UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

25. Tätigkeitsbericht

2013/2014

25. Tätigkeitsbericht

Unabhängiges Datenschutzzentrum Saarland

für die Jahre 2013 und 2014

dem Landtag und der Landesregierung
vorgelegt am 22. April 2015
(Landtagsdrucksache 15/1320)

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

Der Berichtszeitraum des 25. Tätigkeitsberichts der Landesbeauftragten für Datenschutz und Informationsfreiheit im Saarland erstreckt sich über die Jahre 2013 und 2014.

War der 24. Tätigkeitsbericht von der Zusammenlegung des öffentlichen und des nicht-öffentlichen Bereichs geprägt, so sorgt jetzt die immer weiter fortschreitende Digitalisierung unseres Alltags für neue Fragestellungen und Herausforderungen im Datenschutz.

Die Beschwerden über Videokameras haben sich im Berichtszeitraum exorbitant gegenüber früheren Jahren erhöht. Fast täglich gibt es Eingaben wegen Kameras in Geschäften, Restaurants, Diskotheken, an Gebäuden, an Kapellen aber auch an Arbeitsplätzen oder im Wald.

Der Versuch, sich mit günstiger Technik eine wie auch immer geartete verbesserte Rechtsposition zu verschaffen, lässt oft jeglichen Skrupel vor Überwachung der Mitarbeiter oder der Gäste schwinden. Dementsprechend ist auch die Anzahl der Bußgeldverfahren steigend.

Im Berichtszeitraum sind wir erfreulicherweise auch immer öfter von öffentlichen Stellen frühzeitig in Gesetzgebungs- und andere Verfahren eingebunden worden. Dies erleichtert nicht nur die Arbeit, sondern macht auch eine frühzeitige Steuerung möglich.

In das Jahr 2014 fällt aber auch die Verabschiedung der neuen europäischen Datenschutz-Grundverordnung durch das europäische Parlament und die weitere Auseinandersetzung mit diesem Thema in der Kommission und im Ministerrat der EU. Eine abschließende Entscheidung wird Ende 2015 erwartet.

Der Europäische Gerichtshof in Luxemburg hat durch seine Gerichtsentscheidungen zur Vorratsdatenspeicherung, zum Löschungsanspruch in Suchmaschinen und zur Anwendung des Datenschutzrechtes bei privater Videoüberwachung den Datenschutz wesentlich mitgeprägt und in Europa gestärkt.

Schließlich haben die Enthüllungen von Edward Snowden in den vergangen zwei Jahren nicht nur eine neue Diskussion über die Frage des Schutzes der Privatsphäre angestoßen, sondern sie markieren auch einen Umbruch im Denken und Handeln mit unseren persönlichen Daten. Jetzt im zweiten Jahr nach Snowden wird von vielen die Notwendigkeit von neuen Sicherheitstechnologien anerkannt und nach vorne getrieben.

Datensammlungen in Facebook, Twitter und Google-Diensten werden mehr denn je zu Informationen über menschliches Verhalten und damit auch zu einem großen Wirtschaftsfaktor. In der Folge haben es erfreulicherweise auch Datenschutzthemen vom Feuilleton- und IT-Thema in die Wirtschaftsteile der großen Tageszeitungen geschafft. Datenschutz und Datensicherheit sind alltagstauglich geworden.

Notwendig für die digitale Zukunft ist nun eine Technik, die den Datenschutz per se berücksichtigt und den Menschen einfache Mittel an die Hand gibt sich zu schützen. Beim Unabhängigen Datenschutzzentrum

hat dies zu einer Neugestaltung der Homepage geführt, verbunden mit einem sicheren Zugang zur Dienststelle.

Wir hoffen, dass dieser Bericht informiert, aber auch sensibilisiert und den Datenschutz weiter vorantreibt.

Saarbrücken, im April 2015

Judith Thieser

Die Landesbeauftragte
für Datenschutz und Informationsfreiheit
im Saarland

Inhaltsverzeichnis

1 Einführung

Der vorliegende Tätigkeitsbericht beschäftigt sich neben Themen wie der Neuordnung des Europäischen Datenschutzrechtsrahmens und etwa der Videoüberwachung im Saarland auch mit zahlreichen Beiträgen zur Gesetzgebung, zu Bürgerbeschwerden und zu Prüfungen bei saarländischen öffentlichen Stellen und privaten Betrieben und zur technischen Sicherheit bei der Datenübertragung.

Die Europäische Kommission veröffentlichte im Januar 2012 ihren ersten Entwurf zur Neuordnung des Europäischen Datenschutzrechtsrahmens. Hierüber haben wir bereits im 24. Tätigkeitsbericht berichtet.

In den vergangenen zwei Jahren hat sich das Europäische Parlament umfassend mit dieser Verordnung auseinandergesetzt und die Neuregelung einstimmig im Sommer 2014 verabschiedet. Zwischenzeitlich berät der Ministerrat der EU die Datenschutzgrundverordnung und es wird damit gerechnet, dass eine abschließende Stellungnahme bis Sommer 2015 vorliegt. Danach wird sich der Trilog anschließen, eine Art Vermittlungsausschuss zwischen den drei Organisationen der EU, der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union. Dieser wird voraussichtlich einen Zeitraum von einem halben Jahr benötigen. Eine dort erzielte Einigung muss dann vom Parlament bestätigt werden.

Danach kann dann die Verordnung mit einer Übergangsfrist von voraussichtlich zwei Jahren geltendes Recht werden.

Im Berichtszeitraum hat der Europäische Gerichtshof (EuGH) ganz wesentliche und weitreichende Entscheidungen im Datenschutz getroffen.

So hat er in der Entscheidung vom 8. April 2014 die Richtlinie über die Vorratsdatenspeicherung von Telekommunikationsdaten für ungültig erklärt. Das Gericht hat festgestellt, dass das anlasslose und massenhafte Speichern „ohne irgendeine Differenzierung, Einschränkung oder Ausnahme“ gegen die in der Grundrechtcharta verankerten Persönlichkeitsrechte verstößt und Eingriffe in dieses Recht selbst beim Kampf gegen schwere Straftaten auf das „absolut Notwendige“ zu beschränken sind.

In einer weiteren Entscheidung vom 13. Mai 2014 hat der EuGH dann das „Recht auf Vergessen“ im Internet festgeschrieben. Dabei geht es um das Recht, einen in einer Suchmaschine erscheinenden Link unter bestimmten Voraussetzungen löschen zu lassen, selbst wenn die zugrunde liegenden Tatsachen auf einer Homepage rechtmäßig veröffentlicht werden. Diese – rechtmäßig veröffentlichten - Daten müssen nicht gelöscht werden, sondern nur der Verweis in der Suchmaschine.

Am 11. Dezember 2014 schließlich hat der EuGH entschieden, dass die EU-Datenschutzrichtlinie auch auf privat betriebene Videoüberwachungsanlagen Anwendung findet, wenn damit öffentlicher Raum überwacht wird. Das führt unter anderem dazu, dass der Kamerabetreiber sich vor der Inbetriebnahme mit den rechtlichen Anforderungen der Videoüberwachung auseinander setzen und die Anlage bei dem Unabhängigen Datenschutzzentrum Saarland melden muss.

Im öffentlichen Bereich haben wir sowohl die Änderung des Polizeigesetzes als auch die Änderung des Verfassungsschutzgesetzes begleitet.

Als neue Prüftätigkeit haben wir erstmals im Jahre 2014 die Antiterrordatei (ATD) beim Landespolizeipräsidium einer Kontrolle unterzogen. Es handelt sich bei dieser Datei um eine gemeinsame Datenbank von verschiedenen deutschen Sicherheitsbehörden, die auf der Rechtsgrundlage des Antiterrordateigesetzes zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland errichtet wurde.

Auf der Grundlage der Forderung des Bundesverfassungsgerichtes in seinem Urteil vom 24. April 2013 (1 BvR 1215/07) wurden durch die am 1. Januar 2015 in Kraft getretenen Änderungen des Antiterrordateigesetzes und des Rechtsextremismusdateigesetzes verpflichtende, mindestens alle zwei Jahre durchzuführende Datenschutzkontrollen dieser beiden Dateien normiert.

Im Berichtszeitraum haben die Beschwerden über Videoüberwachungsmaßnahmen erneut zugenommen. In Gaststätten und Diskotheken wird vermehrt in Unkenntnis der rechtlichen Gegebenheiten auf Videotechnik gesetzt, ohne dass rechtliche Erfordernisse wie beispielsweise eine Vorabkontrolle oder die Einschaltung eines Datenschutzbeauftragten beachtet wurden.

Ebenso sind uns immer wieder Betriebe gemeldet worden, in denen Videokameras in unzulässiger Weise für eine Verhaltens- und Leistungskontrolle der Mitarbeiter genutzt wurden.

Auch auf Parkplätzen und zum Schutz von Wohneigentum werden in steigender Zahl Kameras eingesetzt, die den rechtlichen Vorgaben vielfach nicht entsprechen.

Gleiches gilt auch für die Vielzahl der Kameras, die mittlerweile in saarländischen Wäldern zu finden sind und deren Einsatz nur unter Beachtung spezifischer rechtlicher Maßgaben als zulässig angesehen werden kann.

Durch die breite Unterstützung des Landes, einiger Landkreise und Sparkassen konnten wir im Berichtszeitraum Schulworkshops für weiterführende Schulen zum Thema Datenschutz und Medienkompetenz anbieten. Auf Vorschlag der Lehrer wurden diese speziell für die Klassenstufe sechs konzipiert.

Die große Nachfrage und die positiven Reaktionen zeigen, dass gerade auch Jugendliche nach Hilfen für den sicheren Umgang im Netz suchen und - neben dem „Learning by Doing" - Medienkompetenz und Datenschutzbewusstsein auch in der schulischen Bildung vermittelt werden sollte. Die Workshops des Unabhängigen Datenschutzzentrums leisten einen wichtigen Beitrag hierzu.

Die technische Sicherheit und die Vertraulichkeit bei der Datenübertragung waren im Berichtszeitraum – nicht zuletzt vor dem Hintergrund

der Enthüllungen von Edward Snowden und des NSA-Untersuchungsausschusses – in den Medien und speziell auch unter den Datenschützern viel diskutierte Themen.

Diese öffentliche Diskussion hat auch bei vielen Menschen das Bewusstsein für die Bedeutung sicherer Übertragungswege für persönliche Daten und damit auch für die Notwendigkeit des Einsatzes von Verschlüsselungstechniken erhöht.

In diesem Bereich ist in den vergangenen zwei Jahren von verschiedenen Unternehmen Einiges auf den Weg gebracht worden, aber längst ist der Einsatz solcher Techniken noch nicht zum Standard geworden.

Aus unserer Sicht müssen die Möglichkeiten und Wege der Verschlüsselung so gestaltet werden, dass sie auch für den Laien mit einem Klick anwendbar sind.

Es ist jedem Nutzer unbenommen, solche „sicheren Wege" zu verlassen und eigene offene Wege zu suchen. Entscheidend ist und bleibt aber, dass der Nutzer die Chance hat, ohne Aufwand sicher zu kommunizieren, ohne dass Anbieter, Firmen oder Nachrichtendienste diese Kommunikation unmittelbar verfolgen können.

Wir wollen die digitale Uhr nicht zurückdrehen oder zum Stillstand bringen, wir wollen aber, dass wir auch im digitalen Zeitalter noch allein entscheiden können, was wir privat halten und was wir für die Öffentlichkeit preisgeben wollen.

Die Mitarbeiter des Unabhängigen Datenschutzzentrums haben daher auch die eigene Homepage - *www.datenschutz.saarland.de* - neu gestaltet und einen sicheren Kommunikationsweg für Nutzer eingerichtet.

Sowohl für Firmen als auch für Verbraucher wird die Nutzung von Cloud Diensten immer interessanter, da die Datenmengen anwachsen, eigene Rechnerkapazitäten nicht immer ausreichen und die Daten ständig und überall verfügbar sein sollen.

Gleichzeitig ist die Sicherheit der persönlichen Daten immer schwieriger zu gewährleisten.

Im Jahr 2014 wurde daher von den Arbeitskreisen Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises eine Orientierungshilfe zur Nutzung von Cloud Diensten erarbeitet.

Diese Orientierungshilfe richtet sich an Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche und soll den datenschutzgerechten Einsatz dieser Technologie fördern. Dieser Tätigkeitsbericht enthält eine kurze Zusammenfassung der wichtigsten datenschutzrechtlichen Anforderungen an Anbieter von Cloud Diensten und soll den Nutzern eine Entscheidungshilfe bei der Auswahl solcher Dienste geben.

2 Internationaler Datenverkehr

Der Bereich des internationalen Datenverkehrs war im Berichtszeitraum maßgeblich durch die Enthüllungen von Edward Snowden geprägt. Insbesondere was Datenflüsse in die USA anbelangt, lassen die bekanntgewordenen Erkenntnisse über die Arbeitsweise und technischen Möglichkeiten der NSA, des größten amerikanischen Auslandsgeheimdienstes, Zweifel daran aufkommen, ob in den Vereinigten Staaten ein angemessenes Datenschutzniveau überhaupt noch gewährleistet werden kann. Insbesondere im sich verstärkenden Trend zum Cloud Computing hat dies erhebliche Auswirkungen, da zahlreiche Anbieter von Cloud-Computing-Dienstleistungen US-Unternehmen sind.

Sowohl die EU-Richtlinie 95/46/EG als auch das Bundesdatenschutzgesetz (BDSG) verlangen aber, dass personenbezogene Daten nur dann in Länder außerhalb der EU/des EWR transferiert werden dürfen, wenn beim Empfänger ein angemessenes Datenschutzniveau gewährleistet ist. Die Gewährleistung dieses Datenschutzniveaus kann dabei durch verschiedene Instrumente erfolgen. Zu den verbreitetsten gehören die Safe Harbor-Zertifizierung der datenempfangenden Stelle, die Verwendung von Standardvertragsklauseln und die Nutzung von verbindlichen Unternehmensrichtlinien (sog. Binding Corporate Rules - BCR).

2.1 Safe Harbor

Safe Harbor ist eine seit dem 06. Juli 2000 bestehende Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA zu den Grundsätzen des sog. „sicheren Hafens“ (Safe Harbor). Ausgangspunkt für diese Vereinbarung bilden die Vorschriften der Art. 25 und 26 der EU-Datenschutzrichtlinie, nach denen ein Datentransfer in Drittstaaten verboten ist, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auf die USA zu, da es dort keine umfassenden gesetzlichen Regelungen zum Datenschutz gibt, die dem europäischen Standard entsprechen. Allerdings sieht Art. 25 Abs. 6 der Richtlinie vor, dass die Kommission der Europäischen Gemeinschaft die Angemessenheit des Datenschutzes in einem Drittland "feststellen" kann, wenn dieses bestimmte Anforderungen erfüllt.

Die Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (FTC) können sich die Unternehmen selbst zertifizieren. So zertifizierte US-Unternehmen schaffen damit grundsätzlich die Voraussetzungen, dass eine Übermittlung personenbezogener Daten aus Europa an sie unter denselben Bedingungen möglich ist, wie Übermittlungen innerhalb des europäischen Wirtschaftsraumes (EU/EWR).

2.2 Standardvertragsklauseln

Eine weitere Möglichkeit, personenbezogene Daten in Drittländer zu transferieren, stellt die Verwendung der sog. Standardvertragsklauseln dar. Schließen das exportierende Konzernunternehmen in der EU und das importierende außerhalb der EU/des EWR einen Vertrag mit den Standardvertragsklauseln der EU-Kommission, so ist damit automatisch ein angemessenes Datenschutzniveau beim Importeur sichergestellt. Der Vorteil der Standardvertragsklauseln ist ihre vergleichsweise leichte Umsetzbarkeit. Dies gilt vor allem, wenn Daten sternförmig zu einer einzigen Gesellschaft in einem Drittland übermittelt werden.

2.3 Gemeinsame Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juli 2013

Den beiden Instrumenten, Safe Harbor und Standardvertragsklauseln, ist gemeinsam, dass sie ein tatsächlich nicht vorhandenes angemessenes Datenschutzniveau beim Datenimporteur fingieren. Diese Fiktion stellt aber sozusagen nur eine Komponente bei der Beurteilung dar, ob personenbezogene Daten zulässigerweise in Drittländer übermittelt werden dürfen. Nach § 4b Abs. 2 Satz 2 BDSG hat eine Übermittlung nämlich zu unterbleiben, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Auch § 4c Abs. 2 BDSG gestattet eine Übermittlung nur, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist.

Auch aus Art. 3 Abs. 1 der Safe-Harbor-Entscheidung der Kommission und der Befugnis nationaler Behörden, bestimmte Datenübermittlungen zu untersagen, wie auch Art. 25 Abs. 1 der Richtlinie 95/46/EG, der ausdrücklich klarstellt, dass eine Übermittlung "vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist", ergibt sich, dass die nationalen Aufsichtsbehörden trotz der Safe-Harbor-Zertifizierung des Empfängers im Einzelfall Übermittlungen dorthin untersagen dürfen. Auch die Standardvertragsklauseln sehen eine entsprechende Befugnis zur Aussetzung von Datentransfers durch die nationalen Aufsichtsbehörden ausdrücklich vor.

Als Reaktion auf die Erkenntnisse über die Überwachungsmaßnahmen durch die NSA, haben die Datenschutzbeauftragten des Bundes und der Länder im Juli 2013 in einer gemeinsamen Stellungnahme darauf hingewiesen, dass sie als Aufsichtsbehörden berechtigt sind, die Datenübertragung auf Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln für unsichere Drittstaaten wie die USA vorerst auszusetzen:

„Angesichts der Berichte über die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste, insbesondere der US-amerikanischen National Security Agency (NSA), weist die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf die Befugnisse hin, die den Aufsichtsbehörden beim internationalen Datenverkehr zwischen Unternehmen in Deutschland und Drittstaaten nach dem Bundesdatenschutzgesetz und der europäischen Datenschutzrichtlinie bereits jetzt zustehen.

Die Europäische Kommission hat in mehreren Entscheidungen Grundsätze des "sicheren Hafens" ("Safe Harbor") zum Datentransfer in die USA (2000) und Standardvertragsklauseln zum Datentransfer auch in andere Drittstaaten (2004 und 2010) festgelegt. Die Beachtung dieser Vorgaben soll gewährleisten, dass personenbezogene Daten, die in die USA oder andere Drittstaaten übermittelt werden, dort einem angemessenen Datenschutzniveau unterliegen. Allerdings hat die Kommission stets betont, dass die nationalen Aufsichtsbehörden die Datenübermittlung dorthin aussetzen können, wenn eine "hohe Wahrscheinlichkeit" besteht, dass die Safe-Harbor-Grundsätze oder Standardvertragsklauseln verletzt sind.

Dieser Fall ist jetzt eingetreten. Die Grundsätze in den Kommissionsentscheidungen sind mit hoher Wahrscheinlichkeit verletzt, weil die NSA und andere ausländische Geheimdienste nach den gegenwärtigen Erkenntnissen umfassend und anlasslos ohne Einhaltung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung auf personenbezogene Daten zugreifen, die von Unternehmen in Deutschland an Stellen in den USA übermittelt werden. Zwar enthält die Safe-Harbor-Vereinbarung eine Regelung, die die Geltung der Grundsätze des "sicheren Hafens" begrenzt, sofern es die nationale Sicherheit erfordert oder Gesetze solche Ermächtigungen vorsehen. Im Hinblick auf das Ziel eines wirksamen Schutzes der Privatsphäre soll jedoch von diesen Eingriffsbefugnissen nur im Rahmen des tatsächlich Erforderlichen und nicht exzessiv Gebrauch gemacht werden. Ein umfassender und anlassloser Zugriff auf personenbezogene Daten kann daher durch Erwägungen zur nationalen Sicherheit in einer demokratischen Gesellschaft nicht gerechtfertigt werden. Auch bei Datenübermittlungen in die USA aufgrund der Standardverträge muss der Datenimporteur zusichern, dass seines Wissens in seinem Land keine Rechtsvorschriften bestehen, die die Garantien aus den Klauseln in gravierender Weise beeinträchtigen. Eine solche Generalermächtigung scheint in den USA zu bestehen; denn nur so lässt sich erklären, dass der US-amerikanische Geheimdienst auf personenbezogene Daten, die aufgrund der Standardverträge übermittelt werden, mit hoher Wahrscheinlichkeit routinemäßig zugreift.

Deshalb fordert die Konferenz die Bundesregierung auf, plausibel darzulegen, dass der unbeschränkte Zugriff ausländischer Nachrichtendienste auf die personenbezogenen Daten der Menschen in Deutschland effektiv im Sinne der genannten Grundsätze begrenzt wird. Bevor dies nicht sichergestellt ist, werden die Aufsichtsbehörden für den Datenschutz keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten (zum Beispiel auch zur Nutzung bestimmter Cloud-Dienste) erteilen und prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind."

Entsprechende Anordnungen wurden im Berichtszeitraum durch unsere Dienststelle nicht erlassen.

2.4 Binding Corporate Rules (BCR)

Ein ausreichendes Datenschutzniveau stellen auch so genannte Binding Corporate Rules (verbindliche Unternehmensrichtlinien) sicher. Bei diesem Instrument, das sich zunehmender Beliebtheit erfreut, erlegt sich eine Gruppe von Unternehmen – meist handelt es sich hierbei um Unternehmen, die einem international tätigen Konzern angehören - rechtsverbindlich Regeln in Bezug auf den Umgang mit personenbezogenen Daten auf. Hierfür gibt es ein zwischen den europäischen Aufsichtsbehörden für den Datenschutz abgestimmtes europaweites Anerkennungs- bzw. Beteiligungsverfahren, das durch die Behörde eines Mitgliedstaates federführend betreut wird.

Ist das Verfahren zur Anerkennung der BCR abgeschlossen, gilt für Datenflüsse zwischen den beteiligten Unternehmen ein angemessenes Datenschutzniveau. Abhängig von der Rechtslage in den jeweiligen Mitgliedstaaten können aber auf die datenübermittelnde Stelle weitere Anforderungen hinzukommen. So sehen die Vorschriften diverser Mitgliedstaaten eine Genehmigungspflicht für Datenflüsse auf der Grundlage von BCR vor.

Für Deutschland wird die Frage der Genehmigungsbedürftigkeit durch die zuständigen Aufsichtsbehörden uneinheitlich beantwortet. Wir vertreten hierzu die Auffassung, dass konkrete Datenflüsse durch verantwortliche Stellen mit Sitz im Saarland, die auf der Grundlage von verbindlichen Unternehmensregelungen erfolgen, vorab durch uns genehmigt werden müssen. Die Rechtsgrundlage für diese Genehmigungsbedürftigkeit ergibt sich aus § 4c Abs. 2 Bundesdatenschutzgesetz.

Soweit wir im Rahmen des europaweiten Abstimmungs- und Beteiligungsverfahrens davon Kenntnis erhalten, dass auch Firmen mit Sitz im Saarland von neu einzuführenden verbindlichen Unternehmensregelungen betroffen sind, weisen wir diese Firmen frühzeitig darauf hin, dass vor der Übermittlung personenbezogener Daten an konzernangehörige Stellen außerhalb der EU/des EWR auf der Grundlage von BCR ein Genehmigungsantrag bei uns zu stellen ist.

2.5 Zwei-Stufen-Prüfung

Allen oben genannten Instrumenten ist gemein, dass sie bei anforderungsgemäßer Umsetzung ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der hiermit verbundenen Rechte vorweisen. In der Beratungspraxis stellen wir jedoch immer wieder fest, dass verantwortliche Stellen nach Verwendung einer der genannten Instrumente davon ausgehen, dass eine Übermittlung personenbezogener Daten ohne weitere Einschränkungen zulässig ist. Hierbei wird jedoch verkannt, dass die Frage der Angemessenheit des Datenschutzniveaus nur eine Voraussetzung ist, um personenbezogene Daten an Stellen in Drittländer zu übermitteln.

Weitere Voraussetzung ist – ebenso wie bei inländischen oder innereuropäischen Datenflüssen – die Einwilligung der betroffenen Personen oder eine Rechtsvorschrift, die die in Frage stehende Übermittlung legitimiert.

Entsprechend hat sich auch der Düsseldorfer Kreis mit Beschluss vom 11. September 2013 geäußert:

Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

Bei Datenübermittlungen in einen Drittstaat, also einen Staat außerhalb des Europäischen Wirtschaftsraums, sind Datenschutzfragen auf zwei Stufen zu prüfen:

Auf der ersten Stufe ist es erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (z.B. §§ 28 und 32 Bundesdatenschutzgesetz (BDSG)) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Abs. 1 BDSG zulässig sein muss (vgl. § 3 Abs. 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfungsmaßstab in der Regel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, bei sensitiven Daten ist § 28 Abs. 6 ff. BDSG zu beachten.

Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4c BDSG vorliegen.

Die Datenübermittlung ist nur zulässig, wenn auf beiden Stufen ein positives Prüfungsergebnis vorliegt.

3 Europäischer Datenschutz

In unserer digitalen Welt nimmt der Datenschutz auf europäischer Ebene eine immer größere Rolle ein. Auch durch die fortschreitende Globalisierung sind länderübergreifende Regelungen von immer größerer Bedeutung.

3.1 EU-Datenschutz-Grundverordnung

Im Berichtszeitraum hat das Europäische Parlament die EU-Datenschutz-Grundverordnung einstimmig verabschiedet. Inhaltlich deckt sich diese Fassung weitgehend mit dem Entwurf der Kommission, der bereits im letzten Tätigkeitsbericht vorgestellt wurde.

Derzeit laufen die Abstimmungen im Ministerrat, die in 2015 abgeschlossen werden sollen. Da Änderungen gegenüber dem Kommissionsvorschlag und dem Parlamentsbeschluss zu erwarten sind, wird sich ein Trilog als Vermittlungsverfahren zwischen Rat und Parlament anschließen.

Bei der grundsätzlichen Absicht, eine für alle EU-Staaten verbindliche Verordnung zum Datenschutz zu verabschieden und damit die Datenschutz-Richtlinie aus dem Jahr 1995 abzulösen, wird es aus heutiger Sicht bleiben.

Die Ausgestaltung der künftigen Datenschutzaufsicht in Europa und die Frage, wer für europaweit agierende Unternehmen als Aufsichtsbehörde zuständig ist, war im Berichtszeitraum eines der wesentlichen Verhandlungsthemen. Deshalb hat die Konferenz hierzu im März 2014 die folgende Entschließung verabschiedet:

Zur Struktur der künftigen Datenschutzaufsicht in Europa

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle („One-Stop-Shop") vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen.

Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

1. *Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.*

2. *Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Ort der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.*

3. *Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.*

4. *Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.*

5. *Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählt die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz Folgeabschätzungen,*

   Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurate Ziehung mit den Aufsichtsbehörden geklärt werden.

6. *Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehördlicher Maßnahmen im Falle von Datenschutzverstößen führen.*

7. *Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.*

3.2 Entscheidungen des EuGH im Berichtszeitraum

Der Gerichtshof der Europäischen Union in Luxemburg (EuGH) hat mit drei wichtigen Entscheidungen den Datenschutz in Europa gestärkt.

3.2.1 „Recht auf Vergessen"

Der Europäische Gerichtshof hat in der Entscheidung vom 13. Mai 2014 zum „Recht auf Vergessen" Geschichte geschrieben. Er urteilte, dass Personen unter bestimmten Voraussetzungen die Löschung von Links mit auf sie bezogenen Daten, zum Beispiel auf alte Presseartikel mit nicht mehr aktuellen oder relevanten Informationen, aus den Ergebnislisten von Suchmaschinen verlangen können. Diese Entscheidung war so von den wenigsten Experten erwartet worden und sorgte europaweit für Kontroversen. Klarzustellen ist, dass es nicht um die generelle Löschung von Einträgen im Internet geht, es geht vielmehr darum, dass die Einträge nicht in der Suchliste von Google erscheinen, wenn bestimmte Voraussetzungen gegeben sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu in der Konferenz vom 8./9. Oktober 2014 die folgende Entschließung verabschiedet:

Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 – C-131/12 „Google Spain" einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar.

Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden.

Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll – nach einer erfolgreichen Beschwerde des Betroffenen – der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z.B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben. Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- *Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.*

- *Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.*

- *Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige*

Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.

- *Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.*

3.2.2 Vorratsdatenspeicherung

Mit seiner Entscheidung vom 8. April 2014 hat der EuGH die Richtlinie 2006/24/EG über die Vorratsspeicherung von Telekommunikationsdaten für ungültig erklärt.

Nach dieser Entscheidung ist die Einführung einer anlassfreien flächendeckenden Verkehrsdatenspeicherung unverhältnismäßig und greift in die Grundrechte auf Privatheit und auf Datenschutz ein, die in Art. 7 und Art. 8 der Europäischen Grundrechte-Charta verbrieft sind.

In der Presseerklärung des Europäischen Gerichtshofes heißt es hierzu:

„Der Gerichtshof stellt zunächst fest, dass den auf Vorrat zu speichernden Daten insbesondere zu entnehmen ist,

1. *mit welcher Person ein Teilnehmer oder registrierter Benutzer auf welchem Weg kommuniziert hat,*

2. *wie lange die Kommunikation gedauert hat und von welchem Ort aus sie stattfand und*

3. *wie häufig der Teilnehmer oder registrierte Benutzer während eines bestimmten Zeitraums mit bestimmten Personen kommuniziert hat.*

Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert werden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen und das soziale Umfeld.

Der Gerichtshof sieht in der Verpflichtung zur Vorratsspeicherung dieser Daten und der Gestattung des Zugangs der zuständigen nationalen Behörden zu ihnen einen besonders schwerwiegenden Eingriff der Richtlinie in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten. Außerdem ist der Umstand, dass die Vorratsspeicherung der Daten und ihre spätere Nutzung vorgenommen werden, ohne dass der Teilnehmer oder der registrierte Benutzer darüber informiert wird, geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist. ….“

Zwar hat das Gericht die Vorratsspeicherung als "nützliches Mittel" angesehen, das zur Aufklärung schwerer Straftaten geeignet sein kann. Zugleich hat es jedoch darauf hingewiesen, dass schon die Pflicht zur

anlasslosen Speicherung einen besonders schwerwiegenden Eingriff in das Recht auf Privatheit und den Datenschutz der Betroffenen darstellt.

