnahmen bekannt geworden sein können.

So sind beispielsweise in einem Fall Bedienungskräfte vom Inhaber eines Gastronomiebetriebes angerufen worden, nachdem er sich von zu Hause aus über sein Notebook auf der Videoanlage der Gastronomie eingeloggt hat, und wurden wegen ihrer Arbeitsbekleidung angemahnt.

Aber auch die Videoüberwachung am Arbeitsplatz stellt keinen rechtsfreien Raum dar und unterliegt gesetzlichen Anforderungen, die auch durch die Gerichtsbarkeit erläutert wurden.

Zu unterscheiden ist die Videoüberwachung in öffentlich zugänglichen Räumlichkeiten sowie die Videoüberwachung am Arbeitsplatz, der nicht öffentlich zugänglich ist. Sind bei der ersten Variante die Voraussetzungen des § 6b Bundesdatenschutzgesetz (BDSG) neben den Vorschriften zu Beschäftigtendaten aus § 32 BDSG zu berücksichtigen, gelten für die zweite Variante lediglich die Vorgaben aus § 32 BDSG.

Eine Prüfung, ob eine Videoüberwachung am Arbeitsplatz aus datenschutzrechtlicher Sicht als zulässig erachtet werden kann oder nicht, kann immer erst nach Betrachtung der Fakten im Einzelfall entschieden werden. Dabei sind die Kriterien der Erforderlichkeit, Verhältnismäßigkeit und Angemessenheit zu beachten. Die Videoüberwachung am Arbeitsplatz stellt einen tiefen Eingriff in die Persönlichkeitsrechte der Betroffenen dar, da durch diese Maßnahmen ein permanenter Überwachungsdruck auf die Belegschaft ausgeübt werden kann und man Rückschlüsse auf Leistung und Verhalten der Belegschaft dokumentieren kann.

Das Bundesarbeitsgericht (BAG) hat bereits in seinem Beschluss vom 14.12.2004 unter dem Aktenzeichen 1 ABR 34/03 festgestellt, dass eine „Rund-um-die-Uhr-Überwachung" von Mitarbeitern aufgrund des schwerwiegenden Eingriffs in die Persönlichkeitsrechte der Beschäftigten unzulässig ist.

In einem weiteren Beschluss des BAG aus dem Jahre 2008 unter dem Aktenzeichen 1 ABR 16/07 wurden Vorgaben für eine Verhältnismäßigkeitsprüfung vor Einführung von Videoüberwachungsmaßnahmen am Arbeitsplatz getroffen.

In jedem Falle ist die Installation einer Videoüberwachung im Betrieb mitbestimmungspflichtig, soweit ein Betriebsrat im Unternehmen existiert. Dabei sollte die Auswertung der Videosequenzen zu Verhaltens- und Leistungskontrolle der Belegschaft ausgeschlossen werden.

16.2.2 Handbuch „Datenschutz am Arbeitsplatz" der BEST e.V.

Im August 2012 wurde das von der Beratungsstelle für sozialverträgliche Technologiegestaltung e.V. (BEST e.V.) im Auftrage der Arbeitskammer des Saarlandes erstellte Handbuch „Datenschutz am Arbeitsplatz" veröffentlicht. Es wurde als Online-Handbuch konzipiert und steht unter folgenden Links zum Download bereit: http://www.best-saarland.de oder http://www.arbeitskammer.de.

Das Handbuch gibt einen Überblick über Fragen des Datenschutzes am Arbeitsplatz und gibt kompakt Antworten. Es beschreibt darüber hinaus die Möglichkeiten der Betriebs- und Personalräte sowie Mitarbeitervertretungen, die schutzwürdigen Belange einzelner Beschäftigter abzusichern. Es zeigt Ansatzpunkte auf, wie Arbeitnehmerinnen und Arbeitnehmer das informationelle Selbstbestimmungsrecht im Arbeitsverhältnis ausüben können.

Meine Dienststelle wurde bei der Erarbeitung des Handbuches mit einbezogen. Das Handbuch spiegelt somit auch die Rechtsaufassung

meiner Dienststelle zu den aktuellen Themen im Arbeitnehmerdatenschutz wieder.

Auszug aus der Pressemitteilung der Arbeitskammer Pressedienstnummer 29-2012 vom 22.08.2012:

„Darf mein Chef wissen, mit wem ich am Arbeitsplatz telefoniere? Dürfen Kameras im Betrieb stehen? Darf mein Vorgesetzter mein Facebook-Profil durchforsten?

Antwort auf diese und andere Fragen bietet das 230 Seiten starke Handbuch "Datenschutz am Arbeitsplatz", das die Beratungsstelle BEST im Auftrag der Arbeitskammer des Saarlandes erstellt hat. Es geht gezielt und verständlich auf die wichtigsten Fragestellungen von Beschäftigten und ihre gesetzlichen Rechte ein.

Die Themen reichen von der Kameraüberwachung über den Umgang mit Krankendaten bis zur Nutzung von Smartphones und Social Media.

Das Handbuch wurde in Abstimmung mit dem Unabhängigen Datenschutzzentrum Saarland erarbeitet und berücksichtigt als einzige Veröffentlichung auch die Rechtslage der Beschäftigten im öffentlichen Dienst des Saarlandes und die Sonderregelungen der kirchlichen Einrichtungen.

"Datenschutz am Arbeitsplatz" wurde als elektronische Publikation erstellt. Eine intuitive Bedienung und die verständliche Sprache tragen dazu bei, Fragen rasch zu beantworten, ohne sich in die gesamte Problematik vertiefen zu müssen.

16.2.3 Datenschutz als rechtliches Neuland in saarländischen Unternehmen

Der Betriebsrat eines mittelständischen saarländischen Unternehmens versuchte vergebens, datenschutzrechtliche Vorgaben in die Unternehmensstruktur einzubinden. Die Unternehmensleitung sah die Umsetzung des Datenschutzes im Unternehmen als nicht erforderlich an und der betriebliche Datenschutzbeauftragte konnte aufgrund seiner hauptberuflichen Einbindung im Unternehmen die Interessen des Datenschutzes nicht entsprechend den gesetzlichen Vorgaben umsetzen. So wurden weder Verfahrensverzeichnisse geführt, noch wurden jemals Mitarbeiter über datenschutzrechtliche Vorgaben in ihrem Arbeitsumfeld informiert.

Da von Seiten der Unternehmensleitung keine Unterstützung in den Bemühungen des Betriebsrates zur Umsetzung datenschutzrechtlicher Vorgaben im Unternehmen festzustellen war, wandte sich der Betriebsrat mit seinen Anliegen an meine Dienststelle.

Die Unternehmensleitung, der Betriebsrat und der betriebliche Datenschutzbeauftragte folgten daraufhin meiner Einladung, die datenschutzrechtlichen Probleme an einem „Runden Tisch“ zu besprechen und die gesetzlichen Vorgaben zu erläutern.

Die Unternehmensleitung lenkte in Folge der Gespräche ein, bestellte zusätzlich zum internen Datenschutzbeauftragten ein externes Daten-

schutzbüro, um die bestehenden datenschutzrechtlichen Mängel im Unternehmen aufzuarbeiten, und ist mittlerweile auf dem besten Wege ein datenschutzrechtliches Vorzeigeunternehmen zu werden. Regelmäßig tauschen sich Unternehmensleitung, Datenschutzbeauftragte und Betriebsrat in einem gemeinsamen Gremium über die Fortschritte und ausstehenden Forderungen datenschutzrechtlicher Art aus. Auf Einladung des Unternehmens konnten wir uns vor Ort ein Bild über die Entwicklung des Datenschutzes im Unternehmen machen und wurden über anstehende Projekte zur Umsetzung des Datenschutzes informiert. Alle Beteiligten sind mittlerweile mit der Entwicklung und der Umsetzung des Datenschutzes im Unternehmen sehr zufrieden.

Generell ist festzustellen, dass die Umsetzung gesetzlicher Vorgaben aus dem Bundesdatenschutzgesetz in vielen saarländischen Unternehmen nicht präsent ist. Die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten sowie die mangelhafte Führung von Verfahrensverzeichnissen sind regelmäßig bei Prüfungen in saarländischen Unternehmen zu beanstanden.

16.2.4 Kopie von EC-Karte und Personalausweis bei Neueinstellungen

Ein Petent hat sich mit der Frage an meine Dienststelle gewandt, ob es zulässig sei, dass die Personalabteilung seines neuen Arbeitgebers im Zusammenhang mit der Neueinstellung eine Kopie des Personalausweises sowie eine Kopie der EC-Karte von ihm fordern darf.

Da es sich hierbei um ein Unternehmen gehandelt hat, das den Vorschriften des Bundesdatenschutzgesetzes (BDSG) unterliegt, finden die Regelungen des § 32 BDSG Anwendung. Demnach ist die Erhebung von Beschäftigtendaten zulässig, soweit diese für die Durchführung oder Eingehung des Beschäftigungsverhältnisses erforderlich sind. Regelmäßig sind die Kontaktdaten des Arbeitnehmers wie Name, Anschrift und Geburtsdatum sowie die Kontoverbindungsdaten zur Gehaltsabrechnung unabdingbar und dürfen erhoben werden.

Bei der Kopie eines Personalausweises werden aber auch Daten wie beispielsweise Augenfarbe oder Größe erhoben, die regelmäßig nicht zur Eingehung eines Beschäftigungsverhältnisses erforderlich sind. Die Prüfung, ob alle im Personalausweis enthaltenen Daten für die Eingehung und Durchführung eines Beschäftigungsverhältnisses benötigt werden, hängt vom jeweiligen Einzelfall ab.

Die Kopie des Ausweises und der EC-Karte stellt rechtlich gesehen eine Datenerhebung dar. Es ist Aufgabe der jeweiligen Personalabteilung als verantwortliche Stelle der Datenerhebung zu prüfen, welche Daten für das Arbeitsverhältnis gebraucht werden und welche nicht. Sollten auf den Kopien Daten enthalten sein, die nicht zur Durchführung oder Eingehung eines Beschäftigungsverhältnisses erforderlich sind, müssen diese entweder unkenntlich gemacht werden oder man verzichtet auf derartige Kopien.

17 Kreditwirtschaft

17.1 Angabe eines Referenzkontos bei Kontenschließung

Ein Kunde suchte seine Sparkasse auf, um sein dort geführtes Girokonto zu kündigen. Im Verlauf der abzuwickelnden Formalitäten wurde er nach seiner neuen Bankverbindung gefragt. Der Kunde war der Meinung, dass es die Sparkasse nichts angehe, bei welchem Institut er zukünftig sein Girokonto führt und verweigerte die Angabe der Bankverbindung. Daraufhin teilte man ihm mit, man könne die Kontoschließung nur durchführen, wenn er die neue Kontonummer mitteile. Das Computerprogramm würde eine Eingabe verlangen.

Meine diesbezügliche Anfrage bei der betroffenen Sparkasse ergab, dass das Abrechnungsverfahren bei Kontenauflösungen durchaus zwei Wege zulässt. Zum einen ist es möglich, im Wege des bargeldlosen Zahlungsverkehrs entsprechende Saldi mittels der neuen Bankverbindung auszugleichen. Zum anderen hat der Kunde natürlich auch die Möglichkeit, sein Konto bei Auflösung mittels Bargeld auszugleichen, falls er seine Bankverbindung nicht preisgeben möchte.

Die Sparkasse hat zugesagt, ihre Mitarbeiter nochmals über die Verfahren bei Kontoauflösung zu unterrichten.

18 Handel und Gewerbe

Kaum ein datenschutzrechtlicher Themenkomplex wirkt in der Auseinandersetzung so polarisierend wie die Videoüberwachung. Einerseits wird Videoüberwachung als ultimativer Schutz für einen in der persönlichen Wahrnehmung immer unsicherer werdenden öffentlichen Raum gerechtfertigt, andererseits als zutiefst verletzenden Eingriff in das individuelle Persönlichkeitsrecht wahrgenommen. Wie so oft ist die Wahrheit irgendwo zwischen diesen Positionen zu suchen. Es ist die nicht immer einfache Aufgabe der Aufsichtsbehörde gestützt auf die einschlägigen Vorschriften des Bundesdatenschutzgesetzes (BDSG) einen Ausgleich zwischen den berechtigten Interessen der Überwachenden und den schützwürdigen Interessen der Betroffenen zu erreichen.

18.1 Videoüberwachung im Außenbereich eines Cafés

Der Betreiber eines Cafés bat die Aufsichtsbehörde um Stellungnahme hinsichtlich der Zulässigkeit einer Videoüberwachung im überdachten Außenbereich vor der Gaststätte. Entsprechend den Ausführungen des Betreibers steht der zu überwachende Außenbereich in dessen Eigentum und wird, sofern die Wetterverhältnisse dies zulassen, für Außengastronomie genutzt. Im Übrigen waren der zu überwachende Bereich und die umgebende Verkehrsfläche aufgrund Widmung durch die Kommune zur öffentlichen Nutzung preisgegeben. Der Café-Betreiber teilte weiterhin mit, dass die Überwachung aufgrund mehrerer Einbruchsversuche und Eigentumsdelikte zu seinen Lasten notwendig sei. Die Maßnahme sollte dergestalt sein, dass der überdachte Bereich ganztätig überwacht werde.

Die Zulässigkeit dieser Videoüberwachungsmaßnahme war nach § 6b Abs. 1 BDSG zu beurteilen.

§ 6b BDSG

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. *zur Aufgabenerfüllung öffentlicher Stellen,*
2. *zur Wahrnehmung des Hausrechts oder*
3. *zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke*

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Der mithilfe der Videokameras zu überwachende Bereich stellt einen öffentlich zugänglichen Bereich im Sinne der Vorschrift dar, da dieser zu jeder Zeit uneingeschränkt von jedermann betreten werden kann. Die Tatsache, dass der Inhaber der Gaststätte nachweislich Eigentü-

mer dieses Bereichs ist, war insofern für die Beurteilung der Zulässigkeit nicht maßgebend, als dieser Bereich aufgrund der öffentlich-rechtlichen Widmung durch die Kommune für jedermann zur Nutzung offen steht.

Die geschilderten Einbruchsversuche und Diebstähle in der Gaststätte während der Öffnungszeiten sind durch den Betreiber der Gaststätte auch durch Vorlage von Unterlagen betreffend anhängiger und eingestellter staatsanwaltlicher Ermittlungsverfahren belegt worden, so dass von einer konkreten Gefährdungslage auszugehen war. Grundsätzlich kann das Ziel der Verhinderung zukünftiger Diebstähle, Sachbeschädigungen und Einbrüche und die hiermit in Verbindung stehende Sammlung von Beweismaterial, um eine Strafverfolgung und Durchsetzung zivilrechtlicher Schadensersatzansprüche zu ermöglichen, die Videoüberwachung durch den Inhaber der Gaststätte legitimieren. Jedoch ist dieses berechtigte Interesse des Cafébetreibers an dem Schutz des Eigentums mit den schutzwürdigen Interessen der von der Videoüberwachung Betroffenen, das heißt deren Recht auf informationelle Selbstbestimmung, abzuwägen. Die zu überwachende Fläche ist situationsbezogen einer unterschiedlichen Nutzung unterworfen. Sofern die Wetterverhältnisse es zulassen, wird der Bereich für gastronomische Zwecke genutzt, das heißt eine Außenbestuhlung wird aufgestellt und die Kunden können sich für einen unbestimmten Zeitraum dort niederlassen. Außerhalb der Öffnungszeiten und bei schlechtem Wetter ist der Bereich als Teil des öffentlichen Gehwegs für jedermann uneingeschränkt nutzbar.

Im Zeitraum der gastronomischen Nutzung dient der Außenbereich des Cafés vor allem der freizeitlichen Entfaltung, Kommunikation und Entspannung der Kunden. Deren Anspruch auf Persönlichkeitsentfaltung ohne einem ständigen Überwachungsdruck durch permanente Beobachtung und Aufzeichnung ausgesetzt zu sein, ist dabei besonders schützenswert und schwerwiegender als das Interesse des Inhabers an der Überwachung. Da der Bereich außerhalb der Öffnungszeiten als öffentlicher Gehweg für jedermann nutzbar ist, ist eine Videoüberwachung auch in diesem Zeitraum unzulässig. Das schutzwürdige Interesse der Passanten, sich ungezwungen in der Öffentlichkeit bewegen zu können, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung zu werden, ist höher zu gewichten als das Interesse des Inhabers an der Überwachung.

Die zivilrechtliche Rechtsprechung[12] erkennt jedoch bei Vorliegen berechtigter Interessen des Überwachenden die Miterfassung eines begrenzten, unmittelbar an das Gebäude grenzenden Bereichs öffentlicher Wege an. Unter Berücksichtigung dieser Rechtsprechung und im Hinblick auf die stattgefunden Einbruchsversuche, wäre eine Videoüberwachung begrenzt auf einen Meter ab der Hausfassade als zulässig zu erachten. Einerseits könnten durch die abschreckende Wirkung der Maßnahme weitere Einbruchs- und Diebstahlversuche vermieden werden, andererseits wäre die Videoüberwachung dazu geeignet, bei einem erneuten Versuch Beweismaterial für Zwecke der Strafverfolgung der Verursacher zu sammeln. Jedoch wären Passanten und Kunden des Cafés von der Videoüberwachung dieses begrenzten Bereichs in lediglich geringem Umfang betroffenen, da diese gegebenenfalls für einen kurzen Zeitraum beim Vorbeigehen oder Betreten

[12] Vgl. AG Berlin-Mitte, Urteil v. 18.12.2003 – 16 C 427/02.

des Cafés im Blickwinkel der Kamera wären und somit ein vergleichsweise geringer Eingriff in das informationelle Selbstbestimmungsrecht stattfindet.

Dem Betreiber der Gaststätte wurde die Zulässigkeit einer Videoüberwachung begrenzt auf den Bereich von einem Meter ab der Hausfassade kommuniziert, verbunden mit der Auflage die Notwendigkeit der Fortführung der Videoüberwachung in regelmäßigen Abständen zu evaluieren.

18.2 Videoüberwachung im Mietshaus

Eine Hausverwaltung trat an die Aufsichtsbehörde heran, mit der Bitte die Zulässigkeit einer beabsichtigten Videoüberwachungsmaßnahme im Fahrstuhl eines Mietshauses mit einer zweistelligen Anzahl an Stockwerken zu beurteilen. Nach Schilderung der Hausverwaltung kam es mehrfach zu erheblichen Verunreinigungen der Aufzugskabine, die mit Geruchsbelästigungen im ganzen Mietshaus einhergingen und zeit- und kostenintensive Wartungsarbeiten nach sich zogen.

Da es sich bei diesem Mietshaus um ein reines Wohnhaus handelt, dass aufgrund seiner Zweckbestimmung regelmäßig nur von den Bewohnern des Miethauses, deren Gästen und Besuchern sowie einer überschaubaren Anzahl weiterer Personen betreten wird, handelt es sich bei der zu überwachenden Aufzugskabine somit nicht um einen öffentlich-zugänglichen Raum im Sinne des § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG), der maßgeblich dadurch bestimmt ist, dass für diesen eine Nutzungsmöglichkeit durch eine potentiell unbegrenzte Anzahl von Personen gegeben ist.

§ 6b BDSG konnte somit für die Beurteilung der Zulässigkeit der Überwachungsmaßnahme nicht herangezogen werden, so dass die Videoüberwachung ausgehend von § 4 Abs. 1 BDSG dann zulässig ist, wenn die Betroffenen dem zustimmen oder eine gesetzliche Regelung dies ermöglicht.

§ 4 BDSG

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder einer andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Das Einholen der Einwilligung der von der Videoüberwachung Betroffenen, das sind die Mieter und Bewohner des Wohnhauses sowie eine große Anzahl weiterer Personen (Besucher, Reinigungs- und Hausmeisterdienst etc.), ist aus mehreren Gründen nicht zielführend. Zum einen ist vor dem Hintergrund der Schilderungen der Hausverwaltung, wonach nicht ausgeschlossen werden kann, dass ein Bewohner des Hauses für die Verunreinigungen verantwortlich ist, wahrscheinlich, dass nicht alle Bewohner der Maßnahme zustimmen. Zum anderen kann, selbst wenn alle Betroffenen der Überwachung zu-

stimmen, die Einwilligung jederzeit widerrufen werden, wodurch die weitere Videoüberwachung unzulässig wird und einzustellen ist.[13]

Somit könnte die Videoüberwachung in der Aufzugskabine nur noch zulässig sein, wenn eine gesetzliche Regelung dies erlaubt. Nach Auffassung der Datenschutzaufsichtsbehörden, kann eine Videoüberwachungsmaßnahme auch auf Grundlage von § 28 Abs. 1 BDSG legitimiert sein.

§ 28 BDSG

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig,

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt,

...

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

Da die Videoüberwachung nicht zur Begründung, Durchführung oder Beendigung des Mietverhältnisses erforderlich ist, kann die Beurteilung der Zulässigkeit nur nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG erfolgen. Danach ist die Verarbeitung personenbezogener Daten mithilfe der Videoüberwachung gerechtfertigt, soweit sie zur Wahrung berechtigter Interessen der Eigentümer erforderlich ist und das schutzwürdige Interesse der betroffenen Hausbewohner am Ausschluss der Verarbeitung nicht überwiegt.

Die Videoüberwachung in einer Fahrstuhlkabine stellt aus mehreren Gründen einen sehr intensiven Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar. Die Überwachung von Bereichen, die von den Bewohnern regelmäßig betreten und durchquert werden müssen, um die eigene Wohnung zu erreichen und die damit im unmittelbaren räumlichen Umfeld von grundsätzlich höchstpersönlichen Bereichen der Privatsphäre anzusiedeln sind, sind besonders kritisch zu hinterfragen. Gerade Bewohner höher liegender Stockwerke sind regelmäßig auf die Nutzung des Fahrstuhls angewiesen und können sich somit der Überwachung nicht entziehen. Darüber hinaus ist durch die räumliche Enge im Fahrstuhl und die geringe Distanz zwischen Objekt und Objektiv die Datenerhebung sehr detailliert und der damit verbundene Überwachungsdruck besonders groß.

Damit berechtigte Interessen der Eigentümer vor in diesem Zusammenhang besonders schutzwürdigen Interessen der Betroffenen überwiegen, muss grundsätzlich eine Verletzung hochrangiger Rechtsgüter vorliegen oder nachweisbar drohen. Dies ist dann der

[13] Siehe dazu auch die Entscheidung des LG Berlin vom 23.05.2005, 62 S 37/05.

Fall, wenn belegbare Gefahren für Leib und Leben der Bewohner bestehen oder Beeinträchtigungen des unmittelbaren Wohnbereichs gegeben sind. Einfache Sachbeschädigungen sind nicht ausreichend um eine Videoüberwachung zu rechtfertigen.