Ausdrücklich hat der Gerichtshof festgestellt, dass das an sich legitime Ziel der Bekämpfung schwerer Straftaten für sich genommen die Erforderlichkeit der Pflicht zur Vorratsspeicherung nicht rechtfertigt.

Dem genügte die Richtlinie offenkundig nicht.

Insbesondere schrieb sie die Speicherung von Telekommunikations-Verkehrsdaten fast der gesamten europäischen Bevölkerung vor.

Hierzu gehörten auch solche Personen, deren Verhalten nicht einmal in einem entfernten Zusammenhang zu schweren Straftaten steht oder die einem Berufsgeheimnis unterliegen. Auch musste kein Zusammenhang zwischen den auf Vorrat gespeicherten Daten und einer Bedrohung der öffentlichen Sicherheit bestehen.

In der mündlichen Verhandlung vor dem Europäischen Gerichtshof konnten die Verteidiger der Richtlinie auch nicht die zwingende Erforderlichkeit zur Bekämpfung schwerer Straftaten nachweisen.

Die bisherige EU-Innenkommissarin Cecilia Malmström hat in einem Interview angekündigt, nach dem EuGH-Urteil keinen erneuten Gesetzesentwurf zur Vorratsdatenspeicherung vorzulegen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu dieser Entscheidung am 25. April 2014 die folgende Entschließung verabschiedet:

Ende der Vorratsdatenspeicherung in Europa:

Der Europäische Gerichtshof hat in seinem Urteil vom 8. April 2014 die Europäische Richtlinie zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten (Richtlinie 2006/24/EG) für ungültig erklärt.

Dieses Urteil hat weitreichende Folgen für den Datenschutz in Europa.

Die Datenschutzbeauftragten des Bundes und der Länder haben die anlasslose und massenhafte Speicherung von Verkehrsdaten der Telekommunikation stets abgelehnt. Sie begrüßen die Entscheidung des Europäischen Gerichtshofs als wichtigen Schritt zur Bekräftigung der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses.

Der Europäische Gerichtshof hat in seinem Urteil der undifferenzierten und automatischen Totalerfassung solcher Daten eine klare Absage erteilt. Er hat darauf hingewiesen, dass schon die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff großen Ausmaßes in das Recht auf Privatleben und den Datenschutz der Betroffenen darstellt. Diese in der Europäischen Grundrechte Charta verbrieften Rechte dürften nur eingeschränkt werden, soweit dies absolut notwendig ist. Die für ungültig erklärte Richtlinie entsprach diesen Vorgaben nicht, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung der Verkehrsdaten verpflichtete.

Nach dem Urteil des Gerichtshofs kann eine undifferenzierte Pflicht zur anlasslosen und flächendeckenden Vorratsdatenspeicherung unionsrechtlich nicht mehr neu begründet werden. Die Absichtserklärung der

Bundesregierung, zurzeit kein Gesetz zur Speicherung von Verkehrsdaten einzuführen, wird von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt. Etwaige Diskussionen auf europäischer Ebene sollten abgewartet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist ausdrücklich darauf hin, dass der Maßstab des EuGH auch für das anlasslose exzessive Überwachen durch sämtliche Nachrichtendienste gelten muss. Zudem hält der Gerichtshof die Pflicht zur großflächigen Speicherung von personenbezogenen Daten nur dann für zulässig, wenn die Daten in der Europäischen Union gespeichert werden und damit unter die Kontrolle unabhängiger Datenschutzbehörden fallen. Dies zwingt auch zu einer Neubewertung z.B. der Fluggastdaten-Übermittlung in die USA und des Safe-Harbor-Abkommens.

3.2.3 Private Videoüberwachung

Mit Urteil vom 11. Dezember 2014 hat der EuGH entschieden, dass die EU-Datenschutzrichtlinie auch auf privat betriebene Videoüberwachungen Anwendung findet, wenn damit öffentlicher Raum, wie z.B. Straßen und Gehwege, überwacht wird. Der EuGH kam zu dem Ergebnis, dass solche Videoüberwachungen nicht als ausschließlich persönliche oder familiäre Tätigkeiten von der Anwendung der EU-Datenschutzrichtlinie ausgenommen sind, da durch die – auch nur teilweise – Überwachung des öffentlichen Raums die private Sphäre des Anlagenbetreibers verlassen wird.

Darüber hinaus hat der EuGH bestätigt, dass eine Speicherung der mittels einer Videoüberwachung gewonnenen Bilddaten als automatisierte Verarbeitung im Sinne der EU-Datenschutzrichtlinie zu qualifizieren ist.

Für Betreiber von Videoüberwachungsmaßnahmen hat diese Entscheidung weitreichende Konsequenzen. Das Bundesdatenschutzgesetz, in welchem die Regelungen der EU-Datenschutzrichtlinie in deutsches Recht umgesetzt sind, sieht u.a. vor, dass Videoüberwachungsmaßnahmen, mit deren Hilfe Bilddaten gespeichert werden und die somit als Verfahren automatisierter Verarbeitung anzusehen sind, grundsätzlich vor ihrer Inbetriebnahme der zuständigen Aufsichtsbehörde zu melden sind (§ 4d Abs. 1 BDSG).

Bereits mit Pressemitteilung vom 23. Januar 2014 hatte das Unabhängige Datenschutzzentrum Saarland darauf hingewiesen, dass für Betreiber von Videoüberwachungsanlagen eine gesetzliche Pflicht besteht, diese der Aufsichtsbehörde zu melden und dass die unterlassene, unrichtige oder verspätete Meldung mit einem Bußgeld sanktioniert werden kann.

Durch die Verpflichtung, Videoüberwachungsanlagen der Aufsichtsbehörde zu melden, wird der gängigen Praxis solche Geräte ohne weitere Prüfung einzusetzen, ein Riegel vorgeschoben.

Der Kamerabetreiber muss sich zunächst einmal mit den rechtlichen Anforderungen an den zulässigen Betrieb einer solchen Anlage auseinandersetzen und über weniger einschneidende Alternativen nachdenken. Zudem wird die Aufsichtsbehörde in die Lage versetzt, solche Anlagen auf ihre datenschutzrechtliche Zulässigkeit hin zu überprüfen, bevor personenbezogene Daten erhoben und gespeichert werden.

4 Technisch-organisatorischer Datenschutz

4.1 Datenschutz in Smartphone-Apps

Man geht davon aus, dass mittlerweile mehr als 30 Millionen Deutsche mindestens ein, wenn nicht sogar mehrere Smartphones besitzen. Neben der Kommunikation an sich ermöglichen diese Geräte die Nutzung sogenannter Apps (engl.: application). Hierbei handelt es sich um kleine Programme, die die Funktionalität des Smartphones ergänzen und die von Drittanbietern – teilweise kostenfrei – zur Verfügung gestellt werden. Diese Apps bergen aber ein gewisses Risiko für das Recht auf informationelle Selbstbestimmung der Betroffenen. Denn abhängig von dem verwendeten System, können diese Apps Zugriff auf eine Vielzahl persönlicher Daten nehmen: sei es die Kontaktdaten von Freunden, Familienangehörigen oder Geschäftspartnern, über Fotos und Videos bis hin zu privater Kommunikation per SMS oder E-Mail. Dies geschieht, ohne dass der Anwender hiervon Kenntnis erlangt. Die Nutzer sollten sich daher vor der Installation entsprechender Apps darüber informieren, welche personenbezogenen Daten die App erhebt und verarbeitet und zu welchem Zweck dies geschieht.

Leider konnten wir feststellen, dass in Bezug auf die datenschutzrechtlichen Anforderungen an Apps sowohl bei App-Entwicklern als auch bei den App-Anbietern eine Unkenntnis über die Rechtslage besteht und dass mit den personenbezogenen Daten der Nutzer vereinzelt eher sorglos umgegangen wird. Dies wird dadurch verstärkt, dass durch die Verbreitung der Apps der Markt sich hin zugunsten von eher kleinen Entwicklerstudios verschoben hat, die mitunter keine ausreichenden Kenntnisse hinsichtlich (datenschutz-) rechtlicher Anforderungen haben. Waren es früher die großen Anbieter wie Microsoft, IBM und Adobe, deren Software-Entwicklungen von Rechtsabteilungen begleitet wurden, so hat die Verbreitung von Smartphones und die damit verbundene Einführung von sogenannten App-Stores dazu geführt, dass auch einzelne Entwickler mit einer eigenen Idee schnell und einfach einen breiten Kundenmarkt zur Verfügung haben.

Um sowohl App-Entwickler als auch App-Anbieter bei den datenschutzrechtlichen Implikationen beim Anbieten von Smartphone-Apps zu unterstützen hat der Düsseldorfer Kreis (Zusammenschluss der Aufsichtsbehörden im nicht-öffentlichen Bereich) eine Orientierungshilfe „Apps“ veröffentlicht. App-Entwickler und -Anbieter sollen damit bereits in der Konzeptions- und Entwicklungsphase einer App die datenschutzrechtlichen Vorgaben kennen und durch datenschutzgerechte Gestaltung („privacy by design“) sowie datenschutzfreundliche Voreinstellungen („privacy by default“) dafür Sorge tragen, dass die App später ohne datenschutzrechtliche Mängel angeboten werden kann.

4.1.1 Unterrichtung des Nutzers

In vielen Fällen ist dem Anbieter einer App gar nicht bekannt, dass er eine Datenschutzerklärung vorhalten muss, soweit seine App personenbezogene Daten verarbeitet. Gemäß § 13 Abs. 1 S. 1 Telemediengesetz (TMG) hat er den Nutzer „zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten [außerhalb der EU bzw. des EWR] (...) in allgemein verständlicher Form zu unterrichten". Nach Satz 3 des § 13 Abs. 1 TMG muss der Inhalt der Unterrichtung für den Nutzer jederzeit abrufbar sein. Zudem ist der Nutzer zu Beginn eines automatisierten Verfahrens, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, hierüber zu informieren (vgl. § 13 Abs. 1 S. 2 TMG).

Wie dieser Unterrichtungsverpflichtung im Falle von Smartphone-Apps konkret nachgekommen werden kann ist umstritten. Aus Sicht des Düsseldorfer Kreises bedarf es hierfür einer frühzeitigen und jederzeit abrufbereiten Unterrichtung. Dies bedeutet, dass die Datenschutzerklärung somit entweder im App-Store oder nach dem Herunterladen und vor dem Start der App für den Nutzer zum Abruf bereitgehalten werden muss. Dies kann am besten dadurch erzielt werden, dass die Datenschutzerklärung im jeweiligen App-Store eingestellt wird. Die großen Anbieter wie Google und Apple bieten entsprechende Möglichkeiten an. Jederzeitige Abrufbarkeit bedeutet, dass die Unterrichtung dabei innerhalb der App leicht auffindbar platziert werden muss. Hierbei muss auch dafür gesorgt werden, dass im Offline-Betrieb der App die Datenschutzerklärung zur Verfügung steht.

4.1.2 Sichere Datenübertragung

Regelmäßig kommuniziert die App auf dem Gerät des Nutzers mit den Server-Systemen (Backends) des Anbieters oder sonstiger Dritter. Um sicherzustellen, dass personenbezogene Daten mit normalem Schutzbedarf während des Transports nicht unbefugt gelesen oder verändert werden, verlangen wir, dass sowohl beim Versand als auch beim Empfang entsprechender Daten die Kommunikationsverbindung mit dem Backend durch eine Transportverschlüsselung abgesichert ist. Die App und auch das Backend müssen daher so konfiguriert sein, dass eine sichere Verbindung auf Grundlage einer dem Stand der Technik entsprechenden Protokollvariante nach den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder höher ausgehandelt wird (zurzeit bspw. TLS 1.1 oder höher). Sollten diese Protokolle etwa aus Kompatibilitätsgründen nicht nutzbar sein, dürfen unsichere Varianten, wie bspw. SSL 3.0 bzw. TLS 1.0, allenfalls für einen kurzen Übergangszeitraum genutzt werden. Das Server-Backend sollte bei der Aushandlung der Verschlüsselung nur starke Chiffren ($\geq$ 128 Bit, bspw. 3DES, AES) verwenden und ausreichend große Schlüssellängen ($\geq$ 2048 Bit) einsetzen. Dabei sollten nur vertrauenswürdige Zertifikate, also solche, die von einer bekannten Zertifizierungsstelle ausgestellt wurden, zum Einsatz kommen.

Personenbezogene Daten dürfen auch bei der Nutzung von Transportverschlüsselung nicht in der URL bzw. im GET-Parameter der https-Anfrage übermittelt werden, da es durch Protokollierung der Aufrufe auf Seiten der App oder des Backend-Servers (etwa durch den Serverbetreiber) trotz Verschlüsselung zur Offenbarung personenbezogener Daten kommen kann.

Durch den Einsatz kurzlebiger Sitzungsschlüssel (Perfect Forward Secrecy) ist sicherzustellen, dass ein Angreifer aufgezeichnete Verbindungen selbst bei Brechen der Verschlüsselung einer Verbindung nicht nachträglich entschlüsseln kann. Zudem sollte darauf geachtet werden, dass die zum Einsatz kommenden Softwarebibliotheken zumindest mit FIPS-140-2 Zertifizierung Stufe 1 kompatibel sind.

Werden durch oder an die App Daten mit erhöhtem Schutzbedarf, wie z.B. Gesundheits- oder Kreditkartendaten übertragen, so muss mittels Zertifikats- oder Public-Key-Pinning zusätzlich sichergestellt werden, dass Angreifer nicht durch Unterschieben vermeintlich valider Zertifikate die Verbindung kompromittieren können. Die zum Einsatz kommenden kryptographischen Algorithmen und Schlüssellängen müssen sich an der Dauer der Schutzwürdigkeit der personenbezogenen Daten orientieren (z.B. kann eine notwendige Schlüssellänge von bis zu 15360-Bit bei RSA-Verfahren bei Gesundheitsdaten höhere Anforderungen nach sich ziehen, als aktuell eingesetzte Standardverfahren anbieten).

4.2 Verbindungsverschlüsselung bei Webauftritten

Sobald personenbezogene Daten elektronisch übertragen werden, verlangen sowohl das Bundesdatenschutzgesetz als auch das Saarländische Datenschutzgesetz, dass dafür Sorge zu tragen ist, dass diese Daten während des Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies kann insbesondere durch die Anwendung kryptographischer Verfahren erreicht werden.

Insbesondere bei Webauftritten von öffentlichen und nicht-öffentlichen Stellen fordern wir den Einsatz einer Verbindungsverschlüsselung, sobald personenbezogene Daten – beispielsweise durch Verwendung eines einfachen Kontaktformulars – erhoben oder verarbeitet werden. Entsprechende Zertifikate sind bereits für geringe Euro-Beträge erhältlich und auch bereits bestehende Webseiten können im Regelfall problemlos nachgerüstet werden.

Wir empfehlen den Betreibern eines Webauftritts, ihre Seiten nur entsprechend gesichert anzubieten, auch wenn hierüber keine personenbezogenen Daten verarbeitet werden. Eine intakte Verbindungsverschlüsselung verhindert, dass die Nutzung des Internets durch Unbefugte überwacht wird oder unbefugte Dritte den Inhalt der Seite manipulieren, indem sie etwa Schadcode einschleusen. Gerade in öffentlichen Netzen ist es für die Betreiber der Netzinfrastruktur, seien dies große Internet Service Provider oder das kleine Bistro, das seinen Kunden kostenlosen WLAN Zugang ermöglicht, ohne nennenswerten Aufwand möglich, mit zu protokollieren welche Webseiten der Kunde besucht oder welche Informationen der Kunde abruft. Zudem ist es möglich diese Informationen zu manipulieren, indem etwa Werbung oder Schadcode in die Seite eingeschleust wird.

Daher haben auch die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung "Gewährleistung der Menschenrechte bei der elektronischen Kommunikation" vom 27./28. März 2014 die sichere und vertrauenswürdige Bereitstellung von Internetangeboten gefordert:

Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wieder herzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wieder hergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. *Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,*
2. *Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,*
3. *Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,*
4. *Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,*
5. *Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,*
6. *Ausbau der Angebote und Förderung anonymer Kommunikation,*
7. *Angebot für eine Kommunikation über kontrollierte Routen,*
8. *Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,*
9. *Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,*
10. *Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,*

11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,

12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o.g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

4.2.1 HeartBleed

Allein die einmalige Umsetzung einer Verbindungsverschlüsselung genügt jedoch im Regelfall nicht. Vielmehr muss die Verschlüsselung regelmäßig an die Sicherheitsanforderungen angepasst werden, indem etwa die kryptographischen Parameter (etwa die Schlüssellänge) geändert werden oder aufgetauchte Sicherheitslücken beseitigt werden.

Der letztgenannte Fall eines HeartBleed betraf im Jahr 2014 eine Vielzahl von Webdiensten weltweit. Durch einen Programmierfehler in OpenSSL, einer Softwarebibliothek, die bei der Verschlüsselung von Daten eine sehr hohe Verbreitung hat, war es möglich, bei Internetdiensten den zur Verschlüsselung von Daten verwendeten privaten (geheimen) Schlüssel auszulesen, mit der Folge, dass ein potentieller Angreifer durch Kenntnis des privaten Schlüssels nun verschlüsselte Verbindungen problemlos entschlüsseln konnte.

Als Sofortmaßnahme konnten die Webseitenbetreiber den sog. HeartBleed, eine für die Verbindungsverschlüsselung nicht zwingend erforderliche Komponente, abschalten. Eine langfristige Lösung konnte aber nur mittels einer Aktualisierung der OpenSSL-Software erreicht werden. Da zudem nicht ausgeschlossen werden konnte, dass bereits ein Angriff stattgefunden hatte und der private Schlüssel kompromittiert wurde, haben wir von den betroffenen Stellen gefordert die Weiterverwendung des bestehenden Zertifikats zu unterlassen und stattdessen ein neues Zertifikat zu installieren.

4.3 Reichweitenanalyse auf Webseiten öffentlicher Stellen

Bereits im 24. Tätigkeitsbericht für den Berichtszeitraum 2011/2012 wurde über den Beschluss des Düsseldorfer Kreises vom 26./27. November 2009 zur datenschutzkonformen Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten berichtet.

Darin hatten die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich Vorgaben für den Einsatz solcher Analyseverfahren gemacht:

- Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.

- Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.

- Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.

- Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.

- Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

Bedient sich der Seitenbetreiber bei der Einbindung von Tools zur Reichweitenanalyse Drittanbietern, so sind die oben genannten Vorgaben durch den Abschluss eines Auftragsdatenverarbeitungsvertrages sicherzustellen.

Dies hat bei einigen öffentlichen Stellen allerdings für Verwirrung gesorgt. Denn die großen kommerziellen Anbieter stellen dem Neukunden bereits alle Vertragsdokumente zur Unterzeichnung zur Verfügung. Dabei wird aber in den meisten Fällen verkannt, dass die vom Anbieter zur Verfügung gestellten Vertragsmuster zur Auftragsdatenverarbeitung für öffentliche Stellen im Saarland in der Regel ungeeignet sind. Dies liegt daran, dass die Muster in der Regel an die gesetzlichen Anforderungen des § 11 Bundesdatenschutzgesetz (BDSG) angelehnt sind und inhaltlich auf die Vorschriften des BDSG Bezug nehmen. Für öffentliche Stellen im Saarland normiert jedoch das Saarländische Datenschutzgesetz in § 5 besondere rechtliche Anforderungen für die Verarbeitung personenbezogener Daten im Auftrag. Diese Anforderungen sind in einigen Punkten mit denen des BDSG nicht kompatibel, mit der Folge, dass ein wirksamer Auftragsdatenverarbeitungsvertrag nicht zustande kommen kann und die Reichweitenanalyse nicht datenschutzkonform betrieben wird.

Öffentliche Stellen sollten also darauf achten, dass Sie vor Einsatz eines Verfahrens zur Reichweitenanalyse einen Vertrag mit dem Betreiber

abschließen, der den Anforderungen des SDSG entspricht. Hierbei ist zu berücksichtigen, dass nach § 5 Abs. 3 Satz 2 SDSG die Landesbeauftragte für Datenschutz von der Beauftragung zu unterrichten ist, soweit die dort genannten Voraussetzungen gegeben sind.[1]

4.4 Cloud Computing – technische und organisatorische Aspekte

Cloud Computing ist kein Hype mehr,
Cloud Computing wird genutzt. [2]

4.4.1 Einleitung

Was ist Cloud Computing?

Eine Definition, die in Fachkreisen meist herangezogen wird, ist die Definition der US-amerikanischen Standardisierungsstelle NIST (National Institute of Standards and Technology),[3] die auch von der ENISA (Europäische Agentur für Netz- und Informationssicherheit genutzt wird)[4]:

„Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen(z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können."

Die Datenschutzbeauftragten des Bundes und der Länder beschäftigen sich bereits seit längerer Zeit mit der Thematik des Cloud Computing. Da das Thema weiter an Aktualität gewonnen hat, wurde von den Arbeitskreisen Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises die Orientierungshilfe Cloud Computing erarbeitet. Die Orientierungshilfe richtet sich an Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche und soll den datenschutzgerechten Einsatz dieser Technologie fördern.

Der Schwerpunkt liegt dabei auf Hinweisen bei der Nutzung von Cloud-Computing-Diensten durch datenverarbeitende Stellen.

Anbieter von Cloud-Computing-Dienstleistungen können aus dieser Orientierungshilfe diejenigen Anforderungen entnehmen, die ihre Kunden aus datenschutzrechtlicher Sicht stellen.

---

[1] Uns ist derzeit kein Anbieter eines entsprechenden Analyseverfahrens bekannt, bei dem die Voraussetzungen des § 5 Abs. 3 Satz 2 SDSG nicht gegeben wären.
[2] Sichere Nutzung von Cloud-Diensten, Bundesamt für Sicherheit in der Informationstechnik.
[3] Wayne Jansen, Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, NIST, Draft Special Publication 800-144, January 2011.
[4] ENISA, CloudComputing: Benefits, Risks and Recommendations for Information Security, November 2009.

Die o.g. Orientierungshilfe Cloud Computing (Version 2.0, Stand 09. Oktober 2014) finden Sie auf unserer Homepage.

Neben den Datenschutzbeauftragten hat sich beispielsweise auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem Thema Cloud-Computing befasst und hierzu eigene Publikationen veröffentlicht.

https://www.bsi.bund.de/DE/Themen/CloudComputing/CloudComputing_node.html

Im Nachfolgenden werden wir auf einige technisch-organisatorische Aspekte bei der Einführung, Nutzung und Beendigung von Cloud-Diensten eingehen.

4.4.2 Cloud-Modelle

Bei Cloud Computing kann man die bereitgestellten Lösungen anhand unterschiedlicher **Service- und Bereitstellungsmodelle** kategorisieren.

Hierbei muss geklärt werden, welche Dienste bzw. Services durch die geplante Cloud-Lösung angeboten werden sollen (Infrastrukturen, Plattformen oder Anwendungen) und wer die zukünftige Cloud-Lösung bereitstellen soll (beispielsweise die eigene Institution oder ein Cloud Service Provider (CSP)).

Im Bereich der **Servicemodelle** wird zwischen drei verschiedene Kategorien unterschieden:

1. ***Infrastructure as a Service (IaaS)***

   Bei IaaS werden IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze als Dienst angeboten. Ein Cloud-Kunde kauft diese virtualisierten und in hohem Maß standardisierten Services und baut darauf eigene Services zum internen oder externen Gebrauch auf. So kann ein Cloud-Kunde z. B. Rechenleistung, Arbeitsspeicher und Datenspeicher anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.

2. ***Platform as a Service (PaaS)***

   Ein PaaS-Provider stellt eine komplette Infrastruktur bereit und bietet dem Kunden auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. So kann die Plattform z. B. Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe, etc. als Service zur Verfügung stellen. Der Kunde hat keinen Zugriff auf die darunterliegenden Schichten (Betriebssystem, Hardware), er kann aber auf der Plattform eigene Anwendungen laufen lassen, für deren Entwicklung der CSP in der Regel eigene Werkzeuge anbietet.

3. ***Software as a Service (SaaS)***

   Sämtliche Angebote von Anwendungen, die den Kriterien des Cloud Computing entsprechen, fallen in diese Kategorie. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt. Als Bei-

spiele seien Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung oder Kollaborationsanwendungen genannt.

Der Begriff „as a Sevice" wird noch für eine Vielzahl weiterer Angebote benutzt, wie z. B. für Security as a Service, BP as a Service (BusinessProcess), Storage as a Service, so dass häufig auch von „XaaS" geredet wird, also „irgendwas als Dienstleistung". Dabei lassen sich die meisten dieser Angebote zumindest grob einer der obigen Kategorien zuordnen.

Die Servicemodelle unterscheiden sich auch im Einfluss des Kunden auf die Sicherheit der angebotenen Dienste. Bei IaaS hat der Kunde die volle Kontrolle über das IT-System vom Betriebssystem aufwärts, da alles innerhalb seines Verantwortungsbereichs betrieben wird, bei PaaS hat er nur noch Kontrolle über seine Anwendungen, die auf der Plattform laufen, und bei SaaS übergibt er praktisch die ganze Kontrolle an den CSP.[5]

Hinsichtlich der unterschiedlichen **Bereitstellungsmodelle** (Deployment Models) unterscheidet die NIST zwischen:

*» In einer **Private Cloud** wird die Cloud-Infrastruktur nur für eine Institution betrieben. Sie kann von der Institution selbst oder einem Dritten organisiert und geführt werden und kann dabei im Rechenzentrum der eigenen Institution oder einer fremden Institution stehen.*

*» Von einer **Public Cloud** wird gesprochen, wenn die Services von der Allgemeinheit oder einer großen Gruppe, wie beispielsweise einer ganzen Industriebranche, genutzt werden können und die Services von einem Anbieter zur Verfügung gestellt werden.*

*» In einer **Community Cloud** wird die Infrastruktur von mehreren Institutionen geteilt, die ähnliche Interessen haben. Eine solche Cloud kann von einer dieser Institutionen oder einem Dritten betrieben werden.*

*» Werden mehrere Cloud Infrastrukturen, die für sich selbst eigenständig sind, über standardisierte Schnittstellen gemeinsam genutzt, wird dies **Hybrid Cloud** genannt.*

Die oben genannten Definitionen decken aber nicht alle Varianten von Cloud Angeboten ab, was zu weiteren Definitionen wie „Virtual Private Cloud", etc. führt. Während bei einer Private Cloud, bei der im Prinzip Anbieter und Nutzer identisch sind, der Nutzer die komplette Kontrolle über die genutzten Services hat, überträgt der Nutzer bei einer Public Cloud die Kontrolle an den Cloud Computing Anbieter.

4.4.3 Technische und organisatorische Aspekte

Cloud-Computing-Systeme der Cloud-Anbieter unterliegen bestimmten infrastrukturellen Rahmenbedingungen, deren Schutz bezüglich der Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz, Intervenierbarkeit und Nicht-Verkettbarkeit gewährleistet werden muss.

[5] Sicherheitsempfehlungen für Cloud Computing Anbieter, Bundesamt für Sicherheit in der Informationstechnik.

Dieser Schutz orientiert sich an dem Schutzbedarf der zu verarbeitenden personenbezogenen Daten. Die Umsetzung der Schutzziele ist durch technische und organisatorische Maßnahmen abzusichern. Die wirksame Umsetzung der technischen und organisatorischen Maßnahmen ist schriftlich nachzuweisen.[6]

4.4.4 Bedrohungen bei Cloud-Diensten

Bedrohungen für die Cloud-Infrastruktur und den Cloud-Dienst

Die Infrastruktur und die Cloud-Dienste des Cloud-Anbieters müssen von ihm gegen folgende Bedrohungen geschützt werden:

- *Datenverlust bzw. Informationsabfluss*
- *Beeinflussung der verschiedenen Nutzer in der gemeinsamen (shared) Cloud-Infrastruktur bis hin zu Angriffen aus der Cloud heraus.*
- *Ausfall der Internet- oder Netzverbindung, der den Zugriff auf Daten bzw. Anwendungen unmöglich macht.*
- *Denial-of-Service Angriffe auf Cloud-Anbieter, die sicher noch zunehmen werden.*
- *Fehler in der Cloud-Administration, die aufgrund der sehr hohen Komplexität zu erheblichen Sicherheitsproblemen führen (Dienstausfall, Datenverlust, etc.) können. Kleine Fehler oder Pannen können in einer Cloud-Infrastruktur große Auswirkungen (nicht nur auf die Sicherheit) haben.*

Bedrohungen bei der Nutzung von Cloud-Diensten

Der Cloud-Nutzer ist insbesondere folgenden Bedrohungen ausgesetzt:

- *Identitätsdiebstahl bzw. Missbrauch von Accounts*
- *Verlust der Kontrolle über die Daten und Anwendungen*
- *Verletzung geltender Vorgaben und Richtlinien (z. B. Datenschutzanforderungen)*
- *Sicherheit der Endgeräte, mit denen die Cloud-Dienste verwendet werden.*
- *Daten können über das Netz abgefangen und (bei schlechter oder nicht vorhandener Verschlüsselung) ausgespäht werden.*

Bedrohungen bei Einführung und Nutzung der Cloud

Die oben genannten Bedrohungen treten auf, wenn der Cloud-Dienst angeboten und genutzt wird. Doch auch auf dem Weg in die Cloud lauern auf einen Cloud-Anwender weitere Gefahren.

[6] Orientierungshilfe Cloud Computing (Version 2.0/09.10.2014).