Jedoch könnte auch die Summierung besonderer Umstände zu einem Überwiegen der Eigentümerinteressen führen. Aufgrund häufiger und längerfristiger Ausfälle des Fahrstuhls verbunden mit kostenintensiven Instandsetzungsmaßnahmen sowie eines im Einzelfall besonderen Angewiesenseins auf die Funktionsfähigkeit des Aufzugs, kann man im Rahmen der Abwägung durchaus zu dem Ergebnis gelangen, dass eine Videoüberwachung in begrenztem Umfang zulässig sein könnte. Die Hausverwaltung wurde daher gebeten, den Umfang der Schäden und die damit verbundenen Kosten sowie die Anzahl der Zwischenfälle darzulegen. Weiterhin war für die Gesamtbeurteilung relevant, ob Mieter aufgrund des Nutzungsausfalls des Fahrstuhls oder etwaiger Geruchsbelästigungen die Miete minderten oder gar das Mietverhältnis kündigten beziehungsweise dies androhten. Anscheinend wurde jedoch das Vorhaben von der Hausverwaltung nicht weiterverfolgt, da keine weiteren Stellungnahmen mehr zu verzeichnen waren.

Zusammenfassend sollten folgende Punkte von Vermietern und Hausverwaltungen, die einen Einsatz von Videoüberwachungsmaßnahmen innerhalb reiner Wohnhäuser in Betracht ziehen, bedacht werden:

Einfache Sachbeschädigungen sind nicht ausreichend um in der nach § 28 Abs. 1 Satz Nr. 2 BDSG gebotenen Abwägung zwischen den berechtigten Interessen des Eigentümers und den schutzwürdigen Interessen der Betroffenen zu einem Überwiegen der berechtigten Interessen zu gelangen. Vielmehr muss die Verletzung hochrangiger Rechtsgüter vorliegen oder nachweisbar drohen.

Da Betroffene auch über den Zivilrechtsweg Abwehrrechte[14] hinsichtlich einer Videoüberwachungsmaßnahme geltend machen können, bleibt zu bemerken, dass sich mittlerweile eine überwiegend betroffenenfreundliche Rechtsprechung etabliert hat.

Ferner gilt zu beachten, dass eine unzulässige Videoüberwachung ggf. als Einschränkung der Gebrauchstauglichkeit der Mietsache[15] angesehen werden kann und eine dementsprechende Geltendmachung von Mängelrechten oder gar Schadensersatzansprüchen zur Folge haben könnte.

18.3 Videoüberwachung in Taxis

Aufgrund der Berichterstattung einer regionalen Tageszeitung wurde die Aufsichtsbehörde darauf aufmerksam, dass in Fahrzeugen saarländischer Taxiunternehmen Videokameras im Einsatz befindlich sind.

Da das Thema bereits zu einem früheren Zeitpunkt von verschiedenen Aufsichtsbehörden anderer Bundesländer aufgegriffen wurde und die Interessen des Taxigewerbes in der Auseinandersetzung von den je-

[14] §§ 823, 1004 BGB
[15] §§ 535 ff BGB

weiligen Landesverbänden vertreten wurden, wurde der für das Taxigewerbe zuständige Landesverband Verkehrsgewerbe Saarland (LVS) um Mitteilung gebeten, ob den angeschlossenen Taxiunternehmen verbandsseitig eine Position zu diesem Thema kommuniziert worden ist. Laut Stellungnahme des LVS hatte sich dieser bis zu diesem Zeitpunkt nicht mit der Videoüberwachung in Taxis auseinandergesetzt, bot jedoch umgehend an, dieses Thema bei der anstehenden Mitgliederversammlung auf die Tagesordnung zu nehmen.

Vor diesem Hintergrund wurden seitens der Aufsichtsbehörde stichprobenartig saarländische Taxiunternehmen hinsichtlich einer im Einsatz befindlichen oder geplanten Videoüberwachung um Stellungnahme gebeten. Nach dem Ergebnis der Befragung hatte lediglich ein einziges Unternehmen Kameras in den Fahrzeugen angebracht. Noch bevor die Zielsetzung und technische Ausgestaltung der Videoüberwachungsmaßnahme durch die Aufsichtsbehörde ermittelt werden konnte, teilte das Unternehmen mit, dass die Kameras deinstalliert werden.

Im Hinblick darauf, dass sich mehrere Aufsichtsbehörden bereits mit der Fragestellung nach der Zulässigkeit der Videoüberwachung in und auch an Taxis auseinandergesetzt haben, wurde der Sachverhalt zudem im Düsseldorfer Kreis, als gemeinsames Beratungsgremium der Landesaufsichtsbehörden im Bereich des Datenschutzes, diskutiert.

Zur Gewährleistung einer einheitlichen Rechtsauslegung wurde auf der Sitzung des Düsseldorfer Kreises am 26./27. Februar 2013 folgender Beschluss gefasst:

Videoüberwachung in und an Taxis

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

Die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen bestimmt sich nach § 6b Bundesdatenschutzgesetz (BDSG). Gemäß § 6b Abs. 1 Nr. 3, Abs. 3 BDSG ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

1. Innenkameras

Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines „stillen Alarms" oder eines GPS-gestützten Notrufsignals.

Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbsttätig (z.B. über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6b Abs. 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

2. Außenkameras

Die Voraussetzungen des § 6b Abs. 1, Abs. 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum – etwa zwecks vorsorglicher Beweis sichernder Dokumentation für den Fall eines Schadensereignisses – einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kameras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird.

Die Ausstattung von Taxis mit "Unfallkameras", wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig. Die Taxiunternehmen müssen sich darüber im Klaren sein, dass nicht das Versicherungsunternehmen, sondern sie selbst in der datenschutzrechtlichen Verantwortlichkeit stehen.

18.4 Anzeigetafeln im Autohaus als datenschutzrechtliches Problem

Es scheint mittlerweile ein weit verbreitetes Phänomen zu sein, dass Autohäuser ihre Kunden zu vereinbarten Werkstattterminen mit elektronischen oder analogen Anzeigetafeln willkommen heißen. Dies ist vor dem Hintergrund einer möglichst individuellen Kundenorientierung durchaus nachvollziehbar, jedoch sind im Einzelfall bei der Umsetzung dieser Maßnahme datenschutzrechtliche Belange zu beachten.

In einem Autohaus wurde eine Kundin zu ihrem Werkstatttermin durch eine Anzeigetafel, die die Nachnamen aller Kunden des Tages und die Uhrzeit der Termine permanent auflistete, begrüßt. Da die Petentin mit dieser Veröffentlichung ihres Namens und der damit verbundenen Kenntnisnahme dieses personenbezogenen Datums durch andere Kunden und Besucher des Autohauses nicht einverstanden war, bat sie die Aufsichtsbehörde um Überprüfung des Sachverhalts.

Bei dieser öffentlichen Auflistung von Kundennamen handelt es sich um eine Übermittlung des personenbezogenen Datums „Nachname" an Dritte, die nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) nur zulässig ist, wenn sie aufgrund einer gesetzlichen Regelung erfolgt oder wenn der von der Datenverarbeitung Betroffene dem zustimmt.

§ 4 BDSG

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder einer andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Der Stellungnahme des Autohauses konnte entnommen werden, dass hierbei eine Handlungsempfehlung des Automobilherstellers, für den das Autohaus als Vertriebspartner tätig ist, umgesetzt wird. Neben der eigentlichen Begrüßung des Kunden soll diese Maßnahme dem Kunden signalisieren, dass man ihn bereits erwarte und dass das zur Erledigung des Termins Erforderliche durch das Autohaus bereits in die Wege geleitet wurde. Vom Automobilhersteller wurde es dem jeweiligen Vertriebspartner selbst überlassen, ob die Handlungsempfehlung nunmehr mittels Begrüßungsbildschirm oder einfacher Hinweistafel umgesetzt wird, wobei die Kundendaten aus einem standardisierten und allen angeschlossenen Autohäusern zugänglichen Datenverarbeitungssystem entnommen werden.

Da außerhalb des Bundesdatenschutzgesetzes eine gesetzliche Grundlage für die Übermittlung nicht gegeben ist und eine Zustimmung des Kunden vorab nicht eingeholt wurde, kann die Übermittlung nur nach § 28 Abs. 1 BDSG zulässig sein.

§ 28 BDSG

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig,

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

Da die Übermittlung nicht zur Begründung, Durchführung oder Beendigung eines zwischen Kunde und Werkstatt vorliegenden vertraglichen Verhältnisses erforderlich ist, ist die Zulässigkeit nicht nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG, sondern nach Nr. 2 zu beurteilen. Danach ist die Übermittlung gerechtfertigt, soweit sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung nicht überwiegt.

Im Rahmen der Vorschrift war nun eine Abwägung hinsichtlich des berechtigten Interesses des Autohauses an einem individualisierten Willkommenheißen des Kunden und dem Interesse des Betroffenen an der Wahrung seines informationellen Selbstbestimmungsrechts zu treffen. Zwar wurde durch das Autohaus lediglich das personenbezogene Datum „Nachname" des jeweiligen Kunden inklusive der geschlechtsspezifischen Anrede öffentlich aufgelistet, jedoch war dies während der gesamten Öffnungszeit für eine unbestimmte Anzahl weiterer Kunden und Besucher des Autohauses wahrnehmbar. Somit war ein Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Kunden feststellbar. Das Ziel der individuellen Kundenbegrüßung hätte durch das Autohaus auch ohne Eingriff in das informationelle Selbstbestimmungsrecht erreicht werden können, indem bei der Vereinbarung des Werkstatttermins mit dem Kunden ein individuelles Kennzeichen vereinbart worden wäre, das dem betroffenen Kunden beim Betreten des Autohauses auf gleiche Art und Weise wie die Nennung des Nachnamens signalisiert, dass er erwartet wird.

Die öffentliche Auflistung des Nachnamens ist somit nicht erforderlich im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG, weshalb die Übermittlung desselben nicht auf die Vorschrift gestützt werden konnte.

Diese Auffassung wurde dem Autohaus mitgeteilt, verbunden mit der Vorgabe, zukünftig zum Zeitpunkt der Terminvereinbarung entweder ein kundenindividuelles Kennzeichen zu vereinbaren oder die Einwilligung der Kunden zur Namensnennung zum Zeitpunkt der Terminabsprache einzuholen.

18.5 Finderprämie und Kundendaten

Wie sich an nachfolgendem Sachverhalt zeigen lässt, führt oftmals lediglich mangelnde Transparenz bezüglich der Zwecke der Erhebung personenbezogener Daten durch verantwortliche Stellen dazu, dass sich Bürgerinnen und Bürger an die Aufsichtsbehörde wenden.

Eine Einzelhandelskette bietet Kunden, die Lebensmittel mit abgelaufenem Mindesthaltbarkeitsdatum in den Auslagen auffinden, für jedes aufgefundene Produkt eine Finderprämie an. Da eine Kundin seitens der Service-Mitarbeiter keine ausreichende Auskunft darüber erhalten hat, für welche Zwecke Name und Anschrift des Finders festgehalten werden, bat sie die Aufsichtsbehörde um Klärung des Sachverhalts.

Nach einer ersten Stellungnahme des Einzelhändlers erfolge die Erhebung der Kundendaten aufgrund der steuergesetzlichen Verpflichtung zur ordnungsgemäßen Buchführung und sei im Übrigen auf das berechtigte Interesse zu stützen, systematische Manipulationen durch einzelne Kunden, wie zum Beispiel das Verstecken und Umlagern von Waren bis zum Ablauf des Mindesthaltbarkeitsdatums, zu vermeiden.

Diese erste Stellungnahme war für die Beurteilung, ob diese Erhebung und -speicherung von Kundendaten datenschutzrechtlich zulässig ist, nicht ausreichend. Die Angabe, dass die Erhebung und Speicherung allein auf Grundlage der ordnungsgemäßen Buchführung erfolgt[16], war insofern kritisch zu hinterfragen, als zwar für jeden Zahlvorgang ein Beleg zu erstellen wäre, diese Auszahlung aber aufgrund der vergleichsweise geringen Höhe des Zahlbetrags nicht zwangsläufig personenbezogen, sondern auch anonymisiert dokumentiert werden kann. Im Einzelhandel ist es schließlich auch nicht erforderlich, dass personenbezogene Daten des Kunden durch den Einzelhändler erhoben werden, wenn der Kunde Waren des täglichen Bedarfs im Rahmen eines Bargeschäfts einkauft. Auch das angeführte berechtigte Interesse, Manipulationen und somit das missbräuchliche Erschleichen von Zahlungen zu vermeiden, konnte ohne weitere Ausführungen des Einzelhändlers nicht bejaht werden.

Aufgrund einer weiteren Stellungnahme des Einzelhändlers konnte festgestellt werden, dass die Datenerhebung und –speicherung auf § 160 Abgabenordnung (AO) gestützt werden kann. Die Finderprämie wird steuerrechtlich wie eine Betriebsausgabe behandelt, so dass zur Erreichung der Abzugsfähigkeit von dem steuerpflichtigen Einzelhändler auf Verlangen der Finanzbehörde der Nachweis über den Zahlungsempfänger zu führen ist. Die Erhebung und Speicherung der Kundendaten erfolgte auf einer steuergesetzlichen Grundlage und war somit gemäß § 4 Abs. 1 BDSG zulässig.

Abschließend wurde dem Einzelhändler seitens der Aufsichtsbehörde mitgeteilt, dass ungeachtet der Zulässigkeit der Datenerhebung die nach § 4 Abs. 3 BDSG notwendige Transparenz bezüglich des Datenumgangs herzustellen ist.

[16] § 146 Abs. 1 AO, § 239 Abs. 2 HGB

§ 4 BDSG

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,

2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und

3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

Der Einzelhändler erstellte daraufhin entsprechende Informationsblätter, die den Kunden den Zweck der Datenerhebung und –speicherung verdeutlichen.

18.6 Datenschutzkonformer Umgang mit Personalausweisen

Zum 01.11.2010 ist der neue Personalausweis eingeführt worden. Dieser hat neben der hoheitlichen Ausweisfunktion auch die Möglichkeit zur Signatur und zur Authentisierung erhalten.

Der Umgang mit diesem neuen Identitätsdokument wirft in der Praxis zahlreiche Fragen auf, die immer wieder zu Eingaben von Bürgerinnen und Bürgern und Anfragen von Unternehmen bei der Aufsichtsbehörde führen. Überwiegend geht es um die Fragestellung, unter welchen Voraussetzungen die Anfertigung einer Personalausweiskopie durch Unternehmen zulässig ist bzw. welche Daten des Personalausweises von diesen gespeichert werden dürfen.

Deutsche Staatsbürger, die das 16. Lebensjahr vollendet haben, sind nach § 1 Abs. 1 Personalausweisgesetz (PAuswG) zum Besitz eines Personalausweises und zu dessen Vorlage gegenüber berechtigten Behörden für den Zweck der Identitätsfeststellung verpflichtet. Der Personalausweis kann jedoch nach dem PAuswG vom Inhaber auch im privaten Rechtsverkehr als Identitätsnachweis und Legitimationspapier genutzt werden.[17] Im privatrechtlichen Verwendungskontext ist die Forderung nach der Vorlage des Personalausweises dann als unproblematisch anzusehen, wenn die Feststellung der Identität einer

[17] § 18 Abs. 1 und § 20 Abs. 1 PAuswG

Person vor Eingehung einer vertraglichen Vereinbarung erforderlich oder gar gesetzlich vorgeschrieben ist.

Gesetzlich eindeutig geregelt ist in § 1 Abs. 1 S. 3 PAuswG auch, dass vom Ausweisinhaber nicht verlangt werden darf, den Personalausweis zu als Pfand zu hinterlegen oder in sonstiger Weise den Gewahrsam hieran aufzugeben.

Schwierigkeiten tauchen immer wieder bei der Frage auf, ob eine Vervielfältigung des Personalausweises durch Kopieren oder Scannen zulässig ist. Ein ausdrückliches Fotokopierverbot lässt sich weder dem PAuswG noch sonstigen gesetzlichen Regelungen entnehmen.

Grundsätzlich zulässig ist die Vervielfältigung des Personalausweises jedenfalls dann, wenn eine Rechtsvorschrift ausdrücklich dazu berechtigt. Der Gesetzgeber hat solche Regelungen bisher lediglich im Geldwäschegesetz (GWG) und im Telekommunikationsgesetz (TKG) getroffen. Nach § 8 Abs. 1 Satz 3 GWG und § 95 Abs. 4 Satz 2 TKG sind die zur Identifizierung des Kunden angehaltenen Kreditinstitute und Finanzdienstleister sowie Telekommunikationsanbieter dazu berechtigt, Ausweiskopien zu erstellen.[18] Gegen den erklärten Willen des Kunden ist dies jedoch ausschließlich dem Telekommunikationsanbieter gestattet.

Neben den gesetzlich geregelten Erlaubnistatbeständen ist das Anfertigen einer Personalausweiskopie dann als zulässig zu erachten, wenn dies im Einzelfall erforderlich ist. Diese Erforderlichkeit kann im Rahmen der Geltendmachung eines Selbstauskunftsanspruchs nach § 34 Bundesdatenschutzgesetz (BDSG) über die bei einer verantwortlichen Stelle gespeicherten personenbezogenen Daten eines Betroffenen gegeben sein. Stellt zum Beispiel eine um Auskunft ersuchte Stelle eine Diskrepanz zwischen den Angaben des Antragstellers und den gespeicherten Daten fest und bestehen somit berechtigte Zweifel an der Identität des Antragstellers, kann die Anforderung einer Ausweiskopie zulässig sein.

Darüber hinaus sollten Kunden jedoch der Anforderung einer Ausweiskopie durch Unternehmen regelmäßig kritisch begegnen. Kann im Einzelfall die Erforderlichkeit zur Anfertigung einer Ausweiskopie bejaht werden, ist darauf zu achten, dass auf der möglichst vom Ausweisinhaber selbst anzufertigenden Kopie lediglich die für den konkreten Identifikationszweck notwendigen Daten erkennbar sind und die verbliebenen Angaben, hier insbesondere Serien- und Zugangsnummer[19] sowie das Bild, unkenntlich gemacht werden. Die Ausweiskopie ist nach erfolgter Identifikation von dem jeweiligen Unternehmen umgehend zu vernichten.

---

[18] Bezüglich der Zulässigkeit von Personalausweiskopien im Bankwesen, siehe 19.6.2

[19] Die Zugangsnummer ist ein im Rahmen der Online-Ausweisfunktion notwendiges Merkmal des neuen Personalausweises und sollte nur dem Ausweisinhaber bekannt sein.

18.6.1 Unzulässige Erhebung der Seriennummer aus dem Personalausweis

Eine Petentin teilte der Aufsichtsbehörde mit, dass von einem Großhandelsunternehmen zur Ausstellung von Tageskundenausweisen neben Name und Anschrift der Kunden auch die Seriennummer des Personalausweises erhoben wird. Der Stellungnahme des verantwortlichen Unternehmens war zu entnehmen, dass die Einsichtnahme in den Personalausweis sowie die Erhebung des Namens, der Anschrift des Kunden und der Seriennummer des Ausweises aufgrund steuerrechtlicher Vorschriften erfolge. Die Erhebung und Speicherung des Namens und der Anschrift der Kunden aus dem vorgelegten Personalausweis war auf Grundlage der genannten steuerrechtlichen Vorschriften erforderlich und somit nicht zu beanstanden. [20] Da im Rahmen der steuerrechtlichten Identifikations- und Nachweiszwecke eine Erhebung der Seriennummer gesetzlich nicht vorgesehen war und darüber hinaus auch keine legitimen Gründe dafür angeführt werden konnten, war diese, auch im Hinblick auf das Gebot der Datensparsamkeit nach § 3a BDSG, als unzulässig zu beurteilen.

§ 3a BDSG

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Weiterhin untersagt der Gesetzgeber durch § 20 Abs. 3 PAuswG ausdrücklich eine Verwendung der Seriennummer zum automatisierten Abruf personenbezogener Daten oder zur Verknüpfung von Dateien.

§ 20 PAuswG

(3) Die Seriennummern, die Sperrkennwörter und die Sperrmerkmale dürfen nicht so verwendet werden, dass mit ihrer Hilfe ein automatisierter Abruf personenbezogener Daten oder eine Verknüpfung von Dateien möglich ist. Dies gilt nicht für den Abgleich von Sperrmerkmalen durch Diensteanbieter zum Zweck der Überprüfung, ob ein elektronischer Identitätsnachweis gesperrt ist.

Dementsprechend wäre eine Nutzung der Seriennummer als eigenes Ordnungsmerkmal für die beim Handelsunternehmen gespeicherten Kundendaten unzulässig und bußgeldbewehrt.[21] Aufgrund der abschließenden Stellungnahme der Aufsichtsbehörde bestätigte das betroffene Unternehmen, dass die unzulässigerweise erhobenen Seriennummern gelöscht wurden und zukünftig auf deren Erhebung verzichtet wird.

[20] § 144 Abs. 3 AO
[21] § 32 Abs. 1 Nr. 8 PAuswG

18.6.2 Zulässigkeit der Personalausweiskopie bei Eröffnung eines Girokontos

Ein Petent bat die Aufsichtsbehörde um Mitteilung, ob ein Kreditinstitut bei der Eröffnung eines weiteren Girokontos auch dann eine Kopie des Personalausweises anfertigen darf, wenn der Ausweisinhaber bereits Kunde der Bank und Inhaber eines Girokontos ist. Grundsätzlich hat das Kreditinstitut nach den Vorschriften des Geldwäschegesetzes die Identität des Vertragspartners festzustellen und die zur Identifizierung notwendigen Angaben Name, Geburtsort, Geburtsdatum, Staatsangehörigkeit und Anschrift aufzuzeichnen.[22] Diese zur Identifizierung des Vertragspartners notwendigen und aufzuzeichnenden Angaben sind durch Vorlage eines gültigen Ausweisdokumentes zu bestätigen und um die Seriennummer und die ausstellende Behörde des Ausweisdokuments zu ergänzen.[23] Das Kreditinstitut kann darüber hinaus eine Kopie des Ausweisdokuments anfertigen[24], sofern der Kunde dem zustimmt.

Von einer erneuten Erhebung dieser Daten kann abgesehen werden, wenn der Kunde bereits bei früherer Gelegenheit, so zum Beispiel bei einer früheren Eröffnung eines Girokontos, von dem Kreditinstitut identifiziert und die Angaben zum Kunden erfasst wurden, es sei denn, für das Kreditinstitut ergeben sich Zweifel an der Gültigkeit der bei früherer Gelegenheit aufgezeichneten Angaben.[25]

Dem Petenten wurde unter Bezugnahme auf die Vorschriften des GWG mitgeteilt, dass die Anfertigung einer Personalausweiskopie durch das Kreditinstitut von seiner Einwilligung abhängig zu machen ist und die erneute Erhebung seiner Kundendaten im Hinblick auf das bereits existierende Girokonto bei derselben Bank nicht zwangsläufig notwendig sein muss.

18.6.3 Personalausweiskopie im Online-Handel

Ein im Saarland ansässiger Online-Händler forderte zur Abwicklung von Bestellungen ab einem bestimmten Warenwert die Kunden zur Übersendung einer Personalausweiskopie auf. Ein Kunde bat die Aufsichtsbehörde um Überprüfung dieser Vorgehensweise. Seitens des Online-Händlers wurde die Anforderung der Personalausweiskopie damit begründet, dass in der Vergangenheit Bestellungen mit hohem Warenwert mit gestohlenen Kreditkarten getätigt wurden und zukünftig durch die Anforderung von Ausweiskopien bei Bestellungen mit einem bestimmten Warenwert der jeweilige Kunde eindeutig identifiziert werden solle. Die Personalausweiskopie würde nach erfolgter Identifizierung durch den Händler umgehend vernichtet und, unter Vorwegnahme zukünftiger Bestellungen, lediglich vermerkt, dass sich der Kunde mit einem amtlichen Dokument ausgewiesen hat. Kommt der Kunde dem nicht nach, wird die Bestellung durch den Händler storniert.

[22] § 4 Abs. 1 und 3 GWG, § 8 Abs. 1 Satz 1 GWG
[23] § 4 Abs. 4 Satz 1 Nr. 1 GWG, § 8 Abs. 1 Satz 2 GWG
[24] § 8 Abs. 1 Satz 3 GWG
[25] § 4 Abs. 2 GWG

Die Notwendigkeit zur Verifizierung von Kundendaten ist vor dem Hintergrund drohender Zahlungsstörungen und -ausfälle zu Lasten des Händlers bei Bestellungen in betrügerischer Absicht unstrittig gegeben, jedoch ist die abhängig von einem bestimmten Bestellwert erfolgende Verifizierung anhand einer übersandten Ausweiskopie weder zielführend noch datenschutzkonform.

Um im Fernabsatzhandel die Wahrscheinlichkeit einer nachträglichen Rückbelastung einer Kreditkartentransaktion aufgrund einer nicht durch den Karteninhaber autorisierten Verfügung, sogenannte Chargebacks, zu minimieren, stehen dem Online-Händler verschiedene Prozesse zur Identifizierung des Kunden und der Authentifizierung der Kreditkartendaten zur Verfügung. Zu nennen sind beispielsweise Verfahren wie eine vergleichende Abfrage der Kreditkartenprüfziffer (CVC2, CVV2 CID), das 3-D Secure-Protokoll, welches zur Authentifizierung die Eingabe eines kundenspezifischen Passworts erforderlich macht, der in Deutschland kaum gebräuchliche Adress-Verification-Service und die Identifizierung mittels der Online-Ausweisfunktion des neuen Personalausweises.[26] Zwar ist auch mit Einsatz derartiger, zudem teilweise für den Händler kostenpflichtiger Verfahren kein vollkommener Schutz vor betrügerischen Bestellungen gewährleistet, jedoch wird durch die Anforderung einer Ausweiskopie durch den Händler in keiner Weise garantiert, dass eventuelle betrügerische Absichten entlarvt werden können, wenn schließlich eine fingierte Ausweiskopie übermittelt wird. Darüber hinaus ist davon auszugehen, dass sich auch redliche Kunden in der Erwartung an die schnelle Abwicklung des Bestellvorgangs durch die Aufforderung zur Übersendung einer Ausweiskopie veranlasst sehen, diesen abzubrechen und einen anderen Online-Shop zu suchen.

Weiterhin wurde seitens des Händlers eine Kopie des Ausweises angefordert, ohne auf die Schwärzung der für die Identifizierung nicht notwendigen personenbezogenen Daten im Ausweis hinzuweisen, so dass für die Abwicklung der Bestellung nicht notwendige personenbezogene Daten erhoben wurden.

Da eine Anforderung von Ausweiskopien zur Identifizierung des Kunden und der Authentifizierung der Kreditkartendaten im Hinblick auf die zur Verfügung stehenden Identifikations- und Authentifizierungsprozesse regelmäßig nicht erforderlich ist und Bestellungen mit einem hohen Warenwert schließlich auch über den sicheren Zahlungsweg Vorkasse abgewickelt werden können, wurde der Online-Händler abschließend aufgefordert, keine Ausweiskopien mehr anzufordern.

[26] Vgl. www.personalausweisportal.de

19 Versicherungen

19.1 Bußgeld gegen selbstständigen Versicherungsmakler

Im Berichtszeitraum sind zwei Bußgeldbescheide gegen einen selbstständigen Versicherungsmakler in Höhe von jeweils 250 Euro rechtskräftig geworden. Der zu Grunde liegende Sachverhalt geht zwar schon in das Jahr 2010 zurück, allerdings hatte der Betroffene damals Rechtsmittel eingelegt.

Hintergrund beider Bußgeldverfahren waren die Beschwerden von Bürgern, wonach Mitarbeiter des Versicherungsbüros junge Familien mit kleinen Kindern aufgesucht hatten, um Versicherungen für die Kinder abzuschließen. Auf die Frage der Familien nach Herkunft der personenbezogenen Daten reagierten die Mitarbeiter des Versicherungsbüros ausweichend bzw. verwiesen auf die Auskunft durch Personen am jeweiligen Wohnort der Petenten.

Aus datenschutzrechtlicher Sicht ist hierzu Folgendes festzustellen: Nach § 28 Abs. 4 Satz 2 Bundesdatenschutzgesetz (BDSG) ist der Betroffene bei der Ansprache zum Zwecke der Werbung oder der Markt- oder Meinungsforschung über das Widerspruchsrecht zu unterrichten. Soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Nach § 43 Abs. 1 Nr. 3 BDSG handelt ordnungswidrig, wer nicht sicherstellt, dass der Betroffene Kenntnis über die Herkunft der ihn betreffenden Daten erhalten kann. Die Ordnungswidrigkeit konnte in der zu diesem Zeitpunkt geltenden Fassung des § 43 BDSG mit einer Geldbuße bis zu 25.000 Euro (heute 50.0000 Euro) geahndet werden.

Was die Erhebung von personenbezogenen Daten der Familien bzw. deren Kinder bei bekannten Personen im örtlichen Umfeld durch die Mitarbeiter des Versicherungsbüros angeht, liegt auch ein Verstoß gegen § 4 Abs. 2 BDSG vor, wonach personenbezogene Daten grundsätzlich beim Betroffenen zu erheben sind. Ausnahmen hiervon sind nur zulässig, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt, die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde. Im vorliegenden Fall greift jedoch keiner dieser Ausnahmetatbestände, so dass es sich um eine unbefugte Erhebung personenbezogener Daten, die nicht allgemein zugänglich sind, handelt, die gemäß § 43 Abs. 2 Nr. 1 BDSG ebenfalls bußgeldbewehrt ist.

19.2 Zentralruf der Autoversicherer

Eine durch einen Kfz-Unfall geschädigte Petentin erkundigte sich bei der Aufsichtsbehörde, ob es rechtens sei, dass ihre Unfallgegnerin über

ein Informationssystem der Kfz-Versicherer ihre personenbezogenen Versicherungsdaten erhalten kann.

Die Petentin wurde darauf hingewiesen, dass ein an einem Kfz-Unfall Beteiligter die Versicherungsdaten der anderen am Unfall Beteiligten über den Zentralruf der Autoversicherer in Erfahrung bringen kann.

Über den Zentralruf der Autoversicherer kann nach einem Unfall die gegnerische Versicherung ermittelt werden. Hierzu benötigen die Mitarbeiter vom Zentralruf der Autoversicherer lediglich das Kennzeichen des Unfallgegners und den Schadenstag. Bei Unfällen im Ausland muss zusätzlich noch das Unfallland angegeben werden. Diese Möglichkeit der Ermittlung der gegnerischen Versicherung bzw. der Unfallbeteiligten über den Zentralruf der Autoversicherer steht allen am Unfall beteiligten Personen zu. Die Einschaltung einer Versicherung ist dazu nicht erforderlich.

Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Gesetzliche Grundlage für die Auskunftserteilung des Zentralrufes der Autoversicherer sind die §§ 8 und 8a des Gesetzes über die Pflichtversicherung für Kraftfahrzeughalter (PflVG). Danach sind Versicherungsunternehmen, die zum Betrieb der Kraftfahrzeug-Haftpflichtversicherung für Kraftfahrzeuge und Anhänger mit regelmäßigem Standort im Inland befugt sind, u. a. verpflichtet, eine Auskunftsstelle einzurichten, die Geschädigten, deren Versicherern, dem deutschen Büro des Systems der Grünen Internationalen Versicherungskarte und dem Entschädigungsfonds auf Anforderung folgende Angaben übermittelt, soweit dies zur Geltendmachung von Schadenersatzansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr erforderlich ist:

1. Namen und Anschrift des Versicherers des schädigenden Fahrzeugs sowie dessen in der Bundesrepublik Deutschland benannten Schadenregulierungsbeauftragten,

2. die Nummer der Versicherungspolice und das Datum der Beendigung des Versicherungsschutzes, sofern dieser abgelaufen ist,

3. bei Fahrzeugen, die nach Artikel 4 Buchstabe a der Richtlinie 72/166/EWG des Rates vom 24. April 1972 betreffend die Angleichung der Rechtsvorschriften der Mitgliedstaaten bezüglich der Kraftfahrzeug-Haftpflichtversicherung und der Kontrolle der entsprechenden Versicherungspflicht (ABl. EG Nr. L 103 S. 1) von der Versicherungspflicht befreit sind, den Namen der Stelle oder Einrichtung, die dem Geschädigten nach geltendem Recht ersatzpflichtig ist,

4. Namen und Anschrift des eingetragenen Fahrzeughalters oder, soweit die Auskunftsstelle diese Informationen erlangen kann, des Fahrzeugeigentümers oder des gewöhnlichen Fahrers; § 39 Abs. 1 des Straßenverkehrsgesetzes gilt entsprechend.

Geschädigte sind berechtigt, sich an die Auskunftsstelle zu wenden, wenn sie ihren Wohnsitz in der Bundesrepublik Deutschland haben, wenn das Fahrzeug, das den Unfall verursacht haben soll, seinen gewöhnlichen Standort in der Bundesrepublik Deutschland hat oder wenn sich der Unfall in der Bundesrepublik Deutschland ereignet hat. Die

Aufgaben und Befugnisse der Auskunftsstelle werden von der GDV Dienstleistungs-GmbH & Co. KG - "Zentralruf der Autoversicherer" - in Hamburg wahrgenommen. Bei der Auskunftserteilung prüft der Zentralruf der Autoversicherer nicht, wer den Unfall tatsächlich verursacht hat. Sollte dies unter den Beteiligten strittig sein, bleibt die Klärung einem späteren zivilrechtlichen Verfahren zwischen den Unfallbeteiligten bzw. den Versicherer vorbehalten.

19.3 Hinweis- und Informationssystem (HIS) des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV)

Ein Betroffener, der bei einem großen Versicherungsunternehmen einen Antrag auf Berufsunfähigkeitsversicherung gestellt hatte, der jedoch vom Versicherer aufgrund des Gesundheitszustandes des Antragstellers abgelehnt worden war, bat die Aufsichtsbehörde um datenschutzrechtliche Prüfung. Nachdem er durch einen Beitrag in der TV-Sendung „WISO“ darauf aufmerksam wurde, dass personenbezogene Daten von Versicherungen an eine „schwarze Liste“ weitergegeben würden, wandte er sich an den Versicherer, der seinen Antrag abgelehnt hatte, mit der Frage, ob und gegebenenfalls welche seiner Daten an diese „schwarze Liste“ weitergemeldet worden seien. Daraufhin teilte ihm der Versicherer mit, dass an die Sonderwagnisdatei des Gesamtverbandes der Deutschen Versicherungswirtschaft gemeldet worden sei, dass es eine Erschwernis beim Antrag auf Lebens- und Berufsunfähigkeitsversicherung gegeben habe. Daten über seinen Gesundheitszustand seien nicht übermittelt worden.

Aus datenschutzrechtlicher Sicht ist hierzu Folgendes anzumerken:

Schon seit 1993 wird beim Gesamtverband der Deutschen Versicherungswirtschaft ein Hinweis- und Informationssystem (früher: Uniwagnis-Datei) geführt, dessen Aufgabe darin besteht, Versicherungsbetrug zu bekämpfen und die Risikoprüfungen bei Neukunden für die Versicherer effizienter zu gestalten. Hierzu melden die teilnehmenden Versicherer unter bestimmten Voraussetzungen Kundendaten in das Hinweissystem ein. Das Hinweissystem wurde schon in der Vergangenheit von den Aufsichtsbehörden für Datenschutz als zulässig angesehen. Allerdings hatten die Aufsichtsbehörden immer wieder Mängel bei der Transparenz zu diesem System festgestellt und auf deren Abhilfe hingewirkt. So wurde auf Drängen der Aufsichtsbehörden das Hinweis- und Informationssystem von der Versicherungswirtschaft ab dem 1. April 2011 in folgenden wesentlichen Punkten modifiziert:

- Das Hinweis- und Informationssystem wird bei der Informa Insurance Risk and Fraud Prevention GmbH, Rheinstraße 99, 76532 Baden-Baden als Auskunftei im Sinne des § 29 Bundesdatenschutz (BDSG) geführt.

- Den Betroffenen wird von der Informa Insurance Risk and Fraud Prevention GmbH Auskunft über die zu ihrer Person im Hinweis- und Informationssystem gespeicherten Daten erteilt.

- Die Betroffenen, die in das Hinweis- und Informationssystem eingemeldet wurden, werden benachrichtigt.

- Es dürfen keine Gesundheitsdaten eingemeldet werden.

Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Gesetzliche Grundlage für die Datenübermittlung der Versicherer an das Hinweis- und Informationssystem ist § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Das berechtigte Interesse der Versicherer an der Datenübermittlung liegt darin begründet, Versicherungsbetrug aufzudecken und die Risikoprüfungen bei Neukunden effizienter zu gestalten, um auf dieser Basis einen risikoadäquaten Beitrag für alle Versicherten festzulegen. Dem steht das schutzwürdige Interesse der Betroffenen an der Geheimhaltung ihrer Daten gegenüber. Dies bedeutet, dass eine Abwägung zwischen den berechtigten Interessen der verantwortlichen Stelle und den schutzwürdigen Interessen der Betroffenen zu treffen ist. Bei dieser Abwägung ist allgemein anerkannt, dass die schutzwürdigen Interessen der Betroffenen im vorliegenden Fall gegenüber den Interessen der Solidargemeinschaft der Versicherten an einer korrekten Schadensregulierung und damit einhergehend an einer sparsamen Tarifgestaltung nicht überwiegen. Weiter ist bei der Abwägung zu berücksichtigen, dass Kunden beim Abschluss eines Versicherungsvertrages nach dem Versicherungsvertragsgesetz verpflichtet sind, alle für das Versicherungsverhältnis relevanten Informationen richtig anzugeben und schon allein aus diesem Grund kein schutzwürdiges Interesse der Kunden an einer Geheimhaltung dieser Daten besteht.

Die Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG liegen somit vor.

Personenbezogene Daten dürfen grundsätzlich nur solange gespeichert werden, wie ihre Kenntnis für den Zweck, zu dem sie gespeichert wurden, erforderlich ist. Nach § 35 Abs. 2 Satz 2 Nr. 2 BDSG beträgt die Speicherdauer der ins Hinweis- und Informationssystem eingemeldeten Daten vier Jahre. Sie beginnt mit dem Kalenderjahr, das der erstmaligen Speicherung folgt und verlängert sich entsprechend in den Fällen, in denen vor Ablauf dieser Frist eine erneute Einmeldung in das Hinweis- und Informationssystem erfolgt. Damit soll sichergestellt werden, dass bei nachhaltig relevanten Fällen, etwa bei einem wiederholten Versicherungsbetrug, auch frühere Informationen nicht verloren gehen.

20 Statistik

20.1 Zensus 2011

Bereits in meinem vorherigen Tätigkeitsbericht habe ich über die umfangreichen Vorbereitungsmaßnahmen berichtet, die zur Durchführung der Volks- und Wohnungszählung (Zensus 2011) notwendig waren.

Im Mai 2011 begann dann die eigentliche Befragung der ausgewählten Haushalte durch die bei den Landkreisen eingerichteten Erhebungsstellen.

Eingaben aus dem Bereich der Gebäude- und Wohnungszählung betrafen in erster Linie die Frage, ob grundsätzlich eine Auskunftspflicht besteht und ob man als Eigentümer eines Mietshauses Angaben zu den Mietern machen darf. Durch Hinweis auf § 18 Zensusgesetz 2011 konnte den Petenten dargelegt werden, dass eine Auskunftspflicht grundsätzlich besteht. Auch die Angaben zu den Mietern sind gesetzlich geregelt. § 6 Absatz 3 Zensusgesetz gibt vor, welche Angaben vom Hauseigentümer verlangt werden dürfen.

Das Erinnerungsverfahren zur Abgabe der Erhebungsbögen führte zu Beschwerden auch in meiner Dienststelle, da viele der angemahnten Auskunftspflichtigen ihrer Pflicht nachgekommen waren und nun vermuteten, dass ihre Briefsendungen nicht angekommen oder gar in falsche Hände geraten waren. Die ungerechtfertigten Schreiben waren zum einen darauf zurückzuführen, dass manche Eigentümer mehrerer Häuser die Rücksendung der Bögen in einem Kuvert vorgenommen hatten und zum anderen in dem Zeitraum zwischen Fertigung der Mahnschreiben und deren Versendung noch einige Rücksendungen erfolgten, entsprechende Mahnschreiben jedoch nicht aussortiert wurden. Diese Erklärungen wurden von den Betroffenen in den meisten Fällen akzeptiert.

Die eigentliche „Volkszählung“, die mittels einer Haushaltebefragung auf Stichprobenbasis durchgeführt wurde, verlief aus datenschutzrechtlicher Sicht relativ problemlos. Hier zeigte sich, dass die effiziente Zusammenarbeit der Statistischen Ämter und der Datenschutzbeauftragten von Bund und Ländern in der vorbereitenden Gesetzgebung und der organisatorischen Umsetzung in den Ländern erfolgreich war.

Die Anfragen zur Volkszählung erfolgten zumeist telefonisch. Vielen Fragestellern war nicht bekannt, dass die Erhebungsbeauftragten kein Recht dazu haben, Einlass in die Wohnung zu begehren, sondern lediglich Hilfestellung beim Ausfüllen der Fragebögen leisten. In kleineren Ortschaften war dies gelegentlich problematisch, da die Erhebungsbeauftragten ebenfalls aus dem Ort stammten und die Befragten kannten. Die Erhebungsstellen boten den Auskunftspflichtigen in diesen Fällen an, an Amtsstelle vorzusprechen oder schickten in Ausnahmefällen andere Mitarbeiter in die Haushalte.

Ein Petent vermutete, dass die Fragebögen, die er persönlich in den Briefkasten einer Erhebungsstelle eingeworfen hatte, entwendet worden sein könnten, da er mehrmals angemahnt wurde, die Fragebögen einzureichen. Mein Kontrollbesuch ergab, dass die Fragebögen bei der

Erhebungsstelle vorlagen. Inhaltlich und formal waren sie aber derart ausgefüllt, dass man die Vermutung haben konnte, der Petent wolle seiner Auskunftspflicht nicht nachkommen. Die Mahnschreiben an den Petenten waren allerdings in der Tat so formuliert, dass der Petent davon ausgehen durfte, seine Fragebögen lägen der Erhebungsstelle gar nicht vor. Es gelang mir, den Petenten dazu zu bringen, zusammen mit dem Erhebungsstellenleiter die Fragebögen durchzugehen und formgerecht auszufüllen.

21 Sonstiges

21.1 Veröffentlichung von Einsatzberichten durch die Feuerwehr

Immer mehr Hilfsorganisationen im Saarland wie die Freiwilligen Feuerwehren nutzen das Internet als Plattform, ihre Arbeit zu präsentieren und in der Bevölkerung ein positives Bild der Hilfsorganisation zu festigen. Leider wird sich auf so manchen Homepages nicht darauf beschränkt, zulässige Bilder von Übungseinheiten oder Festakten zu veröffentlichen, immer mehr ist festzustellen, dass auch detaillierte Einsatzberichte sowie Fotos oder Filmaufnahmen von Einsätzen ihren Weg ins Netz finden.

In einem uns vorgelegten Fall wurden Einsatzbilder eines Kaminbrandes auf der Internetseite einer Feuerwehr eingestellt. Die Versicherung des Hausbesitzers wollte den beim Kaminbrand entstanden Schaden nicht übernehmen, weil man dem Eigentümer anhand dieser im Internet veröffentlichten Einsatzbilder der Feuerwehr zur Last legte, dass Efeu im Außenbereich am Kamin hochgerankt sei, was auf eine fahrlässige Handlung des Hausbesitzers hindeutete.

Aufgrund unserer Intervention hat man sich in der entsprechenden Kommune darauf verständigt, künftig auf die Veröffentlichung von Einsatzfotos mit personenbezogenen oder personenbeziehbaren Daten zu verzichten.

Das Ministerium für Inneres und Sport hat hierzu für ehrenamtliche Feuerwehrangehörige, die Helferinnen und Helfer im Katastrophenschutz sowie den im Rettungsdienst ehrenamtlich Tätigen bereits im Jahre 2009 den Erlass „Pflicht zur Verschwiegenheit in der nichtpolizeilichen Gefahrenabwehr“ veröffentlicht. Dort ist genau geregelt, wer welche Daten veröffentlichen darf, wer welche Informationen an die Presse weitergeben darf und welche Daten nur für interne Zwecke der Hilfsorganisationen genutzt werden dürfen.

Neben den möglichen Rechtsverstößen gegen das Recht am eigenen Bild bei Aufnahmen, die Personen am Einsatzort zeigen, können auch veröffentlichte Sachgegenstände personenbeziehbar sein und für den Betroffenen Konsequenzen nach sich ziehen, wie das im eben geschilderten Fall des Kaminbrandes geschehen war. Auch aus Pietätsgründen sollte man auf das Veröffentlichen von beispielsweise Autowracks verzichten, wenn darin Personen ihr Leben verloren haben oder schwer verletzt wurden. Die Angehörigen haben für solche Veröffentlichungen kein Verständnis und die für die Einstellung Verantwortlichen riskieren, mit einem Bußgeld nach § 26 Kommunales Selbstverwaltungsgesetz (KSVG) belegt zu werden.

21.2 Aufzeichnung von Notrufen bei Versorgungsunternehmen

Mehrere Anbieter von Strom, Gas, Wasser und Wärme haben beschlossen, im Rahmen einer „Saarländischen Kooperation" enger zusammenzuarbeiten und zu diesem Zweck u. a. eine gemeinsame Notrufzentrale eingerichtet. Es sollten spezielle Telefonnummern bekannt gegeben werden, die die Kunden bei Notrufen oder Störfallmeldungen benutzen sollten.