- *Es gibt keine Cloud-Strategie und deshalb sind die Ziele, die mittels Cloud Computing erreicht werden sollen, weder klar noch überprüfbar.*

- *Kritische Elemente im Einführungsprozess wurden aufgrund einer mangelhaften Planung übersehen, und das angedachte Cloud Projekt scheitert.*

- *Der Cloud Service ist ungenau definiert und es kommt zu Differenzen über die Servicequalität mit dem Cloud-Anbieter. Infolgedessen erhält der Cloud-Anwender entweder eine ungenügende Service-Qualität oder teure Nachbesserungen werden notwendig.*

- *Großer (politischer) Wille, Cloud Computing auf jeden Fall einzusetzen, führt zu illusorischen Annahmen und zu „geschönten" Kosten-Nutzen-Analysen. Im Endeffekt kommt es zu finanziellen Einbußen.*

- *Der Weg in die Cloud kann sehr schwierig sein und es kann leicht übersehen werden, dass auch an einen Weg aus der Cloud heraus gedacht werden muss. Andernfalls entsteht eine starke Abhängigkeit vom Cloud-Anbieter, die finanziell von Nachteil sein kann.*

- *Flexibilität beziehen Cloud-Anbieter auf die innerhalb eines Service zur Verfügung gestellten Kapazitäten. Andere Wünsche der Cloud-Anwender können oft nicht erfüllt werden, eigene Eingriffsmöglichkeiten sind sehr begrenzt.*

- *Ein Cloud-Anbieter bezieht selbst häufig Dienste (z. B. Administration oder Backup von Daten) von Unterauftragnehmern. Dadurch können beispielsweise personenbezogene Daten an nicht erlaubte Stellen gelangen (was ggf. Bußgeld-bewährt ist) oder es kann dadurch ein Sicherheitszertifikat gefährdet werden, weil ein Auditor diesen Unterauftragnehmer nicht überprüfen kann.*

- *Notfall? Welcher Notfall? Die Cloud ist doch immer da und deshalb hat der Cloud-Anwender keinen Notfallplan.*[7]

4.4.5 Einführung, Nutzung und Beendigung eines Cloud-Dienstes

Die Gefahr, dass ein Cloud-Projekt scheitert, ist ohne ein strukturiertes Vorgehen deutlich erhöht. Zwar können in manchen Fällen ad-hoc eingeführte Cloud-Dienste erfolgreich genutzt werden, doch das ist eher die Ausnahme. Planung und Evaluierung dürfen aber nicht so umfangreich werden, dass das Ziel – die Nutzung von Cloud-Diensten und den damit einhergehenden Vorteilen – nicht erreicht werden kann.

Um zu einer tragfähigen und auch wirtschaftlichen Entscheidung zu kommen, müssen die Ziele, die mit dem avisierten Cloud-Service ver-

[7] Sichere Nutzung von Cloud-Diensten, Bundesamt für Sicherheit in der Informationstechnik.

knüpft sind, klar sein. Vonseiten des Cloud-Anwenders ist aber auch Flexibilität gefordert: in Bereichen der Funktionalität ebenso wie in der Sicherheit. Nicht alle Wünsche und Anforderungen werden sich realisieren lassen, da Cloud-Angebote meist stark standardisiert sind. Im Zuge der Evaluation von Cloud-Diensten muss klar werden, wie weit ein angebotener Service von den eigenen Zielen entfernt ist. Nur so lassen sich ggf. alternative Wege einschlagen.[8]

Das Bundesamt für Sicherheit in der Informationstechnologie gibt in seiner Publikation „Sichere Nutzung von Cloud-Diensten" Empfehlungen zu einem sicheren Weg in die Cloud.

https://www.bsi.bund.de/DE/Themen/CloudComputing/Dossiers/Anwender/AnwenderEinsteiger/Sichere_Nutzung_Cloud.html

4.4.6 Fazit

Cloud Computing steht für vielfältige Möglichkeiten, Dienstleistungen zur Datenverarbeitung unter Verwendung des Internet oder anderer Wide Area Networks wie Konzernnetze oder die Landesnetze der Verwaltungen in Anspruch zu nehmen. Ob Public, Private, Community oder Hybrid Clouds, ob SaaS, PaaS oder IaaS: Allen Varianten gemein ist, dass die Anwender Leistungen von Anbietern in Anspruch nehmen, die über das jeweilige Netz erreicht werden können, die wegen ihrer Skalierbarkeit flexibel an den jeweils aktuellen Bedarf angepasst werden können und nach Verbrauch bezahlt werden. Bei allen Varianten unterschiedlich sind jedoch der Umfang und die Art der Dienstleistung, die Bestimmt- oder Unbestimmtheit der Verarbeitungsorte, die Einflussmöglichkeiten der Anwender auf die örtlichen, infrastrukturellen und qualitativen Rahmenbedingungen der Verarbeitung. Unterschiedlich sind auch die datenschutzrechtlichen und informationssicherheitstechnischen Anforderungen.

Zu verlangen sind also mindestens

- *offene, transparente und detaillierte Informationen der Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Anwender klare Entscheidungskriterien bei der Wahl zwischen den Anbietern haben, aber auch, ob Cloud Computing überhaupt in Frage kommt;*
- *transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud gestützten Auftragsdatenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und Interoperabilität für den Fall, dass z. B. wegen einer Insolvenz des Anbieters die Datenverarbeitung zu einem anderen Anbieter „umziehen" kann;*
- *die Umsetzung von abgestimmten Sicherheitsmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender;*

[8] Sichere Nutzung von Cloud-Diensten, Bundesamt für Sicherheit in der Informationstechnik.

- *die Vorlage aktueller Zertifikate, die die Infrastruktur betreffen, die bei der Auftragserfüllung in Anspruch genommen wird, zur Gewährleistung der Informationssicherheit und der o. g. Portabilität und Interoperabilität durch anerkannte und unabhängige Prüfungsorganisationen.*[9]

4.5 Datenschutzfreundlichere Browsereinstellungen

Durch das Nutzen des Internets und seiner Vielzahl an Diensten fallen unzählige Informationen an, die gespeichert und ausgewertet werden.

All diese Informationen stellen Spuren dar, die von den Endgeräten selbst, aber auch von den zum Datentransfer genutzten Serversystemen weiterverarbeitet werden.

Beim Aufruf einer Website werden vom verwendeten Endgerät unter Umständen Informationen über die Einstellungen des genutzten Webbrowsers, Bildschirminformationen, Standortdaten, sowie die IP-Adresse an den Webserver übermittelt. Der angesteuerte Webserver bietet Cookies an, die vom Webbrowser auf dem Endgerät gespeichert werden. Diese Cookies ermöglichen eine Wiedererkennung und somit eine Profilbildung des Internetbenutzers.

Eventuell sind noch Formularfelder auf der jeweiligen Website auszufüllen oder es wird ein Login von der Website angefordert. Je nach Browsereinstellungen werden die eingegebenen Informationen sowie die eingegebenen Passwörter auf dem lokalen System abgespeichert.

4.5.1 Handreichung, Browser datenschutzfreundlicher einzustellen

Um den Datenschutz im Umgang mit dem Internet zu erhöhen, bestehen Möglichkeiten, die jeweiligen Browsersysteme entsprechend zu konfigurieren. Allerdings stellen diese Einstellungen keine allumfassende Sicherheit dar, da auch z. B. beim anonymen Surfen Daten an Kommunikationspartner im Internet übermittelt werden.

Vor diesem Hintergrund erstellte das Unabhängige Datenschutzzentrum Saarland eine Handreichung mit Tipps und Empfehlungen im Hinblick auf datenschutzfreundlichere Browsereinstellungen.

Nachfolgend werden einige Themen der Handreichung vorgestellt.

Nachverfolgung

Beim Navigieren durch das Internet hinterlässt der Browser Informationen über sich, das verwendete IT-System und über die bisher besuchten Internetseiten.

[9] Orientierungshilfe Cloud Computing (Version 2.0/09.10.2014).

Der Nutzer hinterlässt dadurch im Internet Spuren, die zu einem Nutzerprofil zusammengefasst werden können.

Heutige Browser bieten Einstellungsmöglichkeiten an, die eine Nachverfolgung durch Websites vermindern.

Das Unabhängige Datenschutzzentrum empfiehlt, den Browser so zu konfigurieren, dass die angesteuerten Websites die getätigten Aktivitäten nicht verfolgen.

Cookies

Websites bieten den zugreifenden Browsern kleine Dateien an, in denen sie Informationen abspeichern, die sogenannten Cookies. Diese bieten die Möglichkeit der eindeutigen Wiedererkennung des Benutzers. Sie werden oft zu Marketingzwecken eingesetzt, um unter anderem das Benutzerverhalten zu ermitteln und kundenspezifische Werbung anzubieten.

Aus dem Grund, dass aus Datenschutzsicht die Erhebung von Benutzerinformationen nicht erforderlich ist und um einem Missbrauch entgegenzuwirken, empfiehlt das Unabhängige Datenschutzzentrum den Browser so zu konfigurieren, dass er keine Cookies abspeichert.

Chronik, Verlauf

Über die Chronik bzw. den Verlauf des Browsers können bereits besuchte Websites schnell wiedergefunden werden. Die Chronik birgt jedoch die Gefahr, dass Dritte Kenntnis z. B. über die besuchten Internetseiten erlangen.

Um den Gefahren entgegenzuwirken wird empfohlen, den Browser so einzustellen, dass er keine Chronik bzw. keinen Verlauf anlegt.

Pop-ups

Beim Aufruf von Websites öffnen sich gelegentlich sogenannte Pop-Up-Fenster, die z. B. Produktwerbungen enthalten. Mit diesen Pop-ups besteht beispielsweise auch die Möglichkeit, einen schadhaften Code auf den Rechner des Benutzers einzuschleusen.

Daher empfiehlt das Datenschutzzentrum, generell Pop-ups zu blockieren.

Plug-ins und Add-ons

Um den Browser mit weiteren Funktionalitäten auszustatten, werden kleine Programme zur Installation angeboten, die sogenannten Add-ons oder Plug-ins. Dadurch dass diese Software oftmals von Drittherstellen stammt, kann eine fehlerfreie Programmierung nicht garantiert werden. Ebenso lässt sich nicht feststellen, ob diese Erweiterungen Daten an die jeweiligen Hersteller übermitteln.

Es wird empfohlen, vor der Installation von Browser-Erweiterungen zu überprüfen, ob sie notwendig sind und von welchen Anbietern die Software stammt.

Darüber hinaus sollte der Browser so eingestellt werden, dass der Benutzer gewarnt wird, wenn Websites versuchen Add-ons zu installieren.

Passwörter

Eine besondere Gefahr für Datenschutz und Datensicherheit besteht darin, wenn der Browser Passwörter abspeichert.

Diese sollten niemals abgespeichert werden, denn diese könnten in die falschen Hände geraten. Zum Beispiel könnte das verwendete Computersystem von einer Schadsoftware befallen sein, welche die gespeicherten Passwörter, mitsamt Benutzerdaten, an Unbefugte weiterleitet.

Browser immer aktuell halten

Die Browserentwickler arbeiten permanent an Aktualisierungen der Browsersoftware, einerseits um neue Funktionalitäten einzuprogrammieren, andererseits um entstandene Sicherheitslücken zu schließen.

Um möglichen Gefahren, die durch fehlerhafte Browser entstehen entgegenzuwirken, empfiehlt das Datenschutzzentrum die eingesetzten Browser auf dem aktuellen Stand zu halten.

Betrachtete Webbrowser

Desktop

- Mozilla Firefox (Version 33.1),
- Microsoft Internet Explorer (Version 11),
- Google Chrome (Version 39.0.2171.71).

Mobil

- Apple Safari (iOS 8),
- Google Browser (Android 4.2.2),
- Microsoft Internet Explorer (WindowsPhone 8.1).

Die in der Handreichung behandelten Themen stellen Momentaufnahmen dar. Behandelt werden verschiedene gängige Webbrowser für Desktop-PCs, Smartphones und Tablets.

Die Handreichung steht in Form einer Internetpräsentation unter *www.datenschutz.saarland.de* zur Verfügung.

5 Verfassungsschutz

5.1 Änderung des Saarländischen Verfassungsschutzgesetzes

5.1.1 Urteil des Bundesverfassungsgerichts zur Bestandsdatenauskunft

Mit Beschluss vom 24. Januar 2012 (1 BvR 1299/05) hat das Bundesverfassungsgericht die Regelungen über das manuelle Auskunftsverfahren in § 113 des Telekommunikationsgesetzes (TKG) teilweise für verfassungswidrig erklärt.

Gegenstand der Entscheidung war u.a. die in § 113 Abs. 1 Satz 1 TKG a. F. enthaltene Verpflichtung von Anbietern von Telekommunikationsdiensten, Bestandsdaten ihrer Kunden (d. h. Name und Anschrift des Anschlussinhabers, zugeteilte Rufnummer und andere Anschlusskennungen) den Strafverfolgungs- und Ermittlungsbehörden preiszugeben. Dies galt nach § 113 Abs. 1 Satz 2 TKG a.F. auch für Auskunftsverlangen hinsichtlich solcher Daten, mittels derer der Zugriff zu Endgeräten geschützt wird, wie Passwörter, PINs oder PUKs.

Das Bundesverfassungsgericht hatte entschieden, dass die in dem bisherigen § 113 Abs. 1 Satz 1 TKG normierte Auskunftsverpflichtung der Telekommunikationsunternehmen in verfassungskonformer Auslegung mit dem Grundgesetz vereinbar ist. Voraussetzung für eine zulässige Datenübermittlung sei allerdings, dass den abrufberechtigten Behörden eigenständige und normklare Erhebungsbefugnisse zustünden. Ein Datenaustausch vollziehe sich nämlich durch einander korrespondierende Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen. Beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten („Doppeltürenmodell").

Zum anderen dürfe die Vorschrift - mangels entsprechender normenklarer Regelung in Anbetracht des damit verbundenen Eingriffs in das Fernmeldegeheimnis des Artikel 10 Abs. 1 Grundgesetz (GG) - nicht zur Zuordnung dynamischer IP-Adressen angewendet werden.

Außerdem hatte das Gericht entschieden, dass die Regelung des § 113 Abs. 1 Satz 2 TKG insoweit verfassungswidrig ist, als sie Auskünfte über Zugangscodes unabhängig davon erlaube, ob den empfangenden Behörden überhaupt eine Befugnis zu deren Nutzung zukomme. Das Bundesverfassungsgericht gestand den Gesetzgebern und Behörden allerdings eine Übergangsfrist bis zum 30. Juni 2013 zu; bis zu diesem Zeitpunkt durften die genannten Behörden Auskünfte über den Inhaber dynamischer IP-Adressen sowie über Zugangscodes aufgrund der bisherigen Regelung verlangen und erhalten, sofern im Falle eines Auskunftsersuchens über Zugangscodes eine einzelfallbezogene Befugnis zu deren Nutzung vorlag.

Das aufgrund dieser Entscheidung verabschiedete Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestands-

datenauskunft ist zum 1. Juli 2013 in Kraft getreten (BGBl. I S. 1602). Durch dieses Gesetz werden die Anforderungen des Bundesverfassungsgerichts sowohl durch Änderung des TKG umgesetzt als auch die geforderten spezifischen Erhebungsbefugnisse in den bundesrechtlichen Fachgesetzen geregelt.

5.1.2 Anpassung des Saarländischen Verfassungsschutzgesetzes

Da die Gesetzgebungskompetenz für den Bereich des Gefahrenabwehrrechts bei den Ländern liegt, waren durch den Landesgesetzgeber sowohl im Saarländischen Verfassungsschutzgesetz als auch im Saarländischen Polizeigesetz (s. Kapitel 7.1) die für eine Bestandsdatenauskunft erforderlichen Erhebungsbefugnisse zu schaffen.

In einem erst nach Ablauf der vom Bundesverfassungsgericht vorgegebenen Umsetzungsfrist von den Regierungsfraktionen eingebrachten Gesetzentwurf sollten dem saarländischen Landesamt für Verfassungsschutz in Bezug auf die Erhebung der Bestandsdaten die gleichen Befugnisse eingeräumt werden, wie sie die Neuregelung im Bundesrecht auch dem Bundesamt für Verfassungsschutz zugesteht. Aus diesem Grunde enthielt die entsprechende Vorschrift im Gesetzentwurf lediglich pauschale Verweise auf die Regelung in § 8d des Bundesverfassungsschutzgesetzes (BVerfSchG).

Im Rahmen der Beteiligung unserer Dienststelle im parlamentarischen Verfahren wurde darauf hingewiesen, dass die beabsichtigte Ausgestaltung dieser Abfrageermächtigung dem Gebot der Normenklarheit und Normenbestimmtheit nicht gerecht wird, da sich die tatbestandlichen Voraussetzungen und der Umfang der geregelten Maßnahmen dem Wortlaut des Entwurfes nicht eindeutig entnehmen ließen; insbesondere war auch die Reichweite der Verweisung auf § 8d BVerfSchG nicht hinreichend klar.

Aus diesem Grunde haben wir eine Neuformulierung der betreffenden Vorschrift im Gesetzentwurf als erforderlich angesehen. Neben weiteren, dem Schutz der Betroffenen dienenden Verfahrensregelungen haben wir insbesondere auch eine Pflicht zur Benachrichtigung der Betroffenen im Anschluss an Auskunftsverfahren über Zugangssicherungscodes und über die Zuordnung von dynamischen IP-Adressen eingefordert. Denn nur durch eine nachträgliche Benachrichtigung wird den Betroffenen die Möglichkeit eröffnet, zumindest im Nachgang des Auskunftsverfahrens dieses gerichtlich auf seine Rechtmäßigkeit hin überprüfen zu lassen. Ebenso wurde es unsererseits als erforderlich angesehen, bei einer Auskunft über die Zuordnung von dynamischen IP-Adressen die G 10-Kommission zu beteiligen, da die Telekommunikationsunternehmen für die Identifizierung einer dynamischen IP-Adresse die entsprechenden Verbindungsdaten ihrer Kunden sichten und somit auf konkrete, vom Schutzbereich des Art. 10 GG umfasste Telekommunikationsvorgänge zugreifen müssen.

Die letztlich durch das Parlament verabschiedete Fassung der Regelung enthält nunmehr nicht lediglich einen Verweis auf § 8d BVerfSchG, sondern regelt die Voraussetzungen für den Abruf der Bestandsdaten. Inhaltlich ist die Norm der Vorschrift des § 8d BVerfSchG angelehnt und enthält auch die geforderte Verpflichtung zur Benachrichtigung. Auf

eine Beteiligung der G 10-Kommission bei Auskünften über den Inhaber einer IP-Adresse wurde jedoch verzichtet. Ebenso wie sämtliche Bundes- und auch die Mehrzahl der Landesnormen, die die Erhebung von Zugangssicherungscodes regeln, sieht das Gesetz vor, dass diese Auskunft nur verlangt werden kann, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Welches die gesetzlichen Voraussetzungen für die Nutzung von Zugangssicherungscodes sind, wird jedoch nicht definiert.

Neben der Regelung über die Durchführung einer Bestandsdatenauskunft wurden mit dem Gesetzentwurf auch die Vorschriften für die akustische Wohnraumüberwachung an die Rechtsprechung des Bundesverfassungsgerichts angepasst, eine rechtliche Grundlage für den Einsatz des sog. IMSI-Catchers geschaffen sowie die Regelungen der parlamentarischen Kontrolle des Verfassungsschutzes überarbeitet.

In unserer Stellungnahme wurde hinsichtlich der Befugnis zur Durchführung einer akustischen Wohnraumüberwachung darauf hingewiesen, dass nach der Formulierung in dem Gesetzentwurf – wie auch bereits in der geltenden Fassung des Gesetzes - eine Wohnraumüberwachung bereits dann zulässig ist, wenn *tatsächliche Anhaltspunkte für den Verdacht verfassungsfeindlicher Bestrebungen* vorliegen. Damit knüpfe die Vorschrift nicht an eine absehbare konkrete Gefahr, sondern an einen Eingriffsanlass im Vorfeld einer solchen Gefahr an. Da eine Wohnraumüberwachung jedoch einen besonders intensiven Eingriff in das Grundrecht der Unverletzlichkeit der Wohnung nach Art. 13 GG darstellt, genügt eine gesetzliche Regelung, die zu einem solchen heimlichen Eingriff berechtigt, nur dann dem Grundsatz der Verhältnismäßigkeit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt.

Diesem Kritikpunkt wurde durch eine Neuformulierung der Eingriffsschwelle Rechnung getragen.

Durch die in das Gesetz aufgenommenen Regelungen zur Verwertung von Gesprächsinhalten, die sich auf den Kernbereich privater Lebensgestaltung beziehen, wird der Rechtsprechung des Bundesverfassungsgerichts in seiner Entscheidung zur akustischen Wohnraumüberwachung Rechnung getragen. In dem Gesetz wurden die in diesem Zusammenhang geäußerten datenschutzrechtlichen Bedenken im Wesentlichen berücksichtigt. Allerdings beziehen sich die getroffenen Vorkehrungen allein auf Überwachungsmaßnahmen innerhalb des Schutzbereichs des Artikels 13 GG. Da aber auch bei der Durchführung von Telekommunikationsüberwachungsmaßnahmen hinreichende Vorkehrungen dafür zu treffen sind, dass Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung unterbleiben, hätte es auch hier dringend einer gesetzlichen Regelung bedurft. Eine solche wurde vom Landesgesetzgeber jedoch nicht umgesetzt.

Schließlich wurden auch die im Gesetzentwurf noch unklaren und unbestimmten Vorschriften bezüglich des Umgangs mit den durch die Maßnahme gewonnenen Daten sowie der Benachrichtigung der von der Maßnahme betroffenen Personen in dem schließlich verabschiedeten Gesetz konkretisiert, so dass sie nunmehr die Anforderungen an die Klarheit und Bestimmtheit von Rechtsnormen erfüllen.

Leider nicht berücksichtigt wurden unsere Anregungen und Einwände in Bezug auf die Regelungen über die parlamentarische Kontrolle.

Bisher sah § 23 Abs. 4 des Saarländischen Verfassungsschutzgesetzes (SVerfSchG) vor, dass der für die parlamentarische Kontrolle der Tätigkeit des Landesamtes für Verfassungsschutz zuständige Ausschuss für Fragen des Verfassungsschutzes seine Tätigkeit über das Ende der Wahlperiode des Landtages hinaus bis zur Bestimmung eines neuen Ausschusses durch den neuen Landtag ausübte. Aufgrund verfassungsrechtlicher Bedenken wurde diese Regelung aufgehoben, so dass nunmehr auch dieser Ausschuss der Diskontinuität unterliegt.

Allerdings steht die jetzige Rechtslage nicht in Einklang mit den Vorschriften des SVerfSchG über die parlamentarische Kontrolle. Hiernach ist der Ausschuss nämlich vierteljährlich über bestimmte Maßnahmen zu unterrichten. Da es nach den Regelungen der Saarländischen Verfassung nach einer Landtagswahl bis zur Regierungsbildung und damit bis zur Zusammensetzung der Ausschüsse aber bis zu vier Monate dauern kann, kann dies dazu führen, dass die gesetzlich vorgegebene parlamentarische Kontrolle nicht mehr sichergestellt ist.

Ebenfalls nicht aufgegriffen wurden unsere Forderungen nach mehr Transparenz der nachrichtendienstlichen Aktivitäten gegenüber dem Parlament sowie nach einer Stärkung der parlamentarischen Kontrollgremien. Verloren gegangenes Vertrauen in die nicht zuletzt im Zusammenhang mit den Taten des rechtsextremistischen Nationalsozialistischen Untergrunds (NSU) in die Kritik geratene Tätigkeit der Sicherheitsbehörden kann unserer Auffassung nach nur durch mehr Offenheit und eine bessere parlamentarische Kontrolle zurückgewonnen werden.

Im Zuge einer solchen künftigen Gesetzesänderung sollten daher die Kontrollbefugnisse des Ausschusses für Fragen des Verfassungsschutzes ausgeweitet und eine Pflicht zur regelmäßigen Berichterstattung des Ausschusses über seine Kontrolltätigkeit an den Saarländischen Landtag festgelegt werden.

Schließlich haben wir in dem laufenden Gesetzgebungsverfahren darauf hingewiesen, dass weitere Anpassungen des Verfassungsschutzgesetzes an die Rechtsprechung des Bundesverfassungsgerichts dringend erforderlich sind. Es bleibt zu hoffen, dass die notwendigen Änderungen baldmöglich durch den Gesetzgeber auf den Weg gebracht werden.

Das Gesetz wurde am 12. November 2014 durch den Landtag beschlossen und ist am 19. Dezember 2014 in Kraft getreten.

6 Justiz

6.1 Saarländisches Strafvollzugsgesetz

Im Zuge der im Jahre 2006 verabschiedeten Föderalismusreform ist die Gesetzgebungskompetenz für den Justizvollzug auf die Länder übergegangen. Im Berichtszeitraum erfolgte in Wahrnehmung dieser Gesetzgebungsbefugnis die Verabschiedung eines Erwachsenenstrafvollzugsgesetzes. Im Rahmen dieses Gesetzgebungsverfahrens wurden auch einige Regelungen des bereits 2009 in Kraft getretenen Saarländischen Untersuchungshaftvollzugsgesetzes und des Jugendstrafvollzugsgesetzes aus dem Jahre 2010 den neuen Regelungen für den Erwachsenenvollzug angepasst.

Im Rahmen der Beteiligung unserer Dienststelle an dem Verfahren haben wir auf einige datenschutzrechtliche Defizite in dem Gesetzentwurf hingewiesen, die jedoch bedauerlicherweise nur in wenigen Bereichen Berücksichtigung gefunden haben.

Wie schon im Saarländischen Untersuchungshaftvollzugsgesetz und im Saarländischen Jugendstrafvollzugsgesetz ist es auch vorliegend zu beanstanden, dass es das Gesetz zulässt, bei unüberwindlichen sprachlichen Verständigungsschwierigkeiten bei der Aufnahme eines neuen Gefangenen in der Anstalt einen anderen Gefangenen zu dem Zugangsgespräch hinzuzuziehen. Ein anderer - wenn auch zuverlässiger - Gefangener ist jedoch grundsätzlich nicht befugt, die sensiblen personenbezogenen Daten des aufzunehmenden Gefangenen, die zwangsläufig in einem Zugangsgespräch erörtert werden, zur Kenntnis zu nehmen.

Soweit es das Gesetz erlaubt, erkennungsdienstliche Unterlagen aller Gefangenen auch in kriminalpolizeilichen Sammlungen vorsorglich zu verwahren, um – entsprechend der Gesetzesbegründung - die Fahndung nach abgängigen Gefangenen zu beschleunigen, widerspricht diese Befugnis dem Grundsatz der Datensparsamkeit, da für diesen – sehr selten eintretenden Fall - eine spezielle Befugnis zur Übermittlung der Daten an die zuständigen Stellen ausreichend wäre.

Im Rahmen der Datenschutzprüfung der Justizvollzugsanstalt Saarbrücken im Jahre 2012 (24. Tätigkeitsbericht, 5.1.4) wurde eine Vielzahl von Videoüberwachungsanlagen in der Anstalt vorgefunden, allerdings fehlte zumindest für die durch die Anstalt vorgenommene Speicherung von Aufnahmen eine bereichsspezifische rechtliche Grundlage. Dass nunmehr eine ausdrückliche Regelung für den Einsatz von Videoüberwachungsanlagen verabschiedet worden ist, ist ausdrücklich zu begrüßen, allerdings ist die in dem Gesetz vorgesehene Speicherdauer von vier Wochen unverhältnismäßig lang. Um den mit der Speicherung personenbezogener Daten verbundenen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen so gering wie möglich zu halten, müssen die erhobenen Daten dann gelöscht werden, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr erforderlich sind. Nach dem Gesetzeswortlaut ist es der Zweck der Speicherung, die Sicherheit der Anstalt zu gewährleisten. Zur Feststellung, ob es tatsächlich

zu Vorfällen gekommen ist, die die Sicherheit der Anstalt beeinträchtigt haben, wird ein Zeitraum von maximal 48 Stunden als ausreichend anzusehen sein. Eine längerfristige Speicherung stellt hingegen eine unzulässige Datensammlung auf Vorrat dar.

6.2 Verordnung über die elektronische Aktenführung in Bußgeldverfahren

In dem vorangegangenen Tätigkeitsbericht (24. Tätigkeitsbericht, Ziffer 9.2) haben wir angemahnt, dass die Zentrale Bußgeldbehörde die Akten der Verkehrsordnungswidrigkeitenverfahren im Wesentlichen bereits in elektronischer Form führt, das Saarland aber bislang noch nicht von seiner Ermächtigung zum Erlass der erforderlichen Rechtsverordnung für die elektronische Aktenführung nach § 110b Abs. 1 Satz 2 Ordnungswidrigkeitengesetz (OWiG) Gebrauch gemacht hat. Im Berichtszeitraum hat die Landesregierung nunmehr diese erforderliche Grundlage für eine elektronische Aktenführung in Bußgeldverfahren erlassen (Amtsbl. 2014, 147). Dabei wurde die Forderung der Landesbeauftragten in Bezug auf die Zweckbindung der gespeicherten Daten, die Gewährleistung von Zugriffsbeschränkungen und die Sicherstellung der Verfügbarkeit der Daten aufgegriffen.

6.3 Einführung eines bundesweiten Vollstreckungsportals

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung (BGBl. I S. 2258) wurden im Jahre 2009 die rechtlichen Voraussetzungen dafür geschaffen, dass der Inhalt der Schuldnerverzeichnisse über eine zentrale länderübergreifende Abfrage im Internet eingesehen werden kann. Seit dem 1. Januar 2013 ist das Gemeinsame Vollstreckungsportal der Länder (*www.vollstreckungsportal.de*) verfügbar. Hier werden die bundesweiten Daten aus den Schuldnerverzeichnissen zum kostenpflichtigen Abruf bereitgestellt. Für jedes Bundesland wurde ein zentrales Vollstreckungsgericht eingerichtet.

Die Einzelheiten der Einsichtnahme sollten vom Bundesministerium der Justiz durch eine Rechtsverordnung geregelt werden. Ein erster Entwurf genügte jedoch nicht den gebotenen datenschutzrechtlichen Anforderungen. Vorgesehen war, dass bereits bei der Suche mit einem Nachnamen und dem zuständigen Vollstreckungsgericht eine Trefferliste mit allen Personen angezeigt werden sollte, auf die beide Kriterien zutreffen. Dies hätte dazu geführt, dass die anfragende Person Informationen über Schuldner erhielte, für deren Kenntnis kein berechtigtes Interesse besteht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte daher in einer Entschließung vom 07. Februar 2012 gefordert, bei der Regelung der Einsicht in das Schuldnerverzeichnis die Angabe weiterer Identifizierungsmerkmale zwingend vorzusehen.

„Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert das Bundesministerium der Justiz auf, für einen besseren Datenschutz bei der geplanten Internetabfrage aus dem Schuldnerverzeichnis Sorge zu tragen. Es sollen möglichst nur diejenigen Personen angezeigt werden, auf die sich der Abfragezweck bezieht.

Wer eine Wohnung vermieten oder einen Ratenkredit einräumen will, möchte wissen, ob sein zukünftiger Schuldner Zahlungsschwierigkeiten hat. Er hat unter bestimmten Voraussetzungen ein legitimes Interesse an der Einsicht in das von den zentralen Vollstreckungsgerichten geführte Schuldnerverzeichnis. So können sich mögliche Geschäftspartner darüber informieren, ob ihr Gegenüber in wirtschaftliche Not geraten ist.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung aus dem Jahr 2009 will der Gesetzgeber die Stellung des Gläubigers stärken. Das Gesetz sieht unter anderem vor, dass der Inhalt des Schuldnerverzeichnisses ab dem 01.01.2013 über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden kann. Die Ausgestaltung der damit wesentlich erleichterten Einsicht wird derzeit vom Bundesministerium der Justiz durch eine Rechtsverordnung im Einzelnen vorbereitet.

Die gesetzliche Regelung erlaubt Privatpersonen die Einsicht in das Schuldnerverzeichnis nur für bestimmte Zwecke, die bei einer Anfrage darzulegen sind, zum Beispiel, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Dennoch ist es derzeit vorgesehen, dass bereits nach Eingabe eines Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Bundesland eingerichtet sind, erhielte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner, deren Kenntnis sie zum angestrebten Zweck nicht benötigt.

Es ist zu befürchten, dass beispielsweise Vermieter Mietinteressenten nicht berücksichtigen, weil im Schuldnerverzeichnis namensgleiche Personen stehen und es ihnen zu mühsam oder zu schwierig erscheint, anhand weiterer Angaben zu prüfen, ob es sich beim Mietinteressenten tatsächlich um eine der eingetragenen Personen handelt. Auch aus der Sicht der Gläubiger ist die Anzeige von derart umfangreichen Ergebnislisten wenig hilfreich, denn um den auf die Anfrage bezogenen Datensatz aus der Liste auswählen zu können, müssen ohnehin weitere Daten wie zum Beispiel der Vorname bekannt sein. Da es für Geschäftspartner erforderlich ist, mehr als nur den Nachnamen und den Sitz des zuständigen Vollstreckungsgerichts voneinander zu kennen, ist es auch nicht unangemessen, eine Einsicht von vornherein von weiteren Angaben abhängig zu machen.

Aus Sicht des Datenschutzes ist eine Anzeige von Schuldnerdaten, die nicht vom legitimen Abfragezweck erfasst werden, zu vermeiden. Deshalb halten es die Datenschutzbeauftragten des Bundes und der Länder für notwendig, bei der Regelung der Einsicht in das Schuldnerverzeich-

nis die zwingende Angabe weiterer Identifizierungsmerkmale vorzusehen."

Die schließlich vom Bundesministerium der Justiz erlassene Schuldnerverzeichnisführungsverordnung (SchuFV) hat dieser Forderung Rechnung getragen. Für eine Übermittlung von Daten an einen Nutzer müssen der Name und Vorname oder die Firma des Schuldners und der Sitz des zuständigen zentralen Vollstreckungsgerichts oder der Wohnsitz des Schuldners oder das Geburtsdatum oder der Ort, an dem der Schuldner seinen Sitz hat, angegeben werden. Sofern zu einer Abfrage mehrere Datensätze vorhanden sind, muss der Nutzer zusätzlich auch das Geburtsdatum des Schuldners eingeben. Sollten danach wiederum mehrere Datensätze vorhanden sein, ist zudem die Angabe des Geburtsortes des Schuldners erforderlich.

Erste bundesweite Erfahrungen in der Praxis haben gezeigt, dass die bisherige Regelung des § 8 SchuFV zu zahlreichen Falschmeldungen führt. Zum großen Teil ist dies auf das verlangte Identifikationsdatum „Geburtsort" zurückzuführen, da dieses Datum bei Eintragung in das Schuldnerverzeichnis häufig nicht vorliegt und auch nicht ermittelt werden kann. Auch die Angabe des Sitzes des zentralen Vollstreckungsgerichts wird teilweise für überflüssig gehalten, da hierdurch die Trefferwahrscheinlichkeit nur unwesentlich erhöht werde. Die geplante Änderung ist aber bislang nicht in Kraft getreten. Ob sich die Änderung des Suchsystems bewährt, wird im Rahmen einer weiteren Evaluierung zu prüfen sein.

6.4 Fortlaufender Bezug von Vollabdrucken aus dem Schuldnerverzeichnis

Bis zum 1. Januar 2013 oblag die Führung des Schuldnerverzeichnisses den Amtsgerichten als Vollstreckungsgerichte. Aufgrund des Gesetzes zur Reform der Sachaufklärung in der Zwangsvollstreckung (BGBl. I S. 2258) wird das Schuldnerverzeichnis mittlerweile landesweit bei dem zentralen Vollstreckungsgericht, das im Saarland bei dem Amtsgericht Saarbrücken eingerichtet wurde, geführt. Die Einsicht in das Schuldnerverzeichnis ist nach § 882f Zivilprozessordnung (ZPO) jedem gestattet, der darlegt, die dort gespeicherten Angaben zu den in der Vorschrift aufgeführten Zwecken, wie beispielsweise zur Zwangsvollstreckung, zu benötigen. Nach § 882g Abs. 2 Nr. 3 ZPO können u.a. Antragstellern, deren berechtigtem Interesse durch Einzeleinsicht in die Länderschuldnerverzeichnisse nicht hinreichend Rechnung getragen werden kann, auf Antrag Abdrucke zum laufenden Bezug aus dem Schuldnerverzeichnis erteilt werden.

Seit Inkrafttreten der Regelung zur Einführung des Zentralen Vollstreckungsgerichts haben sich mehrere Beschwerdeführer an die Landesbeauftragte für Datenschutz gewandt, da sie im Rahmen von Selbstauskünften aus dem Schuldnerverzeichnis festgestellt hatten, dass einer bestimmten Gemeinde Abdrucke aus dem Schuldnerverzeichnis auch über ihre Person erteilt worden sind. Da die Betroffenen in keinerlei Beziehung zu dieser Kommune standen und die Kommune auch keine offenen Forderungen ihnen gegenüber hatte, waren sie der Ansicht, die

Übermittlung der Angaben aus dem Schuldnerverzeichnis sei zu Unrecht erfolgt.

Auf Nachfragen teilten das Zentrale Vollstreckungsgericht und die betroffene Gemeinde mit, dass der Gemeinde bereits nach dem bis zum 1. Januar 2013 geltenden Recht die Bewilligung des laufenden Bezugs von Abdrucken aus dem Schuldnerverzeichnis bezogen auf das Vollstreckungsgericht, in dessen Amtsgerichtsbezirk die Gemeinde liegt, erteilt worden sei. Nach Inkrafttreten der Neuregelung sei dem Antrag der Gemeinde auf Bewilligung des laufenden Bezugs von Vollabdrucken aus dem Schuldnerverzeichnis für Zwecke der Zwangsvollstreckung stattgegeben worden. Ein besonderes Bedürfnis an dem laufenden Bezug von Abschriften wurde durch die Gemeinde nicht geltend gemacht.

Gegenüber dem Zentralen Vollstreckungsgericht als der bewilligenden Stelle haben wir darauf hingewiesen, dass weder erkennbar ist noch von der Gemeinde dargelegt wurde, weshalb sie in einem derart großen Umfang Informationen aus dem Länderschuldnerverzeichnis benötigt.

Bereits aus der Gesetzesbegründung zu § 882g ZPO (BT-Drs. 16/10069) ergibt sich, dass bei Verwaltungsbehörden ein berechtigtes Interesse am Bezug nicht schon vermutet wird. Vielmehr führt die Gesetzesbegründung aus, dass die Voraussetzungen für Zwecke der Zwangsvollstreckung regelmäßig nur dann vorliegen, wenn eine Verwaltungsbehörde in großem Umfang Informationen aus dem Schuldnerverzeichnis benötigt.

Zwar ist die Gemeinde auch Vollstreckungsgläubigerin, bei einer Einwohnerzahl von unter 15.000 Einwohnern kann indes nicht angenommen werden, dass regelmäßig eine besonders große Anzahl von Informationen aus dem Schuldnerverzeichnis benötigt wird. Vielmehr ist davon auszugehen, dass ihren Bedürfnissen auch durch Einzeleinsichten Rechnung getragen werden kann. Besteht jedoch kein Bedürfnis für einen laufenden Bezug von Abdrucken aus dem Schuldnerverzeichnis, erfolgt die Übermittlung der großen Anzahl von für die Gemeinde nicht erforderlichen Daten insoweit ohne eine ausreichende Rechtsgrundlage.

Dem Interesse der Gemeinde, bei Bedarf jederzeit in das Schuldnerverzeichnis Einsicht nehmen zu können, könnte auch durch eine gesonderte Registrierung für Behörden nach § 7 Schuldnerverzeichnisführungsverordnung Rechnung getragen werden.

Mit Blick auf diese Rechtslage haben wir den Präsidenten des Amtsgerichts um Prüfung gebeten, ob vorliegend eine Rücknahme der Bewilligung zum laufenden Bezug von Abdrucken aus dem Schuldnerverzeichnis in Erwägung gezogen wird. Hierauf teilte der Präsident des Amtsgerichts mit, dass die Gemeinde auf den bewilligten Bezug von Abdrucken aus dem Schuldnerverzeichnis mit sofortiger Wirkung verzichtet habe.

Damit ist sichergestellt, dass die Gemeinde zukünftig nur noch in den für sie erforderlichen Fällen Einblick in das Schuldnerverzeichnis erhält und hiermit das informationelle Selbstbestimmungsrecht der in das Schuldnerverzeichnis Eingetragenen gewahrt bleibt.

6.5 Tätigwerden einer Hilfsperson im Schiedsverfahren

Eine Gemeinde ist an die Landesbeauftragte für Datenschutz mit der Frage herangetreten, ob es zulässig sei, dass eine Mitarbeiterin der Kommune auch die Sachbearbeitung für eine Schiedsperson übernehme. Deren Tätigkeit im Rahmen des Schiedsverfahrens umfasse die Entgegennahme von Anträgen, die Anforderung und Zusammenstellung der erforderlichen Unterlagen, die Erstellung von Kostenrechnungen, Protokoll- und Kassenbuchführung sowie die Fertigung der Abschlussberichte für das Amtsgericht.

Nach den Vorschriften der Saarländische Schiedsordnung ist für jede Gemeinde zur Schlichtung streitiger Rechtsangelegenheiten eine Schiedsfrau oder ein Schiedsmann zu bestellen, die ehrenamtlich tätig sind und die der Verschwiegenheitsverpflichtung unterliegen. Die Sachkosten des Amtes der Schiedspersonen tragen die Gemeinden.

Im Rahmen der geschilderten Tätigkeiten zur Unterstützung der Aufgaben der Schiedsperson werden zahlreiche, zum Teil auch sensible personenbezogene Daten von den am Schlichtungsverfahren beteiligten Parteien verarbeitet. Nach § 4 des Saarländischen Datenschutzgesetzes (SDSG) ist eine Verarbeitung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder die oder der Betroffene eingewilligt hat.

Die Saarländische Schiedsordnung enthält keine Regelung, die es der Schiedsperson erlaubt, sich zur Erfüllung ihrer Aufgaben einer Hilfsperson zu bedienen. Die Tatsache, dass die Schiedsordnung ausdrücklich auch nur eine Erstattung von Sachkosten regelt, belegt zudem, dass das Anfallen von Personalkosten nicht vorgesehen ist.

Die Aufgabenübertragung einschließlich der hierbei anfallenden Verarbeitung personenbezogener Daten kann auch nicht auf der Grundlage einer Auftragsdatenverarbeitung nach § 5 SDSG auf Mitarbeiter der Gemeinde übertragen werden. Denn hierbei würde es sich nicht um eine Datenübertragung im technischen Sinne, sondern um eine teilweise inhaltliche Zuständigkeitsverlagerung handeln. Eine solche Übertragung einer hoheitlichen Tätigkeit ist ohne eine gesetzliche Regelung nicht zulässig.

Da die hier heranzuziehenden Rechtsvorschriften die Möglichkeit der Hinzuziehung von Hilfskräften für die Bearbeitung der Verfahren gerade nicht vorsehen, kann die fehlende gesetzliche Befugnis schließlich auch nicht durch eine jeweils individuell zu erteilende Einwilligung der Betroffenen zur Verarbeitung ihrer personenbezogenen Daten durch Dritte umgangen werden. Dies insbesondere auch deshalb, weil die Schiedsfrau oder der Schiedsmann durch die Schiedsordnung zur Amtsverschwiegenheit verpflichtet ist, diese Verschwiegenheitspflicht nicht aber auch für eine Hilfsperson gelten würde. Das von einem Gemeindebediensteten zu wahrende Datengeheimnis bezüglich aller im Rahmen dieser Tätigkeit zur Kenntnis gelangten personenbezogenen Daten beinhaltet keine Verschwiegenheitspflicht für sonstige außerdienstliche Tätigkeiten wie sie hier beabsichtigt sind.

Daher musste der Gemeindeverwaltung mitgeteilt werden, dass eine Verarbeitung von im Schiedsverfahren anfallender personenbezogener Daten durch Mitarbeiter der Gemeindeverwaltung nach der derzeitigen

Rechtslage datenschutzrechtlich unzulässig ist. Dem durchaus nachvollziehbaren Interesse der Schiedspersonen, sich für die Erfüllung ihrer Aufgaben einer Hilfsperson zu bedienen, kann nur durch eine Änderung der Schiedsordnung Rechnung getragen werden.

7 Polizei

7.1 Gesetz zur Änderung des Polizeirechts

Bereits im Jahre 2011 wurde unserer Dienststelle ein Referentenentwurf zur Änderung des Saarländischen Polizeigesetzes (SPolG) und des Saarländischen Verfassungsschutzgesetzes (SVerfG) zur Stellungnahme übersandt. Dieser Gesetzentwurf wurde allerdings nicht weiter verfolgt. Erst Anfang 2014 wurde uns ein neuer, deutlich umfangreicherer Referentenentwurf für ein Polizeirechtsänderungsgesetz zur Stellungnahme im Rahmen der externen Anhörung vorgelegt, durch den unter anderem das Saarländische Polizeigesetz (SPolG) sowie die Verordnung über die Zulassung der Informationsübermittlung von der Polizei an ausländische Polizeibehörden geändert werden sollte.

Ein großer Teil der in unserer umfangreichen Stellungnahme geäußerten datenschutzrechtlichen Kritikpunkte und Anregungen wurde aufgegriffen und fand Niederschlag in dem im Mai 2014 dem Parlament zur Beratung vorgelegten Gesetzentwurf (LT-Drs. 15/899).

Neu in das SPolG eingefügt wurde neben einer Befugnis zur Aufzeichnung eingehender Notrufe zur Dokumentation des Notfallgeschehens auch eine Befugnis zur Aufzeichnung sonstiger Anrufe, soweit dies zur Gefahrenabwehr erforderlich ist. Unserer Forderung, in der Vorschrift deutlich zum Ausdruck zu bringen, dass eine Aufzeichnung solcher Anrufe nur im Einzelfall erfolgen darf, wurde nicht nachgekommen. Zumindest wurde aber die Vorschrift dahingehend ergänzt, dass der Anrufer – soweit nicht der Zweck der Aufzeichnung gefährdet wird - auf die Aufzeichnung hinzuweisen ist.

Erstmals enthält das Polizeigesetz nunmehr eine Legaldefinition der Begriffe Observation und längerfristige Observation. Zudem ist die Einführung eines zusätzlichen Richtervorbehalts beim Einsatz einer längerfristigen Observation und eine zeitliche Befristung dieser richterlichen Anordnung für zunächst drei Monate normiert. Soweit die Voraussetzungen fortbestehen, kann die Anordnung wiederholt um bis zu drei Monate verlängert werden. Angesichts des mit der längerfristigen Observation verbundenen erheblichen Grundrechtseingriffs in das informationelle Selbstbestimmungsrecht und das Persönlichkeitsrecht des Betroffenen haben wir jedoch beanstandet, dass keine zeitliche Höchstdauer für wiederholende Anordnungen vorgesehen ist.

Im Zuge der Novellierung des Polizeigesetzes wurde im Sinne des vom Bundesverfassungsgericht (BVerfG) entwickelten sog. Doppeltürenmodells (Beschluss vom 24. Januar 2012 - BvR 1299/05 – (s.a. Kapitel 5.1.1) für eine manuelle Bestandsdatenauskunft eine sich auf die Datenübermittlungsbefugnis der Telekommunikationsanbieter nach § 113 Telekommunikationsgesetz (TKG) beziehende gesetzliche Abfragegrundlage für die Polizei geschaffen. Diese Erhebungsbefugnis entspricht im Wesentlichen den (Mindest-)Anforderungen des Verfassungsgerichts. Allerdings sieht die Vorschrift vor, dass die Erhebung der in § 113 Abs. 1 Satz 2 TKG genannten Zugangsdaten nur dann verlangt werden kann, wenn auch die Voraussetzungen für deren Nutzung gegeben sind. Mit

dieser Formulierung übernimmt das Gesetz nur diese abstrakt formulierte Anforderung des Bundesverfassungsgerichts, ohne konkret festzulegen, für welche Zwecke und unter welchen Voraussetzungen eine Nutzung der Zugangssicherungscodes durch die Polizei in Frage kommt. Dies wäre jedoch zu konkretisieren gewesen.

Als nicht akzeptabel haben wir die in dem Referentenentwurf enthaltene Regelung angesehen, wonach ein Auskunftsverlangen ohne richterliche Anordnung erfolgen sollte, wenn der Betroffene von dem Auskunftsverlangen bereits Kenntnis hat oder haben muss. Ein lediglich nachträglicher Rechtsschutz vermag keine ausreichende Sicherung für die Grundrechtspositionen des Betroffenen zu gewährleisten. Diesen Bedenken wurde im weiteren Gesetzgebungsverfahren durch Streichung dieser Vorschrift Rechnung getragen, so dass der Richtervorbehalt uneingeschränkt gilt.

Durch den Gesetzentwurf sind darüber hinaus die Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung, die bislang allein für die akustische Wohnraumüberwachung sowie für die Überwachung und Aufzeichnung der Telekommunikation galten, auch auf Observationen, das Abhören oder Aufzeichnen des gesprochenen Wortes auf Tonträger und den Einsatz von verdeckten Ermittlern erstreckt worden.

Schließlich werden durch das Polizeirechtsänderungsgesetz verschiedene Rechtsakte der Europäischen Union zum EU-weiten Austausch personenbezogener Daten in nationales Recht umgesetzt. In diesem Zusammenhang wurde von unserer Seite insbesondere eingefordert, jede Übermittlung personenbezogener Daten zum Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung und der Sicherstellung der Integrität und Sicherheit der Daten zu dokumentieren. Entsprechende Nachbesserungen waren in dem in das parlamentarische Verfahren eingebrachten Gesetzentwurf sodann enthalten und wurden durch den Landtag verabschiedet.

Aufgehoben wurde durch den Gesetzgeber schließlich die Befugnis der Ortspolizeibehörden zur offenen Bildaufzeichnung an öffentlich zugänglichen Orten. Damit wurden die bereits bei der Einführung der Befugnis im Jahre 2007 durch unsere Dienststelle erhobenen massiven Zweifel an der Erforderlichkeit einer solchen Regelung bestätigt und nunmehr unserer Forderung auf Streichung Rechnung getragen.

Ebenso wurde endlich auch die gleichfalls schon bei ihrer Einführung aus datenschutzrechtlicher Sicht kritisierte Befugnis zur automatisierten Kennzeichenerfassung aufgehoben, nachdem das Bundesverfassungsgericht schon im Jahre 2008 eine vergleichbare landesrechtliche Regelung als zu unbestimmt und unverhältnismäßig und damit als verfassungswidrig angesehen hat.

Am 12. November hat der Landtag das Polizeirechtsänderungsgesetz verabschiedet; am 19. Dezember 2014 ist das Gesetz in Kraft getreten.

7.2 Antiterrordatei (ATD)

Bei der Antiterrordatei (ATD) handelt es sich um eine gemeinsame Datenbank von verschiedenen deutschen Sicherheitsbehörden wie dem

Bundeskriminalamt, der Bundespolizei, dem Bundesamt für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, dem Zollkriminalamt, den Länderpolizeien und den Landesämtern für Verfassungsschutz. Diese Verbunddatei wurde auf der Rechtsgrundlage des Antiterrordateigesetzes (ATDG) zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland errichtet.

7.2.1 Änderungsbedarf des Antiterrordateigesetzes (ATDG) aufgrund der hierzu ergangenen Rechtsprechung des Bundesverfassungsgerichts

Das Bundesverfassungsgericht (BVerfG) hat durch Urteil vom 24. April 2013 (1 BvR 1215/07) entschieden, dass die ATD in ihren Grundstrukturen mit dem Recht auf informationelle Selbstbestimmung vereinbar ist, jedoch hinsichtlich ihrer Ausgestaltung im Einzelnen den verfassungsrechtlichen Anforderungen nicht genügt. Dem Gesetzgeber wurde eine Frist bis zum 31. Dezember 2014 eingeräumt, die beanstandeten Regelungen nach den Vorgaben des Gerichts zu überarbeiten und umzusetzen. Die beanstandeten Regelungen wurden jedoch nicht mit sofortiger Wirkung ungültig, sondern durften bis zum 31. Dezember 2014 weiter mit besonderen Maßgaben hinsichtlich Datenzugriff und -recherchen angewendet werden.

Eine Verbunddatei zwischen Sicherheitsbehörden wie die ATD bedarf nach Auffassung des Gerichts hinsichtlich der zu erfassenden Daten und ihrer Nutzungsmöglichkeiten einer hinreichend bestimmten und dem Übermaßverbot entsprechenden gesetzlichen Ausgestaltung. Im Einzelnen war demnach zur **Bestimmung der beteiligten Behörden**, zur **Reichweite der als terrorismusnah erfassten Personen**, zur **Einbeziehung von Kontaktpersonen**, zur **Nutzung von verdeckt bereitgestellten erweiterten Grunddaten**, zur **Konkretisierungs-befugnis** der Sicherheitsbehörden für die zu speichernden Daten und zur **Gewährleistung einer wirksamen Aufsicht** durch den Gesetzgeber nachzubessern.

Das Gesetz zur Änderung des Antiterrordateigesetztes und anderer Gesetze (ATDGuaÄndG) wurde am 18. Dezember 2014 im Bundesgesetzblatt veröffentlicht (BGBl I 2014, 2318) und trat fristgemäß zum 1. Januar 2015 in Kraft.

Hinsichtlich der Bestimmung der beteiligten Behörden wurde in § 1 Abs. 2 ATDG nunmehr eine Verordnungsermächtigung geschaffen, die es dem Bundesministerium des Innern gestattet, per Rechtsverordnung auf Ersuchen des jeweiligen Landes weitere Polizeivollzugsbehörden zur Teilnahme an der ATD zuzulassen, jedoch nur sofern auf diese die in den Ziffern 1 und 2 festgelegten Voraussetzungen zutreffen.

Zu den als terrorismusnah erfassten Personen erfolgte in § 2 Satz 1 ATDG insoweit eine Klarstellung, als mit dem Unterstützen einer terroristischen Gruppierung nur die willentliche Förderung derselben gemeint ist. Für die Erfassung von Personen als Befürworter von Gewalt wurde ebenso klargestellt, dass es Anhaltspunkte geben muss, dass die zu erfassende Person tatsächlich Gewalt anwendet, unterstützt, vorbereitet und hervorrufen will.

Bei Kontaktpersonen handelt es sich nun nach § 3 Abs. 2 ATDG um solche Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie mit den als terrorismusnah erfassten Personen nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind. Angaben zu Kontaktpersonen dürfen nur noch als erweiterte Grunddaten mit nunmehr gesetzlich bestimmten Datenarten zur Identifizierung und Kontaktaufnahme gespeichert werden.

Wenn die abfragende Behörde ohne Angabe eines Namens in den erweiterten Grunddaten sucht, erhält sie im Falle eines Treffers künftig nach § 5 Abs. 1 Satz 5 ATDG lediglich Zugriff auf Daten wie Angabe der Behörde, die über die Erkenntnisse verfügt, das zugehörige Aktenzeichen oder sonstige Geschäftszeichen und - soweit vorhanden - die jeweilige Einstufung als Verschlusssache.

Da Datenkategorien wie Volkszugehörigkeit, Religionszugehörigkeit, besondere Fähigkeiten, Tätigkeiten in sicherheitsempfindlichen Bereichen und besuchte Orte relativ unbestimmt und auch weit auslegbar sind, forderte das BVerfG eine entsprechende Konkretisierung sowie zur Gewährleistung der Transparenz eine nachvollziehbare Dokumentation und Veröffentlichung etwaiger Konkretisierungsrichtlinien. Durch § 3 Abs. 4 ATDG wurde das Bundeskriminalamt demzufolge verpflichtet, in einer Verwaltungsvorschrift entsprechende Konkretisierungskriterien festzulegen, welche im Bundesanzeiger zu veröffentlichen sind.

In § 10 Abs. 2 ATDG wurde nunmehr für die Bundesbeauftragte und die Landesbeauftragten für Datenschutz eine verpflichtende, mindestens alle zwei Jahre durchzuführende Datenschutzkontrolle normiert.

7.2.2 Prüfung der ATD beim Landespolizeipräsidium (LPP)

Mit Blick auf die oben ausgeführte Rechtsprechung des BVerfG zur ATD und die nunmehr normierte Prüfpflicht der Datenschutzbeauftragten hat unsere Dienstelle im März 2014 eine entsprechende schriftliche Prüfankündigung zur Datenschutzkontrolle der ATD an das LPP gerichtet. Zur Vorbereitung der Prüfung baten wir, uns im Rahmen einer Informationsveranstaltung zunächst die Grundzüge der Datenverarbeitung in der Antiterrordatei (wer wird wo wie lange gespeichert), etwaige Datenübermittlungen, die jeweiligen Zugriffsberechtigungen, die Funktionsweise von Suchabfragen sowie ggf. besondere Datensicherheitsaspekte zu erläutern.

Da der Protokollserver für die ATD sich beim Bundeskriminalamt (BKA) befindet und ein Direktzugriff der Länderpolizeien auf die zu ihren ATD-zugriffsberechtigten Mitarbeitern gespeicherten Protokolldaten nicht möglich ist, baten wir gleichzeitig die für einen von uns festgelegten Zeitraum von zwei Wochen angefallenen Protokolldaten der im LPP auf die ATD zugriffsberechtigten Personen beim BKA anzufordern. Auf dem Protokollserver des BKA wurden sogenannte Reports zur Ausweisung bestimmter Auswertungskriterien programmiert, wie neu angelegte Objekte, geänderte Objekte, gelöschte Objekte, angesehene Objekte und Suchanfragen.

Das LPP kam unserer Bitte um eine Informationsveranstaltung am 29. April 2014 nach und legte uns gleichzeitig die für das Verfahren ATD erforderliche Errichtungsanordnung vor. Die angeforderten Protokolldaten konnten jedoch trotz frühzeitiger Anforderung durch das LPP beim BKA nicht vorgelegt werden.

Erst fünf Wochen nach Anforderung der Protokolldaten beim BKA wurden diese an das LPP zur Durchführung der Datenschutzkontrolle übersandt. Da im angeforderten Auswertezeitraum nur wenige Protokolldaten angefallen sind und auch nicht zu sämtlichen Auswertekriterien Protokolldaten vorlagen, haben wir erneut um eine entsprechende Anforderung beim BKA, diesmal für einen Auswertezeitraum von einem Jahr und Anlieferungsfrist binnen zwei Wochen, gebeten.

Zwischenzeitlich wurden von uns die bereits vorliegenden Protokolldaten geprüft, indem beispielsweise getätigte Suchanfragen mit angesehenen Objekten abgeglichen wurden, so dass in einem Fall die Vorlage des Aktenrückhalts erforderlich wurde. Nach Prüfung desselben stellte sich heraus, dass es sich im konkreten Fall um eine zulässige Datenabfrage handelte.

Die Zulieferung der für einen Jahreszeitraum angeforderten Protokolldaten erfolgte durch das BKA diesmal fristgerecht. Allerdings wurden die übersandten Unterlagen - laut BKA aus Zeitgründen ohne vorherige Prüfung - als Verschlusssache „VS-Geheim" eingestuft, was besondere Sicherheitsmaßnahmen zur Ansicht der Protokolldaten erforderlich machte. Da das LPP in seinen Räumlichkeiten und mit seiner technischen Ausstattung die bei der Einstufung „VS-Geheim" erforderlichen Sicherheitsmaßnahmen gewährleisten konnte, haben wir die Protokolldaten auch dort geprüft. Mit Blick darauf, dass bei der ersten Anlieferung der Protokolldaten diese lediglich als Verschlusssache „VS - Nur für den Dienstgebrauch" eingestuft waren und nicht ersichtlich war, weshalb nunmehr höhere Anforderungen gelten mussten, war die Einstufung mit einem höheren Geheimhaltungsgrad nicht plausibel und bedeutete für unsere Dienststelle eine Erschwernis bei der Prüfung.

Nach einer ersten Prüfung der nunmehr umfassenden Protokolldaten zu allen Auswertekriterien baten wir das LPP um Erstellung einer Geschäftsprozessdarstellung hinsichtlich Erfassung, Änderung und Löschung ATD-relevanter Daten auch betreffend das Quellsystem, also der Datei, aus der Daten in die ATD geliefert werden. Im weiteren Prüfverfahren haben wir uns sodann stichprobenartig auch die entsprechenden Datensätze des Quellsystems und zu bestimmten in der ATD gespeicherten Personen auch die kompletten Gefahrenerforschungsverfahrensakten angesehen.