Aus Erfahrung weiß man, dass es bei diesen Notfallmeldungen zu Missverständnissen in der mündlichen Kommunikation kommen kann, was deshalb besonders fatal ist, weil bei Notrufen oft Leben und Gesundheit auf dem Spiel stehen.

Man beabsichtigte deshalb, alle eingehenden Notrufe auf Tonband aufzuzeichnen und fragte meine Dienststelle, ob einer solchen Aufzeichnung datenschutzrechtliche Gründe entgegenstehen.

Die Frage war durchaus berechtigt, steht doch hier eine Verletzung der Strafvorschrift des § 201 Strafgesetzbuch im Raum, wonach bestraft wird, wer unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt.

Es stellte sich somit die Frage nach einer Rechtsgrundlage für die beabsichtigte Tonbandaufzeichnung. Selbstverständlich zulässig wäre der Mitschnitt mit Einwilligung des Anrufers. Dazu müsste der Anrufer zu Beginn des Gesprächs auf den Mitschnitt hingewiesen und um seine Einwilligung gebeten werden. Ich halte eine solche Vorgehensweise bei der Ausnahmesituation eines Notrufes für wenig praktikabel. Ich bin mir sicher, dass eine entsprechende Frage in dieser Situation auf Unverständnis bei den meisten Anrufern stoßen würde. Ich halte die Abfrage einer Einwilligung aber auch nicht für erforderlich, da die Datenschutzgesetze eine ausreichende Rechtsgrundlage für die Aufzeichnung darstellen. Nach dem Saarländischen Datenschutzgesetz ist eine Speicherung personenbezogener Daten zulässig, wenn diese zur Aufgabenerfüllung erforderlich ist. Diese Voraussetzung sehe ich hier als gegeben an, da bei den aus dem Spiel stehenden Rechtsgütern (Leben, Gesundheit, schwerwiegende Eigentumsbeeinträchtigungen) unbedingt gewährleistet sein muss, dass jedes Anliegen richtig verstanden wurde.

Im Ergebnis habe ich deshalb den Versorgungsunternehmen mitgeteilt, dass ich gegen eine Aufzeichnung von Notrufen bei der Leitstelle keine datenschutzrechtlichen Bedenken habe.

21.3 Bekanntgabe einer beabsichtigten Eheschließung

Bis zum Jahr 1998 waren die Standesämter verpflichtet, alle beabsichtigten Eheschließungen in Form des sogenannten „Aufgebotes" öffentlich bekannt zu machen. Der öffentliche Aushang hatte den Sinn, eventuell bestehende Ehehindernisse zu melden. Nachdem sich im Laufe der Zeit herausgestellt hatte, dass das Aufgebot kein taugliches Mittel zur Aufdeckung von Ehehindernissen darstellte, wurde es mit Gesetz zur Neuordnung des Eheschließungsrechts vom 04.05.1998 abgeschafft.

Dies war ein auch aus datenschutzrechtlicher Sicht folgerichtiger Schritt, da eine Bekanntgabe personenbezogener Daten unzulässig ist, wenn es an deren Erforderlichkeit fehlt.

Im Berichtszeitraum hat mich eine Eingabe erreicht, deren Thema ebenfalls die Bekanntgabe eines Heiratstermins war.

Die Petenten hatten sich beim Standesamt einen Wunschtermin zur Hochzeit eintragen lassen. Der Zufall wollte es, dass die Standesbeamtin eine Wohnung zur Vermietung anbot und die Mutter der Braut, die von den Hochzeitsplänen ihrer Tochter offensichtlich nichts wusste, sich für die Wohnung interessierte. Bei der Wohnungsbesichtigung soll die Standesbeamtin erwähnt haben, dass ja bald die Hochzeit anstehe. Auf Grund von Umständen, die meiner Dienststelle nicht bekannt sind, wollten die Petenten ihre Eheschließung geheim halten und beschwerten sich deshalb über die betreffende Standesbeamtin.

Eine Anfrage bei dem Dienstvorgesetzten der Standesbeamtin brachte keine Klärung des Sachverhaltes. Die Standesbeamtin konnte sich an Einzelheiten des Gespräches anlässlich der Wohnungsbesichtigung wegen des bereits länger zurückliegenden Termins nicht erinnern. Im vorliegenden Fall steht somit der Vorwurf der unzulässigen Datenweitergabe unbewiesen im Raum.

Unabhängig davon möchte ich darauf aufmerksam machen, dass alle Mitarbeiter der Öffentlichen Verwaltung strikt darauf achten müssen, dass dienstlich erlangten Informationen im privaten Umfeld nicht erwähnt werden dürfen.

21.4 Dokumente der Saarländischen Universitäts- und Landesbibliothek im Internet

Ein Petent wunderte sich, als er bei Eingabe seines Namens in Google auf einen Treffer stieß, der im Amtlichen Bekanntmachungsblatt einer Gemeinde unter der Rubrik „Amtliche Bekanntmachungen“ veröffentlich worden war. Dort war als Tagesordnung der Sitzung des Ortsrates für die Behandlung in nicht-öffentlicher Sitzung das Bauvorhaben des Petenten wegen Errichtung einer Grundstückseinfriedung aufgeführt. Der Petent bat meine Dienststelle um Aufklärung und darum, die Verantwortlichen zu einer Entfernung aus der Trefferliste zu veranlassen.

Auf Grund meiner Recherchen habe ich die Saarländische Universitäts- und Landesbibliothek als die für die Veröffentlichung im Internet verantwortliche Stelle ermittelt. Hintergrund ist, dass nach dem Saarländischen Mediengesetz von jedem Druckwerk, das im Saarland verlegt wird, ein Stück dieser Bibliothek anzubieten ist.

In den einschlägigen Rechtsvorschriften finden sich keine Regelungen, wie mit den zur Verfügung gestellten Druckwerken, also auch mit den gemeindlichen Bekanntmachungsblättern, umzugehen ist. Bei meinen Überlegungen bin ich davon ausgegangen, dass es Aufgabe einer Bibliothek ist, die bei ihr vorhanden Dokumente zugänglich zu machen. Auch eine Internetveröffentlichung sehe ich als zulässig an, auch wenn diese Form der Veröffentlichung eine ganz andere Qualität hat, als die Veröffentlichung in der herkömmlichen Papierform. Jeder Interessierte kann weltweit jederzeit auf die veröffentlichten personenbezogenen

Daten zugreifen, obwohl gemeindliche Bekanntmachungsblätter sich nach ihrer Zielrichtung an die Einwohner der jeweiligen Gemeinden richten und regelmäßig auch nur dieser Personenkreis ein Interesse an den dort veröffentlichten Informationen hat. Gleichwohl habe ich meine Bedenken hinsichtlich dieser Form der Veröffentlichung zurückgestellt, weil es sich um Informationen handelt, die grundsätzlich öffentlich zugänglich sind und durch die Internetveröffentlichung nur der Gang zur Bibliothek, wo die Blätter von jedem interessierten Bürger eingesehen werden können, entfällt.

Einen unzulässigen Eingriff in das informationelle Selbstbestimmungsrecht sehe ich allerdings dann, wenn die Qualität der Veröffentlichung sich dadurch verändert, dass unmittelbar - oder weil die Informationen durch Suchmaschinen erschlossen werden - Such- und Auswertungsmöglichkeiten mit Personenbezug entstehen. Ich habe deshalb die Bibliothek gebeten sicherzustellen, dass die Namen einzelner Personen in Amtlichen Bekanntmachungsblättern nicht mehr über Suchmaschinen zu finden sind.

Die Bibliothek hat mir mitgeteilt, dass sie für ihre Server eine robots.txt-Datei angelegt und aktiviert habe. Dies verhindere zuverlässig den Zugriff von allen gängigen Suchmaschinen und Suchrobotern auf den gesamten dort archivierten Bestand.

22 Aus der Dienststelle

Die Tätigkeit des Unabhängigen Datenschutzzentrums Saarland ist neben der Bearbeitung von Eingaben, Beschwerden und Stellungnahmen durch zahlreiche andere Aufgaben geprägt. An dieser Stelle will ich einen kleinen Einblick geben in die vielfältigen weiteren Bereiche der Tätigkeit der Landesbeauftragten für Datenschutz und Informationsfreiheit und ihrer Mitarbeiter.

22.1 Zusammenarbeit mit dem Landtag

Im Innenausschuss des saarländischen Landtages wurden 2011 durch meine Dienststelle aktuelle Themen – etwa die Problematik Zensus und Datenschutz - diskutiert sowie die Themen der Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und die Eckpunkte eines modernen Datenschutzes vorgetragen.

In der Sitzung vom 03.05.2011 hatten wir die Gelegenheit, ausführlich unsere Stellungnahme zur Novellierung des Saarländischen Datenschutzgesetzes vorzutragen und zu erörtern.

In der Sitzung vom 03.11.2011 konnten wir zu aktuellen Themen Stellung nehmen und am 08.12.2011 den Tätigkeitsbericht für die Jahre 2009/2010 vortragen.

Der 2012 neu gegründete Ausschuss „Datenschutz und Informationsfreiheit" tagt seit Juni 2012 regelmäßig zu aktuellen Datenschutzthemen.

In der konstituierenden Sitzung stellte ich mit den Referatsleitern der Dienststelle die Tätigkeit und Aufgaben des Unabhängigen Datenschutzzentrums vor und ging auf aktuelle Themen seit dem letzten Tätigkeitsbericht ein.

In der Sitzung vom 20.09.2012 ging es um eine Pressemitteilung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Frage der zukünftigen Zusammenarbeit mit den Landesbeauftragten für Datenschutz im Hinblick auf die neue EU-Datenschutz-Grundverordnung.

In einer gemeinsamen Sitzung mit dem Europaausschuss im Dezember 2012 haben wir den Entwurf der Europäischen Datenschutz-Grundverordnung im Einzelnen vorgestellt und die mit der Verordnung verbundenen Chancen und Risiken mit den Abgeordneten diskutiert.

In der Sitzung des Ausschusses für Datenschutz und Informationsfreiheit vom 11.10.2012 haben wir im Ausschuss über die Voraussetzungen der Videoüberwachung im öffentlichen Raum vorgetragen und den Stand des Tätigkeitsberichtes für 2011 und 2012 erläutert.

Am 22.11.2012 konnten wir die Abgeordneten des Ausschusses in der Dienststelle zu einem Informationsbesuch und einer Sitzung begrüßen. Wir haben über die Ergebnisse der Herbstkonferenz der Datenschutz-

beauftragten des Bundes und der Länder vom 07./08.11.2012 berichtet sowie das Recht auf Informationsfreiheit anhand einer Präsentation erläutert.

Den Abschluss des Berichtszeitraumes bildete die Sitzung vom 06.12.2012, in der über die Ergebnisse der Konferenz der Informationsfreiheitsbeauftragten vom 27.11.2012 in Mainz berichtet wurde.

Ausführlich wurden auch die Voraussetzungen von Live-Video-Streaming Übertragungen aus Stadt- und Gemeinderatssitzungen vorgetragen und über die datenschutzrechtlichen Anforderungen an Ratsinformationssystemen referiert.

22.2 Zusammenarbeit mit anderen Stellen

22.2.1 Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Die Datenschutzkonferenz ist ein freiwilliger Zusammenschluss des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz. Die Konferenz tagt zweimal im Jahr; der Vorsitz wechselt jährlich.

Durch die Konferenz wurden besondere Arbeitskreise gebildet, z.B. für Soziales, für Justiz oder für Technik, in denen sich Spezialisten mit bestimmten Datenschutzproblemen beschäftigen und Stellungnahmen und Entschließungen der Konferenz vorbereiten.

In der Konferenz selbst werden dann zu aktuellen Datenschutzfragen politische Forderungen diskutiert und als Entschließungen formuliert. Die Entschließungen enthalten gegenüber der Politik, der Fachöffentlichkeit und den Medien die abgestimmten Standpunkte der Datenschutzbeauftragten und werden veröffentlicht.

22.2.2 Düsseldorfer Kreis

Der Düsseldorfer Kreis ist seit März 2012 ein privilegierter Arbeitskreis der Datenschutzkonferenz mit sechs Unterarbeitskreisen mit eigenen Beschlüssen für den Bereich des nicht-öffentlichen Datenschutzes. Der Vorsitz wird vom Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen geführt. Bis zur Neuorganisation der Datenschutzaufsicht durch die Zusammenlegung der Aufsichtsbehörden für den öffentlichen und den nicht-öffentlichen Bereich in allen Bundesländern mit Ausnahme von Bayern waren hier die obersten Aufsichtsbehörden für den Datenschutz im privaten Bereich organisiert.

Der Düsseldorfer Kreis dient der Kommunikation, Kooperation und Koordinierung der unabhängigen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich.

Ziel des Düsseldorfer Kreises ist die bundesweit einheitliche Auslegung des geltenden Rechts in wesentlichen Fragen des Datenschutzes im nicht-öffentlichen Bereich sowie die Verständigung zwischen den Aufsichtsbehörden über ein aufsichtsbehördliches Vorgehen, um zu einem

verlässlichen, bundesweit möglichst einheitlich angewandten Datenschutzniveau im nicht-öffentlichen Bereich zu gelangen.

Die im Berichtszeitraum gefassten Beschlüsse des Düsseldorfer Kreises sind in der Anlage beigefügt.

22.2.3 Zusammenarbeit in der Konferenz der Informationsfreiheitsbeauftragten

Die Informationsfreiheitsbeauftragten des Bundes und der Länder haben sich in der Konferenz der Informationsfreiheitsbeauftragten zusammengeschlossen und tagen im halbjährlichen Rhythmus. Der Vorsitz wechselt jährlich.

In dem zugehörigen Arbeitskreis für Informationsfreiheit werden die aktuellen Themen erörtert und für die Konferenz vorbereitet.

Die Konferenz selbst tagt grundsätzliche öffentlich und stimmt die Stellungnahmen zu den aktuellen politischen Entwicklungen in diesem Bereich ab und fasst Entschließungen hierzu, die der Politik, der Fachöffentlichkeit und den Medien übergeben werden.

In der Anlage sind die Entschließungen aus dem Berichtszeitraum beigefügt.

22.3 Öffentlichkeitsarbeit

22.3.1 Bundesweite Veranstaltungen:

Am 28. Januar 2011 fand zum Thema „Datenschutz in Europa – Quo Vadis?“ anlässlich des 5. Europäischen Datenschutztages eine Veranstaltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in der Vertretung des Landes Baden-Württemberg beim Bund in Berlin statt.

Fragen rund um das Thema „Vorratsdatenspeicherung“ und Datenschutz wurden bei der zentralen Veranstaltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder anlässlich des 6. Europäischen Datenschutztages am 27. Januar 2012 in der Vertretung des Freistaates Bayern beim Bund diskutiert.

22.3.2 Veranstaltungen im Saarland

Im Berichtszeitraum wurden seitens des Unabhängigen Datenschutzzentrums Informationsveranstaltungen und auch Fortbildungen angeboten, um die Datenschutzthemen und auch die Ansprechpartner in der Dienststelle bekannt zu machen. Dies soll auch die Basis für die Arbeit des Unabhängigen Datenschutzzentrums sein.

Nur wer die Grundlagen des Datenschutzrechts und der Informationsfreiheit kennt, kann diese auf Dauer gesetzeskonform anwenden oder bittet frühzeitig um Rat.

2011:

Den Auftakt machte am 11.04.2011 eine Veranstaltung für Juristinnen in der die Grundlagen des Datenschutzrechtes und des Rechtes auf Informationsfreiheit einerseits und die Zuständigkeiten der Landesbeauftragten und die rechtlichen Folgen der Entscheidung des Europäischen Gerichtshofes über die Unabhängigkeit der Datenschutzaufsicht andererseits vorgetragen und diskutiert wurden.

In zwei Veranstaltungen für behördliche Datenschutzbeauftragte am 10. und 20.05.2011 unter dem Titel „Der Datenschutz bekommt ein Gesicht" habe ich mich mit meinen Mitarbeitern rund 140 interessierten Datenschutzbeauftragten von Behörden mit unseren Aufgaben vorgestellt und Grundsätze des Datenschutzrechtes nebst aktuellen Themen vorgestellt.

Am 11.05.2011 konnten wir bei der Sparkassenakademie zu aktuellen Datenschutzthemen aus dem Bankenbereich und dem Beschäftigtendatenschutz referieren.

Zwei für den Bereich Videoüberwachung und Beschäftigtendatenschutz zuständige Mitarbeiter/innen der Dienststelle haben am 21. Juni 2011 im Arbeitskreis Best der Arbeitskammer einen Vortrag zum Thema Kameraüberwachung in öffentlichen Einrichtungen im Saarland präsentiert.

Am 21.10.2011 hatten wir die Gelegenheit, unsere Dienststelle beim Arbeitskreis Datenschutz und Datensicherheit der ZPT/IHK anlässlich deren Sitzung in Mettlach bei Villeroy und Boch vorzustellen und aktuelle Datenschutzthemen vorzutragen.

Am 24.10.2011 konnten wir Hauptamtsleiter von Kommunen zu einer Vortragsveranstaltung: "Informationsfreiheit im Saarland – da kann ja jeder kommen!" einladen. Als Referent konnten wir Herrn Sven Müller, Mitarbeiter der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht von Brandenburg, begrüßen.

Für ein Ganztagesseminar am 22.11.2011 zum Saarländischen Informationsfreiheitsgesetz mit dem Thema – Das Recht auf Neugier - transparentes staatliches Handeln – konnten wir Herrn Dr. Huber, Vorsitzender Richter am Verwaltungsgericht Frankfurt am Main, gewinnen und durften rund 70 Behördenvertreter begrüßen.

2012:

Am 07.03.2012 hielten wir bei der Christlichen Erwachsenenbildung in Weiskirchen einen Vortrag zum Thema: „Facebook & Co. - Soziale Netze im Alltag von Kindern und Jugendlichen".

Am 26.04.2012 konnte ein Mitarbeiter bei der Landesmedienanstalt Saarland für die Gesamtelternvertretung einen Vortrag zum Thema: „In sozialen Netzwerken aktiv - wo bleibt der Datenschutz?" halten.

Anlässlich einer bundesweiten Veranstaltung zum Thema E-Governement am 03.05.2012 in der Staatskanzlei stellten wir zusammen

mit dem bayerischen Kollegen die Grundzüge der geplanten Europäischen Datenschutz–Grundverordnung vor.

Für den Bereich des Datenschutzes nach dem BDSG haben wir am 29.05.2012 eine erste gut besuchte Veranstaltung bei der IHK zu den Themen: „Vom "Gefällt mir Button" zur Videoüberwachung und Arbeitnehmerdatenschutz im Web“ angeboten.

Am 31.05.2012 fand die Veranstaltung „Neues zum Datenschutz aus Berlin und Brüssel“ bei der Sparkassenakademie statt.

„Warum Datenschutz Chefsache ist“ - war eine weitere gut besuchte Veranstaltung am 30.08.2012 bei der IHK, bei der neben einführenden Datenschutzthemen, das Thema Überwachung von Beschäftigten und Verwendung von Adress- und Kundendaten nach der Reform des Bundesdatenschutzgesetzes im Jahre 2009 Gegenstand waren.

Mitarbeiter der Kreisverwaltungen nahmen an einer Fortbildungsveranstaltung zum Thema Sozialdatenschutz am 15.11.2012 in Saarbrücken teil. Hierzu konnten wir einen Referenten aus Mainz gewinnen. Die Veranstaltung war sehr gut besucht. Beim 1. P@d-Day des Landesinstituts für Pädagogik und Medien am 19.11.2012 präsentierte ein Mitarbeiter einen Vortrag zum Thema „E-Learning & Privacy - Schülerdaten im Netz“.

22.3.3 Neugestaltung der Homepage zum Informationsmedium

Im Berichtszeitraum wurde die Homepage des Unabhängigen Datenschutzzentrums Saarland zu einem modernen Informationsmedium neu gestaltet und bietet heute neben aktuellen Informationen eine Reihe von Handreichungen und Orientierungshilfen für die Praxis.

So können sich Bürger, Betriebe und Behörden gleichermaßen über datenschutzrechtliche Themen und auch über die Voraussetzungen von Anwendungen informieren.

22.3.4 Werbekampagne zum Saarländischen Informationsfreiheitsgesetz

Im Herbst 2012 haben wir schließlich anlässlich einer Sitzung des Ausschusses für Datenschutz und Informationsfreiheit in der Dienststelle eine Werbekampagne mit Plakaten und Flyern zum Saarländischen Informationsfreiheitsgesetz gestartet.

23 Beschlüsse des Düsseldorfer Kreises

23.1 Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 8. April 2011

Am 1. März 2011 hat der Branchenverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) einen Datenschutz-Kodex für Geodatendienste vorgelegt, der den schutzwürdigen Interessen der Eigentümer und Bewohner bei der Veröffentlichung der sie betreffenden Gebäudeansichten im Internet Rechnung tragen soll. Das Bundesministerium des Innern hatte der Internetwirtschaft in Aussicht gestellt, bei der Vorlage einer angemessenen und mit den Datenschutzbehörden des Bundes und der Länder abgestimmten Selbstverpflichtung auf gesetzliche Spezialregelungen für Internet-Geodatendienste wie Google Street View zu verzichten.

Der Düsseldorfer Kreis stellt fest, dass die Selbstregulierung der Internetwirtschaft mit dem vom BITKOM vorgelegten Datenschutz-Kodex nicht gelingt. Der Kodex entspricht in wesentlichen Bereichen nicht den datenschutzrechtlichen Anforderungen und ist nicht mit den Datenschutzbehörden des Bundes und der Länder abgestimmt.

Der Kodex sieht zwar ein Widerspruchsrecht gegen die Veröffentlichung von Gebäudeansichten im Internet vor, ohne dass Gründe dargelegt werden müssen. Der Widerspruch ist jedoch erst nach der Veröffentlichung vorgesehen. Alle Gebäudeansichten sind deshalb zunächst im Internet verfügbar. Bereits mit der Veröffentlichung der Bilder wird aber das Recht auf informationelle Selbstbestimmung verletzt. Auch bei weiteren Regelungen weist der Datenschutz-Kodex datenschutzrechtliche Defizite auf: Viele Veröffentlichungen, die die Privatsphäre beeinträchtigen, werden vom Kodex nicht erfasst, so etwa Schrägaufnahmen aus der Luft. Hinzu kommt, dass der Datenschutz-Kodex nur für die Unternehmen bindend ist, die ihn unterzeichnet haben.