Es wurde deutlich, dass zwar eine Einstufung der Personen unter Staatsschutzaspekten und nach Vorgabe der Innenministerkonferenz stattfand, jedoch kein aktenkundlicher Nachweis über die Prüfung der ATD-Relevanz für die in der ATD gespeicherten Personen auf der Grundlage des ATDG. In einem Zwischengespräch mit den für die ATD zuständigen Mitarbeitern haben wir diese Problematik bereits thematisiert und gebeten, ein Formblatt zu erarbeiten, aus welchem nachprüfbar ersichtlich ist, welche Rechtsgrundlage nach dem ATDG für die Speicherung Anwendung findet und welche tragenden tatsächlichen Gesichtspunkte für die Bewertung der ATD-Relevanz ausschlaggebend sind. Zwischenzeitlich wurde durch das LPP ein Protokolldatenblatt ATD-Erfassung erstellt, das den von uns vorgetragenen Erfordernissen Rechnung trägt.

Wir beabsichtigen nach Erstellung unseres Prüfberichts eine abschließende Besprechung mit dem LPP zu führen. Schon jetzt kann aber gesagt werden, dass das LPP während der gesamten, sehr umfangreichen Prüfung konstruktiv im Sinne von § 28 Abs. 1 SDSG mit uns zusammengearbeitet hat.

Bundesweit haben die Landesbeauftragten für Datenschutz im Dezember 2014 eine Sonderarbeitsgruppe „Erfahrungsaustausch Prüfung Antiterrordatei" ins Leben gerufen. Unsere Dienststelle hat den Länderkollegen im Rahmen des Erfahrungsaustauschs zunächst über die Herangehensweise, Strukturierung der Prüfung sowie auch die bisherigen Prüfergebnisse berichtet. Vor dem Hintergrund der seit dem 1. Januar 2015 geltenden gesetzlichen Verpflichtungen zu turnusmäßigen Datenschutzkontrollen der ATD als auch der Rechtsextremismusdatei (RED) halten wir einen solchen Erfahrungsaustausch für unerlässlich.

7.3 Einsatz von Videotechnik

7.3.1 Einsatz einer Drohne durch die saarländische Polizei

Bereits im September 2011 wurde vom damaligen Landeskriminalamt (LKA) zu einer ersten Präsentationsveranstaltung zum beabsichtigten Einsatz eines unbemannten Flugsystems (Drohne) durch die saarländische Polizei eingeladen. Die Drohne sollte einer Spezialeinheit des LKA zur Einsatz- und Ermittlungsunterstützung dienen. Gleichzeitig wurde uns ein erster Entwurf einer Errichtungsanordnung (EAO) zur datenschutzrechtlichen Prüfung vorgelegt.

Da es sich bei einer solchen Drohne um ein Luftfahrzeug im Sinne des Luftverkehrsgesetzes handelt, war eine Aufstiegserlaubnis nach der Luftverkehrsordnung erforderlich, welche auch durch die zuständige Luftfahrtbehörde, dem damaligen Ministerium für Wirtschaft und Arbeit, erteilt wurde.

Der Einsatz der Drohne sollte auf der Grundlage der Spezialnormen für die Verarbeitung von Video- und Bilddaten des Saarländischen Polizeigesetzes (SPolG), der Strafprozessordnung (StPO) und des Versammlungsgesetzes (VersG) erfolgen.

Aufgrund der Rechtsprechung verschiedener Verwaltungsgerichte zur Beobachtung einer Versammlung durch die Polizei sowie auch des Bayerischen Verfassungsgerichts zur Verfassungsmäßigkeit neu geschaffener Vorschriften zur Beobachtung einer Versammlung durch die Polizei im Bayerischen Versammlungsgesetz haben wir im Rahmen der Präsentationsveranstaltung erhebliche Zweifel an der Zulässigkeit einer Videoüberwachung von Versammlungen mittels Drohne erhoben. Abschließend bestand mit den Vertretern der Polizei Konsens, den Drohneneinsatz von der Beobachtung von Versammlungen auszunehmen. Wir haben daher um Überarbeitung und Neuvorlage der EAO gebeten. Bei der uns vorgestellten Drohne handelte es sich um einen Octokopter mit der Möglichkeit, eine Tageslichtvideokamera oder eine Wärmebildkamera zu montieren. Die Bilddaten werden durch einen Videoscrambler verschlüsselt, wodurch sowohl der Zugriff auf die Daten durch unberechtigte Dritte als auch die Möglichkeit der Einspeisung anderen Bildmate-

rials verhindert wird. Die Entschlüsselung findet erst bei Speicherung auf einem externen Medium oder zur Visualisierung auf einem Monitor statt.

Im Januar 2012 wurde uns dann durch das jetzige Landespolizeipräsidium (LPP) mitgeteilt, dass sich wegen der Umsetzung der Neuorganisation der saarländischen Polizei die Überarbeitung der Errichtungsanordnung verzögern wird und diese eventuell noch ergänzt werden soll. Die umfassend überarbeitete EAO sowie auch das durch die Behördenleitung genehmigte Betriebskonzept für den Drohneneinsatz im Zuständigkeitsbereich der saarländischen Polizei wurde uns alsdann Anfang des Jahres 2013 mit der Bitte um Stellungnahme vorgelegt. Gleichzeitig wurden wir darüber informiert, dass eine entsprechende Betriebsabsprache über die Durchführung von Drohnenflügen der saarländischen Polizei in der Kontrollzone des Flughafens Saarbrücken seit dem 1. August 2012 in Kraft sei.

Das Betriebskonzept regelt Betriebsanforderungen, wann unter welchen Bedingungen der Betrieb der Drohne zulässig ist, bzw. wie in bestimmten Situationen, z.B. bei der Annäherung von anderen Luftfahrzeugen, vorzugehen ist. Darüber hinaus werden Regelungen zur Aus- und Fortbildung von Drohnenpiloten und die von ihnen zu treffenden Vorbereitungen vor einem Dohnenflug sowie Dokumentations- und Meldepflichten getroffen. Die Betriebsabsprache enthält Vereinbarungen zum Flugbetrieb wie An- und Abmeldungen beim Tower Saarbrücken und auch Festlegungen zu Flughöhe und Einsatzradius der Drohne.

In der überarbeiteten EAO war nunmehr, wie bereits mit dem LPP erörtert, der Einsatzzweck zur Beobachtung von Versammlungen ausdrücklich ausgenommen.

Was die mobile Videoüberwachungsmaßnahme durch Drohnen anbelangt, sind sowohl offene als auch verdeckte Überwachungen zulässig. Bei offenen Maßnahmen ist auf diese in geeigneter Weise hinzuweisen, verdeckte Maßnahmen lösen nachträgliche Benachrichtigungspflichten aus. Hierzu haben wir das LPP um erneute Überarbeitung und Klarstellung in der EAO gebeten. Hinsichtlich der Prüf- und Löschfristen waren die Ausführungen aus unserer Sicht zu allgemein gefasst und auch mit Blick auf die Zwischenspeicherung auf der Speicherkarte der Digitalkamera, den Datenexport auf externe Speichermedien und die entsprechenden Verantwortlichkeiten für die Löschung der Daten in den verschiedenen Organisationseinheiten des LPP für die praktische Umsetzung nicht ausreichend konkret ausformuliert. Wir haben deshalb auch hier um Nachbesserung gebeten.

Im Juni 2013 erhielten wir nunmehr eine nochmals umfassend überarbeitete EAO, welche sämtlichen zuvor dargelegten datenschutzrechtlichen Anforderungen Rechnung trug. Die maßgeblichen Rechtsgrundlagen wurden in Bezug auf offene und verdeckte Videoüberwachungen und die sich hieraus ergebenden Hinweis- oder Benachrichtigungspflichten klar strukturiert. Für die Praxis wurden Einsatzgrundsätze formuliert und die Prüf- und Löschfristen unter dem Gesichtspunkt der besseren Anwendbarkeit für die verantwortlichen Personen überarbeitet.

Mithin bestanden aus datenschutzrechtlicher Sicht, basierend auf der EAO vom 13. Juni 2013, keine Bedenken mehr gegen den Einsatz der saarländischen Polizeidrohne.

7.3.2 Einsatz mobiler Endgeräte durch die Polizei

Im Berichtszeitraum wurde bekannt, dass im Internet eine Videoaufnahme kursierte, die eine männliche Person in einem Polizeifahrzeug zeigte, die die nicht im Bild zu sehenden Polizeibeamten beschimpfte und beleidigte. Die polizeilichen Ermittlungen hierzu ergaben, dass das Verhalten des Mannes von einem Polizeibeamten zum Zwecke der Beweisführung mit dem Privat-Handy des Beamten auf Video festgehalten und der Strafakte beigefügt worden war. Anschließend wurde das Video auf dem Handy des Beamten gelöscht. In das Internet eingestellt wurde das Video durch eine nicht im Saarland wohnende Person, die nach den polizeilichen Ermittlungen über keinerlei Bezüge zur saarländischen Polizei verfügt. Wie das Video in dessen Hände gelangt ist, konnte nicht aufgeklärt werden.

Wenngleich vorliegend eine Verantwortlichkeit des Polizeibeamten für die Veröffentlichung des Videos nicht erkennbar war, zeigt der Sachverhalt deutlich, welche Gefahren mit der dienstlichen Nutzung privater Handys verbunden sind. Gerade bei der Polizei werden in großem Umfang besonders schützenswerte Daten verarbeitet, so dass bei dem Einsatz von mobilen Endgeräten strenge Sicherheitsvorkehrungen eingehalten werden müssen. Obwohl die Polizei bereits im Jahre 2009 in einem Erlass zu IT-Sicherheit und Datenschutz Regelungen für den Einsatz mobiler Endgeräte getroffen und eine Datenverarbeitung zu dienstlichen Zwecken mit privaten IT-Systemen und Softwareprodukten grundsätzlich untersagt hat, sahen wir die Notwendigkeit, die Polizeibeamten erneut für einen rechtmäßigen und verantwortungsvollen Umgang mit personenbezogenen Daten zu sensibilisieren. Als erste Maßnahme wurde durch den behördlichen Datenschutzbeauftragten der Polizei eine im polizeiinternen Intranet veröffentlichte Mitarbeiterinformation erstellt, die auf die strenge Beachtung der datenschutzrechtlichen Vorschriften hinwies. In einem zweiten Schritt wurde ein Leitfaden zur Nutzung mobiler Endgeräte erstellt, der den Polizeibeamten erneut die Gefahren bei der Nutzung mobiler Endgeräte sowie die Notwendigkeit der Beachtung geeigneter Schutzmaßnahmen vor Augen führen und somit auch Rechtssicherheit in der praktischen Anwendung geben soll.

7.4 Auskunftserteilung nach § 40 SPolG

Nach § 40 Abs. 1 Saarländisches Polizeigesetz (SPolG) ist der oder dem Betroffenen von der speichernden Stelle auf Antrag unentgeltlich Auskunft über die zu ihrer oder seiner Person gespeicherten personenbezogenen Daten sowie den Zweck und die Rechtsgrundlage der Speicherung zu erteilen.

Im Berichtszeitraum erhielten wir diverse Eingaben zu Auskunftsersuchen bei der saarländischen Polizei. In den konkreten Fällen stellte sich heraus, dass den Petenten entweder keine Auskunft erteilt wurde, da die Vorlage einer Kopie des Personalausweises für die erforderliche Identitätsfeststellung als unzureichend angesehen wurde, oder nur die in den polizeilichen Systemen und Inpol-Z gespeicherten personenbezogenen Daten beauskunftet wurden.

Zunächst wurde das Landespolizeipräsidium (LPP) daher zu den konkreten Eingaben um Stellungnahme gebeten. Darüber hinaus hielten wir es jedoch für geboten, sowohl das Verfahren als auch den Umfang der Auskunft mit Vertretern des Landespolizeipräsidiums zu erörtern und haben daher den behördlichen Datenschutzbeauftragten des LPP sowie Vertreter der für die Auskunftserteilung zuständigen Stelle zu einem gemeinsamen Besprechungstermin in unsere Dienststelle eingeladen.

Seitens des LPP wurde nachvollziehbar dargelegt, dass gerade wegen der in polizeilichen Systemen gespeicherten sensiblen personenbezogenen Daten an die Überprüfung der Identität des jeweiligen Antragstellers hohe Anforderungen - nicht zuletzt in dessen eigenem Interesse - zu stellen sind. Bislang wurde deshalb die Vorlage einer beglaubigten Ausweiskopie verlangt.

Die Vorlage einer beglaubigten Ausweiskopie ist jedoch für den Antragsteller mit entsprechenden Kosten verbunden und läuft demnach der in § 40 Abs. 1 Satz 1 SPolG geregelten Verpflichtung zur unentgeltlichen Auskunftserteilung zuwider. In dem gemeinsamen Besprechungstermin haben wir uns daher darauf verständigt, dass künftig, um der auch aus unserer Sicht erforderlichen Personenidentitätsüberprüfung Rechnung zu tragen, eine polizeilich bestätigte Ausweiskopie vorgelegt werden soll, welche in allen Polizeidienststellen des Landes kostenfrei eingeholt werden kann. Des Weiteren wurden von unserer Dienststelle Musteranträge für den Erhalt einer Auskunft nach § 40 SPolG sowie entsprechende Hinweis- und Erläuterungstexte erarbeitet, welche nach endgültiger Abstimmung mit dem LPP in Kürze auf unserer Internetseite zur Verfügung gestellt werden.

Gemäß § 40 Abs. 1 Satz 1 SPolG sind dem Betroffenen alle zu seiner Person gespeicherten Informationen mitzuteilen, es sei denn, es liegen besondere Auskunftsverweigerungsgründe nach § 40 Abs. 2 SPolG vor. Wie die im Rahmen des gemeinsamen Besprechungstermins erörterten Eingaben bei unserer Dienststelle gezeigt haben, wurde in der Vergangenheit dem Erfordernis der Beauskunftung sämtlicher zur ersuchenden Person gespeicherter Daten nicht vollumfänglich Rechnung getragen, sondern erstreckte sich die Auskunft lediglich auf POLIS-Daten und Speicherungen durch saarländische Dienststellen in Inpol-Z.

Mit Blick auf die vom Gesetzgeber gewählte eindeutige Formulierung haben wir daher das LPP gebeten, hausintern einen entsprechenden Abstimmungsprozess in die Wege zu leiten, der künftig den gesetzlichen Anforderungen Rechnung trägt und demzufolge auch die Beauskunftung von Vorgangsverwaltungsdaten in POLADIS sowie etwaiger personenbezogener Daten aus den Inpol-Fall-Dateien und auch dem saarländischen Auswerte- und Analysesystem KRISTAL vorsieht.

7.5 Abfrage und Übermittlung von POLIS-Daten in einem Beamtenrechtsstreit

Eine Datenabfrage aus dem polizeilichen Informationssystem POLIS und die anschließende Übermittlung dieser Daten an das Verwaltungsgericht haben uns veranlasst, das Vorgehen der Polizei in dem folgenden Fall zu kritisieren: Im Rahmen eines beamtenrechtlichen Verfahrens, den ein Polizeibeamter gegen seinen Dienstherrn führte, hatte das Justizia-

riat der Polizei Daten über einen von dem Kläger benannten Zeugen aus dem Polizeilichen Informationssystem Saarland (POLIS-Saarland) abgerufen und diese Daten zum Gegenstand des Verwaltungsstreitverfahrens gemacht. Alleiniger Zweck dieser Datenübermittlung war es, die Glaubwürdigkeit dieses Zeugen zu erschüttern.

POLIS-Saarland ist ein polizeiliches Informationssystem, das der Aufklärung von Straftaten sowie der Gefahrenabwehr einschließlich der vorbeugenden Bekämpfung von Straftaten dient. Daten aus dieser Datei dürfen grundsätzlich nur für die Zwecke genutzt oder übermittelt werden, für die sie erhoben worden sind. Durchbrechungen dieses Zweckbindungsprinzips sind nur dann zulässig, wenn die Daten ebenfalls für die Erfüllung der genannten polizeilichen Aufgaben erforderlich sind. Dieses Prinzip der Zweckbindung dient dazu, die Risiken einer Datenverwendung für den Betroffenen möglichst gering zu halten.

Dementsprechend sind auch die Zugriffsberechtigungen auf diese Datenbank so auszugestalten, dass nur denjenigen Polizeibeschäftigten Zugang einzuräumen ist, die die Daten für die polizeiliche Aufgabenerfüllung benötigen.

Auf Nachfrage trug das Landespolizeipräsidium vor, die Tatsache, dass der Zeuge bereits mehrfach kriminalpolizeilich in Erscheinung getreten sei, sei für die Beurteilung der Glaubwürdigkeit dieses Zeugen durch das Gericht und damit für den Ausgang des Rechtsstreits von Bedeutung. Bei der Übermittlung der aus POLIS-Saarland entnommenen Daten handele es sich mithin im weiteren Sinne um eine Gefahrenabwehrmaßnahme. Alle im Justiziariat der Polizei tätigen Polizeibeamten seien zur Gefahrenabwehr berufen. Ebenso sei auch das Verwaltungsgericht eine zur Gefahrenabwehr berufene öffentliche Stelle.

Diesen Ausführungen vermochten wir jedoch nicht zu folgen. Bei der Tätigkeit der Polizei muss nämlich ihre Aufgabenerfüllung im Bereich der Gefahrenabwehr oder Strafverfolgung klar von ihrer innerbehördlichen Aufgabenwahrnehmung, wie etwa der Führung eines beamtenrechtlichen Streitverfahrens, abgegrenzt werden. Entgegen ihrer Auffassung ist die Polizei vorliegend gerade nicht im Rahmen ihrer Aufgabe nach § 1 Abs. 2 Saarländisches Polizeigesetz (SPolG) zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung, sondern im Rahmen ihrer Verantwortung für Personalangelegenheiten tätig geworden.

Dementsprechend durfte die Polizei in dem anhängigen Gerichtsverfahren auch nicht das nur für die polizeilichen Aufgaben eingerichtete Informationssystem nutzen. Hierbei ist auch zu berücksichtigen, dass die POLIS-Datenbank selbst keine Aussage darüber trifft, wie die gespeicherten Informationen über Personen zu bewerten sind. Die Tatsache, dass eine Person mehrfach Gegenstand polizeilicher Ermittlungen war, sagt noch nichts über deren kriminelles Verhalten aus. Strafrechtlich relevantes Verhalten von Personen wird nur unter präzisen Voraussetzungen in das dafür vorgesehene Bundeszentralregister eingetragen. Die Einsichtsrechte in dieses Register werden vom Bundeszentralregistergesetz (BZRG) für alle Fälle abschließend und klar geregelt.

Im Übrigen obliegt es dem Gericht, den Sachverhalt von Amts wegen aufzuklären und gegebenenfalls im Rahmen einer Beweisaufnahme in eigener Verantwortung aufgrund des persönlichen Eindrucks des Zeugen festzustellen, ob ein Zeuge glaubwürdig und seine Schilderung glaubhaft ist. Ohne ausdrückliche Aufforderung des Gerichts ist es nicht

die Aufgabe eines Prozessbeteiligten, eigene Ermittlungen über Zeugen anzustellen, die keinen Bezug zu dem Sachverhalt aufweisen, sondern allein dem Zweck dienen, die Glaubwürdigkeit dieses Zeugen in Zweifel zu ziehen.

Die POLIS-Abfrage zu dem Zeugen und die Einbringung der gewonnenen Erkenntnisse in das Gerichtsverfahren waren damit als ein Eingriff in das informationelle Selbstbestimmungsrecht des Zeugen zu bewerten.

Um für die Zukunft ein datenschutzgerechtes Verhalten bei der Nutzung der polizeilichen Datenbanken zu gewährleisten, wurde in einem Gespräch mit Vertretern des Landespolizeipräsidiums neben der Erörterung des konkreten Falles die Vereinbarung getroffen, dass durch das Justiziariat in Zusammenarbeit mit dem behördlichen Datenschutzbeauftragten ein Leitfaden für die saarländischen Polizeibeamten erstellt werden soll, der konkrete Hinweise darauf enthält, zu welchen dienstlichen Zwecken Abfragen aus polizeilichen Informationssystemen zulässig sind. Leider haben wir trotz mehrfacher Nachfragen bislang noch nicht einmal eine Entwurfsfassung eines solchen Leitfadens erhalten.

8 Steuern

8.1 Staatsvertrag zwischen den Ländern Rheinland-Pfalz und Saarland

Mitte 2014 wurde uns vom Ministerium für Finanzen und Europa im Rahmen der externen Anhörung der Vorentwurf für einen Staatsvertrag zwischen Rheinland-Pfalz und Saarland über die Kooperation auf den Gebieten der Erbschaft- und Schenkungsteuer sowie der Grunderwerbsteuer zur Stellungnahme vorgelegt.

Die Erbschaft- und Schenkungsteuerfälle beider Länder werden künftig in Rheinland-Pfalz, die Grunderwerbsteuerfälle im Saarland bearbeitet. Durch diese Maßnahme sollen Kompetenzen konzentriert und Aufgaben länderübergreifend gebündelt werden. Die verfassungsrechtliche Verantwortlichkeit der Länder sowie die Zuweisung des Aufkommens bleiben durch den Staatsvertrag unberührt.

In Artikel 4 des Vorentwurfs waren die Prüfungsrechte der Rechnungshöfe geregelt. Eine entsprechende Formulierung über die Kontrollrechte der Datenschutzbeauftragten von Rheinland-Pfalz und Saarland fand sich nicht.

Daher setzten wir uns umgehend mit den Kollegen in Rheinland-Pfalz in Verbindung, um das weitere Vorgehen abzustimmen. Zeitgleich wandten wir uns an die beiden Länderfinanzministerien und baten um Aufnahme einer Regelung, die klarstellt, dass die Landesbeauftragten für Datenschutz weiterhin die Kontrollrechte für die Steuerfälle ihres jeweiligen Landes, auch wenn diese durch die Finanzbehörden des jeweils anderen Landes bearbeitet werden, innehaben.

Der zum 1. Januar 2015 in Kraft getretene Staatsvertrag enthält nun die von uns eingebrachte Regelung.

8.2 Service-Center der Finanzämter

Eine Petentin beklagte sich über die mangelnde Vertraulichkeit der Gespräche im Service-Center eines Finanzamtes. Man habe Teile ihrer Besprechung bis in die Wartezone hinein hören können. Dadurch sei der Datenschutz, ja sogar das Steuergeheimnis verletzt worden.

Petitionen zu dieser Thematik waren seit längerer Zeit nicht mehr bei uns eingegangen.

Die Einführung der Service-Center der Finanzämter erfolgte im Wesentlichen zwischen den Jahren 2000 und 2003. Sie hatte das Ziel, den Bürgern eine kundenfreundliche Anlaufstelle für einfache Verwaltungsvorgänge in den Finanzämtern anzubieten. Hierzu wurden in der Nähe des Eingangsbereichs Großraumbüros mit mehreren Bearbeiterplätzen (Servicezonen) eingerichtet. Vorgeschaltet ist ein Wartebereich, in dem sich in aller Regel ein Informationsschalter befindet.

Bereits damals war unsere Dienststelle prüfend und beratend tätig und die damals gestellten Anforderungen wurden abhängig von räumlichen Gegebenheiten weitgehend umgesetzt. Diese bestanden im Wesentlichen in der räumlichen Trennung von Warte- und Servicebereich, ausreichender Distanz zwischen den Bearbeiterplätzen mit ergänzenden Sicht- und Schallschutzmaßnahmen, die auch ein Mithören von Gesprächen verhindern, sowie der Einrichtung von Back-Offices für umfangreichere Beratungsmaßnahmen und zur Wahrung des Steuergeheimnisses. Hinweise auf das Back-Office sollten deutlich erkennbar in den Wartezonen und auf den Schreibtischen angebracht werden.

Da in der Zwischenzeit weitere Service-Center eingerichtet und bestehende durch Umbaumaßnahmen verändert wurden, haben wir uns Vorort bei den Finanzämtern des Landes ein aktuelles Bild von den örtlichen Gegebenheiten gemacht.

Während in einigen Finanzämtern die Wartezonen baulich von den Bearbeiterplätzen getrennt sind, haben andere lediglich mit Stellwänden und Pflanzenzonen optische Barrieren zwischen Wartebereich und Servicezone geschaffen. In einem Finanzamt sind nur geringe Vorkehrungen für den Sichtschutz getroffen.

Relevant aus Sicht des Datenschutzes ist es, inwieweit Beratungsgespräche von Dritten mitgehört werden können, einmal im Verhältnis Wartebereich zu Servicezone und zum andern innerhalb der Servicezone von Tisch zu Tisch.

Soweit die Wartebereiche eine räumliche Abtrennung erfahren haben, sind in aller Regel keine Gesprächsinhalte aus den Servicezonen vernehmbar. Aber auch dort, wo dies nicht der Fall ist, konnten wir nicht feststellen, dass man Details der Beratungsgespräche hören konnte. Stellwände und Pflanzenzonen bieten in aller Regel in Verbindung mit einer genügenden Entfernung zu den Bearbeiterplätzen eine ausreichende Diskretionszone.

Besondere Beachtung hat aber die Situation innerhalb der eigentlichen Servicezone gefunden. Überwiegend konnten wir beobachten, dass die Ausgestaltung der Servicezonen hinnehmbar ist, da bei normaler Stimmlautstärke Details eines Gesprächsverlaufs nicht wahrgenommen werden können. Lediglich in einem Finanzamt erschien der Abstand von ca. 2 m zwischen zwei Tischen zu gering.

Grundsätzlich ist zu berücksichtigen, dass eine Einrichtung von Service-Centern in Großraumbüros keine optimale Gestaltung von Vertraulichkeit ermöglicht.

Für das Massengeschäft, z. B. Entgegennahme von Steuer-Erklärungen, Anträge und Änderungen von Lohnsteuermerkmalen etc. sind die bestehenden Einrichtungen ausreichend. Für weitergehende Beratungen ist allerdings darauf zu achten, dass die hierfür vorgesehenen Back-Offices nicht nur bereit stehen, sondern auch genutzt werden. Entsprechende Hinweise auf das Back-Office sind sowohl in der Wartezone als auch auf den Schreibtischen anzubringen. Die Mitarbeiter in den Servicestellen sind anzuhalten, bei entsprechendem Gesprächsverlauf von sich aus eine Fortführung des Gesprächs im Back-Office anzuregen und zu ermöglichen.

In dem konkreten Fall, der zur Prüfung führte, hätten mehrere Maßnahmen die unbefugte Kenntnisnahme vertraulicher Gesprächsinhalte verhindern können. Zum einen befindet sich zwischen Bearbeiterplatz und Wartezone eine Tür. Diese war leider während des Gesprächs nicht geschlossen. Zum anderen hätte eine Verlegung der Beratung in das Back-Office die Vertraulichkeit wesentlich stärker schützen können.

Das Ministerium für Finanzen hat zwischenzeitlich die Mitarbeiter der Service-Center angehalten, bei entsprechendem Gesprächsverlauf auf die Nutzung des Back-Office hinzuweisen.

8.3 Erstellen von Abgabebescheiden durch Externe

Eine saarländische Kreisstadt beabsichtigte, die Aufbereitung zur Kuvertierung und den Versand von Abgabebescheiden (Grundbesitzabgaben, Gewerbesteuer, Hundesteuer) an einen externen privaten Dienstleister zu vergeben. Zur datenschutzrechtlichen Prüfung wurde uns der Entwurf eines Vertrages zur Auftragsdatenverarbeitung vorgelegt.

Nach § 12 Kommunales Abgabengesetz sind die Gemeinden an das Steuergeheimnis gemäß § 30 Abgabenordnung (AO) gebunden. Mit der beabsichtigten Auftragsdatenverarbeitung würden dementsprechend personenbezogene Daten, die einem besonderen Amtsgeheimnis, nämlich dem Steuergeheimnis, unterliegen, gegenüber Dritten offenbart. Da die Vorschriften der Auftragsdatenverarbeitung lediglich die Übertragung der Datenverarbeitung im technischen Sinne regeln und nicht Rechtsgrund für eine inhaltliche Aufgabenübertragung sein können, war zu prüfen, ob eine der in § 30 Abs. 4 bis 6 AO abschließend geregelten Befugnisse zur Offenbarung von Steuerdaten gegeben ist.

In Betracht zu ziehen war lediglich eine Offenbarungsbefugnis nach § 30 Abs. 4 Nr. 1 AO, wonach eine Offenbarung von Steuerdaten u.a. zulässig ist, soweit sie der Durchführung eines Verwaltungsverfahrens dient.

Die Daten „dienen" der Durchführung eines Verwaltungsverfahrens, wenn sie eine Prüfung der in einem solchen Verfahren relevanten Tatbestandmerkmale ermöglichen, erleichtern oder auf eine festere Grundlage stellen können, also ein unmittelbarer funktionaler Zusammenhang zwischen der Offenbarung und der Verfahrensdurchführung besteht. Bereits aus der Definition des Begriffes „dienen" folgt, dass nur solche Offenbarungen privilegiert sind, die die Entscheidungsfindung vorbereiten. Im hier vorliegenden Fall ist die Bearbeitung des Vorgangs jedoch bereits mit einer Entscheidung des Sachbearbeiters abgeschlossen. Lediglich um eine Zustellung bzw. Bekanntgabe der Entscheidung an den Steuerpflichtigen zu erreichen, werden private Helfer eingeschaltet. Diese Konstellation ist jedoch nicht von der Offenbarungsbefugnis des § 30 Abs. 4 Nr. 1 AO gedeckt.

Damit ist aufgrund des Steuergeheimnisses eine Beauftragung privater Unternehmer mit dem Druck, der Kuvertierung und dem Versand von Steuerbescheiden ausgeschlossen. Diese Auffassung wird auch von dem Ministerium der Finanzen geteilt.

Mit Blick auf diese Rechtslage verzichtete die Kreisstadt in der Folge auf ihr Vorhaben.

8.4 Kontrollmitteilungen der Volkshochschulen an die Finanzbehörden

Eine Dozentin bei einer Volkshochschule fragte bei uns nach, in welchem Umfang Daten von den zur Meldung verpflichteten Stellen an die Finanzbehörden zu übermitteln sind. In ihrem Fall hatte die Volkshochschule die Bankverbindung der Dozentin an die Finanzbehörden weitergeleitet.

Rechtsgrundlage für die Übermittlung von Daten an Finanzbehörden ist § 93a Abs. 1 Satz 2 AO. Hiernach kann durch Rechtsverordnung bestimmt werden, dass zur Sicherung der Besteuerung bei Zahlungen von Behörden und anderen öffentlichen Stellen der zuständigen Finanzbehörde der Empfänger, der Rechtsgrund, die Höhe und der Zeitpunkt der Zahlungen mitzuteilen sind. Die entsprechende Rechtsverordnung ist die „Verordnung über die Mitteilung an die Finanzbehörden durch andere Behörden und öffentlich-rechtliche Rundfunkanstalten (Mitteilungsverordnung – MV)".

§ 8 Abs. 2 MV regelt den Inhalt der Mitteilungen wie folgt: „In Mitteilungen über Zahlungen sind die anordnende Stelle, ihr Aktenzeichen, die Bezeichnung (Name, Vorname, Firma), die Anschrift des Zahlungsempfängers und, wenn bekannt, seine Steuernummer sowie sein Geburtsdatum, der Grund der Zahlung (Art des Anspruchs), die Höhe der Zahlung, der Tag der Zahlung oder der Zahlungsanordnung anzugeben. Als Zahlungsempfänger ist stets der ursprüngliche Gläubiger der Forderung zu benennen, auch wenn die Forderung abgetreten, verpfändet oder gepfändet ist."

Eine Verpflichtung zur Übermittlung von Bankdaten enthält die Mitteilungsverordnung jedoch nicht. Aufgrund unseres Hinweises auf die geltende Rechtslage hat die betreffende Volkshochschule uns mitgeteilt, den Finanzbehörden künftig lediglich die an die Dozenten gezahlten Honorare und Fahrtkosten mitzuteilen.

9 Meldewesen

9.1 Neuregelung des Meldewesens

Bereits in unserem letzten Tätigkeitsbericht hatten wir einen Ausblick auf die Neuregelung des Meldewesens gegeben, wonach das bisherige Melderechtsrahmengesetz und die Landesmeldegesetze durch ein Bundesmeldegesetz abgelöst werden. Das Gesetz zur Fortentwicklung des Meldewesens (MeldFortG) vom 03. Mai 2013 sah das Inkrafttreten des neuen Bundesmeldegesetzes (BMG) zum 01. Mai 2015 sowie das gleichzeitige Außerkrafttreten des Melderechtsrahmengesetzes vor.

In ihrer Entschließung vom 22. August 2012 hatten die Datenschutzbeauftragten des Bundes und der Länder eingefordert, das Melderecht datenschutzkonform zu gestalten. Schwerpunkt war die Forderung, einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels, entgegen der im Entwurfsstadium der Gesetzesnovelle vorgesehenen Widerspruchslösung, nur mit Einwilligung des Meldepflichtigen zuzulassen. In der Vorschrift über die einfache Melderegisterauskunft, § 44 BMG in der am 03. Mai 2013 verkündeten Fassung, wird dieser Forderung nunmehr Rechnung getragen.

§ 44 Abs. 3 BMG

Die Erteilung einer einfachen Melderegisterauskunft ist nur zulässig, wenn

1. *die Identität der Person, über die eine Auskunft begehrt wird, auf Grund der in der Anfrage mitgeteilten Angaben über den Familiennamen, den früheren Namen, die Vornamen, das Geburtsdatum, das Geschlecht oder eine Anschrift eindeutig festgestellt werden kann, und*

2. *die Auskunft verlangende Person oder Stelle erklärt, die Daten nicht zu verwenden für Zwecke*

   a) der Werbung oder

   b) des Adresshandels,

es sei denn, die betroffene Person hat in die Übermittlung für jeweils diesen Zweck ausdrücklich eingewilligt.

Noch vor Inkrafttreten des BMG wurde jedoch eine Änderung notwendig. Insbesondere war die Regelung hinsichtlich des Zeitpunkts des Inkrafttretens anzupassen, damit die entsprechenden Ermächtigungsgrundlagen für die Länder früher in Kraft treten als das übrige Gesetz. Die Landesgesetzgeber sollten so in die Lage versetzt werden, die ihnen per Verordnungsermächtigung zugewiesenen Regelungsbefugnisse auch gleichzeitig mit den Regelungen des Bundesmeldegesetzes in Kraft treten lassen zu können. §§ 55 bis 57 BMG sind daher bereits seit 26. November 2014 in Kraft. Das übrige Bundesmeldegesetz tritt nun-

mehr erst zum 01. November 2015 in Kraft und löst gleichzeitig das Melderechtsrahmengesetz ab.

Darüber hinaus waren im BMG Anpassungen aufgrund der bereits erfolgten Gleichstellung von Ehen und Lebenspartnerschaften in § 2 Abs. 8 des Einkommenssteuergesetzes (EStG) vorzunehmen.

Aus datenschutzrechtlicher Sicht ist zu begrüßen, dass hinsichtlich der in § 10 BMG normierten Auskunftsrechte der Betroffenen eine Klarstellung insoweit erfolgte, dass auch bei automatisierten Melderegisterauskünften dem Betroffenen im Einzelfall auf Antrag Auskunft über die Arten der übermittelten Daten und ihre Empfänger zu erteilen ist. Ebenso wurde in § 42 Abs. 1 BMG eine Klarstellung im Sinne des Arbeitnehmerdatenschutzes vorgenommen. Die Meldebehörde darf den öffentlich-rechtlichen Religionsgemeinschaften zwar unter bestimmten Voraussetzungen im Gesetz festgelegte personenbezogene Daten übermitteln, ausdrücklich jedoch nicht zu arbeitsrechtlichen Zwecken.

9.2 Anpassung des saarländischen Melderechts an das Bundesmeldegesetz

Im Mai 2014 übersandte uns das Ministerium für Inneres und Sport im Rahmen der externen Anhörung zur Anpassung des saarländischen Melderechts an das Bundesmeldegesetz den Entwurf eines Gesetzes zur Ausführung des Bundesmeldegesetzes und zur Änderung weiterer Rechtsvorschriften, den Entwurf einer Verordnung über die Zulassung der regelmäßigen Übermittlung von Daten aus dem Melderegister an Behörden oder andere öffentliche Stellen, den Entwurf einer Melderechtsdurchführungsverordnung und den Entwurf einer Verordnung über die Bestimmung der nach dem Melderecht zuständigen Stelle als Vermittlungsstelle mit der Bitte um Stellungnahme.

9.2.1 Entwurf eines Gesetzes zur Ausführung des Bundesmeldegesetzes und zur Änderung weiterer Rechtsvorschriften (SaarlAGBMG-E)

§ 4 SaarlAGBMG-E regelt, welche Daten durch die saarländischen Meldebehörden grundsätzlich an öffentlich-rechtliche Religionsgesellschaften über deren Mitglieder und Familienangehörige übermittelt werden dürfen. Sofern jedoch ein Familienangehöriger gemäß § 42 Abs. 3 Satz 2 BMG von seinem Widerspruchsrecht Gebrauch macht, ist der ihn betreffende Datenkatalog auf die lediglich für Zwecke des Steuererhebungsrechts erforderlichen Daten zu begrenzen (§ 42 Abs. 3 Sätze 2 und 3 BMG). Zur Gewährleistung der Normenklarheit wurde unsererseits daher empfohlen, § 4 Abs. 1 Satz 2 SaarlAGBMG-E um den Halbsatz, … „soweit diese nicht von ihrem Widerspruchsrecht nach § 42 Abs. 3 Satz 2 Bundesmeldegesetz Gebrauch gemacht haben." zu ergänzen.

Entgegen der zu § 4 SaarlAGBMG-E lautenden Überschrift „Datenübermittlungen an öffentlich-rechtliche Religionsgesellschaften" soll Absatz 5 dieser beabsichtigten Norm nunmehr auch eine verpflichtende Datenübermittlung der öffentlich-rechtlichen Religionsgesellschaften an die Meldebehörden normieren.

Zweifelsfrei gehört die Speicherung des Datums „rechtliche Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft“ nach § 3 Abs. 1 Nr. 11 BMG zur Aufgabenerfüllung der Meldebehörden. Die entsprechende Datenerhebungsnorm des § 24 Abs. 1 Satz 1 BMG erlaubt daher den Meldebehörden, dieses Datum beim Betroffenen zu erheben. Gleichzeitig verpflichtet § 25 BMG den Betroffenen zur entsprechenden Mitwirkung.

Weder die in Abschnitt 4 des BMG festgelegten besonderen Meldepflichten noch die den Ländern gemäß § 55 BMG zugestandenen Regelungsbefugnisse lassen aber eine Datenübermittlung öffentlich-rechtlicher Religionsgesellschaften an die Meldebehörden zu. Im Ergebnis mangelt es daher an einer entsprechenden Regelungskompetenz. Da dies in der Folge zu einer unzulässigen Datenübermittlung führen würde, haben wir daher die Streichung von § 4 Abs. 5 SaarlAG-BMG-E angeregt.

9.2.2 Entwurf einer Verordnung über die Zulassung der regelmäßigen Übermittlung von Daten aus dem Melderegister an Behörden oder andere öffentliche Stellen (MeldDÜV-E)

Wiederholt war festzustellen, dass sich die Zahl der Stellen, denen regelmäßig Daten aus dem Melderegister übermittelt werden sollen sowie auch die Zahl der Stellen, welchen eine Abrufbefugnis im automatisierten Abrufverfahren eingeräumt werden soll, erneut vergrößern sollte.

In der Vergangenheit wurde durch unsere Dienststelle bereits mehrfach - auch in den Tätigkeitsberichten der letzten Jahre - darauf hingewiesen, dass durch die stetige Ausweitung der regelmäßigen Datenübermittlungen und Abrufbefugnisse das kommunale Melderegister immer mehr einem öffentlichen Register gleichkommt, was aber so durch den Gesetzgeber nicht beabsichtigt war.

In unserer Stellungnahme zur Änderung der derzeit gültigen Meldedatenübermittlungsverordnung wurde daher bereits angeregt, in einer gesonderten, den automatisierten Abrufverfahren vorangestellten Norm Grundvoraussetzungen des Datenabrufs, technisch-organisatorische Maßnahmen, die Protokollierung des Datenzugriffs und den Umgang mit den Protokolldaten für datenabrufende Stellen zu regeln. Daraufhin wurde seitens des Ministeriums für Inneres und Sport signalisiert, diese Anregung mit Blick auf die durch das BMG vorzunehmenden neuerlichen Änderungen der Meldedatenübermittlungsverordnung aufgreifen zu wollen.

Durch die §§ 39 und 40 BMG (Verfahren des automatisierten Abrufs und Protokollierungspflicht bei automatisiertem Abruf) hat der Bundesgesetzgeber nunmehr bereits diesem Erfordernis Rechnung getragen. Dies zeigt deutlich, wie wichtig derartige grundsätzliche Verfahrensregelungen zur Bewusstseinsschärfung und auch für die Rechtssicherheit der handelnden Personen im Umgang mit personenbezogenen Daten sind. Ebenso wird hierdurch auch die Möglichkeit einer effektiven Datenschutzkontrolle gewährleistet.

Mit der Vorschrift § 29 MeldDÜV-E soll dem SaarForst-Landesbetrieb erstmals die Möglichkeit eines automatisierten Abrufverfahrens einge-

richtet werden. In der Begründung hierzu wird lediglich ausgeführt, dass dies der Aufgabenerfüllung des SaarForst-Landesbetriebs diene, um den Aufklärungsprozess in Liegenschaftsangelegenheiten zu beschleunigen. Mit Blick auf das Erfordernis der Aufgabenerfüllung zur Zulässigkeit eines solchen Abrufverfahrens, halten wir es daher für geboten, ähnlich der zu § 41 MeldDÜV-E (Abrufverfahren für die öffentlich bestellten Vermessungsingenieure) gegebenen dezidierten Begründung, die entsprechenden Rechtsgrundlagen auch in der Begründung zum Abrufverfahren für den SaarForst auszuweisen.

9.2.3 Entwurf einer Melderechtsdurchführungsverordnung und Entwurf einer Verordnung über die Bestimmung der nach dem Melderecht zuständigen Stelle als Vermittlungsstelle

Beide im Entwurf vorgelegten Verordnungen begegneten keinen datenschutzrechtlichen Bedenken.

10 Kommunales

10.1 Erstellung eines qualifizierten Mietspiegels

Bei Mietspiegeln handelt es sich um Übersichten über die üblichen Entgelte für Wohnraum in einer Gemeinde. Von einem qualifizierten Mietspiegel nach § 558d Bürgerliches Gesetzbuch (BGB) spricht man, wenn er nach anerkannten wissenschaftlichen Grundsätzen erstellt und von der Gemeinde oder den Interessenvertretern der Vermieter und Mieter anerkannt wurde. Der qualifizierte Mietspiegel ist im Abstand von zwei Jahren der Marktentwicklung anzupassen und nach vier Jahren neu zu erstellen.

Ein Landkreis hatte sich im Jahre 2008 für die Erstellung eines qualifizierten Mietspiegels entschieden und hierfür eine Mieter- bzw. Vermieterbefragung durch Versand entsprechender Erhebungsbögen durchgeführt. Im Tätigkeitsbericht 2007/2008 hatten wir bereits über das Beteiligungsverfahren und die zu beachtenden datenschutzrechtlichen Erfordernisse berichtet.

Da nunmehr gemäß § 558d Abs. 2 Satz 3 BGB die Neuerstellung des Mietspiegels anstand, wandte sich der Landkreis zur Abstimmung des Verfahrens erneut an unsere Dienststelle.

Mit dem Inkrafttreten des Mietrechtsänderungsgesetzes zum 01. Mai 2013 wurde das Merkmal „Energetische Ausstattung und Beschaffenheit“ neu eingefügt und somit klargestellt, dass die energetische Qualität von Wohnraum bei der Bildung der Vergleichsmiete (§ 558 BGB) zu berücksichtigen ist. Energetische Kriterien sollen so künftig auch in Mietspiegeln abgebildet werden. Der Landkreis beabsichtigte daher, auch energetische Differenzierungsmerkmale mittels eines an die Vermieter gerichteten Energiefragebogens zu erheben.

Diese Vermieterbefragung sollte durch eigens hierfür geschulte Interviewer stattfinden und die erforderlichen Adressdaten mittels Stichprobe aus dem Melderegister gezogen werden. Da sich aber aus den Meldedaten nicht ergab, ob es sich bei der unter der gemeldeten Adresse wohnhaften Person um einen Mieter oder Vermieter handelte, sollte zusätzlich ein Abgleich mit den Grundsteuer–B-Daten durchgeführt werden.

Gemäß § 31 Abs. 3 der Abgabenordnung (AO) sind die für die Verwaltung der Grundsteuer zuständigen Behörden berechtigt, die nach § 30 AO geschützten Namen und Anschriften von Grundstückseigentümern, die bei der Verwaltung der Grundsteuer bekannt geworden sind, zur Erfüllung sonstiger öffentlicher Aufgaben zu verwenden oder den hierfür zuständigen Behörden des öffentlichen Rechts auf Ersuchen mitzuteilen, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Da die Gemeinden nach § 558c BGB Mietspiegel erstellen sollen, wenn hierfür ein Bedürfnis besteht, dies mit einem vertretbaren Aufwand möglich ist und ihnen demnach eine entsprechende öffentliche Aufgabe per Gesetz zugewiesen ist, begegnete die zuvor dargelegte Verfahrensweise keinen datenschutzrechtlichen Bedenken.

Zur Erstellung des kreisweiten qualifizierten Mietspiegels sollte dann erneut eine Mieterbefragung durchgeführt werden, um einen Überblick über die ortsübliche Vergleichsmiete zu erhalten. Die Erhebung erfolgte über eine Stichprobenziehung aus der Einwohnermeldedatei, wobei für die Größe der Stichprobe die Einwohnerzahl der jeweiligen Gemeinde/Stadt maßgeblich war. Um erkennen zu können, ob es sich um eigengenutzte oder vermietete Objekte handelte, musste ebenfalls zusätzlich die Grundsteuer-B-Datei herangezogen werden.

Zunächst wurden alle Mieter der Stichproben mit einem Kontaktbogen angeschrieben, um einerseits die mietspiegelrelevanten Objekte herauszufiltern und andererseits die Bereitschaft der Bürger zur Teilnahme an der Befragung abzuklären. Der mit uns abgestimmte Kontaktbogen wurde zusammen mit einem Anschreiben übersandt, in welchem präzise auf das Verfahren eingegangen, über die Datenschutzbestimmungen informiert und wiederholt auf die Freiwilligkeit der Beantwortung hingewiesen wurde.

Das Anschreiben sollte bei dem Befragten verbleiben. Die zurückzusendenden Kontaktbogen enthielten keine Adressdaten, sondern wurden mit einer Identifikationsnummer versehen, damit kein Dritter einen Bezug zwischen Anschrift und Fragebogen herstellen konnte. Bei freiwilliger Teilnahme, also Rückübersendung des ausgefüllten Fragebogens, wurde über die Identifikationsnummer der Bezug hergestellt und geprüft. Sofern es sich um ein mietspiegelrelevantes Objekt handelte, wurde ein beauftragter Interviewer (Erhebungsbeauftragter) zu der Kontaktadresse gesandt, um ein Vollinterview (Hauptfragebogen) durchzuführen. Zuvor waren jedoch mit sämtlichen Interviewern entsprechende Werkverträge zu schließen, die den besonderen Erfordernissen nach § 5 SDSG (Auftragsdatenverarbeitung) Rechnung tragen mussten. Ebenso wurden alle Interviewer vor ihrem Einsatz auf das Datengeheimnis verpflichtet und geschult. Sobald der Interviewer alle Befragungen zu den ihm zugewiesenen Objekten erledigt hatte, musste er alle Unterlagen beim beauftragenden Landkreis abgeben. Sodann wurden die Fragebogen auf Vollständigkeit und Auswertbarkeit überprüft. Nach Abschluss des Prüfverfahrens wurden die Namen und Adressen der Teilnehmer gelöscht. Stellte sich heraus, dass die Anzahl auswertbarer mietspiegelrelevanter Fragebogen für eine statistische Auswertung nicht ausreichte, war eine zweite Erhebung durchzuführen.

Der Landkreis hat sämtliche Verfahrensschritte, wie Stichprobenziehung, Datenabgleiche, Versand der Fragebogen, Rücklaufkontrolle, Einsatz der Interviewer sowie Auswertung und Löschkonzept frühzeitig mit uns abgestimmt, sodass nach Vorlage der erforderlichen Verfahrensbeschreibung keine datenschutzrechtlichen Bedenken gegen das geschilderte Procedere bestanden.

10.2 Einsatz von Smartphones als Dienstgeräte

Aufgrund der geplanten Anschaffung von Smartphones zur Erfassung von Verkehrsordnungswidrigkeiten durch ihre Hilfspolizeibeamten wandte sich eine Gemeinde an unsere Dienststelle. Nach Angaben des Ordnungsamtes würden bei der Verwendung von Smartphones erfasste Daten, wie das Kfz-Kennzeichen sowie Ort und Zeit der Ordnungswidrigkeit, auf Servern der beauftragten Software-GmbH gehostet, wäh-

rend Name, Geburtsdatum und weitere persönliche Daten nur beim Ordnungsamt gespeichert und weiterverarbeitet würden. Die Gemeinde bat uns um eine datenschutzrechtliche Stellungnahme hinsichtlich des Einsatzes der Smartphones sowie um Mitteilung gegebenenfalls zu treffender Sicherheitsvorkehrungen.

Beim Einsatz von Smartphones als Dienstgeräte ist zunächst festzuhalten, dass angesichts der umfangreichen Möglichkeiten zur Ortung von Mitarbeitern und Erstellung von Bewegungsprofilen, gerade beim Einsatz zu dienstlichen Zwecken, Vorsicht geboten ist. Diesbezüglich erhobene Daten dürfen auf keinen Fall zu einer Verhaltens- oder Leistungskontrolle der Mitarbeiter i. S. d. § 31 Abs. 5 SDSG genutzt werden. Dies sollte auch in einer Dienstvereinbarung mit dem Personalrat festgehalten werden.

Daneben sind zur Abwehr von Hackerangriffen und zur Verhinderung von Zugriffen auf das Smartphone durch die Betriebssystem- und App-Hersteller umfassende Sicherheitsmaßnahmen zu implementieren, die einen Schutz von eventuell auf dem Smartphone gespeicherten personenbezogenen Daten oder Zugangsdaten zu Systemen nichtöffentlicher Stellen gewährleisten.

Diese Schutzmaßnahmen sind so zu gestalten, dass das mobile Gerät lediglich als Zugangspunkt zu den Servern der öffentlichen Stelle fungiert. Die eigentliche Tätigkeit ist demnach nur auf dem Server auszuführen, damit keine Daten auf dem mobilen Gerät selbst abgelegt werden. Da jedoch trotzdem Daten, beispielsweise während des E-Mail-Synchronisationsvorgangs auf dem Smartphone abgelegt werden, muss zusätzlich der Zugriff auf das Gerät mittels ausreichend sicheren Passworts/PIN abgesichert werden. Darüber hinaus soll nach mehrmaliger Falscheingabe der PIN eine automatische, vollständige Löschung der auf dem Gerät gespeicherten Daten erfolgen.

Nach Angaben der Gemeinde soll zwischen mobilem Gerät (Remotedatenbank) und Server (Hostdatenbank) eine Ende-zu-Ende-Verschlüsselung erfolgen, wobei eine RSA-Verschlüsselung integriert sei. Hierbei ist vor allem die Schlüssellänge (Blocklänge) für die Sicherheit maßgeblich. Allerdings nimmt der Berechnungsaufwand eines geheimen RSA-Schlüssels angesichts der steigenden Rechnerkapazitäten fortlaufend ab, sodass diese Art der Verschlüsselung letztlich nur als relativ sicher eingestuft werden kann.

Weiterhin müssen eindeutige Regelungen dahingehend getroffen werden, ob oder inwieweit eine private Nutzung des Dienstgerätes gestattet sein soll. Lässt man diese zu, muss sichergestellt werden, dass keine dienstlichen Daten in als privat eingestufte Online-Dienste (wie Facebook, Twitter u.a.) kopiert und damit verschickt werden können. Überdies sollten mittels einer Dienstvereinbarung diejenigen Anwendungen genau bestimmt werden, welche installiert und genutzt werden dürfen.

Letztlich sollte der jeweiligen IT-Abteilung die Möglichkeit eingeräumt werden, im Falle des Verlusts oder Diebstahls des Geräts dienstliche personenbezogene Daten vollständig vom Smartphone aus der Ferne zu löschen. Daneben muss auf dem Gerät eine Sicherheitssoftware (Virenschutz etc.) installiert sein und außerdem durch eine zentrale Konfiguration und Verteilung der Sicherheitseinstellung verhindert werden, dass ein durch Viren befallenes Gerät eine Bedrohung für die gesamte IT-Infrastruktur der öffentlichen Stelle wird. Auch für die Entsorgung der

Geräte müssen Regelungen getroffen werden um sicher zu gehen, dass keine personenbezogenen Daten mehr auf dem Smartphone gespeichert sind.

Diese technischen Aspekte und Sicherheitsvoraussetzungen teilte unsere Dienststelle der Gemeinde mit und empfahl gleichzeitig, von einer Verwendung dienstlich bereitgestellter Smartphones aus datenschutzrechtlicher Sicht solange abzusehen, wie die genannten Anforderungen nicht erfüllt sind.

10.3 Nutzung dienstlicher Unterlagen durch einen Hilfspolizeibeamten für private Zwecke

Im Dezember 2013 wandte sich ein Petent an unsere Dienststelle, da er sich und seine Ehefrau durch die Datenerhebung und -verarbeitung durch einen Hilfspolizeibeamten einer saarländischen Gemeinde in seinem informationellen Selbstbestimmungsrecht verletzt sah.

Aufgrund eines Vorfalls im öffentlichen Straßenverkehr erstattete der Petent Anzeige gegen eine Privatperson wegen Nötigung im Straßenverkehr. Die daraufhin zur Stellungnahme aufgeforderte Privatperson legte zunächst dar, dass sie sich an den besagten Vorfall nicht mehr erinnern könne. Ergänzend führte sie jedoch aus, Nachforschungen in ihren dienstlichen Unterlagen, welche ihr aufgrund ihrer dienstlichen Tätigkeit als Hilfspolizeibeamter zur Verfügung standen, durchgeführt zu haben. Es handelte sich dabei um bereits einige mehrere Jahre zurückliegende und somit verjährte Verwarn- und Bußgeldverfahren gegen den Petenten und seine Ehefrau. Diese Unterlagen fügte der Beschuldigte seiner Stellungnahme bei, um die Glaubwürdigkeit des Anzeigenerstatters zu erschüttern.

Bei den Unterlagen handelte es sich um sogenannte Datenblätter, d.h. Ausdrucke aus einem maschinellen Verfahren zur Bearbeitung von Verkehrsordnungswidrigkeiten. Allerdings war auf den uns zur Verfügung gestellten Kopien nicht ersichtlich, wann die Ausdrucke erstellt wurden. Die Verwarn- und Bußgeldverfahren datierten aus den Jahren 2006 und 2009 und waren vom Petenten bzw. seiner Ehefrau hinsichtlich der Forderungshöhe zeitnah beglichen worden, so dass bereits eine Löschung der Datenbestände hätte erfolgt sein müssen. Daher stellte sich zunächst die Frage, ob der Hilfspolizeibeamte ein eigenes Archiv ohne Genehmigung des Dienstherrn führte oder die für das Verfahren verantwortliche Kommune ihren Löschpflichten nicht nachgekommen war und der Hilfspolizeibeamte auf ihm noch dienstlich zur Verfügung stehende Daten zugegriffen hatte. Wir haben daher die betreffende Gemeinde um entsprechende Stellungnahme sowie um Vorlage der für das Verfahren nach § 9 Saarländisches Datenschutzgesetz (SDSG) zu führende Verfahrensbeschreibung inklusive der Festlegungen im Rechte-Rollenkonzept zum Verfahren gebeten. Auch welche Protokolldaten durch die Nutzung des Verfahrens erhoben und wie lange diese gespeichert werden, sollte von der Gemeinde dargelegt werden.

Erst nach mehrfachen schriftlichen und telefonischen Erinnerungen erhielten wir Monate später eine erste schriftliche Stellungnahme. Hiernach handelte es sich bei den durch den Hilfspolizeibeamten beigefügten Unterlagen um Ausdrucke aus dem Programm OWI-ASSISTENT,

eine Software zur Bearbeitung von Verkehrsordnungswidrigkeitsverfahren. Diese war bei der betreffenden Kommune von 2002 bis 2011 im Einsatz und wurde ab 2012 von dem Programm WiNOWiG abgelöst. Eine Migration der in OWI-ASSISTENT noch zu führenden Datenbestände in das Programm WiNOWiG fand nicht statt. Nach der Neuinstallation des Programm WiNOWiG sollten daher noch benötigte Datenbestände für eine Übergangsphase in OWI-ASSISTENT den Anwendern zur Verfügung stehen. Aufgrund unserer Bitte um Stellungnahme wurde festgestellt, dass die Gemeinde vergessen hatte, das nicht mehr benötigte Verfahren OWI-ASSISTENT abzuschalten, den Anwendern die Zugriffsberechtigungen zu entziehen und die längst zur Löschung anstehenden Datenbestände zu löschen. Weder für das Altverfahren OWI-ASSISTENT noch für das im Einsatz befindliche Verfahren WiNOWiG konnte die erforderliche Verfahrensbeschreibung vorgelegt werden.

Aufgrund unserer Intervention wurden die Datenbestände des Altverfahrens umgehend gelöscht. Die Kommune wurde ausdrücklich auf die Beteiligungspflichten unserer Dienststelle vor dem Einsatz eines automatisierten Verfahrens nach § 7 Abs. 2 SDSG sowie unser entsprechendes Internetangebot unter *www.datenschutz.saarland.de* hingewiesen und aufgefordert, die erforderliche Verfahrensbeschreibung für das Verfahren WiNOWiG umgehend zur Prüfung vorzulegen.

Zwischenzeitlich erfolgte die ordnungsgemäße Beteiligung unserer Dienststelle für das bereits im Einsatz befindliche Verfahren (WiNOWiG) nach §§ 9 i.V.m. 7 Abs. 2 SDSG. Hinsichtlich des Löschkonzepts mussten wir jedoch nochmals ausdrücklich darauf hinweisen, dass mit Begleichen eines festgesetzten Verwarnungsgeldes auch die Erledigung des Verfahrens nach § 94c Ordnungswidrigkeitengesetz (OWiG) i.V.m. § 483 Strafprozessordnung (StPO) erreicht wird und die erhobenen Daten sodann zeitnah zu löschen sind.

Die betreffende Kommune hat sich daraufhin mit dem Softwareanbieter ins Benehmen gesetzt und in Abstimmung mit unserer Dienststelle die Anonymisierung personenbezogener Daten in Verwarngeldfällen vier Wochen nach Abschluss des Verfahrens und die Löschung der anonymisierten Daten nach 14 Monaten realisiert. Die anonymisierten Daten werden für statistische Auswertungen benötigt.

Im Ergebnis pflegte der Hilfspolizeibeamte demnach keine eigenen Datenbestände, sondern erstellte einen Ausdruck aus den ihm dienstlich zur Verfügung stehenden Datenbestände, wenngleich diese zum maßgeblichen Zeitpunkt bereits hätten gelöscht sein müssen. Als datenschutzrechtlich unzulässig ist aber in jedem Fall die Nutzung dienstlich zugänglicher personenbezogener Daten durch den Hilfspolizeibeamten für private Zwecke zu bewerten.

Gegenüber der Gemeinde wurde daher eingefordert, die Mitarbeiter nochmals ausdrücklich darüber zu informieren, dass eine Nutzung von in dienstlichem Zusammenhang zugänglichen personenbezogenen Daten für private Zwecke unzulässig ist und entsprechende Bußgeldverfahren nach sich ziehen kann.

Im konkreten Fall wird die Einleitung eines Bußgeldverfahrens noch geprüft.

10.4 Veröffentlichung nicht-öffentlicher Dokumente im Bürgerinformationssystem

Infolge eines Presseartikels wurden wir darauf aufmerksam, dass mehrere nicht-öffentliche Dokumente einer saarländischen Stadt im Bürgerinformationssystem via Internet veröffentlicht wurden. Nach Angaben der Presse handelte es sich hierbei insbesondere um Dokumente in Beschäftigtenangelegenheiten, wobei Ergebnisse von Bewerbungsverfahren sowie die Namen der Bewerber öffentlich zugänglich gemacht wurden.