Deshalb ist jetzt der Gesetzgeber gefordert, das Recht auf informationelle Selbstbestimmung im Internet mit einer umfassenden Regelung zu schützen, die dem besonderen Gefährdungspotential für das Persönlichkeitsrecht im Internet Rechnung trägt. Hierzu zählt insbesondere ein gesetzlich verbrieftes Widerspruchsrecht gegen die Veröffentlichung, das es den Betroffenen ermöglicht, bereits vor der Veröffentlichung personenbezogener Daten im Internet Widerspruch einzulegen.

Ein solches Vorab-Widerspruchsrecht entspricht den Anforderungen, die der Düsseldorfer Kreis in seinem Beschluss vom 13./14. November 2008 nach Auslegung des geltenden Rechts konkretisiert hat. Besonders wichtig sind demnach die folgenden Punkte:

- Gesichter und Kfz-Kennzeichen sind unkenntlich zumachen.
- Eigentümer und Bewohner eines Hauses müssen die Möglichkeit erhalten, die Veröffentlichung der Gebäudefassade durch

einen Widerspruch zu verhindern; die Widerspruchsmöglichkeit muss vor wie auch nach der Veröffentlichung bestehen.

- Die geplante Datenerhebung und der Hinweis auf die Widerspruchsmöglichkeit sind rechtzeitig bekannt zu geben.

23.2 Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 4./5. Mai 2011)

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

An die Anbindung von Praxis-EDV-Systemen an medizinische Netze sind folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b) eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet, mit der zum Zugang verwendeten Hard- und Softwareausschließlich Zugang zu medizinischen Netzen besteht sowie die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

23.3 Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 4./5. Mai 2011)

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 Aufsichtsbehörden im nichtöffentlichen Bereich fordern daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck

wurde von den Datenschutzbeauftragten der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen.

Die Orientierungshilfe konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Die Aufsichtsbehörden im nichtöffentlichen Bereich werden sich an dem vorliegenden Dokument als Leitlinie bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit orientieren. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Aufsichtsbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen.

Die Aufsichtsbehörden nehmen die Orientierungshilfe zustimmend zur Kenntnis.

23.4 Datenschutzgerechte Smartphone-Nutzung ermöglichen!

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 4./5. Mai 2011)

Smartphones sind Mobiltelefone, die insbesondere im Zusammenhang mit der Nutzung des Internet über deutlich mehr Computerfunktionalitäten und Kommunikationsmöglichkeiten verfügen als herkömmliche Mobiltelefone. Smartphones werden für eine Vielzahl von Aktivitäten genutzt und sind damit in weitaus größerem Umfang als sonstige Geräte der Informations- und Kommunikationstechnik „persönliche“ Geräte, die den Nutzer im Alltag permanent begleiten. Über das Telefonieren

hinaus eröffnen auf den Geräten installierbare Programme („Apps"), Lokalisierungsfunktionen (GPS) und Bewegungssensoren eine breite Palette von Anwendungsbereichen. Die dabei anfallenden Daten lassen detaillierte Rückschlüsse auf Nutzungsgewohnheiten, Verhaltensweisen oder Aufenthaltsorte der Nutzer zu.

Im Gegensatz zu herkömmlichen PCs bieten Smartphones den Nutzern jedoch nur rudimentäre Möglichkeiten, die Preisgabe personenbezogener Daten zu kontrollieren oder zu vermeiden; gängige Funktionen des Selbstdatenschutzes können nicht genutzt werden. Häufig werden personenbezogene Daten ohne Wissen der Nutzer an die Anbieter von Diensten übermittelt. Mit einiger Berechtigung wird davon gesprochen, ein solches Gerät sei ein „Spion in der Hosentasche".

Vor diesem Hintergrund ist aus datenschutzrechtlicher Sicht insbesondere Folgendes zu fordern:

- Transparenz bezüglich der Preisgabe personenbezogener Daten:

  In allen aktuellen Untersuchungen zeigt sich, dass in einer Vielzahl von Fällen durch die Geräte selbst mittels Betriebssystemen oder durch Anwendungen eindeutige Gerätekennungen, Standortdaten, E-Mail- und Telefontakte, SIM-Kartennummer und weitere personenbezogene Daten ohne Unterrichtung der Nutzer an Gerätehersteller, Provider oder Anbieter von Analysediensten übermittelt werden. Die Nutzer müssen in die Lage versetzt werden, diese Übermittlungen nachzuvollziehen. Sie müssen auch über den jeweiligen Zweck der Datennutzungen unterrichtet werden.

- Steuerungsmöglichkeiten der Nutzer für die Preisgabe personenbezogener Daten:

  Die Konzepte gängiger Smartphones sind oftmals darauf reduziert, dass, wenn überhaupt, lediglich während der Installation einer Anwendung der Nutzer pauschal einen Datenzugriff steuern kann. Auch erhalten zugelassene Anwendungen meist eine generelle Zugriffsmöglichkeit z.B. auf Kontaktinformationen. Den Nutzern müssen Möglichkeiten an die Hand gegeben werden, mit denen aus der Nutzungssituation heraus gesteuert werden kann, ob und welche Daten einer Applikation zugänglich gemacht werden und an wen sie übermittelt werden.

- Einflussmöglichkeiten auf das Löschen von Spuren bei der Internet-Nutzung:

  Im Gegensatz zu der für herkömmliche PCs bestehenden Situation fehlt es im Smartphonebereich weitgehend an Möglichkeiten, Datenspuren, die bei der Internet-Nutzung auf dem Gerät entstehen, zu vermeiden, zu reduzieren, mindestens jedoch, diese erkennbar zu machen und ggf. zu löschen. Solche Möglichkeiten müssen geschaffen und angeboten werden.

- Anonyme und pseudonyme Nutzungsmöglichkeiten:

  Generell sollte die Möglichkeit geschaffen werden, Smartphones und die über sie vermittelten Dienste anonym oder pseudonym zu nutzen.

23.5 Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 22./23. November 2011)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben. Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen

Zu verlangen sind also mindestens:

offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,

transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,

die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und

aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe[27] der Arbeitskreise „Technik" und „Medien" zu entnehmen, die der Düsseldorfer Kreis zustimmend zur Kenntnis genommen hat.

[27] Vgl. http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

23.6 Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 22./23. November 2011)

Der Düsseldorfer Kreis hat sich bereits mehrfach mit dem Problem des Mitarbeiterscreenings befasst, zuletzt durch Beschluss vom 23./24.04.2009. Es gibt Anlass, die Problematik erneut aufzugreifen.

In den letzten Jahren ist insbesondere die Zollverwaltung im Rahmen der Bewilligung des zollrechtlichen Status eines „zugelassenen Wirtschaftsbeteiligten" (AEO-Zertifizierungen) dazu übergegangen, von den Unternehmen umfangreiche Screenings von Mitarbeitern – und gegebenenfalls Daten Dritter – zu verlangen. Diese Screenings werden zum Teil in Abständen von wenigen Wochen ohne konkreten Anlass und undifferenziert durchgeführt. In diesem Geschäftsfeld betätigen sich bereits spezialisierte Dienstleister, die sich die bestehende Unsicherheit bei den Unternehmen zunutze machen. Dies ist auch der Grund, warum diese Screenings immer häufiger durchgeführt werden. Nach den praktischen Erfahrungen der Aufsichtsbehörden mangelt es an klaren Regelungen, wie mit den Ergebnissen von Datenscreenings umzugehen ist (Treffermanagement). Das Bundesministerium der Finanzen hat zwar am 14. Juni 2010 anlässlich dieser Praxis einschränkende Vorgaben erlassen, diese werden jedoch von den zuständigen Zollbehörden nicht einheitlich umgesetzt. Der Düsseldorfer Kreis hält in seinem vorgenannte n Beschluss derartige Screenings nur aufgrund einer speziellen Rechtsgrundlage für zulässig. Eine solche Rechtsgrundlage fehlt.

Weder die geltenden EU-Antiterrorverordnungen noch andere Sanktionslisten erfüllen die Anforderungen an eine solche spezielle Rechtsgrundlage. Diese Verordnungen enthalten lediglich die allgemeine Handlungspflicht, den in den Anlagen genannten Personen und Institutionen keine rechtlichen Vorteile zu gewähren, verpflichten jedoch nicht zu Screenings von Mitarbeitern, Kunden oder Lieferanten.

Auch die Bundesregierung ist der Auffassung, dass die Terrorismusverordnungen keinen systematischen, anlassunabhängigen Abgleich von Mitarbeiterdateien mit den Sanktionslisten verlangen. Allenfalls nach Maßgabe von Sorgfaltspflichten und differenzierend nach verschiedenen Verkehrskreisen und Risikolagen seien solche Abgleiche zulässig. Es bleibe den Unternehmen überlassen, wie sie die Einhaltung der Terrorismusverordnungen sicherstellen (Bundestags-Drucksache 17/4136 vom 03.12.2010).

Vor diesem Hintergrund empfiehlt und fordert der Düsseldorfer Kreis:

- Unternehmen sollten Datenscreenings nicht pauschal und anlasslos durchführen. Da die Lohnzahlung nur unbar erfolgt, die Kreditinstitute nach § 25c Kreditwesengesetz (KWG) ohnehin Abgleiche mit den Terrorlisten vornehmen, ist ein Datenabgleichverfahren innerhalb des Unternehmens mit Mitarbeiterdaten nicht geboten.

- Die Zollbehörden werden aufgefordert, die rechtsstaatlichen Vorgaben im Rahmen der AEO-Zertifizierung zu beachten. Eine einheitliche Praxis nach diesen Vorgaben gibt den Unternehmen Rechtssicherheit.

- Die Bundesregierung wird gebeten, die derzeitige AEO-Zertifizierungspraxis einer baldigen und umfassenden Evaluation zu unterziehen.

23.7 Anonymes und pseudonymes elektronisches Bezahlen von Internet-Angeboten ermöglichen!

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 22./23. November 2011)

Die Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich haben zur Kenntnis genommen, dass zahlreiche Internet-Anbieter planen, ihre Geschäftsmodelle so umzustellen, dass ihre Angebote – insbesondere Informationsdienste und Medieninhalte – nicht mehr nur werbefinanziert, sondern auch gegen Bezahlung angeboten werden. Das darf nicht dazu führen, dass den Nutzern die Möglichkeit genommen wird, sich im Internet anonym zu bewegen und Inhalte zur Kenntnis zu nehmen, ohne dass sie sich identifizieren müssen.

Das Recht, sich möglichst anonym aus öffentlichen Quellen zu informieren, ist durch das Recht auf informationelle Selbstbestimmung und durch Artikel 5 GG (Recht auf Informationsfreiheit) verfassungsrechtlich geschützt. Dementsprechend ist in § 13 Abs. 6 Telemediengesetz vorgeschrieben, dass die Möglichkeit bestehen muss, Telemedien anonym oder unter Pseudonym zu nutzen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

Diese Rechte sind in Gefahr, wenn Daten über die Nutzung einzelner Medienangebote entstehen. Wenn Inhalte gegen Bezahlung angeboten werden sollen, muss verhindert werden, dass personenbeziehbare Daten über jeden einzelnen Abruf von Beiträgen aus Online-Zeitungen oder einzelner Sendungen im Internet-TV entstehen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern die Anbieter von Telemedien auf, ihren gesetzlichen Verpflichtungen aus § 13 Abs. 6 des Telemediengesetzes bei der Einführung von kostenpflichtigen Inhalten nachzukommen. Es muss ein Bezahlungsverfahren angeboten werden, das „auf der ganzen Linie“ anonym oder mindestens pseudonym ausgestaltet ist. Eine Zahlung über pseudonyme Guthabenkarten würde die datenschutzrechtlichen Anforderungen erfüllen. Es reicht dagegen nicht aus, wenn sich z. B. der Inhalteanbieter für die Abwicklung der Zahlverfahren eines Dritten bedient und dieser eine Identifizierung der Betroffenen verlangt.

Die Kreditwirtschaft hat es bisher versäumt, datenschutzgerechte Verfahren mit ausreichender Breitenwirkung anzubieten oder zu unterstützen. Die Aufsichtsbehörden fordern diese auf, zu überprüfen, inwieweit bereits im Umlauf befindliche elektronische Zahlungsmittel (wie z.B. die Geldkarte) zu einem zumindest pseudonymen Zahlungsmittel für Telemedien weiterentwickelt werden können. Dies könnte z. B. durch die

Ausgabe nicht personengebundener „White Cards" erfolgen, die über Einzahlungsautomaten bei Banken und anderen Kreditinstituten anonym aufgeladen werden können.

Schließlich nehmen die Aufsichtsbehörden mit Sorge zur Kenntnis, dass ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) die Gefahr birgt, dass das anonyme elektronische Bezahlen gesetzlich unterbunden wird. Die Intention des Telemediengesetzes, die pseudonyme bzw. anonyme Nutzung von Telemedien zu ermöglichen, würde zunichte gemacht. Die Aufsichtsbehörden unterstützen die Forderung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München, die Möglichkeit zum elektronischen anonymen Bezahlen insbesondere für Kleinbeträge (sog. „Micropayment") zu erhalten.

23.8 Datenschutz in sozialen Netzwerken

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 8. Dezember 2011)

Der Düsseldorfer Kreis sieht die Bemühungen von Betreibern von sozialen Netzwerken als Schritt in die richtige Richtung an, durch Selbstverpflichtungen den Datenschutz von Betroffenen zu verbessern. Er unterstreicht, dass eine Anerkennung von Selbstverpflichtungen durch die Datenschutzaufsichtsbehörden gemäß § 38a Bundesdatenschutzgesetz (BDSG) die Gewähr dafür bietet, dass die Anforderungen des geltenden Datenschutzrechts erfüllt werden und ein Datenschutzmehrwert entsteht.

Ungeachtet dieser allgemeinen Bemühungen um eine Verbesserung des Datenschutzes in sozialen Netzwerken müssen die Betreiber schon heute das Datenschutzrecht in Deutschland beachten. Für deutsche Betreiber ist dies unumstritten. Aber auch Anbieter, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, unterliegen hinsichtlich der Daten von Betroffenen in Deutschland gemäß § 1 Abs. 5 Satz 2 BDSG dem hiesigen Datenschutzrecht, soweit sie ihre Datenerhebungen durch Rückgriff auf Rechner von Nutzerinnen und Nutzern in Deutschland realisieren. Dies ist regelmäßig der Fall. Die Anwendung des BDSG kann in diesen Fällen nicht durch das schlichte Gründen einer rechtlich selbstständigen Niederlassung in einem anderen Staat des Europäischen Wirtschaftsraumes umgangen werden (§ 1 Abs. 5 Satz 1 BDSG). Nur wenn das soziale Netzwerk auch in der Verantwortung dieser europäischen Niederlassung betrieben wird, kann die Verarbeitung der Daten deutscher Nutzerinnen und Nutzer unter Umständen dem Datenschutzrecht eines anderen Staates im Europäischen Wirtschaftsraum unterliegen.

Betreiber von sozialen Netzwerken müssen insbesondere folgende Rechtmäßigkeitsanforderungen beachten, wenn sie in Deutschland aktiv sind:

- Es muss eine leicht zugängliche und verständliche Information darüber gegeben werden, welche Daten erhoben und für welche Zwecke verarbeitet werden. Denn nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft bzw. informierte Einwilligungen gewährleisten die Wahrung des

Rechts auf informationelle Selbstbestimmung. Die Voreinstellungen des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, ist nicht gesetzmäßig.

- Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können.

- Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne ausdrückliche und bestätigte Einwilligung der abgebildeten Person unzulässig.

- Das Telemediengesetz erfordert jedenfalls pseudonyme Nutzungsmöglichkeiten in sozialen Netzwerken. Es enthält im Hinblick auf Nutzungsdaten - soweit keine Einwilligung vorliegt - ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen.

- Das direkte Einbinden von Social Plugins, beispielsweise von Facebook, Google+ oder Twitter, in Websites deutscher Anbieter, wodurch eine Datenübertragung an den jeweiligen Anbieter des Social Plugins ausgelöst wird, ist ohne hinreichende Information der Internetnutzerinnen und -nutzer und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden, unzulässig.

- Die großen Mengen an teils auch sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben.

- Daten von Minderjährigen sind besonders zu schützen. Datenschutzfreundlichen Standardeinstellungen kommt im Zusammenhang mit dem Minderjährigenschutz besondere Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und also auch für diese leicht verständlich sein.

- Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen gemäß § 1 Abs. 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

In Deutschland ansässige Unternehmen, die durch das Einbinden von Social Plugins eines Netzwerkes auf sich aufmerksam machen wollen oder sich mit Fanpages in einem Netzwerk präsentieren, haben eine eigene Verantwortung hinsichtlich der Daten von Nutzerinnen und Nutzern ihres Angebots. Es müssen zuvor Erklärungen eingeholt werden, die eine Verarbeitung von Daten ihrer Nutzerinnen und Nutzer durch

den Betreiber des sozialen Netzwerkes rechtfertigen können. Die Erklärungen sind nur dann rechtswirksam, wenn verlässliche Informationen über die dem Netzwerkbetreiber zur Verfügung gestellten Daten und den Zweck der Erhebung der Daten durch den Netzwerkbetreiber gegeben werden können.

Anbieter deutscher Websites, die in der Regel keine Erkenntnisse über die Datenverarbeitungsvorgänge haben können, die beispielsweise durch Social Plugins ausgelöst werden, sind regelmäßig nicht in der Lage, die für eine informierte Zustimmung ihrer Nutzerinnen und Nutzer notwendige Transparenz zu schaffen. Sie laufen Gefahr, selbst Rechtsverstöße zu begehen, wenn der Anbieter eines sozialen Netzwerkes Daten ihrer Nutzerinnen und Nutzer mittels Social Plugin erhebt. Wenn sie die über ein Plugin mögliche Datenverarbeitung nicht überblicken, dürfen sie daher solche Plugins nicht ohne weiteres in das eigene Angebot einbinden.

23.9 Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 17. Januar 2012)

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen. Der Text lautet wie folgt:

Einwilligung in die Erhebung und Verwendung von Gesundheitsdaten und Schweigepflichtentbindungserklärung[28]:

Die Regelungen des Versicherungsvertragsgesetzes, des Bundesdatenschutzgesetzes sowie anderer Datenschutzvorschriften enthalten keine ausreichenden Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen. Um Ihre Gesundheitsdaten für diesen Antrag und den Vertrag erheben und verwenden zu dürfen, benötigt die Versicherung XY[29] daher Ihre datenschutzrechtliche(n) Einwilligung(en). Darüber hinaus benötigt die Versicherung XY Ihre Schweigepflichtentbindungen, um Ihre Gesundheitsdaten bei schweigepflichtigen Stellen, wie z.B. Ärzten, erheben zu dürfen. Als Unternehmen der Lebensversicherung (Krankenversicherung)[30] benötigt die Versicherung XY Ihre Schweigepflichtentbindung ferner, um Ihre Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch ge-

[28] Der Text der Einwilligungs-/Schweigepflichtentbindungserklärung wurde 2011 mit den Datenschutzaufsichtsbehörden inhaltlich abgestimmt.

[29] Hier und im Folgenden kann anstelle von „die Versicherung XY" der Name des verwendenden Unternehmens oder nach einmaliger Nennung (etwa „wir, die Versicherung XY") jeweils „wir" eingefügt werden.

[30] Hier kann die konkrete Sparte genannt werden.

schützte Daten, wie z. B. die Tatsache, dass ein Vertrag mit Ihnen besteht, an andere Stellen, z. B.[31] weiterleiten zu dürfen.

Die folgenden Einwilligungs- und Schweigepflichtentbindungserklärungen[32] sind für die Antragsprüfung sowie die Begründung, Durchführung oder Beendigung Ihres Versicherungsvertrages in der Versicherung XY unentbehrlich. Sollten Sie diese nicht abgeben, wird der Abschluss des Vertrages in der Regel nichtmöglich sein.[33]

Die Erklärungen betreffen den Umgang mit Ihren Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

- durch die Versicherung XY [Versicherungsgesellschaft, mit der der Versicherungsvertrag abgeschlossen wird] selbst (unter 1.),
- im Zusammenhang mit der Abfrage bei Dritten (unter 2.),
- bei der Weitergabe an Stellen außerhalb der Versicherung XY (unter 3.) und
- wenn der Vertrag nicht zustande kommt (unter 4.).

Die Erklärungen gelten für die von Ihnen gesetzlich vertretenen Personen wie Ihre Kinder, soweit diese die Tragweite dieser Einwilligung nicht erkennen und daher keine eigenen Erklärungen abgeben können.[34]

1. Erhebung, Speicherung und Nutzung der von Ihnen mitgeteilten Gesundheitsdaten durch die Versicherung XY

Ich willige ein, dass die Versicherung XY die von mir in diesem Antrag und künftig mitgeteilten Gesundheitsdaten erhebt, speichert und nutzt, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Versicherungsvertrages erforderlich ist.

---

[31] Das Beispiel soll verdeutlichen, dass Versicherer diese Daten nicht willkürlich an x-beliebige Stellen weitergeben. Daher können hier einige für die verwendende Versicherung typische Beispiele genannt werden, die die Breite der Weitergabemöglichkeiten erkennen lassen, wie z. B. Assistancegesellschaften, HIS-Betreiber oder IT-Dienstleister.

[32] Die Klausel ist zunächst nur für Kranken-, Lebens- und Berufsunfähigkeitsversicherungen zu verwenden, weil in diesen Sparten von Vertragsbeginn an Gesundheitsdaten erhoben und verwendet werden. In anderen Sparten ist der Text entsprechend anzupassen und ggf. nur auszugsweise zu verwenden. In Abstimmung mit den Sparten Unfall und Haftpflicht wird den Unternehmen ein angepasster Vorschlag zur Verfügung gestellt.

[33] Verweis auf die Folgen der Verweigerung der Einwilligung gemäß § 4a Abs. 1 Satz 2 BDSG

[34] Werden bei einem Versicherungsprodukt generell keine Kinder und / oder gesetzlich vertretende Personen mitversichert, ist der Absatz bzw. der entsprechende Satz zu streichen. Werden Kinder oder andere gesetzlich vertretene Personen mitversichert, unterschreiben diese ab dem 16. Lebensjahr eine eigene Erklärung, wenn davon auszugehen ist, dass diese einsichtsfähig sind. Diese Erklärung ist aus zivilrechtlichen Gründen auch vom gesetzlichen Vertreter (in der Regel dem Versicherungsnehmer) zu unterzeichnen(siehe unten, Unterschriftenfelder). Damit verbleibt die Entscheidung über das tatsächliche Bestehen der Einsichtsfähigkeit bei dem gesetzlichen Vertreter.

2. Abfrage von Gesundheitsdaten bei Dritten

2.1. Abfrage von Gesundheitsdaten bei Dritten zur Risikobeurteilung und zur Prüfung der Leistungspflicht[35]

Für die Beurteilung der zu versichernden Risiken kann es notwendig sein, Informationen von Stellen abzufragen, die über Ihre Gesundheitsdaten verfügen. Außerdem kann es zur Prüfung der Leistungspflicht erforderlich sein, dass die Versicherung XY die Angaben über Ihre gesundheitlichen Verhältnisse prüfen muss, die Sie zur Begründung von Ansprüchen gemacht haben oder die sich aus eingereichten Unterlagen (z. B. Rechnungen, Verordnungen, Gutachten) oder Mitteilungen z. B. eines Arztes oder sonstigen Angehörigen eines Heilberufs ergeben.

Diese Überprüfung erfolgt nur, soweit es erforderlich ist. Die Versicherung XY benötigt hierfür Ihre Einwilligung einschließlich einer Schweigepflichtentbindung für sich sowie für diese Stellen, falls im Rahmen dieser Abfragen Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Informationen weitergegeben werden müssen.

Sie können diese Erklärungen bereits hier (I) oder später im Einzelfall (II) erteilen. Sie können Ihre Entscheidung jederzeit ändern. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:

Möglichkeit I:

☐ Ich willige ein, dass die Versicherung XY – soweit es für die Risikobeurteilung oder für die Leistungsfallprüfung erforderlich ist – meine Gesundheitsdaten bei Ärzten, Pflegepersonen sowie bei Bediensteten von Krankenhäusern, sonstigen Krankenanstalten, Pflegeheimen, Personenversicherern, gesetzlichen Krankenkassen, Berufsgenossenschaften und Behörden[36] erhebt und für diese Zwecke verwendet.

Ich befreie die genannten Personen und Mitarbeiter der genannten Einrichtungen von ihrer Schweigepflicht, soweit meine zulässigerweise gespeicherten Gesundheitsdaten aus Untersuchungen, Beratungen, Behandlungen sowie Versicherungsanträgen und -verträgen aus einem Zeitraum von bis zu zehn Jahren[37] vor Antragstellung an die Versicherung XY übermittelt werden.

Ich bin darüber hinaus damit einverstanden, dass in diesem Zusammenhang – soweit erforderlich – meine Gesundheitsdaten durch die Versicherung XY an diese Stellen weitergegeben werden und befreie auch insoweit die für die Versicherung XY tätigen Personen von ihrer Schweigepflicht.

---

[35] Wenn Unternehmen stets eine Einwilligung im Einzelfall einholen, wird Ziffer 2.1 gestrichen und der Erläuterungstext über dem grauen Kasten wird für die Einzelfalleinwilligung entsprechend angepasst.

[36] Der 2008 in Kraft getretene § 213 VVG führt enumerativ die Stellen auf, bei denen der Versicherer mit Einwilligung des Betroffenen dessen Gesundheitsdaten erheben darf. Hinsichtlich der fehlenden sonstigen Heilberufe (Heilpraktiker, Physiotherapeut, Psychotherapeut) sowie der Versicherer, die keine Personenversicherer im herkömmlichen Sprachgebrauch sind, aber dennoch zur Regulierung von Personenschäden Gesundheitsdaten verarbeiten, wird § 213 VVG weit ausgelegt, vgl. auch Eberhardt in: Münchener Kommentar, § 213 VVG, Rn. 35-40.

[37] Entsprechend der Annahmepolitik der Versicherungsunternehmen kann für alle oder bestimmte Antragsfragen ein kürzerer Zeitraum zugrunde gelegt werden.

Ich werde vor jeder Datenerhebung nach den vorstehenden Absätzen unterrichtet, von wem und zu welchem Zweck die Daten erhoben werden sollen, und ich werde darauf hingewiesen, dass ich widersprechen und die erforderlichen Unterlagen selbst beibringen kann[38].

Möglichkeit II:

☐ Ich wünsche, dass mich die Versicherung XY in jedem Einzelfall informiert, von welchen Personen oder Einrichtungen zu welchem Zweck eine Auskunft benötigt wird. Ich werde dann jeweils entscheiden,

- ob ich in die Erhebung und Verwendung meiner Gesundheitsdaten durch die Versicherung XY einwillige, die genannten Personen oder Einrichtungen sowie deren Mitarbeiter von ihrer Schweigepflicht entbinde und in die Übermittlung meiner Gesundheitsdaten an die Versicherung XY einwillige
- oder die erforderlichen Unterlagen selbst beibringe.

Mir ist bekannt, dass dies zu einer Verzögerung der Antragbearbeitung oder der Prüfung der Leistungspflicht führen kann.

Soweit sich die vorstehenden Erklärungen auf meine Angaben bei Antragstellung beziehen, gelten sie für einen Zeitraum von fünf Jahren[39] nach Vertragsschluss. Ergeben sich nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte[40] dafür, dass bei der Antragstellung vorsätzlich unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde, gelten die Erklärungen bis zu zehn Jahre nach Vertragsschluss.

2.2. Erklärungen für den Fall Ihres Todes

Zur Prüfung der Leistungspflicht kann es auch nach Ihrem Tod erforderlich sein, gesundheitliche Angaben zu prüfen. Eine Prüfung kann auch erforderlich sein, wenn sich bis zu zehn Jahre nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte dafür ergeben, dass bei der Antragstellung unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde. Auch dafür bedürfen wir einer Einwilligung und Schweigepflichtentbindung. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:[41]

---

[38] Umsetzung der Unterrichtungs- und Hinweispflicht nach § 213 Abs. 2 S. 2 i.V.m. Abs. 4 VVG

[39] Bei der privaten Krankenversicherung ist wegen § 194 Abs. 1 Satz 4 VVG eine Frist von drei Jahren einzusetzen. Bei vorsätzlichem Verhalten gilt auch für die PKV die Zehn-Jahresfrist.

[40] Anhaltspunkte für vorsätzlich falsche Angaben können sich etwa aus Unstimmigkeiten zwischen der Erkrankung und den Angaben im Antrag ergeben. Eine Überprüfung kann dann ergeben, dass es am Vorsatz fehlt und die Datenerhebung für den Betroffenen keine negativen Konsequenzen hat.

[41] Bei Abschnitt 2.2 ist es möglich, das zweite Ankreuzfeld nicht zu nutzen, sodass keine Wahlmöglichkeit besteht und nur das erste Feld angekreuzt werden kann. Der letzte erläuternde Satz vor dem grau unterlegten Feld entfällt dann. Wird das erste (einzige) Ankreuzfeld dann nicht angekreuzt, würde bei einer gerichtlichen Prüfung entweder eine andere Willenserklärung herangezogen (z.B. Testament) oder bei Fehlen einer solchen auf den mutmaßlichen Willen des Betroffenen abgestellt. Ein

Möglichkeit I:

□ Für den Fall meines Todes willige ich in die Erhebung meiner Gesundheitsdaten bei Dritten zur Leistungsprüfung bzw. einer erforderlichen erneuten Antragsprüfung ein wie im ersten Ankreuzfeld beschrieben (siehe oben 2.1. – Möglichkeit I).

Möglichkeit II:

□ Soweit zur Prüfung der Leistungspflicht bzw. einer erforderlichen erneuten Antragsprüfung nach meinem Tod Gesundheitsdaten erhoben werden müssen, geht die Entscheidungsbefugnis über Einwilligungen und Schweigepflichtentbindungserklärungen auf meine Erben oder – wenn die se abweichend bestimmt sind – auf die Begünstigten des Vertrags über.

3. Weitergabe Ihrer Gesundheitsdaten und weiterer nach § 203 StGB geschützter Daten an Stellen außerhalb der Versicherung XY

Die Versicherung XY verpflichtet die nachfolgenden Stellen vertraglich auf die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit[42].

3.1. Datenweitergabe zur medizinischen Begutachtung

Für die Beurteilung der zu versichernden Risiken und zur Prüfung der Leistungspflicht kann es notwendig sein, medizinische Gutachter einzuschalten. Die Versicherung XY benötigt Ihre Einwilligung und Schweigepflichtentbindung, wenn in diesem Zusammenhang Ihre Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten übermittelt werden. Sie werden über die jeweilige Datenübermittlung unterrichtet[43].

---

automatischer Übergang der höchstpersönlichen Verfügungsbefugnis auf Erben oder Bezugsberechtigte des Vertrags erfolgt regelmäßig nicht. Bei Anbieten einer echten Wahlmöglichkeit und einem vorliegenden Kreuz erscheint der Bestand der Erklärungen vor Gericht als wahrscheinlicher, sodass die Bezugnahme auf den mutmaßlichen Willen in einem möglichen Zivilprozess nicht nötig erscheint.

42 Die vertragliche Verpflichtung auf Einhaltung von Datenschutz und Datensicherheit auch für Stellen, die eigenverantwortlich Aufgaben übernehmen, ergibt sich aus dem künftigen Art. 21 Abs. 4 Code of Conduct (CoC). Diese Verpflichtung wurde dort für die Funktionsübertragung an Dienstleister als datenschutzrechtlicher Mehrwert für die Betroffenen vereinbart. Rückversicherer werden nicht als Dienstleister des Erstversicherers im Sinne von Art. 21 angesehen, wenn sie den Erstversicherer im Rahmen von Rückversicherungsverträgen bei der Risiko- und Leistungsprüfung unterstützen. Sofern der Erstversicherer Rückversicherer außerhalb von Rückversicherungsverträgen als Dienstleister einsetzt und diese noch nicht vertraglich auf die Einhaltung von Datenschutz und Datensicherheit verpflichtet hat, ist dies nachzuholen (vgl. auch Hinweis 18).

43 Die Unterrichtungspflicht wurde aufgenommen, um mehr Transparenz zu schaffen. Hierfür ist mitzuteilen, welche konkreten Daten, für welchen Zweck, an welche Stelle übermittelt werden sollen.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten an medizinische Gutachter übermittelt, soweit dies im Rahmen der Risikoprüfung oder der Prüfung der Leistungspflicht erforderlich ist und meine Gesundheitsdaten dort zweckentsprechend verwendet und die Ergebnisse an die Versicherung XY zurück übermittelt werden. Im Hinblick auf meine Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten entbinde ich die für die Versicherung XY tätigen Personen und die Gutachter von ihrer Schweigepflicht.

3.2. Übertragung von Aufgaben auf andere Stellen (Unternehmen oder Personen)

Die Versicherung XY führt bestimmte Aufgaben, wie zum Beispiel die Risikoprüfung, die Leistungsfallbearbeitung oder die telefonische Kundenbetreuung, bei denen es zu einer Erhebung, Verarbeitung oder Nutzung Ihrer Gesundheitsdaten kommen kann, nicht selbst durch, sondern überträgt die Erledigung einer anderen Gesellschaft der XY-Gruppe oder einer anderen Stelle. Werden hierbei Ihre nach § 203 StGB geschützten Daten weitergegeben, benötigt die Versicherung XY Ihre Schweigepflichtentbindung für sich und[44] soweit erforderlich für die anderen Stellen[45].

Die Versicherung XY führt eine fortlaufend aktualisierte Liste[46] über die Stellen[47]und Kategorien von Stellen[48], die vereinbarungsgemäß Gesundheitsdaten für die Versicherung XY erheben, verarbeiten oder nutzen unter Angabe der übertragenen Aufgaben. Die zurzeit gültige Liste ist als Anlage der Einwilligungserklärung angefügt[49]. Eine aktuelle Liste kann auch im Internet unter (Internetadresse) eingesehen oder bei (Ansprechpartner nebst Anschrift, Telefonnummer, ggf. E-Mailadresse) angefordert werden. Für die Weitergabe Ihrer Gesundheitsdaten an und die Verwendung durch die in der Liste genannten Stellen benötigt die Versicherung XY Ihre Einwilligung.

---

[44] Der Satzteil "für sich und" ist nur für die Kranken, Leben- und Unfallversicherung zu verwenden.

[45] Die Mitarbeiter anderer Stellen werden von ihrer Schweigepflicht entbunden, wenn sie ihrerseits im Rahmen der von ihnen zu erledigenden Aufgaben nach § 203 StGB geschützte Daten an den Versicherer oder an andere Stellen, wie z. B. mit der IT-Wartung beauftragte Subunternehmen weitergeben.

[46] In der Liste werden die Stellen und Kategorien von Stellen aufgezählt, die Gesundheitsdaten erheben, verarbeiten oder nutzen. Ebenfalls gemeint sind Stellen und Kategorien von Stellen, die einfache personenbezogene Daten, die nach § 203 StGB geschützt sind, wie z. B. die Information, dass ein Lebensversicherungsvertrag besteht, verwenden. Nicht gemeint sind Stellen, die im Rahmen der ihnen zugewiesenen Aufgaben keine Gesundheitsdaten verarbeiten, diese aber theoretisch einsehen können (Bsp. Personen oder Unternehmen, die mit der IT-Wartung betraut sind). In die Liste werden sowohl Dritte im datenschutzrechtlichen Sinn als auch Auftragdatenverarbeiter, bei denen Abgrenzungsschwierigkeiten zur Funktionsübertragung bestehen (siehe Endnote 23), aufgenommen. Rückversicherer werden als Dienstleister des Erstversicherers angesehen, wenn sie ohne einen Rückversicherungsvertrag nur als Dienstleister des Erstversicherers tätig werden.

[47] Werden Aufgaben im Wesentlichen von einem Unternehmen an ein anderes Unternehmen der XY-Versicherungsgruppe oder an eine externe Stelle abgegeben, ist die andere Stelle namentlich anzugeben unter Bezeichnung der Aufgabe. Hierunter fallen z. B. Stellen, die die Aufgaben Risikoprüfung, Leistungsfallbearbeitung oder Serviceleistung für das Unternehmen übernehmen.

[48] Fehlt es an einer systematischen automatisierten Datenverarbeitung, können die Stellen, an die Gesundheitsdaten weitergegeben werden bzw. die zur Erfüllung ihrer Aufgabe selbst Gesundheitsdaten erheben, in Kategorien zusammengefasst werden unter Bezeichnung der Aufgabe. Dies gilt auch für Stellen, die nur einmalig tätig werden, wie z.B. Krankentransporte.

[49] Die Liste der Dienstleister soll in der Form, in der die Einwilligungs- und Schweigepflichtentbindungserklärung erteilt wird, als Anlage mitgegeben werden.

Ich willige ein[50], dass die Versicherung XY meine Gesundheitsdaten an die in der oben erwähnten Liste genannten Stellen übermittelt und dass die Gesundheitsdaten dort für die angeführten Zwecke im gleichen Umfang erhoben, verarbeitet und genutzt werden, wie die Versicherung XY dies tun dürfte. Soweit erforderlich, entbinde ich die Mitarbeiter der XY Unternehmensgruppe und sonstiger Stellen[51] im Hinblick auf die Weitergabe von Gesundheitsdaten und anderer nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.3. Datenweitergabe an Rückversicherungen

Um die Erfüllung Ihrer Ansprüche abzusichern, kann die Versicherung XY Rückversicherungen einschalten, die das Risiko ganz oder teilweise übernehmen. In einigen Fällen bedienen sich die Rückversicherungen dafür weiterer Rückversicherungen, denen sie ebenfalls Ihre Daten[52] übergeben. Damit sich die Rückversicherung ein eigenes Bild über das Risiko oder den Versicherungsfall machen kann, ist es möglich, dass die Versicherung XY Ihren Versicherungsantrag oder Leistungsantrag der Rückversicherung vorlegt. Das ist insbesondere dann der Fall, wenn die Versicherungssumme besonders hoch ist oder es sich um ein schwierig einzustufendes Risiko handelt.

Darüber hinaus ist es möglich, dass die Rückversicherung die Versicherung XY aufgrund ihrer besonderen Sachkunde bei der Risiko- oder Leistungsprüfung sowie bei der Bewertung von Verfahrensabläufen unterstützt.

Haben Rückversicherungen die Absicherung des Risikos übernommen, können sie kontrollieren, ob die Versicherung XY das Risiko bzw. einen Leistungsfall richtig eingeschätzt hat.

Außerdem werden Daten über Ihre bestehenden Verträge und Anträge im erforderlichen Umfang an Rückversicherungen weitergegeben, da mit diese überprüfen können, ob und in welcher Höhe sie sich an dem Risiko beteiligen können[53]. Zur Abrechnung von Prämienzahlungen und Leistungsfällen können Daten über Ihre bestehenden Verträge an Rückversicherungen weitergegeben werden.

Zu den oben genannten Zwecken werden möglichst anonymisierte bzw. pseudonymisierte Daten, jedoch auch personenbezogene Gesundheitsangaben verwendet.

Ihre personenbezogenen Daten werden von den Rückversicherungen nur zu den vorgenannten Zwecken verwendet. Über die Übermittlung

---

[50] Die Einwilligung gilt in jedem Fall für die Datenübermittlung an eigenverantwortliche Dienstleister. Sie ist außerdem bei Abgrenzungsschwierigkeiten zwischen Auftragsdatenverarbeitung und Funktionsübertragung einzuholen. Das Einwilligungserfordernis gilt nicht, wenn es sich in Übereinstimmung mit der zuständigen Datenschutzaufsichtsbehörde um eine eindeutige Auftragsdatenverarbeitung handelt. In diesen Fällen sollte dennoch eine Schweigepflichtentbindung eingeholt werden.

[51] „und sonstige Stellen" – Dieser Passus wird gestrichen, wenn keine schweigepflichtgebundenen Dienstleister und Auftragnehmer eingeschaltet sind.

[52] Sollen Gesundheitsdaten an den Rückversicherer des Rückversicherers übermittelt werden, ist eine spezielle Einwilligung zu prüfen.

[53] Für die Kumulkontrolle ist eine Schweigepflichtentbindung erforderlich, da nach § 203 StGB geschützte Daten weitergegeben werden, jedoch keine Gesundheitsdaten.

Ihrer Gesundheitsdaten an Rückversicherungen werden Sie durch die Versicherung XY unterrichtet[54].

Ich willige ein, dass meine Gesundheitsdaten – soweit erforderlich – an Rückversicherungen übermittelt und dort zu den genannten Zwecke n verwendet werden. Soweit erforderlich, entbinde ich die für die Versicherung XY tätigen Personen im Hinblick auf die Gesundheitsdaten und weiteren nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.4. Datenaustausch mit dem Hinweis- und Informationssystem (HIS)[55]

Die Versicherungswirtschaft nutzt zur genaueren Risiko- und Leistungsfalleinschätzung das Hinweis- und Informationssystem HIS, das derzeit die informa Insurance Risk and Fraud Prevention GmbH (informa IRFP GmbH, Rheinstraße 99, 76532 Baden-Baden, www.informa-irfp.de) betreibt. Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten, und erhöhte Risiken kann die Versicherung XY an das HIS melden. Die Versicherung XY und andere Versicherungen fragen Daten im Rahmen der Risiko- oder Leistungsprüfung aus dem HIS ab, wenn ein berechtigtes Interesse besteht[56]. Zwar werden dabei keine Gesundheitsdaten weitergegeben, aber für eine Weitergabe Ihrer nach § 203 StGB geschützten Daten benötigt die Versicherung XY Ihre Schweigepflichtentbindung. Dies gilt unabhängig davon, ob der Vertrag mit Ihnen zustande gekommen ist oder nicht.

Ich entbinde die für Versicherung XY tätigen Personen von ihrer Schweigepflicht, soweit sie Daten aus der Antrags- oder Leistungsprüfung an den jeweiligen Betreiber des Hinweis- und Informationssystems (HIS)[57] melden.

Sofern es zur Prüfung der Leistungspflicht erforderlich ist, können über das HIS Versicherungen ermittelt werden, mit denen Sie in der Vergangenheit in Kontakt gestanden haben, und die über sachdienliche Informationen verfügen könnten. Bei diesen können die zur weiteren Leistungsprüfung erforderlichen Daten erhoben werden (siehe unter Ziff. 2.1).

---

[54] Die Unterrichtungspflicht des Erstversicherers ersetzt die anderenfalls von den Datenschutzbehörden geforderte ausführliche Erklärung entsprechend dem Baustein 2.1. zur Erhebung von Gesundheitsdaten bei Dritten. Zu unterrichten ist über die konkret übermittelten Daten, den Zweck der Übermittlung und den Empfänger der Daten.

[55] Da keine einwilligungsbedürftigen besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG (Gesundheitsdaten) an das HIS gemeldet werden, betrifft die Schweigepflichtentbindung nur die nach § 203 StGB geschützten Daten, hier etwa die Tatsache, dass ein Versicherungsvertrag besteht. Da nur die Sparten Unfall und Leben von § 203 Abs. 1 Nr. 6 StGB erfasst werden und mit dem HIS arbeiten, ist der Passus für die anderen Sparten zu streichen. Im Fall der Nutzung ist die Information des Versicherungsnehmers über das Hinweis- und Informationssystem dann in anderer Weise sicherzustellen. Soweit Gesundheitsdaten im Leistungsfall im Rahmen der Detailanfrage ausgetauscht werden, gelten die Einwilligungserklärungen unter 2.1.

[56] Ein berechtigtes Interesse für die Abfrage zum Zweck der Risiko- und Leistungsprüfung ist stets gegeben mit Ausnahme des Erlebensfalls in der Lebensversicherung.

[57] Durch die Formulierung „an den jeweiligen Betreiber" sowie die Aufnahme von „derzeit" im ersten Satz des erläuternden Textes wird deutlich gemacht, dass sich der Betreiber des HIS ändern kann. Die Schweigepflichtentbindungserklärung soll auch künftige Betreiber erfassen.

3.5. Datenweitergabe an selbstständige Vermittler

Die Versicherung XY gibt grundsätzlich keine Angaben zu Ihrer Gesundheit an selbstständige Vermittler weiter. Es kann aber in den folgenden Fällen dazu kommen, dass Daten, die Rückschlüsse auf Ihre Gesundheit zulassen, oder gemäß § 203 StGB geschützte Informationen über Ihren Vertrag Versicherungsvermittlern zur Kenntnis gegeben werden.

Soweit es zu vertragsbezogenen Beratungszwecken erforderlich ist, kann der Sie betreuende Vermittler Informationen darüber erhalten, ob und ggf. unter welchen Voraussetzungen (z. B. Annahme mit Risikozuschlag, Ausschlüsse bestimmter Risiken) Ihr Vertrag angenommen werden kann.

Der Vermittler, der Ihren Vertrag vermittelt hat, erfährt, dass und mit welchem Inhalt der Vertrag abgeschlossen wurde. Dabei erfährt er auch, ob Risikozuschläge oder Ausschlüsse bestimmter Risiken vereinbart wurden.

Bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler kann es zur Übermittlung der Vertragsdaten mit den Informationen über bestehende Risikozuschläge und Ausschlüsse bestimmter Risiken an den neuen Vermittler kommen. Sie werden bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler vor der Weitergabe von Gesundheitsdaten informiert sowie auf Ihre Widerspruchsmöglichkeit hingewiesen.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten und sonstigen nach § 203 StGB geschützten Daten in den oben genannten Fällen – soweit erforderlich – an den für mich zuständigen selbstständigen Versicherungsvermittler übermittelt und diese dort erhoben, gespeichert und zu Beratungszwecken genutzt werden dürfen.