Unsere Dienststelle bat daher die Kommune um eine Stellungnahme hinsichtlich der Art der Dokumente und der Ursache sowie des Ausmaßes der unzulässigen Datenübermittlung. Weiterhin wurde um Mitteilung gebeten, inwieweit bereits Behebungsmaßnahmen getroffen wurden und wie derartige Vorkommnisse künftig vermieden werden können.

Seitens der Stadt teilte man uns daraufhin umgehend mit, dass es sich bei den veröffentlichten Dokumenten um personenbezogene Daten in Form von sensiblen Daten handelte. Daneben wurden unter anderem nicht-öffentliche Sitzungsteile ins Internet gestellt. Statt eines systemtechnischen Fehlers lag die Ursache der Dokumentenveröffentlichung jedoch in der fehlerhaften Einstellung der Vorlagen und ist demnach vielmehr auf ein menschliches Versagen zurückzuführen. Zur Eindämmung der Auswirkungen wurden die Daten allerdings sofort im Wege einer intensiven Kontrolle aller für das Bürgerinformationssystem freigegebenen Vorlagen in diesem gelöscht. Im Hinblick auf entsprechende Präventivmaßnahmen zwecks künftiger Vermeidung derartiger Vorfälle informierte man uns darüber, dass einerseits alle mit der Einstellung von Unterlagen in das System befassten Mitarbeiter erneut einen schriftlichen Hinweis auf die Datenschutzvorschriften erhalten sollten und andererseits eine regelmäßige Kontrolle des Öffentlichkeitsstatus erfolgen solle.

Aus datenschutzrechtlicher Perspektive sahen wir somit aufgrund der ausführlichen Stellungnahme und der angemessenen Präventivmaßnahmen keine weiteren Bedenken.

10.5 Übermittlung personenbezogener Daten aus dem Gewerberegister an natürliche Personen

Eine Petentin wandte sich an unsere Dienststelle mit der Frage, inwieweit und unter welchen Voraussetzungen ein Gewerbeamt Auskünfte aus dem Gewerberegister an Dritte erteilen dürfe. Infolge der Abmeldung ihres Hauptgewerbes und der damit einhergehenden Schließung ihres Cafés sei sie von einem Mann auf ihrer privaten Telefonnummer angerufen worden, welcher einen zuvor käuflich erworbenen Gutschein einlösen wollte. Auf Nachfrage der Petentin stellte sich heraus, dass der Anrufer ihre Telefonnummer vom Gewerbeamt erhalten hatte. Daraufhin bat sie unsere Dienststelle, sowohl die Grundlage der Auskunftserteilung als auch deren Voraussetzungen bei der Gemeinde in Erfahrung zu bringen.

Auf eine diesbezügliche Nachfrage hin bestätigte die Gemeinde, dass tatsächlich eine Auskunft durch die zuständigen Mitarbeiter erteilt wurde. Hinsichtlich der in Betracht kommenden Rechtsgrundlage verwies sie auf § 14 Gewerbeordnung (GewO), welcher sowohl die Grundlage für eine Gewerberegisterauskunft als auch deren Voraussetzungen normiere.

Nach dessen Absatz 5 dürfen der Name, die betriebliche Anschrift und die angezeigte Tätigkeit des Gewerbetreibenden allgemein zugänglich gemacht werden. Für alle weitergehenden Daten ist nach § 14 Abs. 7 GewO seitens des Empfängers ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft zu machen. Ein solches Interesse läge insbesondere im Falle der Geltendmachung von Rechtsansprüchen vor. Vorliegend erfolgte die Auskunftserteilung zum Zweck der Geltendmachung eventueller Rückzahlungsansprüche, sodass ein rechtliches Interesse zu bejahen sei. Weiteren telefonischen Auskunftsanfragen sei mit einem Verweis auf eine schriftliche Formulierung des Anliegens begegnet worden.

Angesichts dieser Sachlage bestehen hinsichtlich der mit dem Gewerberegister verbundenen Datenübermittlung keine datenschutzrechtlichen Bedenken, da eine erforderliche Rechtsgrundlage in Form des § 14 GewO vorlag und überdies eine durchzuführende Interessenabwägung von der Gemeinde in ausführlicher Weise vorgenommen wurde.

10.6 Aushang zu Sitzungsterminen des Kreisrechtsausschusses

Im Berichtszeitraum teilte eine Petentin unserer Dienststelle mit, dass ihr bei einem mündlichen Verhandlungstermin vor einem Kreisrechtsausschuss ein Aushang an der Tür des Sitzungssaales aufgefallen war. Hierauf befanden sich neben Streitgegenständen und entsprechenden Aktenzeichen auch Namen, Vornamen sowie vollständige Adressdaten der streitenden Parteien. In der Annahme, dass es sich hierbei um Datenschutzverletzungen handele, wandte sich die Petentin mit der Bitte um Überprüfung an unsere Dienststelle.

Sitzungen des Rechtsausschusses sind nach § 16 Abs. 2 Ausführungsgesetz zur Verwaltungsgerichtsordnung (AGVwGO) zwar grundsätzlich öffentlich, allerdings ist hierbei der Begriff der Öffentlichkeit dahingehend zu verstehen, dass Räumlichkeiten, in denen die Verhandlung stattfindet, während dieser Dauer jedermann zugänglich sein müssen. Hingegen ist es nicht erforderlich, dass eine Verhandlung in jedem Fall durch Aushang bekanntgegeben werden muss. Vielmehr bedarf es keiner an jedermann gerichteten Bekanntgabe, um dem Öffentlichkeitsgrundsatz des § 16 Abs. 2 AGVwGO zu genügen. Darüber hinaus besteht unserer Ansicht nach kein Anlass, diesen für Sitzungen des Kreisrechtsausschuss geltenden Grundsatz von der Öffentlichkeit von Gerichtsverhandlungen zu unterscheiden oder anders zu bewerten.

Unsere Dienststelle forderte daraufhin den Landkreis zur Beschränkung künftiger Aushänge auf das erforderliche Maß auf. Mit Hinweis auf die räumliche Bedeutung des hier maßgeblichen Öffentlichkeitsbegriffes baten wir zudem um eine datenschutzkonforme Ausgestaltung der

Aushänge, die nunmehr allenfalls Namen und Anfangsbuchstaben des Vornamens, sowie korrespondierende Aktenzeichen enthalten sollten.

11 Wahlen

11.1 Änderung des Kommunalwahlgesetzes (KWG)

Im Oktober 2013 wurde unsere Dienststelle gebeten, zum Entwurf eines Gesetzes zur Änderung des Kommunalwahlgesetzes Stellung zu nehmen.

Datenschutzrechtlich relevant war insbesondere die beabsichtigte Befugnisnorm des § 96 Abs. 2 KWG Saarland (LT-Drucks.: 15/669), welche künftig die Möglichkeit der zusätzlichen Veröffentlichung von Bekanntmachungen nach dem KWG und der Kommunalwahlordnung im Internet schaffen sollte.

Ziel des Änderungsgesetzes war unter anderem eine Angleichung des Kommunalwahlrechts an § 86 Abs. 3 Bundeswahlordnung (BWO), welcher bereits die Veröffentlichung von Bekanntmachungen nach der BWO im Internet vorsieht.

Die Veröffentlichungen umfassen Namen, Beruf oder Stand, Geburtsjahr- und -ort sowie Wohnort eines Wahlbewerbers.

Mit der zusätzlichen Veröffentlichung von Bekanntmachungen im Internet soll die Zugänglichkeit der Informationen erleichtert und dem Grundsatz der Öffentlichkeit der Wahl (§ 33 KWG) Rechnung getragen werden.

Das Unabhängige Datenschutzzentrum wurde insbesondere zu den erforderlichen Löschfristen bezüglich der im Internet veröffentlichten Daten angehört.

Der Entwurf sah bereits vor, dass die Daten spätestens sechs Monate nach Bekanntgabe des endgültigen Wahlergebnisses in Bezug auf gescheiterte Bewerber bzw. sechs Monate nach Ende der Amtszeit einer Person gelöscht werden müssen.

Gerade die dezidierte Festlegung von Löschfristen trägt datenschutzrechtlichen Anforderungen Rechnung. Sie garantiert die informationelle Selbstbestimmung dahingehend, dass der Betroffene die maximale Veröffentlichungsdauer seiner Daten im Internet abschätzen kann.

Hinsichtlich der Löschfrist personenbezogener Daten von gewählten Bewerbern geht der Entwurf sogar über das datenschutzrechtliche Schutzniveau des Bundesrechts hinaus.

Durch die Löschung sechs Monate nach Ende der Amtszeit werden gerade auch vorzeitige Beendigungen von Amtszeiten berücksichtigt.

Deshalb bestanden aus datenschutzrechtlicher Perspektive keine Bedenken gegen den vorgelegten Entwurf eines Gesetzes zur Änderung des Kommunalwahlgesetzes.

11.2 Wahlstatistik

Art. 38 Grundgesetz (GG) schützt u.a. das Wahlgeheimnis bei Bundestagswahlen.

Dennoch werden im Rahmen der Wahlen Daten über die Wähler aus rein statistischen Zwecken in anonymer Form erhoben.

Rechtsgrundlage für die Erhebung bestimmter Merkmale wie Wahlberechtigte, Wahlscheinvermerk, Beteiligung an der Wahl, Geburtsjahresgruppe und Geschlecht im Zusammenhang mit der Bundestagswahl ist § 54 des Wahlstatistikgesetzes (WStatG). Stichprobenartig werden hierfür bestimmte Wahlbezirke einer Gemeinde ausgewählt. Die Gemeinde ist nach § 5 Abs. 1 des WStatG verpflichtet, diese Merkmale zu erheben und auszuwerten.

Für die Auswertung wird ein besonderer Stimmzettel mit Unterscheidungsaufdruck nach Geschlecht und Altersgruppe erstellt.

Im Berichtszeitraum wurden wir durch Eingaben darauf aufmerksam gemacht, dass in vereinzelten Fällen ältere Personen nach ihrem konkreten Alter befragt wurden. Wahlhelfer wollten somit die Einordnung in die Geburtsjahresgruppen vornehmen, die das WStatG vorsieht.

Aus datenschutzrechtlicher Sicht ist es jedoch weder erforderlich noch durch § 54 WStatG legitimiert, nach dem konkreten Alter der betroffenen Wähler zu fragen. Eine Erklärung der jeweiligen Geburtsjahresgruppen und die Frage zu welcher der Gruppen der Wähler gehört wären ausreichend gewesen. Hier sind zur Gewährleistung von Transparenz konkrete Hinweise auf das Wahlstatistikgesetz, insbesondere auf die Vorschriften § 54 und § 5 Abs. 1 WStatG zu geben. Zudem sollte darüber hinaus der Flyer des Bundeswahlleiters zur Durchführung der repräsentativen Wahlstatistik als auch ein Ausdruck des WStatG in den ausgewählten Wahllokalen ausliegen.

11.3 Einsatz der Software PC-Wahl zur Durchführung von Wahlen

Zur Organisation von Wahlen müssen im Vorfeld oft personenbezogene Daten verarbeitet werden. Die Wählerlisten müssen geführt und die Wahlbescheinigungen versendet werden.

Diese Aufgabe kann von den Kommunen durch den Einsatz von spezieller Wahl-Software vereinfacht werden.

Da hierbei die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten mit Hilfe programmgesteuerter Anlagen durchgeführt werden soll, ist vor dem erstmaligen Einsatz eines automatisierten Verfahrens gemäß § 11 Abs. 1 Satz 1 Saarländisches Datenschutzgesetz (SDSG) zunächst durch den behördlichen Datenschutzbeauftragten im Rahmen einer sogenannten Vorab-kontrolle zu prüfen, welche Gefahren durch den Einsatz des beabsichtigten Systems für das informationelle Selbstbestimmungsrecht der Betroffenen erwachsen können. Für die praktische Umsetzung ist es empfehlenswert, mit Blick auf das Schutz-

stufenkonzept und die Umsetzung technisch-organisatorischer Maßnahmen, den IT-Sicherheitsbeauftragten und/oder die jeweiligen IT-Fachleute der Behörde zu beteiligen.

Aufbauend auf den Erkenntnissen der Vorabkontrolle kann sodann die entsprechende Verfahrensbeschreibung (§ 9 SDSG) erstellt werden, welche anschließend unserer Dienststelle im Rahmen des Beteiligungsverfahrens nach § 7 Abs. 2 Satz 5 SDSG vorzulegen ist.

Im Berichtszeitraum wurde vom Unabhängigen Datenschutzzentrum die Einführung einer neuen Wahlsoftware durch einen Landkreis begleitet.

Nach Durchführung der Vorabkontrolle zeigte der behördliche Datenschutzbeauftragte des Landkreises den beabsichtigten Einsatz dieser Wahlsoftware an.

In Bezug auf ein Programm zur Organisation einer Wahl sind dabei insbesondere die Löschfristen zu beachten, die sich aus § 90 Bundeswahlordnung, § 83 Europawahlordnung, § 60 Kommunalwahlordnung und § 66 Landeswahlordnung des Saarlandes für die Aufbewahrung und Vernichtung von Wahlunterlagen ergeben. Die zuvor durch den Landkreis beabsichtigte dauerhafte Speicherung konnte daher aus datenschutzrechtlicher Sicht nicht toleriert werden.

Mit der Maßgabe die sich aus den Wahlrechtsordnungen ergebenden Löschfristen programmseitig einzuhalten, konnte der Einsatz der Wahlsoftware PC-Wahl als datenschutzrechtlich unbedenklich bewertet werden.

12 Öffentliche Wirtschaft

12.1 Vergabeplattform des Landesamtes für Zentrale Dienste

Das Landesamt für Zentrale Dienste veröffentlicht aktuelle Ausschreibungen nicht nur in den Amtlichen Bekanntmachungsblättern, sondern auch im Internet. Neben dem postalischen Versand der Ausschreibungsunterlagen wird interessierten Unternehmen auch der Download dieser Unterlagen angeboten. Eine Registrierung der Unternehmen, die den Download-Weg wählten, erfolgte bisher nicht.

Obwohl die Ausschreibungsunterlagen eine eindeutige und erschöpfende Leistungsbeschreibung enthalten sollen, kann es dennoch im Laufe des Ausschreibungsverfahrens zu Korrekturen kommen, die allen Bewerbern bekannt gemacht werden müssen. Dies ist insbesondere der Fall, wenn einem Bewerber ein Fehler in der Ausschreibung auffällt. Die Korrektur muss dann allen Bewerbern mitgeteilt werden. Dies ist unproblematisch bei Bewerbern, die die Unterlagen schriftlich angefordert haben, da deren Kontaktdaten vorhanden sind. Sind die Ausschreibungsunterlagen jedoch über das Internet heruntergeladen worden, hatte die ausschreibende Stelle bisher keine Kontaktdaten. Eine Gleichbehandlung der Bewerber, die in § 97 Absatz 2 des Gesetzes gegen Wettbewerbsbeschränkung (GWB) gefordert ist, konnte so nicht gewährleistet werden.

Das Landesamt für Zentrale Dienste beabsichtigt deshalb dem Downloadbereich eine Seite vorzuschalten, auf der zumindest die E-Mail-Adresse des Bewerbers einzutragen ist. Weitere Kontaktdaten sollen freiwillig angegeben werden können.

Aus datenschutzrechtlicher Sicht bestehen keine Bedenken die E-Mail-Adresse zu speichern, da sie der ordnungsgemäßen Durchführung des Ausschreibungsverfahrens dient. Das Landesamt wurde jedoch darauf hingewiesen, dass in der Erfassungsmaske auch der mit der Erhebung der Kontaktdaten verbundene Zweck darzustellen ist.

12.2 Energieversorger und Mieterdaten

In mehreren Eingaben wurde von Hausverwaltungen und Eigentümern die Frage an uns herangetragen, ob und in welchem Umfang Mieterdaten an die Energieversorger weitergegeben werden dürfen und ob Energieversorger die Daten des Wohnungs-/Hauseigentümers vorhalten dürfen.

Energieversorger, insbesondere die für die Grundversorgung zuständigen Lieferanten, benötigen selbstverständlich Informationen darüber, wer an einem Netzanschluss Strom entnimmt. Zur Grundversorgung gehört, dass in jeder Wohnung die Möglichkeit besteht, Energie aus dem öffentlichen Stromnetz zu entnehmen.

Bei Bezug einer Immobilie durch einen neuen Mieter wird häufig schon Strom entnommen, ohne dass bereits ein schriftlicher Vertrag mit dem Energieversorger vorliegt. Grundsätzlich wird in einem solchen Fall ein konkludenter Vertragsschluss angenommen, da in dem Leistungsangebot eines Versorgungsunternehmens ein Vertragsangebot zum Abschluss eines Versorgungsvertrags in Form einer sogenannten Realofferte gesehen wird, der von demjenigen angenommen wird, der aus dem Leitungsnetz des Versorgungsunternehmens Elektrizität entnimmt.

In diesen Fällen ist das Interesse des Grundversorgers darauf gerichtet die Person des Entnehmers bzw. Vertragspartners zu identifizieren. Dem Grundversorger muss es dementsprechend möglich sein über den Eigentümer die Information zu erhalten, ob die Immobilie selbst genutzt wird, leer steht oder neu vermietet ist. Die dazu zuvorderst notwendige Erhebung und Nutzung der Daten des Immobilieneigentümers durch den Grundversorger ist nach § 28 Abs. 1 Satz 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) zulässig. Dem berechtigten Interesse des Grundversorgers, den tatsächlichen Vertragspartner zu ermitteln, steht dabei regelmäßig kein überwiegendes schutzwürdiges Interesse des Immobilieneigentümers im Zusammenhang mit der Datenerhebung bzw. -nutzung durch den Grundversorger entgegen.

Die Übermittlung der für den Vertragsschluss des Grundversorgers mit dem Mieter erforderlichen Daten durch den Eigentümer bzw. die Hausverwaltung erfolgt dann nach § 28 Abs. 2 Nr. 2a BDSG datenschutzrechtlich zulässig, da die Weitergabe dieser Daten zur Wahrung der berechtigten Interessen des Grundversorgers, mithin die Identität des Stromabnehmers zu erfahren, erforderlich ist. Die hierfür erforderlichen Daten sind Name, Anschrift und Beginn des Mietverhältnisses.

Den Petenten wurde daher mitgeteilt, dass aus datenschutzrechtlicher Sicht keine Bedenken gegen die Übermittlung der Mieterdaten an den Grundversorger bestehen.

12.3 Erhebung von Kundendaten durch eine Sparkasse

Bereits in unserem 24. Tätigkeitsbericht (Kapitel 18.6.2) haben wir dargelegt, unter welchen Voraussetzungen ein Kreditinstitut von seinen Kunden die Vorlage bzw. eine Kopie des Personalausweises verlangen darf.

In diesem Berichtszeitraum beschäftigte uns diese Problematik erneut. Im Juni 2013 reichte uns ein Sparkassenkunde einen Brief mit folgendem Wortlaut (Auszug) ein:

„… aufgrund gesetzlicher Regelungen sind wir verpflichtet, bei jedem unserer Kunden zusätzlich zu Namen und Anschrift folgende Daten zu erfassen:

- vollständige Legitimation und Staatsangehörigkeit

- Geburtsort

- Beruf

Bitte teilen Sie uns Ihren Beruf mit und senden Sie uns bis spätestens zum 20. Juni 2013 eine Kopie (Vorder- und Rückseite) Ihres derzeit gültigen Personalausweises oder Reisepasses. Andernfalls dürfen wir auf Ihrem Konto keine Verfügungen mehr zulassen. Sie können uns die Unterlagen auf dem für Sie angenehmsten Weg zukommen lassen:

- per Mail an …

- per Post an …

- Selbstverständlich können Sie auch auf einer unserer Filialen vorbeikommen. Die Kollegen vor Ort fertigen gerne eine Ausweiskopie an und leiten sie an uns weiter. …"

Das Vorgehen der Sparkasse war insbesondere hinsichtlich der angeforderten vollständigen Kopie des Personalausweises für uns nicht nachvollziehbar, da wir gegenüber den Sparkassen bereits wiederholt darauf hingewiesen hatten, dass eine vollständige Kopie des Personalausweises gerade nicht erforderlich ist.

Zwar ist es unstrittig, dass das Kreditinstitut nach § 4 Abs. 4 und § 8 Abs. 1 Satz 2 Geldwäschegesetz (GwG) die nach § 4 Abs. 3 GwG erforderlichen Daten Name, Geburtsdatum, Adressdaten, Geburtsort, Staatsangehörigkeit sowie Art, Nummer und ausstellende Behörde des Legitimationspapiers zu erheben und aufzuzeichnen hat, grundsätzlich ist hierfür jedoch die Vorlage des Ausweisdokumentes ausreichend.

Eine Kopie des Ausweisdokuments darf von dem Kreditinstitut hingegen nicht ohne weiteres gefordert werden, vielmehr ist hierfür eine Einwilligung des Kunden erforderlich. Insbesondere ist der Kunde darauf hinzuweisen, dass auf dem Dokument enthaltene Daten, die nicht zur Identifizierung benötigt werden, wie z. B. die 6-stellige Zugangsnummer, Größe und Augenfarbe geschwärzt werden sollen.

Ungeachtet des Umstandes, dass vorliegend bereits die Anforderung einer vollständigen Kopie des Ausweisdokuments nicht zulässig war, ist auch die dem Kunden angebotene Möglichkeit, diese personenbezogenen Daten per E-Mail zu übersenden, datenschutzrechtlich zu beanstanden. Da eine Kenntnisnahme Dritter bei einem unverschlüsselten Versand personenbezogener Daten per E-Mail über das Internet nicht ausgeschlossen werden kann, sollte keine Empfehlung zur Kommunikation auf diesem völlig ungesicherten Weg ausgesprochen werden.

Soweit die Sparkasse zur Erfüllung einer Meldepflicht gegenüber der Deutschen Bundesbank die Angabe des Berufes des Kunden gefordert hatte, geht dies über die Anforderungen zur Berichtspflicht hinaus, da die von der Sparkasse angeführte Richtlinie lediglich die Mitteilung der Angaben „wirtschaftlich Selbstständige", „wirtschaftlich Unselbstständige" und „sonstige Privatpersonen" vorsieht.

Die Sparkasse wurde auf die datenschutzrechtlichen Bedenken gegen ihre Verfahrensweise hingewiesen und aufgefordert, den datenschutzrechtlichen Anforderungen zukünftig Rechnung zu tragen. Diese sicherte zu, ihre Mitarbeiter insgesamt für die Datenschutzbelange zu sensibilisieren.

13 Soziales

13.1 Ärztliches Attest für Tagesmütter

Wer Tagesmutter werden will, muss seine persönliche Eignung gegenüber dem Jugendamt nachweisen. Dazu gehört auch, dass die Tagesmutter gesundheitlich in der Lage ist, Kinder zu betreuen.

Aus diesem Grund regelt die Saarländische Kindertagespflegeverordnung (KitaPflegV SL), dass die Pflegeerlaubnis nur erteilt werden darf, wenn die Pflegeperson ein ärztliches Attest vorlegt. Zur Vorlage verpflichtet sind auch die zum Haushalt gehörenden Familienangehörigen, wenn sie sich während der Betreuungszeiten des Kindes im Haushalt aufhalten.

Die Verordnung sagt allerdings nichts zu dem erforderlichen Umfang dieses Attestes.

Der Ehemann einer Tagesmutter hat meiner Dienststelle ein Formular eines Jugendamtes vorgelegt, das er von seinem Hausarzt ausfüllen lassen sollte.

In diesem Formular soll der Hausarzt umfassend über den Gesundheitszustand des Betroffenen Auskunft geben. Es wird danach gefragt, welche Beeinträchtigungen im Bereich Herz-Kreislauf, des Bewegungsapparates, der Sinnesorgane oder der Psyche bestehen. Anzugeben sind derzeit behandelte bzw. durchgemachte schwere Erkrankungen, regelmäßig eingenommene Medikamente oder auch psychosomatische Störungen.

Für uns hat sich die Frage gestellt, ob die Offenbarung all dieser sehr persönlichen Daten gegenüber den Mitarbeitern des Jugendamtes wirklich erforderlich ist. Der Gesetzgeber stuft Daten über gesundheitliche Verhältnisse als besondere Arten personenbezogener Daten ein, an deren rechtmäßige Verarbeitung hohe Anforderungen zu stellen sind.

Wegen der Bedeutung des Themas für alle saarländischen Jugendämter haben wir in Zusammenarbeit mit Vertretern der Jugendämter folgende Lösung gefunden:

Der Arzt erhält künftig ein Informationsblatt, in dem erläutert wird, welche Erkrankungen einen Ausschlussgrund für die Erteilung einer Pflegeerlaubnis darstellen. Der Arzt bescheinigt ohne Angabe einer Diagnose, ob gegen die Aufnahme eines Kindes in die Kindertagespflege Bedenken bestehen oder nicht.

Falls Bedenken bestehen kann der Betroffene dem zuständigen Gesundheitsamt vorgestellt werden. Dieses entscheidet letztlich aufgrund der Informationen des behandelnden Arztes, ob eine Eignung vorliegt oder nicht.

Die Offenbarung sensibler Gesundheitsdaten der antragstellenden Person sowie ihrer Familienangehörigen ist somit auf ein Mindestmaß beschränkt worden.

Die Praxis wird zeigen, ob sich dieses Verfahren künftig bewährt.

13.2 Runder Tisch zur Vermeidung von Stromsperren

Bei einem Hausbrand in Saarbrücken sind mehrere Kinder ums Leben gekommen. Brandursache war ein unachtsamer Umgang mit Kerzen, die wegen einer Stromsperre als einzige Lichtquelle verblieben sind. Dies hat dazu geführt, dass das Ministerium für Umwelt und Verbraucherschutz einen runden Tisch zur Vermeidung von Stromsperren ins Leben gerufen hat. Ziel sollte es sein, durch eine konstruktive Zusammenarbeit zwischen Versorgungsunternehmen, Sozialleitungsträgern und Sozial- und Verbraucherschutzverbänden Möglichkeiten zu finden, um Unterbrechungen der Stromversorgung in den Fällen von Zahlungsverzug und Zahlungsunfähigkeit bei einkommensschwachen Haushalten zu vermeiden.

Im Laufe der Beratungen hat sich gezeigt, dass nur durch gezieltes Zusammenwirken zwischen den beteiligten Institutionen eine Verbesserung der Situation für die Betroffenen erreicht werden kann. Wir waren in diesem Zusammenhang maßgeblich an der datenschutzgerechten Gestaltung der Datenflüsse zwischen den Institutionen beteiligt.

Es haben sich während der Gespräche drei Varianten herauskristallisiert, die zu einer wirksamen Vermeidung von Stromsperren führen:

- Sozialleistungsbezieher werden bei der Beantragung von Sozialleistungen darauf hingewiesen, dass mittels einer Abtretungserklärung eine mögliche Stromsperre verhindert werden kann, da die Stromkosten direkt zwischen Leistungsträger und Energieversorger abgerechnet werden.

- Sozialleistungsbezieher können darin einwilligen, dass bei Rückständen der jeweilige Energieversorger direkt vom Sozialleistungsträger kontaktiert wird, um eine Lösung der Überzahlung herbeizuführen.

- Energiekunden werden bevor der Strom gesperrt wird von Vertretern der Stromversorger persönlich aufgesucht und über mögliche Hilfen informiert. Auch hier besteht die Möglichkeit, mittels einer Einwilligungserklärung eine Kontaktaufnahme zwischen Energieversorger und Sozialleistungserbringer zur Vermeidung einer Stromsperre zu legitimieren.

Sowohl die Stromversorger als auch die Sozialleistungsträger haben sich darüber hinaus dazu verpflichtet, jeweils eine zentrale Anlaufstelle zur Vermeidung von Stromsperren einzurichten. Des Weiteren prüfen die Energieversorger den vermehrten Einsatz von sogenannten Prepaid-Zählern, die im jeweiligen Haushalt den Strom gegen direkte Zahlung „freischalten".

Mangels einer gesetzlichen Datenübermittlungsbefugnis von den Sozialleistungsträgern zu den Energieversorgern im Sozialgesetzbuch (SGB) auf der einen Seite und von der Energieversorgern zu den Sozialleistungsträgern auf der anderen Seite konnten die Datenflüsse lediglich über die Einwilligung der Betroffenen legitimiert werden. So waren wir

bei der Erstellung einer Einwilligungserklärung der Betroffenen und eines Merkblattes beteiligt, das bei einer drohenden Stromsperre ausgehändigt wird.

13.3 Vorlage des Fahrzeugscheines bei Beantragung von Hartz-IV-Leistungen

Ein Leistungsbezieher hatte bei seinem Weiterbewilligungsantrag angegeben, dass er ein Auto gekauft habe. Dem Antrag hatte er den Versicherungsschein beigefügt.

Das Jobcenter forderte von dem Antragsteller darüber hinaus die Vorlage des Fahrzeugscheines sowie des Kaufvertrages. Der Petent fragte bei meiner Dienststelle nach, ob er zur Vorlage dieser Unterlagen verpflichtet sei.

Die einschlägige Vorschrift (§ 67a Absatz 1 Satz 1 Zehntes Buch Sozialgesetzbuch – SGB X) besagt, dass das Erheben von Sozialdaten zulässig ist, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.

Hartz-IV-Bezieher dürfen zwar ein Auto besitzen, jedoch darf dessen Wert bestimmte Grenzen nicht überschreiten. So hat das Bundessozialgericht (Urteil vom 6. September 2007, Az.: B 14/7b AS 66/06 R) entschieden, dass ein Auto bis zu einem Wert von 7.500 € grundsätzlich angemessen sei.

Es ist unter diesem Gesichtspunkt nachvollziehbar und nicht zu beanstanden, wenn das Jobcenter zur Ermittlung des maßgeblichen Wertes eines Kfz den Kaufvertrag einsehen möchte.