4. Speicherung und Verwendung Ihrer Gesundheitsdaten wenn der Vertrag nicht zustande kommt[58]

Kommt der Vertrag mit Ihnen nicht zustande, speichert die Versicherung XY Ihre im Rahmen der Risikoprüfung erhobenen Gesundheitsdaten für den Fall, dass Sie erneut Versicherungsschutz beantragen. Außerdem ist es möglich, dass die Versicherung XY zu Ihrem Antrag einen Vermerk an das Hinweis- und Informationssystem meldet, der an anfragende Versicherungen für deren Risiko- und Leistungsprüfung übermittelt wird (siehe Ziffer 3.4.). Die Versicherung XY speichert Ihre Daten auch, um mögliche Anfragen weiterer Versicherungen beantworten zu können. Ihre Daten werden bei der Versicherung XY und im Hinweis-

[58] Der Passus ist zu streichen, wenn eine Speicherung von Antragsdaten bei Nichtzustandekommen des Vertrags nicht erfolgt. Daten über nicht zustande gekommene Verträge sind bei dem Versicherungsunternehmen spätestens drei Jahre gerechnet vom Ende des Kalenderjahres nach Antragstellung zu löschen. Auch im Hinweis- und Informationssystem werden diese Daten entsprechend gelöscht. Gesetzliche Aufbewahrungspflichten oder –befugnisse bleiben hiervon unberührt. Werden Schadensersatzansprüche gegen das Unternehmen geltend gemacht oder bei Prüfungen durch Behörden kann sich eine längere Aufbewahrung auch aus § 28 Abs. 6 Nr. 3 BDSG rechtfertigen.

und Informationssystem bis zum Ende des dritten Kalenderjahres nach dem Jahr der Antragstellung[59] gespeichert.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten – wenn der Vertrag nicht zustande kommt – für einen Zeitraum von drei Jahren ab dem Ende des Kalenderjahres der Antragstellung zu den oben genannten Zwecken speichert und nutzt[60].

Hinweise zur Anwendung der Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung und Verwendung von Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

Der vorliegende Text einer Einwilligungs- und Schweigepflichtentbindungsklausel ist vom GDV mit den Datenschutzaufsichtsbehörden abgestimmt worden. Der Verbraucherzentrale Bundesverband war ebenfalls an den Gesprächen beteiligt. Die Klausel wird flankiert durch Verhaltensregeln für den Umgang mit personenbezogen en Daten in der Versicherungswirtschaft (Code of Conduct). Zweck ist, lediglich für die tatsächlich einwilligungsbedürftigen Datenerhebungs- und –verwendungsprozesse eine Einwilligungs- und Schweigepflichtentbindungserklärung einzuholen. Andere Datenverarbeitungen werden in einem Code of Conduct konkretisiert. Sowohl die Klausel als auch der Code of Conduct werden in regelmäßigen Abständen gemeinsam überarbeitet, um aktuelle Entwicklungen der Datenverarbeitung und gesetzliche Änderungen zu berücksichtigen.

Hinweise zur Klausel - BAUSTEINSYSTEM

Die Texte stellen einen maximalen Rahmen für Einwilligungs- und Schweigepflichtentbindungserklärungen dar. Wegen des im BDSG verankerten Prinzips der Datensparsamkeit sind nur die Textpassagen zu verwenden, die benötigt werden. Soweit im Rahmen einer Versicherungssparte oder eines Versicherungsprodukts bestimmte Datenverarbeitungen nicht erfolgen, wie etwa die Erhebung von Gesundheitsdaten bei Dritten zur Risikoprüfung, ist der Text entsprechend zu kürzen. Werden Datenverarbeitungen beschrieben, die das Unternehmen nicht durchführt oder nicht plant, wie zum Beispiel die Datenweitergabe zur medizinischen Begutachtung oder die Datenweitergabe an Rückversicherer, ist der entsprechende Absatz / Satz nicht zu verwenden.

Zu beachten ist dabei jedoch, dass die in Abschnitt 2.1. angebotenen Wahlmöglichkeiten bestehen bleiben müssen. Das heißt, wenn für die Datenerhebung bei Dritten mit dem Antrag eine Einwilligung eingeholt werden soll, müssen auch beide Alternativen (Pauschaleinwilligung / Einzelfalleinwilligung) angeboten werden. Erfolgt keine Wahl, muss spätestens unmittelbar vor der Datenerhebung eine Einwilligung eingeholt werden. Die dafür zu gestaltenden Erklärungen sollten sich an den hier vorliegenden orientieren.

Die vorliegende Einwilligungs- und Schweigepflichtentbindungsklausel bezieht sich auf Gesundheitsdaten und darüber hinaus auf weitere nach

[59] Es zählt das Datum der Unterschrift im Antrag.

[60] Die Nutzung ist nur zu eigenen Zwecken des Versicherers zulässig. Die Übermittlung an ein anderes Unternehmen ist nur auf der Basis einer von diesem einzuholenden Einwilligung/Schweigepflichtentbindung nach Ziffer 2.1. zulässig.

§ 203 Abs. 1 StGB geschützte Daten, wie die Tatsache des Bestehens eines Versicherungsvertrags. Gesundheitsdaten können in allen Versicherungssparten anfallen, auch dort, wo dies nicht sofort vermutet wird, z.B. in der Reisegepäckversicherung (Verletzungen durch Raub) und in der Kfz-Versicherung (Verletzungen durch Unfall). Die Einwilligungs- und Schweigepflichtentbindungserklärungen müssen vor der jeweils ersten Verarbeitung von Gesundheitsdaten im Unternehmen dem Antragsteller bzw. Versicherungsnehmer vorgelegt werden, soweit sie für bevorstehende Datenerhebungen, -verarbeitungen oder -nutzungen benötigt werden.

Sollen andere besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt werden, wie bspw. die Information über eine Gewerkschaftszugehörigkeit zur Prämienberechnung in speziellen Tarifen gewerkschaftsnaher Unternehmen, ist mit dem betreffenden Antrag eine entsprechende Einwilligungserklärung vom Antragsteller einzuholen. Diese kann z. B. wie folgt formuliert und gestaltet werden:

> Ich willige in die Erhebung, Verarbeitung und Nutzung meiner Angaben zur Gewerkschaftszugehörigkeit ein, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Vertrages, insbesondere zur Berechnung meiner Versicherungsprämie, erforderlich ist.

23.10 Near Field Communikation (NFC) bei Geldkarten

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 18./19. September 2012)

Es ist datenschutzrechtlich problematisch, wenn beim Einsatz von Near Field Communication (NFC) bei Geldkarten eine eindeutige Kartennummer, Geldbeträge und Transaktionshistorien unverschlüsselt von unberechtigten Dritten auslesbar sind. Die Geldkartenanbieter haben gemäß § 9 BDSG im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird.

Datenschutzrechtlich erstrebenswert ist die Einräumung einer Wahlmöglichkeit für die Betroffenen, ob sie eine Geldkarte mit NFC-Funktionalität einsetzen wollen. Insoweit nehmen die Aufsichtsbehörden die Ankündigung der Deutschen Kreditwirtschaft zur Kenntnis, das Kartenbetriebssystem so bald wie möglich so zu ändern, dass die Betroffenen die NFC-Funktionalität ein- und ausschalten können. Die Gefahr des (unbemerkten) unberechtigten Auslesens der Transaktionsdaten durch Dritte kann auch dadurch verringert werden, dass insofern nur das kontaktbehaftete Auslesen der Daten zugelassen wird.

Zudem sind die Vorgaben des § 6c BDSG zu beachten. Die Betroffenen müssen ausreichend informiert werden, insbesondere über die Funktionsweise des Mediums, die per NFC auslesbaren Daten, die Schutzmöglichkeiten für die Daten und ihre Rechte als Betroffene nach den §§ 34 und 35 BDSG.

24 Informationsfreiheitsgesetz

24.1 "Informationsfreiheit im Saarland – da kann ja jeder kommen!"

Seit 2006 besteht im Saarland gegenüber öffentlichen Stellen das Recht auf Zugang zu amtlichen Informationen, soweit keine überwiegenden schutzwürdigen Interessen entgegenstehen. Nicht mehr der Antragsteller muss begründen, weshalb er bestimmte Informationen haben möchte, sondern die Verwaltung muss begründen, weshalb im Ablehnungsfall gesetzliche Ausnahmetatbestände der Akteneinsicht entgegenstehen. Staatliches und kommunales Handeln soll durch diese Umkehrung des "Amtsgeheimnisses" transparenter werden.

Da dieses noch sehr junge Recht vielfach noch in der Anwendung unbekannt ist, haben wir am 24.10.2011 eine Fortbildungsveranstaltung für Hauptamtsleiter von Kommunen und Landkreisen angeboten, die auch ein reges Interesse fand.

Herr Sven Müller, ein ausgewiesener Experte aus Brandenburg, referierte über die Grundlagen für den Informationszugang nach dem Saarländische Informationsfreiheitsgesetz (SIFG) sowie den Spezialgesetzen (z.B. dem Umweltinformationsgesetz oder aus dem Sozialgesetzbuch).

Die spezialgesetzlichen Grundlagen fordern entweder eine Beteiligtenfähigkeit oder eine eingeschränkte Art der Informationen. Das Informationsfreiheitsrecht dagegen kann ohne Grund, ohne Anlass und ohne Begründung geltend gemacht werden.

24.1.1 Grundsätzliches zur Informationsfreiheit aus dem Vortrag vom 24.10.2011

Bis heute ist das Recht auf Informationsfreiheit wenig bekannt und selbst auf Bundesebene wird von der Anwendung des Informationsfreiheitsgesetzes des Bundes (IFG) eher zurückhaltend Gebrauch gemacht, wenn auch die Zahlen jährlich steigen. In Baden-Württemberg, Bayern, Hessen, Niedersachsen und Sachsen gibt es bislang noch kein Informationsfreiheitsgesetz.

Demgegenüber haben Bremen, Berlin und Hamburg die Informationszugangsrechte bereits erweitert um Vorschriften, die weitergehende aktive Informationspflichten für öffentliche Stellen normieren, um eine stärkere Transparenz in öffentlichen Institutionen, aber auch von Abläufen für den Bürger zu schaffen und damit die Demokratie und die Teilhabe des Bürgers am Staat zu stärken.

24.1.2 Fragen zur Anwendung des Gesetzes

Das Informationsfreiheitsgesetz gibt freien Zugang zu allen bei öffentlichen Stellen vorhandenen Informationen für „Jedermann“ ohne Voraussetzung.

Bei den Informationen nach dem IFG geht es um alle Informationen, die amtlichen Zwecken dienen – auch unabhängig von der Art der Speicherung. Lediglich Entwürfe, die nicht Aktenbestandteile werden, gehören nicht dazu. Das Bundesverwaltungsgericht hat klargestellt, dass der mit § 4 Abs. 1 Satz 1 IFG bezweckte Schutz des behördlichen Entscheidungsprozesses zeitlich begrenzt ist und spätestens mit dem Abschluss des Verfahrens endet.

Jeder Bürger ist berechtigt, unabhängig von seinem Wohnort und den rechtlichen oder berechtigten Interessen Informationen zu fordern. Der Antrag ist formlos möglich und muss nur, wenn es um personenbezogene Daten geht, begründet werden. Gegebenenfalls muss die öffentliche Stelle den Antragsteller unterstützen.

Auf Seiten der Kommunen gelten als Antragsgegner im Sinne des § 1 SIFG sowohl die Gemeinde selbst, Gemeindeverbände, aber auch die Eigenbetriebe, die Teil der Gemeinde sind. Es gilt der funktionelle Behördenbegriff, d.h. jede Stelle, die öffentliche Aufgaben wahrnimmt, ist Antragsgegner.

Die Anfrage soll unverzüglich bearbeitet werden; spätestens innerhalb eines Monats soll der Informationszugang erfolgen. Eine Untätigkeitsklage ist zulässig.

Grundsätzlich kann der Bürger entscheiden, ob er eine schriftliche oder mündliche Auskunft möchte oder ob Kopien gemacht werden sollen.

Die Ausnahmetatbestände sind im IFG abschließend geregelt und werden – so auch die Rechtsprechung – eng ausgelegt. Es geht dabei um den Schutz von besonderen öffentlichen Belangen nach den §§ 3 und 4 IFG, dem Schutz privater Belange nach den §§ 5 und 6 IFG und den Fragen der Aussonderungen nach § 7 Abs. 2 IFG.

Es können Kosten erhoben werden, die sich nach einer eigenen Gebührenordnung richten. Wir empfehlen den Bürgern vor Antragstellung nach etwaigen Kosten zu fragen. Einfache Auskünfte werden bundesweit in der Regel ohne Gebührenerhebung erteilt.

24.2 Evaluation des Informationsfreiheitsgesetzes des Bundes

Das Institut für Gesetzesfolgenabschätzung und Evaluation (InGFA) des Deutschen Forschungsinstituts für öffentliche Verwaltung Speyer war vom Innenausschuss des Deutschen Bundestages mit der Evaluierung des Informationsfreiheitsgesetzes des Bundes (IFG) beauftragt worden. Der Bericht wurde am 22. Mai 2012 vorgelegt und umfasst über 500 Seiten, auf die ich aufgrund des Umfangs an dieser Stelle im Einzelnen nicht eingehen kann. (Der vollständige Bericht kann unter http://www.bundestag.de/bundestag/ausschuesse17/a04/Analysen_und_Gutachten/Gutachten_IFG.pdf abgerufen werden.)

Da das Saarländische Informationsfreiheitsgesetz (SIFG) ein Verweisgesetz auf das IFG ist, möchte ich jedoch ein Fazit der Evaluation ziehen.

Nach Überzeugung der Berichtsverfasser ist das IFG ein erfolgreiches Gesetz geworden. Befürchtungen, dass durch eine Vielzahl der Anträge auf Informationszugang die Arbeit der Behörden beeinträchtigt würde, haben sich nicht bestätigt. Die Zielsetzung transparenten Verwaltungshandelns und Partizipation der Bürger sei erreicht worden.

Änderungsbedarf wird insbesondere in der Präzisierung, aber auch hinsichtlich der Ausdünnung der Ausnahmetatbestände des IFG gesehen, aufgrund derer den Antragstellern ausnahmsweise der Zugang zu Informationen verweigert werden kann. Oftmals würden die dort enthaltenen auslegungsfähigen Formulierungen missbraucht, um eine Ablehnung zu begründen.

Insbesondere das Fehlen einer Abwägungsklausel, die bewirken könnte, dass der Informationszugang nicht automatisch verweigert werden kann, weil Betriebs- und Geschäftsgeheimnisse Dritter betroffen sein könnten, wird kritisiert.

Angesprochen wird auch die Verpflichtung der Behörden zur „proaktiven" Informationstätigkeit. Hier sieht der Bericht Defizite im Vergleich mit anderen Ländern. In der Tat üben sich Bund und Länder mit Informationen zu Großvorhaben in weitgehender Zurückhaltung. Spektakuläre Beispiele gab es in jüngster Vergangenheit leider zur Genüge.

Festzuhalten ist, dass die Informationsfreiheit auf einem guten Weg ist. Allein die Tatsache, dass sich die Politik weiterhin mit dem Gesetz befasst, lässt hoffen, dass das Gesetz weiter verbessert und das Recht auf Informationsfreiheit in allen Amtsstuben zur Kenntnis genommen und respektiert wird.

24.3 Zugang zu Protokollen von Referentenbesprechungen der Bund/Länderarbeitsgruppen

Die Zusammenarbeit von Bund und Ländern auf ministerieller Ebene wird geprägt durch einen stetigen Meinungsaustausch zur Vorbereitung oder Auslegung von Gesetzen oder beispielsweise Verwaltungsvorschriften. Auch Erfahrungen aus der Verwaltungspraxis werden kommuniziert und finden auf diesem Weg Zugang zu politischen Entscheidungen.

Ein interessierter Bürger begehrte beim saarländischen Ministerium für Inneres Zugang zu den Protokollen der Besprechung der Ausländerreferenten des Bundes und der Länder. Der Antrag wurde meiner Dienststelle nachrichtlich in Kopie zugestellt. Das Ministerium lehnte den Antrag auf Informationszugang in einem formal und inhaltlich vorbildlich korrektem Bescheid ab. Begründet wurde die Ablehnung einerseits damit, dass das Saarland nicht zur Herausgabe der Informationen berechtigt sei. Verfügungsberechtigt sei das federführende Bundesministerium des Innern. In der Protokollierung verschriftete Äußerungen einzelner Ländervertreter verblieben in der Verfügungsberechtigung des entsendenden Landes. Darüber hinaus sei die Vertraulichkeit von Beratungen beeinträchtigt. Die Ländervertreter würden in der Diskussion oftmals fachliche, aber politisch noch nicht abgestimmte Auffassungen äußern,

deren Bekanntwerden durchaus insbesondere in den zugrundeliegenden Bereichen des Asyl- und Aufenthaltsrechts in der Öffentlichkeit zu kontroversen Diskussionen führen könnte.

Der Antragsteller gab sich mit der Ablehnung seines Antrags nicht zufrieden und rief das Verwaltungsgericht (VG) an.

Mit Urteil vom 26.04.2012 wies das VG Saarlouis die Klage ab. Inhaltlich wurde im Wesentlichen der Argumentation des Innenministeriums gefolgt, wonach das Saarland keine Verfügungsberechtigung über das Protokoll habe. Diese läge allein beim federführenden Bundesministerium des Innern, da dieses für die Urheberschaft und Richtigkeit des Protokolls die Verantwortung trage. Ob und wieweit andere Ausnahmegründe zuträfen, insbesondere ob die Vertraulichkeit der Beratungen beeinträchtigt sei, wurde vom Gericht infolgedessen nicht mehr geprüft.

Dies ist nun kein Beispiel für einen positiv verlaufenen Informationszugang, zeigt aber, dass es sehr wohl darauf ankommt, den Antrag an die zuständige Stelle zu richten. Ob sich der Antragsteller mittlerweile an die zuständige Stelle gewandt hat, die ihm ja bereits durch das saarländische Ministerium des Innern benannt worden war, ist mir leider nicht bekannt.

24.4 Entschließungen der Konferenzen der Informationsfreiheitsbeauftragten (IFK)

Im Berichtszeitraum beschäftigte sich die Konferenz der Informationsfreiheitsbeauftragten mit allgemeinen Themen zur Akteneinsicht, aber auch zur proaktiven Veröffentlichung von bei öffentlichen Stellen bereitstehenden Informationen. Hierzu wurden folgende Entschließungen durch die IFK veröffentlicht.

1. Geplantes europäisches Nanoproduktregister – Transparenz für Bürgerinnen und Bürger.

   Die Nanotechnologie gilt als Schlüsseltechnologie. Die geringe Größe der Partikel verleiht ihnen besondere Eigenschaften, die dazu führen, dass diese Technik bereits in vielen konsumorientierten Bereichen wie der Lebensmittel-, Textil- oder Kosmetikindustrie eingesetzt wird. Wo diese Technik zum Einsatz kommt, wird allerdings oft verschwiegen. Eine Kennzeichnung der Produkte wird gefordert, damit die Bürgerinnen und Bürger selbst entscheiden können, ob sie derartige Produkte verwenden wollen.

2. Informationsfreiheit – Lücken schließen!

   Leider gibt es noch nicht in allen Bundesländern ein Informationsfreiheitsgesetz. Mit dieser Entschließung werden Bund und Länder aufgefordert, innerhalb Deutschlands gleiche Zugangsrechte für alle Bürger zu schaffen.

3. Informationsfreiheit ins Grundgesetz und in die Landesverfassungen

   Der Datenschutz genießt durch Rechtsprechung des Bundesverfassungsgerichtes Verfassungsrang. Gleiches fordert die IFK

auch für das Recht auf Informationsfreiheit durch Verankerung im Grundgesetz und den Landesverfassungen.

4. Mehr Transparenz bei der Wissenschaft – Offenlegung von Kooperationsverträgen

   Zur Vermeidung einer verborgenen Einflussnahme auf Forschungen der Universitäten fordert die IFK eine Veröffentlichungspflicht von Kooperationsvereinbarungen zwischen Universitäten und Auftraggebern aus der Privatwirtschaft.

5. Informationsfreiheit auf europäischer Ebene ausbauen, nicht einschränken!

   Auf europäischer Ebene wird einmal mehr versucht, den freien Zugang zu Dokumenten der Europäischen Union zu verhindern. Die Entschließung appelliert an die Bundesregierung sich für mehr Transparenz einzusetzen, namentlich die Transparenz bei der Europäischen Zentralbank und der Europäischen Investitionsbank zu erhöhen.

6. Mehr Transparenz bei Krankenhaushygienedaten

   Durch diese Entschließung wird beabsichtigt, das Vertrauen in das deutsche Gesundheitssystem, insbesondere in die Krankenhäuser, zu stärken. Durch ein weitgehend standardisiertes Melde- und Veröffentlichungsgebot könnten die Patienten die jeweiligen Hygienestandards vergleichen und sich so für ein bestimmtes Krankenhaus entscheiden.

7. Parlamente sollen in eigener Sache für mehr Transparenz sorgen!

   Die Parlamente sind durch die Informationsfreiheitsgesetze nicht erfasst. In den Bundesländern gibt es aber unterschiedliche Selbstverpflichtungen der Parlamente. Die IFK fordert dazu auf, weitergehende Transparenz zu gewährleisten, um einem Verlust an öffentlicher Glaubwürdigkeit vorzubeugen.

Der vollständige Text der Entschließungen ist im Anhang abgedruckt.

24.5 Das Recht auf Neugier - transparentes staatliches Handeln

In einer weiteren Fortbildungsveranstaltung vom 22.11.2011 konnte Dr. Huber, Vorsitzender Richter am Verwaltungsgericht Frankfurt am Main, die Grundlagen des Rechtes auf Neugier an Hand des Bundesinformationsfreiheitsgesetzes referieren. Da das Saarländische Informationsfreiheitsgesetz (SIFG) auf das Informationsfreiheitsgesetz des Bundes (IFG) verweist, sind Auslegung und Rechtsprechung weitgehend als deckungsgleich anzusehen.

24.5.1 Freier Zugang zu Akten der Behörde

Die Informationsrechte nach dem Informationsfreiheitsgesetz des Bundes und damit auch des Saarlandes (Verweisgesetz) gibt nicht nur Zugang zu Informationen, sondern auch einen Zugang zu Akten.

Dieses Informationsrecht ist die Abkehr vom Aktengeheimnis schlechthin – was bleibt ist das Recht auf Datenschutz.

Bis zum Erlass dieser Gesetze gab es eine beschränkte Aktenöffentlichkeit zwar auch in anderen Gesetzen, aber dies war entweder nur für Beteiligte des Verfahrens oder eingeschränkt – etwa bei Umweltinformationen oder als Informationsrechte von Dritten bei berechtigtem Interesse.

24.5.2 Voraussetzungen für die Akteneinsicht

§ 1 IFG gewährt einen voraussetzungslosen Zugang, der weder eine Betroffenheit noch eine Beteiligtenfähigkeit erforderlich macht.

24.5.3 Ausnahmetatbestände für die Akteneinsicht

Die Ausnahmetatbestände sind im IFG abschließend geregelt und werden – so auch die Rechtsprechung – eng ausgelegt. Es geht dabei um den Schutz von besonderen öffentlichen Belangen nach den §§ 3 und 4 IFG, dem Schutz privater Belange nach den §§ 5 und 6 IFG und den Fragen der Aussonderungen nach § 7 Abs. 2 IFG.

Schutz von öffentlichen Belangen nach den §§ 3 und 4 IFG

§ 3 IFG schützt besondere öffentliche Belange wie die innere und äußere Sicherheit, laufende Gerichts- und Ermittlungsverfahren und den Bereich der öffentlichen Sicherheit. Darüber hinaus werden u.a. die Vertraulichkeit von Beratungen und das Sozialgeheimnis vom Zugangsanspruch ausgenommen.

Nach § 4 IFG wird der behördliche Entscheidungsprozess geschützt, also Entwürfe und Vorbereitungen von Entscheidungen in laufenden Verwaltungsverfahren.

Schutz privater Belange nach den §§ 5 und 6 IFG

§ 5 IFG schützt personenbezogene Daten. Diese sind in § 3 Saarländisches Datenschutzgesetz definiert als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Hierzu gehören auch die Angaben über Vermögensverhältnisse, Bauakten, soweit sie persönliche Angaben über den Bauherrn beinhalten, und auch Geodaten des Grundstückseigentümers.

Sofern der betroffene Dritte in die Preisgabe seiner personenbezogenen Daten nicht eingewilligt hat, hat eine Interessensabwägung zu er-

folgen zwischen seinem Geheimhaltungsinteresse und dem Informationsinteresse des Antragstellers. Deshalb gibt es in diesen Fällen ausnahmsweise ein Begründungserfordernis des Antragstellers.

In vielen Fällen kann der Schutz privater Belange dadurch sichergestellt werden, dass Kopien angefertigt werden und die persönlichen Daten geschwärzt werden.

§ 6 IFG schützt das Betriebs- und Geschäftsgeheimnis, also das berechtigte Geheimhaltungsinteresse des Betriebes und das Urheberrecht.

Verfahren und Ausschlussgrund nach § 7 IFG

In der Verfahrensvorschrift des § 7 IFG ist schließlich ein Ausschlussgrund formuliert, der trotz Vorliegens des Anspruches dann eine Ablehnung zulässt, wenn ein unverhältnismäßiger Verwaltungsaufwand entsteht. Die Vorschrift ist als Missbrauchsklausel konzipiert und soll das Lahmlegen der Behörde verhindern. Damit sind sehr hohe Anforderungen an diese Regelung gestellt. In der Rechtsprechung (siehe unter anderem Hess. VGH, Beschluss vom 30. April 2010 - 6 A 1341.09 – Juris) ist die Grenze zur Unverhältnismäßigkeit des Verwaltungsaufwands erst dann überschritten, „wenn durch die Art des Informationszugangsbegehrens oder seinen Umfang ein Verwaltungsaufwand notwendig ist, der den bei üblichen Gesuchen an die Behörde verursachten Aufwand in solch deutlichem Maße übersteigt, dass die Behörde das Gesuch letztlich nur durch außergewöhnliche Maßnahmen, insbesondere durch eine nicht nur vorübergehende Zurückstellung ihrer Kernaufgaben, bewältigen könnte“. Im entschiedenen Fall war dies bei Durcharbeiten von 5000 Seiten bei der Bundesanstalt für Finanzdienstleistungsaufsicht nicht der Fall.

24.5.4 Rechtsmittel

Gegen eine ablehnende Entscheidung über den Antrag auf Informationszugang sind Widerspruch und Verpflichtungsklage möglich.

25 Entschließungen der IFK

25.1 Informationsfreiheit – Lücken schließen!

23. Mai 2011

Der Gedanke der Transparenz staatlichen Handelns ist beim Bund und den meisten Ländern seit einigen Jahren angekommen, wie die Informationsfreiheitsgesetze von Brandenburg (1998), der meisten anderen Länder und auch das Informationsfreiheitsgesetz des Bundes (2005) zeigen.

Vor diesem Hintergrund begrüßt die Konferenz der Informationsfreiheitsbeauftragten die Absicht der neuen Landesregierung von Baden-Württemberg, auch dort ein Informationsfreiheitsgesetz auf den Weg zu bringen. Dabei sollte allerdings, wie in Rheinland-Pfalz vorgesehen, dem Landesbeauftragten für den Datenschutz die Aufgabe der oder des Beauftragten für die Informationsfreiheit übertragen werden. Diese unabhängige Funktion eines oder einer Informationsfreiheitsbeauftragten fehlt gegenwärtig auch noch in Thüringen. Bayern, Hessen, Niedersachsen und Sachsen lehnen dagegen beharrlich jede gesetzliche Regelung für einen Anspruch der Bürgerinnen und Bürger auf Zugang zu behördlichen Informationen ab.

Dies führt zu absurden Ergebnissen: So haben die Bürgerinnen und Bürger gegenüber den Jobcentern mit gemeinsamer Trägerschaft durch Bundesagentur für Arbeit und Kommune auch in den vier Ländern ohne Informationsfreiheitsgesetze einen Anspruch auf der Grundlage des Bundesgesetzes. Dagegen besteht gegenüber den Jobcentern der Optionskommunen in ausschließlich kommunaler Trägerschaft in diesen Ländern kein Anspruch auf Informationszugang.

Unbefriedigend ist auch, dass die Bürgerinnen und Bürger bei Ersuchen auf Zugang zu Verbraucher- und Umweltinformationen nicht durchgängig die gesetzlich garantierte Möglichkeit haben, sich an die Informationsfreiheitsbeauftragten zu wenden. Eine Ombudsfunktion ist zwar in den meisten Informationsfreiheitsgesetzen vorgesehen, fehlt aber für Umwelt- und Verbraucherinformationen auf Bundesebene und in vielen Ländern.

Deshalb appelliert die Konferenz an die Gesetzgeber in Bund und Ländern, diese Regelungsdefizite zu beseitigen und „flächendeckend" allgemeine Regelungen für den Informationszugang zu schaffen und die Ombudsfunktionen der Informations-freiheitsbeauftragten für Verbraucher-, Umwelt- und sonstige Informationen in Bund und Ländern gesetzlich zu regeln.

25.2 Geplantes europäisches Nanoproduktregister – Transparenz für Bürgerinnen und Bürger!

23. Mai 2011

Neue Technologien rufen bei Bürgerinnen und Bürgern nicht nur positive Reaktionen hervor, sondern stoßen häufig auf Skepsis oder lösen Ängste aus. Grund hierfür ist nicht selten eine unzureichende Informationslage bis hin zur Zurückhaltung von Informationen für Verbraucherinnen und Verbraucher. Wer das Potential neuer Technologien ausschöpfen möchte, muss mit offenen Karten spielen. Das bedeutet, dass nicht nur Vorteile, sondern auch Risiken offengelegt werden müssen, um einen demokratischen Diskurs und jedem Menschen eine informierte Willensbildung zu ermöglichen.

Ein aktuelles Beispiel ist der Einsatz von Nanotechnologie: Dabei geht es um künstlich hergestellte winzige Partikel (Nanomaterial), die heute schon in Baustoffen, Textilien sowie Kosmetika und zukünftig immer mehr in verbrauchernahen Produkten wie etwa Lebensmitteln eingesetzt werden. Nanotechnologie soll Produkte z.B. robuster machen. In einem Bericht aus dem Jahre 2009 (nano.DE-Report 2009) geht das Bundesministerium für Wissenschaft und Forschung davon aus, dass nanotechnologisches Know-how in den Bereichen Gesundheit, Informations- und Kommunikations- sowie Energie- und Umwelttechnik immensen Einfluss auf die Wertschöpfung nehmen wird. Ein Weltmarktvolumen von 15 % der globalen Güterproduktion wird prophezeit.

Wenigen ist dies bekannt, denn es besteht derzeit keine Pflicht, Produkte, die Nanomaterial enthalten, zu kennzeichnen. Erst 2013 wird eine solche Pflicht für Kosmetika bestehen. Für Lebensmittel wird die Kennzeichnungspflicht noch diskutiert. Zugleich – stellt die Nano-Kommission der Bundesregierung in ihrem Aktionsplan Nanotechnologie 2015 fest – fehlen vielfach grundlegende Kenntnisse über die Risiken bei der Exposition mit Nanomaterialien.

Die Informationsfreiheitsbeauftragten in Deutschland fordern die Bundesregierung auf, sich bei den Diskussionen und Verhandlungen auf europäischer Ebene dafür einzusetzen, dass Bürgerinnen und Bürgern ein direkter Zugang zu Informationen über Nanotechnologie in Produkten ermöglicht wird. Deshalb ist es notwendig, dass auch Bürgerinnen und Bürger Zugang insbesondere zu dem auf europäischer Ebene diskutierten Nanoproduktregister erhalten. Beim Einsatz neuer Technologien muss verstärkt auf Aufklärung, Transparenz und Einbindung der Menschen gesetzt werden.

25.3 Informationsfreiheit auf europäischer Ebene ausbauen, nicht einschränken!

Mainz, 12. Juni 2012

Mit Besorgnis nehmen die Informationsfreiheitsbeauftragten in Deutschland zur Kenntnis, dass der freie Zugang zu Dokumenten der Europäischen Union gemäß Verordnung 1049/2001 erneut in Frage gestellt wird. Bereits im Jahre 2008 hatte die Europäische Kommission mannigfaltige Vorschläge zu einer drastischen Einschränkung des Zu-

gangs zu europäischen Dokumenten vorgelegt, deren Folge eine massive Reduzierung der gebotenen Transparenz des Handelns europäischer Institutionen gewesen wäre (vgl. Entschließung der Informationsfreiheitsbeauftragten in Deutschland vom 30. Juni 2008). Das Europäische Parlament forderte daraufhin zwar eine Stärkung der Informationsfreiheit, doch arbeiten die Mitgliedstaaten derzeit daran, genau das zu verhindern. Ein "Kompromisspapier" der dänischen Ratspräsidentschaft sah zuletzt vor, das Zugangsrecht zu Akten der Institutionen der Europäischen Union deutlich einzuschränken.

Während bislang alle Arten von Inhalten der Informationsfreiheit unterfallen, sollen zukünftig nur "formell übermittelte" Dossiers öffentlich einzusehen sein. Damit würden der Öffentlichkeit sämtliche Entwürfe oder Diskussionspapiere des Rats, der Kommission und des Parlaments vorenthalten. Dies würde auch Vertragsverletzungsverfahren, Wettbewerbs- und Kartellverfahren betreffen, die von hohem öffentlichem Interesse sind.

Die Konferenz lehnt die Ausnahme einzelner europäischer Institutionen von der Transparenzpflicht ab. Sie tritt dafür ein, dass insbesondere die Europäische Zentralbank und die Europäische Investitionsbank nicht nur hinsichtlich ihrer Verwaltungstätigkeiten auf mehr Transparenz verpflichtet werden.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland appelliert an die Bundesregierung, sich im Europäischen Rat für mehr Transparenz einzusetzen. Verwaltung und Politik auf der Ebene der Europäischen Union dürfen nicht in bürokratische Geheimniskrämerei zurückzufallen. Die Forderungen des Europäischen Parlaments müssen endlich erfüllt werden. Gerade angesichts der zunehmenden Verantwortung, die den europäischen Institutionen von der gemeinsamen Außenpolitik bis zur Bewältigung der Finanzkrise zukommt, gilt es, alle Institutionen der Europäischen Union noch weiter zu öffnen. Denn: Vertrauen basiert auf Transparenz!

25.4 Mehr Transparenz bei der Wissenschaft - Offenlegung von Kooperationsverträgen -

Mainz, 12. Juni 2012

Die Kooperation zwischen Wissenschaft und Wirtschaft hat eine lange Tradition. Dies gilt für gemeinsame Institute ebenso wie für Stiftungsprofessuren und sonstige Formen der Zusammenarbeit.

Unternehmensfinanzierte Forschung nimmt einen immer größeren Anteil an der Wissenschaft ein. Deutschlandweit sollen inzwischen 660 Lehrstühle direkt oder indirekt von Unternehmen finanziert sein. Oft sind Motivation und Umfang der Förderung für Außenstehende nicht erkennbar. Für eine Beurteilung der Forschungsergebnisse und deren Bewertung ist die Kenntnis dieser Hintergründe jedoch Voraussetzung. Die Freiheit von Forschung und Wissenschaft lebt von einer offenen Diskussion; Geheimhaltung engt diese Freiheiten ein.

Einer verborgenen Einflussnahme auf Forschungsgegenstände, Forschungsergebnisse und auf deren Veröffentlichung kann nur durch eine konsequente Politik der Offenheit begegnet werden. Kooperationsver-

träge zwischen Wissenschaft und Unternehmen sind grundsätzlich offenzulegen. Eine solche Veröffentlichungspflicht sollte mindestens die Identität der Drittmittelgeber, die Laufzeit der Projekte, den Förderumfang und die Einflussmöglichkeiten der Drittmittelgeber auf Forschungsziele und -ergebnisse umfassen. Die Pflicht zur Veröffentlichung der Verträge darf nur zurücktreten, soweit und solange die Bekanntgabe gesetzlich geschützte Interessen beeinträchtigt.

Die regelmäßige Offenlegung der Finanzierung von Forschungsprojekten ist nach Auffassung der Informationsfreiheitsbeauftragten ein geeignetes Instrument, um die Freiheit der Forschung zu schützen, indem einseitige Abhängigkeiten oder auch nur deren Anschein vermieden wird. Eine reine Selbstverpflichtung der Universitäten und Forschungseinrichtungen ist hierfür nicht ausreichend. Es bedarf vielmehr konsequenter Regelungen in den Informationsfreiheitsgesetzen des Bundes und der Länder.

25.5 Mehr Transparenz bei Krankenhaushygienedaten

Mainz, 27. November 2012

Das Vertrauen der Bevölkerung in das deutsche Gesundheitssystem, insbesondere in unsere Krankenhäuser, hat im Laufe der letzten Jahre abgenommen. Dies ist auch auf eine verbreitete Intransparenz zurückzuführen.

Zwar wurden in einem von einer Tageszeitung herausgegebenen Klinikführer Berlin-Brandenburg erstmals auch Hygienedaten veröffentlicht, jedoch nahmen nicht alle Krankenhäuser an der dieser Publikation zugrunde liegenden freiwilligen Datenerhebung teil. Das wurde u.a. damit begründet, dass die nur zu internen Zwecken erhobenen Daten falsch interpretiert werden könnten und dass Patientinnen und Patienten möglicherweise andere Krankenhäuser wählen würden, wenn sie über entsprechende Vergleichsdaten verfügten.

Die Entscheidung für oder gegen ein bestimmtes Krankenhaus können die Patientinnen und Patienten aber nur dann verantwortlich treffen, wenn ihnen alle relevanten Parameter zur Verfügung stehen; dazu gehören auch die jeweiligen Hygienedaten und ihre Umsetzung in den einzelnen Kliniken. Nur eine standardisierte Melde- und Veröffentlichungspflicht für alle Hygienedaten ermöglicht es jedem Patienten und jeder Patientin, die jeweiligen Hygienestandards der Krankenhäuser zu bewerten und zu vergleichen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert daher alle Verantwortlichen, insbesondere den Bundes- und die Landesgesetzgeber auf, für Transparenz bei Krankenhaushygienedaten zu sorgen. Dazu gehören auch standardisierte und weit reichende Melde- und Veröffentlichungspflichten und die Erweiterung der Qualitätsberichte der Krankenhäuser. Dies wäre ein wichtiger Schritt, um durch mehr Transparenz das Vertrauen der Bevölkerung in die Gesundheitsversorgung durch Krankenhäuser zu fördern.

25.6 Parlamente sollen in eigener Sache für mehr Transparenz sorgen!

Mainz, 27. November 2012

Die Informationsfreiheitsgesetze von Bund und Ländern nehmen die Parlamente von den für sonstige öffentliche Stellen bestehenden Transparenzpflichten aus. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland sieht, dass der Kernbereich der Abgeordnetentätigkeit in der unabhängigen Wahrnehmung ihres Mandats nicht dem umfassenden Zugangsanspruch der Öffentlichkeit unterliegen kann. Defizite bei der Transparenz führen aber zu einem Verlust an öffentlicher Glaubwürdigkeit. Die Parlamente von Bund und Ländern sollten deshalb Vorreiter in Sachen Transparenz werden und Ausnahmen vom Informationszugang soweit wie möglich zurücknehmen.

In welchem Umfange Transparenz herzustellen ist, ist eine Frage des verfassungsrechtlich gebundenen, gesetzgeberischen Ermessens. Dieses verpflichtet die Parlamente dazu, die bereits vorhandenen Transparenzregelungen regelmäßig daraufhin zu überprüfen, ob sie sich bewährt haben oder ggf. zu konkretisieren und zu ergänzen sind. Dabei sollten - soweit noch nicht geschehen - folgende Punkte berücksichtigt werden:

1. ein möglichst hohes Maß an Transparenz bei den weiteren Tätigkeiten und Einkünften von Abgeordneten unter Berücksichtigung von Berufsgeheimnissen. Den möglichen Besonderheiten des Mandats, insbesondere bei "Teilzeit"-Parlamenten, sollte Rechnung getragen werden,

2. Veröffentlichung von Tagesordnungen von Plena und Ausschüssen, ebenso Stellungnahmen, Protokolle und weitere Unterlagen, die Gegenstand der Beratungen sind,

3. Öffentlichkeit von Sitzungen der Fachausschüsse,

4. grundsätzliche Veröffentlichung von wissenschaftlichen Ausarbeitungen der Parlamentsdienste und sonstiger Gutachten,

Zugang zu Informationen über Beschaffungen, Reisen, Sachausgaben und sonstige kostenträchtige Vorhaben der Parlamente und ihrer Ausschüsse.

26 Sachverzeichnis

L

M

N

O

P

R

S

T

U

V

W

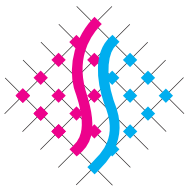
Z

27 Abkürzungsverzeichnis

a.a.O.	an angegebenem Ort
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
ALG	Arbeitslosengeld
Amtsbl.	Amtsblatt des Saarlandes
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaft
BAG	Bundesarbeitsgericht
BBesG	Bundesbesoldungsgesetz
BDSG	Bundesdatenschutzgesetz
BEST	Beratungsstelle für sozialverträgliche Technologiegestaltung e.V.
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMF	Bundesministerium der Finanzen
BR-Drs.	Drucksache des Bundesrates
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
ed	erkennungsdienstlich
eGo-Saar	Zweckverband elektronische Verwaltung für saarländische Kommunen
eGovernment	Electronic Government, elektronische Verwaltung
EU	Europäische Union
EUV	Vertrag über die Europäische Union
EVS	Entsorgungsverband Saar
GBO	Grundbuchordnung
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
GG	Grundgesetz der Bundesrepublik Deutschland
GPS	Global Positioning System
GSL	Größere Schadenslagen
GWG	Geldwäschegesetz
GZPZ	Gemeinsames Zentrum für landesübergreifende Polizei- und Zollzusammenarbeit
HIS	Hinweis- und Informationssystem
i.S.d.	im Sinne des
i.V.m.	in Verbindung mit
ID	Identifikator, Kennung
IFG	Informationsfreiheitsgesetz
IFK	Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder
IHK	Industrie- und Handelskammer
InfÜVPol	Informationsübermittlungsverordnung Polizei Informationssystem der Polizei des Bundes und der

INPOL	Länder
INSPIRE	Infrastructure for spatial information in the European Community
IP	Internetprotokoll
IPSec	Internetprotokoll-Security
IT	Informationstechnik
JVA	Justizvollzugsanstalt
KaInDÜV	Katasterinhalts- und Datenübermittlungsverordnung
KBA	Kraftfahrt-Bundesamt
KommHVO	Kommunalhaushaltsverordnung
KPS	Kriminalpolizeiliche Sammlung
KRISTAL	Kriminalpolizeiliches System zur täter- und tatorientierten Analyse und Lagedarstellung
KSVG	Kommunalselbstverwaltungsgesetz
KWG	Kommunalwahlgesetz
LARS	Landesweite Arlamierung Rheinland-Pfalz und Saarland
LfDI	Die Landesbeauftragte für Datenschutz und Informationsfreiheit
LWG	Landtagswahlgesetz
LWO	Landeswahlordnung
MeldDÜV	Meldedatenübermittlungsverordnung
MG	Meldegesetz
NFC	Near Field Communication
OK	Organisierte Kriminalität
OWiG	Ordnungswidrigkeitengesetz
PAS	Personenauskunftsstelle
PAuswG	Personalausweisgesetz
PflVG	Pflichtversicherung für Kraftfahrzeughalter
PKS	Polizeiliche Kriminalstatistik
PMK	Politisch motivierte Kriminalität
POLADIS	Polizeiliches anwendungsorientiertes dezentrales Informationssystem
SAWG	Saarländisches Abfallwirtschaftsgesetz
SBG	Saarländisches Beamtengesetz
SchoG	Schulordnungsgesetz
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SIFG	Saarländisches Informationsfreiheitsgesetz
SJStVollzG	Saarländisches Jugendstrafvollzugsgesetz
SKRG	Saarländisches Krebsregistergesetz
SPolG	Saarländisches Polizeigesetz
StA	Staatsanwaltschaft
Steuer-ID	Steueridentifikationsnummer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVollzG	Strafvollzugsgesetz
SVerfSchG	Saarländisches Verfassungsschutzgesetz

SWIFT	Society for Worldwide Interbank Financial Tele-communication
TAN	Transaktionsnummer
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TVL	Tarifvertrag für der öffentlichen Dienst der Länder
USA	Vereinigte Staaten von Amerika
Vgl.	Vergleiche
VO	Verordnung
WWW	World wide web
ZEVIS	Zentrales Verkehrsinformationssystem
ZFER	Zentrales Fahrerlaubnisregister
ZFZR	Zentrales Fahrzeugregister
ZKR	Zentrale Kontrollgerätkartenregister
ZPO	Zivilprozessordnung
ZPT	Zentrale für Produktivität und Technologie Saar e.V.



UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

Fritz-Dobisch-Str. 12
66111 Saarbrücken
0681/94781-0
poststelle@datenschutz.saarland.de
www.datenschutz.saarland.de