Der Fahrzeugschein wird nach Erläuterung des Jobcenters benötigt, um zu prüfen, ob das Fahrzeug auch tatsächlich auf den Hartz-IV-Bezieher zugelassen ist. Denn nur dieser erhält bei beruflicher Nutzung einen Zuschuss zur Haftpflichtversicherung. Auch diese Begründung hat uns überzeugt.

Im Ergebnis war der Petent somit zur Vorlage der angeforderten Unterlagen verpflichtet. Allerdings wäre es sinnvoll, wenn das Jobcenter künftig kurz erläutern würde, aus welchem Grund angeforderte Unterlagen benötigt werden. So könnten Irritationen von vornherein vermieden werden.

13.4 Weitergabe von Sozialdaten an Einbürgerungsbehörde

Im Berichtszeitraum ist die Aufsichtsbehörde mit folgender Problematik konfrontiert worden:

Das Ministerium für Inneres und Sport benötigt im Einbürgerungsverfahren u.a. Informationen über die wirtschaftlichen Verhältnisse des Bewerbers. Wenn der Betreffende Sozialleistungen z.B. vom Sozialamt, der Arbeitsagentur oder dem Jobcenter erhält, ist es wichtig zu wissen, ob er diesen Sozialleistungsbezug selbst zu vertreten hat oder ob er

Ausbildungs-, Qualifikations- oder Weiterbildungsangebote angenommen und sich ausreichend um Stellen beworben, aber aufgrund der Arbeitsmarktsituation trotzdem keine Arbeit gefunden hat.

Von einem Jobcenter wurde die Frage gestellt, aufgrund welcher Rechtsgrundlage die von der Einbürgerungsbehörde angeforderten Informationen eigentlich übermittelt werden dürfen.

Die einschlägigen Vorschriften (§§ 67b, 67d Zehntes Buch Sozialgesetzbuch – SGB X) bestimmen, dass Sozialdaten nur übermittelt werden dürfen, wenn eine gesetzliche Übermittlungsbefugnis gemäß den Vorschriften des Sozialgesetzbuchs vorliegt oder der Betroffene eingewilligt hat.

Eine Durchsicht der in Betracht kommenden Vorschriften hat ergeben, dass eine solche Rechtsgrundlage, die die Datenübermittlung legitimieren könnte, zweifelsfrei nicht vorhanden ist.

Alle Beteiligten waren sich einig, dass eine zulässige Datenübermittlung somit eine ausdrückliche Einwilligung voraussetzt. Mit dem Ministerium für Inneres und Sport wurde die Formulierung einer Einwilligungserklärung abgestimmt, die nunmehr verwendet wird.

Allerdings ist die Datenweitergabe aufgrund einer Einwilligung letztlich nicht befriedigend, da eine echte Freiwilligkeit aufgrund der Tatsache, dass die Einbürgerung möglicherweise von der Erteilung dieser Einwilligung abhängt, fraglich ist.

Das Ministerium für Inneres und Sport hat deshalb beim Bundesministerium des Innern eine Ergänzung der Vorschriften im SGB X angeregt, um die von allen Beteiligten als notwendig angesehene Informationsweitergabe gesetzlich zweifelsfrei zu legitimieren.

13.5 Zustimmung zur Einholung von Bankauskünften

Ein Sozialamt legt jedem Antragsteller auf Grundsicherung folgende Erklärung zur Unterschrift vor:

„Ich ermächtige die im Antrag genannten Sparkassen, Banken und sonstigen Geldinstitute, unter Befreiung vom Bankgeheimnis und der datenschutzrechtlichen Bestimmungen, dem Sozialamt weitere Auskünfte, insbesondere über den Kontostand und die Kontobewegungen während der letzten sechs Monate zu erteilen."

Ein Petent war der Meinung, dass er nicht verpflichtet sein könne, diese Erklärung zu unterschreiben. Ein solches Verlangen sei nur zulässig, wenn dem Sozialamt Anhaltspunkte vorlägen, dass seine Angaben über seine Vermögensverhältnisse nicht korrekt seien. Das Sozialamt habe ihm gegenüber diesbezüglich nichts vorgetragen.

Nach einer datenschutzrechtlichen Prüfung sind wir zu folgendem Ergebnis gelangt:

Das Sozialamt kann zwar verlangen, dass es Kenntnis von dem Guthaben bzw. Vermögensverfügungen der letzten sechs Monate erhält, allerdings besteht keine Verpflichtung, eine entsprechende Befreiung

vom Bankgeheimnis zu unterschreiben. Dem Antragsteller ist vielmehr die Möglichkeit zu geben, die relevanten Unterlagen selbst vorzulegen.

Rechtsgrundlage für die Forderung des Sozialamtes ist § 60 Erstes Buch Sozialgesetzbuch (SGB I). Nach § 60 Abs. 1 Satz 1 Nr. 1 SGB I hat jeder, der Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistung erheblich sind und auf Verlangen des Leistungsträgers Beweisurkunden vorzulegen. Das Verlangen nach Vorlage solcher Beweisurkunden setzt dabei nicht voraus, dass das Sozialamt einen konkreten Verdacht hat, dass die vom Antragsteller gemachten Angaben unzutreffend sind. Das hat das Bundessozialgericht für den vergleichbaren Fall der Vorlage von Kontoauszügen des Girokontos ausdrücklich so entschieden (Bundessozialgericht, Urteil vom 19.09.2008, Az.: B 14 AS 45/07 R.).

Allerdings sind die Daten grundsätzlich beim Betroffenen zu erheben (§ 67 a SGB X), d.h. der Hilfesuchende hat im Rahmen der Mitwirkungspflicht die Unterlagen, z.B. Kontoauszüge oder Sparbücher, selbst zur Verfügung zu stellen. So wird vermieden, dass das Geldinstitut von seinem Sozialleistungsbezug erfährt

14 Gesundheit

14.1 Einführung des klinisch-epidemiologischen Krebsregisters im Saarland

Deutschland verfügt über ein hoch entwickeltes Gesundheitssystem, das jeder Person im Falle einer Krebserkrankung umfassende Behandlungsmaßnahmen anbietet. Die Bundesregierung geht von einer steigenden Zahl an Krebsneuerkrankungen aus. Vor diesem Hintergrund wurde der Nationale Krebsplan initiiert, der die Krebsfrüherkennung, die onkologischen Versorgungsstrukturen, die Qualitätssicherung und die Patientenorientierung stärken soll. Zentrales Handlungsfeld ist die Weiterentwicklung onkologischer Versorgungsstrukturen und deren Qualität. Besondere Priorität wurde dabei dem flächendeckenden Ausbau von klinischen Krebsregistern unter einheitlichen Rahmenbedingungen beigemessen. Zu den Aufgaben der Klinischen Krebsregister gehören die möglichst vollzählige und auf den Einzelfall bezogene Erfassung der Daten über das Auftreten, die Behandlung und den Verlauf onkologischer Erkrankungen sowie die Auswertung, Rückmeldung und die Darstellung der Prozess- und Ergebnisqualität der medizinischen Leistungen.

Klinische Krebsregister sollen mit diesen Funktionen eine leitliniengerechte Versorgung unterstützen, eine Beurteilung der Qualität der individuellen Krebstherapie ermöglichen und dazu beitragen, Qualitätsdefizite in der onkologischen Versorgung zu beseitigen. Dies setzt allerdings voraus, dass personenbezogene Daten über jede Krebsneuerkrankung an das klinische Krebsregister gemeldet werden müssen. Da es sich bei diesen Daten um höchstsensible Daten handelt, wurden wir gebeten, die gesetzliche Umsetzung, insbesondere mit Blick auf die Rechte der Betroffenen sowie die datenschutzgerechte Ausgestaltung der Datenflüsse zwischen den beteiligten Institutionen, zu begleiten.

Am 31. Januar 2013 hat der Deutsche Bundestag das „Gesetz zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister“ (Krebsfrüherkennungs- und -registergesetz - KFRG) verabschiedet, welches am 9. April 2013 in Kraft getreten ist. Durch dieses Gesetz verpflichtet der Bund die Länder, zur Verbesserung der Qualität der onkologischen Versorgung, eine flächendeckende klinische Krebsregistrierung aufzubauen. Rechtsgrundlage für die verpflichtende Einführung eines Klinischen Krebsregisters auf Länderebene ist nunmehr die Regelung des § 65c Fünftes Buch Sozialgesetzbuch (SGB V), nach welcher es aber den Ländern vorbehalten ist, die für die Einrichtung und den Betrieb der klinischen Krebsregister notwendigen Rechtsgrundlagen einschließlich der datenschutzrechtlichen Regelungen landesrechtlich festzulegen.

Die Umsetzung der Einführung des Klinischen Krebsregisters im Saarland in der Novellierung des Saarländischen Krebsregisters wurde durch unsere Dienststelle hinsichtlich datenschutzrechtlicher Aspekte intensiv begleitet.

Datenschutzrechtlich bedeutsam ist vor allem die Änderung des Widerspruchsrechts der Patienten hinsichtlich der Verarbeitung ihrer Gesundheitsdaten. Nach den neuen Bestimmungen des Saarländischen Krebsregistergesetzes (SKRG) kann ein Widerspruch nur noch gegen die dauerhafte Klartextspeicherung der Identitätsdaten des Patienten eingelegt werden. Für Ärzte besteht die generelle Verpflichtung, zu jeder Tumorerkrankung die erforderlichen Informationen an das Krebsregister zu übermitteln. Widerspricht ein Patient der dauerhaften Klartextspeicherung seiner Identitätsdaten, so wird die Tatsache des Widerspruchs zusammen mit der Meldung an das Register übermittelt. Das Register speichert in diesem Fall dauerhaft nur Kontrollnummern, die eine Identifizierung des Patienten nicht mehr zulassen. Die anonymisierten Daten zu den Tumorerkrankungen bleiben jedoch zum Zweck der Qualitätssicherung erhalten. In Zusammenarbeit mit unserer Dienststelle wurde eine Patienteninformation erarbeitet.

Darüber hinaus sind zahlreiche Änderungswünsche von unserer Seite in den neuen Gesetzentwurf eingeflossen. Durch die Vorreiterrolle des Saarlandes bei der Krebsregistrierung als eines der ersten Bundesländer, die die Vorgaben des § 65c SGB V im Bundesgebiet umgesetzt haben, wurde ein Mitarbeiter der Dienststelle vom Arbeitskreis Gesundheit und Soziales der Datenschutzbeauftragten des Bundes und der Länder dazu berufen, die Datenflüsse zwischen den Kostenträgern (Krankenkassen) und den Klinischen Krebsregistern für ganz Deutschland datenschutzrechtlich beratend zu begleiten.

Aufgrund der frühzeitigen Beteiligung unserer Dienststelle sowie auch der vorbildlichen Zusammenarbeit zwischen dem Krebsregister des Saarlandes und unserer Dienststelle konnte die Implementierung des Klinischen Krebsregisters im Saarland in einer konstruktiven Art und Weise datenschutzkonform umgesetzt werden.

14.2 Einschulungsfragebogen

Alle Kinder werden vor ihrer Einschulung von Ärzten des Gesundheitsamtes untersucht.

Vor dieser Untersuchung erhalten die Eltern einen Fragebogen mit der Bitte zugesandt, diesen ausgefüllt zur Untersuchung mitzubringen.

Mehrere Eltern haben sich bei unserer Dienststelle über den Inhalt dieses Fragebogens beschwert, weil er Fragen enthalte, die für die Beurteilung der Schulfähigkeit ihres Kindes aus deren Sicht unerheblich seien.

Im Einzelnen werden neben den allgemeinen Angaben wie Anschrift des Kindes und der Eltern, besuchter Kindergarten und vorgesehene Schule, Daten zur Familienanamnese (welche Krankheiten treten in der Familie gehäuft auf) sowie zur Anamnese des Kindes (Angaben zur Schwangerschaft und Geburt, zur Entwicklung, zu Vorerkrankungen, Operationen, Unfällen, Medikamenteneinnahme) erfragt. Zusätzlich sollten die Eltern angeben, welchen Schulabschluss sie haben (Förderschule, Hauptschule, Mittlere Reife, Abitur/Fachabitur, kein Schulabschluss), bei welchem Elternteil das Kind überwiegend lebt, welche Staatsangehörigkeit sie haben und in welchem Land sie geboren wurden (soziodemographische Daten).

Das für die Formulierung des Fragebogens zuständige Ministerium für Soziales, Gesundheit, Frauen und Familie hat uns davon überzeugt, dass die Fragen zur Familienanamnese sowie zur Anamnese des Kindes erforderlich seien, um einerseits die Schultauglichkeit zu beurteilen, andererseits aber auch, um den Gesundheitszustand des Kindes im Hinblick auf eventuelle Fördermöglichkeiten festzustellen.

Die maßgebliche Vorschrift (§ 2 Schulpflichtgesetz) lautet wie folgt:

„…Zur Vorbereitung der Aufnahme in die Schule sind diese Kinder ab dem 1. Januar des dem Beginn der Schulpflicht vorhergehenden Kalenderjahres zur Feststellung des Gesundheits- und Entwicklungsstandes durch eine Schul- oder Amtsärztin oder einen Schul- oder Amtsarzt zu untersuchen; insoweit wird das Recht der körperlichen Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes) eingeschränkt. Soweit erforderlich, werden bei dieser Untersuchung auch fördernde Maßnahmen empfohlen."

Auch die soziodemographischen Daten dürfen grundsätzlich erhoben werden. Allerdings haben diese Daten eine gänzlich andere Zweckbestimmung, nämlich den der Gesundheitsberichterstattung (§ 6 Gesundheitsdienstegesetz (ÖGDG)). Dies muss den Eltern deutlich gemacht werden, damit sie in Kenntnis dieses Zwecks frei entscheiden können, ob sie ihre Daten auch zu diesem Zweck angeben wollen.

Es war deshalb notwendig, den Fragebogen neu zu gestalten. Es gibt nunmehr zwei getrennte Fragebögen: Der erste Fragebogen enthält die Daten zur Familienanamnese und zur Anamnese des Kindes; auf dem zweiten Fragebogen werden die soziodemographischen Daten abgefragt.

Auch die Information über die weitere Verarbeitung der Daten aus den Fragebögen fällt unterschiedlich aus. Während die Gesundheitsfragen zu Angehörigen und Kind personenbezogen gespeichert werden, werden die soziodemographischen Daten schnellstmöglich anonymisiert.

Die Überarbeitung erfolgte in enger Abstimmung zwischen unserer Dienststelle und dem Ministerium für Soziales, Gesundheit, Frauen und Familie, dem eine äußerst konstruktive Zusammenarbeit bescheinigt werden kann.

14.3 Transport von Krankenakten in offenen Behältern

Im Kalenderjahr 2013 wurde die Aufsichtsbehörde durch eine Eingabe auf potentielle Missstände beim Transport von Krankenakten von einem Gesundheitszentrum zu dessen externem Schreibservice aufmerksam gemacht. In diesem Zusammenhang bestand auch aufgrund einer beigefügten Fotodokumentation – darauf waren Akten, die gut sichtbar im Fußraum bzw. im geöffneten Kofferraum eines KFZ lagen, abgelichtet – der Verdacht eines Verstoßes gegen die Anforderungen des § 9 Bundesdatenschutzgesetz (BDSG) i. V. m. Punkt 4 der Anlage zu § 9 S. 1 BDSG. Danach sind Maßnahmen zu treffen, die gewährleisten, dass personenbezogene Daten während ihres Transportes nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Bei den transpor-

tierten Krankenakten handelte es sich darüber hinaus um besondere personenbezogene Daten i. S. d. § 3 Abs. 9 BDSG, weshalb grundsätzlich besondere Sorgfaltspflichten zu beachten gewesen wären.

Des Weiteren ist festzuhalten, dass im geschilderten Sachverhalt die Verarbeitung personenbezogener Daten im Auftrag durch eine andere Stelle erfolgte, weshalb zwischen Gesundheitszentrum als verantwortlicher Stelle i. S. d. § 3 Abs. 7 BDSG und externem Schreibservice als Auftragnehmer ein Auftragsdatenverarbeitungsvertrag i. S. d. § 11 BDSG zu schließen gewesen wäre. Darin sind gemäß § 11 Abs. 2 S. 1 BDSG insbesondere im Einzelnen festzulegen:

1. der Gegenstand und die Dauer des Auftrags

2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,

3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,

4. die Berichtigung, Löschung und Sperrung von Daten,

5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,

6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,

7. die Kontrollrechte des Auftraggebers und die entsprechende Duldungs- und Mitwirkungspflichten des Auftragnehmers,

8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,

10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Das Gesundheitszentrum wurde von der Aufsichtsbehörde zur Stellungnahme zu dem im Raum stehenden Verdacht eines datenschutzrechtlichen Verstoßes aufgefordert. Insbesondere wurde um Vorlage eines Auftragsdatenverarbeitungsvertrags bzw. entsprechender schriftlicher Vereinbarungen zwischen den Beteiligten und um Auskunft über die notwendigerweise zu treffenden technischen und organisatorischen Maßnahmen, z. B. beim Versand der Unterlagen (auch in elektronischer Form), gebeten.

Das Gesundheitszentrum teilte mit, dass es sich bei den fotografierten Akten um private Unterlagen der Mitarbeiterin des Schreibservices gehandelt habe, die diese mit sich geführt habe. Weiterhin wurde mitgeteilt, dass der Transport der Krankenakten grundsätzlich in verschlosse-

nen Kisten erfolge und es nie Probleme bei der Zusammenarbeit mit dem Unternehmen gegeben habe. Auch wurde darauf hingewiesen, dass der Vertrag mit dem Schreibservice aufgrund der Umstellung des Krankenhausinformationssystems (KIS) zum Jahresende auslaufe, da die Schreibarbeiten künftig hausintern erstellt werden. Auf die einzelnen Fragen der Aufsichtsbehörde wurde nicht weiter eingegangen, v.a. konnte kein Auftragsdatenverarbeitungsvertrag vorgelegt werden.

Auf erneute Nachfrage durch die Aufsichtsbehörde teilte das Gesundheitszentrum mit, dass die Zusammenarbeit mit dem Schreibservice nunmehr vorzeitig beendet worden sei.

Abschließend ist festzuhalten, dass bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag gemäß § 11 BDSG der Auftraggeber für die Einhaltung der Vorschriften des BDSG und anderer Vorschriften über den Datenschutz verantwortlich ist („Verantwortliche Stelle"). Dem Auftraggeber obliegt darüber hinaus die Pflicht, den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Ob eine solche Prüfung im vorliegenden Fall erfolgt ist, konnte nicht nachgewiesen werden.

15 Schule und Bildung

15.1 1. Saarländischer Medientag "Neue Chancen für neues Lernen!?"

Am 18. September 2013 fand der 1. Saarländische Medientag in den Räumlichkeiten der Hermann Neuberger Sportschule in Saarbrücken statt. Organisiert wurde die Veranstaltung von den Mitgliedern der AG Medienkompetenz, die sich zum Ziel gesetzt haben, einerseits über neue Entwicklungen im Medienbereich zu informieren, andererseits aber auch über Chancen und Risiken der neuen Medien aufzuklären. Neben dem Unabhängigen Datenschutzzentrum Saarland sind folgende Institutionen ständig in der AG Medienkompetenz organisiert: Die Landesmedienanstalt Saarland, das Ministerium für Bildung und Kultur, das Landesinstitut für Präventives Handeln, das Landesinstitut für Pädagogik und Medien, der Jugendserver-Saar, das Landespolizeipräsidium und die Europäische EDV-Akademie des Rechts.

Die Veranstaltung richtete sich vorrangig an Lehrkräfte und pädagogische Fachkräfte. Sie wurde als offizielle Lehrerfortbildung sowohl im Saarland als auch in Rheinland-Pfalz anerkannt und so haben sich ca. 120 Personen zum Medientag angemeldet.

Prof. Dr. Stefan Aufenanger, Professor für Erziehungswissenschaft und Medienpädagogik an der Universität Mainz, eröffnete den Medientag mit dem Vortrag „Tablets in der Schule - Neue Chancen für neues Lernen!?“ und berichtete von Möglichkeiten und Trends beim Einsatz von Tablets im Unterricht. Den Teilnehmerinnen und Teilnehmern wurde durch die Veranstaltung das breite Angebot präsentiert, das die Mitglieder der AG Medienkompetenz für Schulen bereithalten. In praxisorientierten Workshops wurde der Einsatz digitaler Medien im Unterricht demonstriert und diskutiert. Im Fokus der Tagung standen die Chancen, die mit digitalen Medien - insbesondere mit Tablets und Smartphones - für Lehr- und Lernzwecke verbunden sind. Hierfür waren unter anderem namhafte Projekte wie Klicksafe, der Verein Internet-ABC sowie der SWR mit seinem Projekt „Planet Schule“ vor Ort und präsentierten ihre Unterrichtsmaterialien.

Aufgrund der großen Resonanz der Veranstaltung wird im Herbst des Jahres 2015 der 2. Saarländische Medientag stattfinden.

15.2 Schulworkshops „Mit Datenschützern lernen“

Die fortschreitende Digitalisierung unserer Welt und die zunehmenden Nutzung von Web 2.0 Angeboten wie Facebook, google+ oder Dienste wie WhatsApp und Instagram sind auch im schulischen Bereich eine große Herausforderung.

Wir haben daher mit dem Schuljahr 2013/2014 basierend auf einem Konzept von Rheinland–Pfalz erstmals auch im Saarland Workshops an Schulen angeboten. Ein Pilotprojekt startete im Herbst 2013 in der Klas-

senstufe sechs der weiterführenden Schulen im Landkreis Merzig-Wadern. Zwischenzeitlich werden die Workshops saarlandweit angeboten.

Die Referentinnen und Referenten werden von uns ausgebildet, regelmäßig zu Meetings eingeladen und haben die Möglichkeit, sich in Foren untereinander und mit den Referenten in Rheinland-Pfalz auszutauschen. In der Einführungsphase müssen sie mindestens zweimal an einem Workshop als Zuhörer teilnehmen. Selbstverständlich gibt es auch regelmäßige Ansprechpartner in unserer Dienststelle, die auch in unregelmäßigen Abständen die Workshops besuchen.

Nach jedem Workshop erfolgt durch die Lehrer eine Rückmeldung an die Dienststelle – die sowohl den Ablauf als auch den Inhalt beschreibt, so dass bei Bedarf auch eine regelmäßige Steuerung möglich ist.

Die Schülerinnen und Schüler sollen für einen datenschutzgerechten Umgang mit ihren Daten im Internet sensibilisiert werden. In einem vier Unterrichtsstunden umfassenden Workshop werden standardmäßig Themen wie der datenschutzgerechte Umgang mit Smartphones, Sozialen Netzwerken und Apps genauso vermittelt wie Online-Ethik, Cybermobbing und Selbstdatenschutz. Die Bedeutung und der Verlust der Privatsphäre werden ebenso thematisiert wie aktuelle datenschutzrechtliche Themen.

Das pädagogische Konzept, das vom Bildungsministerium genehmigt wurde, skizziert den Ablauf der Unterrichtseinheit und vereint sowohl Theorie als auch praktische Erarbeitung am Computer. Darüber hinaus werden die Unterrichtsmethoden dargestellt, die eine möglichst optimale Sensibilisierung der Schüler gewährleisten sollen.

Die Unterrichtseinheiten sind in der Regel so gestaltet, dass zunächst eine theoretische sowie praktische Einführung dazu erfolgt, welche Spuren jeder im Netz hinterlässt, und anschließend eine gemeinsame Begründung für den Selbstdatenschutz auf der Grundlage von Kurzfilmen und Web-Clips gefunden wird.

Die Schüler lernen neben der einfachen Installation eines sicheren Passwortes auch die Möglichkeiten, persönliche Daten mit Hilfe von Sicherheitseinstellungen technisch zu sichern.

Aufgrund der Dynamik in dieser Materie müssen unsere Referenten/innen aber auch auf aktuelle Trends bei den Jugendlichen eingehen. Dies war im Winter 2014 etwa das Portal YouNow. Dieses Programm können Schüler/innen leicht auf ihr Handy laden, sich dann mit der Web-Cam filmen und dies live ins Internet stellen. Es funktioniert etwa wie YouTube – ist aber noch einfacher zu bedienen. Da die Missbrauchsgefahr allerdings noch deutlich höher ist, ist gerade hier eine besondere Sensibilisierung notwendig.

Zur Vor- und Nachbereitung der Workshops wird den Lehrkräften und Kindern der Internetauftritt *www.youngdata.de* empfohlen. Youngdata ist eine Webseite, welche als offizielle Jugendseite aller Datenschutzaufsichtsbehörden in Deutschland betrieben wird. Alle Themen, die im Workshop angesprochen werden, sind auch unter *www.youngdata.de* zu finden.

Bis zum Zeitpunkt der Drucklegung haben wir in etwa 135 Workshops ca. 3.400 Schülerinnen und Schüler erreicht und auf den datenschutzgerechten Umgang mit ihren Daten im Internet sensibilisieren können.

Natürlich kann eine Unterrichtseinheit von vier Stunden nur Grundlagen über den Datenschutz vermitteln und die Schüler für einen sorgsamen Umgang mit ihren Daten sensibilisieren.

Die Datenschutzbeauftragten setzen sich daher bundesweit dafür ein, dass dieses Thema sowohl in den Schulunterricht integriert wird - sei es als eigenes Fach oder fächerübergreifend - aber auch in den Ausbildungsplan für Lehrer.

Insgesamt stellt dieses umfangreiche Projekt zwar eine große Herausforderung für unsere Dienststelle dar, wir sehen es aber als einen ganz wichtigen Baustein dafür, jungen Menschen Datenschutz und Medienkompetenz nahe zu bringen.

16 Forschung

16.1 Vigilanz-Test bei Verdacht auf Drogenkonsum

Im Berichtszeitraum hat uns das Landesinstitut für Präventives Handeln ein Forschungsprojekt vorgestellt und um eine datenschutzrechtliche Einschätzung gebeten.

Das Forschungsprojekt befasst sich mit dem Nachweis der Beeinträchtigung im Straßenverkehr in Folge des Konsums psychoaktiver Substanzen (z. B. Cannabisprodukte, Amphetamin oder Medikamente).

Im Unterschied zu Alkohol ist es schwierig, Personen, die solche Substanzen zu sich genommen haben, zu erkennen. Bisher ist man bei der Verdachtsgewinnung auf die Beobachtung der betreffenden Person angewiesen, z. B. durch Polizeibeamte bei einer Verkehrskontrolle. Es liegt auf der Hand, dass dies immer nur ein subjektiver Eindruck ist.

Um die Verdachtsgewinnung auf eine objektive Grundlage zu stellen, möchte das Landesinstitut für Präventives Handeln prüfen, ob ein an der Eidgenössischen Hochschule Zürich entwickelter Vigilanz-Test in diesem Zusammenhang hilfreich sein könnte. Der Test orientiert sich nicht an dem Stoffnachweis, sondern an dem Grad der Beeinflussung der Wachheit bzw. Aufmerksamkeit (Einschränkung der Vigilanz).

Bei diesem Test werden an einem PC über einen Zeitraum von vier Minuten mithilfe eines bestimmten Verfahrens Reaktionszeiten und Aufmerksamkeitsfehler gemessen. Dieser Test soll bei Personen durchgeführt werden, die bei einer herkömmlichen Verkehrskontrolle nach Einschätzung des Polizeibeamten Auffälligkeiten zeigen und sich einer Blutprobe bzw. einer Speichelprobe unterziehen müssen. Anonymisierte Zusatzdaten sollen mit Hilfe eines Formularbogens bei den jeweiligen Probanden erhoben werden. Der den Vigilanztest durchführende Polizeibeamte dokumentiert nach Entnahme der Blutprobe mit Hilfe eines Beurteilungsbogens die Ausfallerscheinungen vor Durchführung des Tests.

Das Ergebnis der mit einer Kennziffer versehenen Blutprobe bzw. Speichelprobe wird dem Projektleiter zugeleitet zum Vergleich mit dem mit der gleichen Kennziffer versehenen Vigilanz-Testergebnis. Nach Zuordnung der Ergebnisse des Tests zu den Probenergebnissen wird der Datensatz anonymisiert und die nicht anonymen Daten werden vernichtet.

Die Aussagekraft des Tests soll durch einen Vergleich der Testergebnisse der durch die genannten Substanzen beeinflussten Personen mit Testergebnissen aus einer zweiten Testreihe, in der freiwillige Probanden (z.B. Fahrschüler) sich ebenfalls dem Vigilanztest und einer Speichelprobe unterziehen, überprüft werden.

Einigkeit bestand von vorneherein, dass die Teilnahme an dem Test freiwillig ist, weil eine entsprechende gesetzliche Verpflichtung nicht besteht. Darüber hinaus sollte der Test zwar im Zusammenhang mit einer Verkehrskontrolle, jedoch deutlich von dieser getrennt durchgeführt werden. Dies bedeutet, dass die im Zusammenhang mit einer Ver-

kehrskontrolle durchgeführten Tests zwar durch Polizeibeamte vorgenommen werden, jedoch der mit der Vigilanztestdurchführung betraute, in zivil gekleidete Beamte nicht mit der Sachbearbeitung im Zusammenhang mit der Blutentnahme befasst ist. Darüber hinaus soll der Test zeitlich nach der Blutentnahme sowie räumlich getrennt von dieser Maßnahme erfolgen.

Die erforderliche schriftliche Einwilligungserklärung muss besonders sorgfältig formuliert werden, um den Probanden, die den Test im Zusammenhang mit der polizeilichen Blutentnahme absolvieren, deutlich zu machen, dass der Test kein verpflichtender Bestandteil der polizeilichen Ermittlung ist, sondern rein wissenschaftlichen Zwecken dient.

In Abstimmung mit unserer Dienststelle wurde eine Einwilligungserklärung erarbeitet, die diesen Anforderungen genügt: Der Zweck und der Umfang des Forschungsvorhabens werden ausführlich erläutert und die verantwortlichen Träger und Leiter des Projekts werden genau benannt. Es wird ausdrücklich darauf hingewiesen, dass bei einer Nichtteilnahme keinerlei Nachteile entstehen und bis zur Anonymisierung der Daten die Einwilligung jederzeit widerrufen werden kann.

Ergebnisse dieses Projekts sollen im Oktober 2015 präsentiert werden.

17 Beschäftigtendatenschutz

17.1 Beschäftigtendatenschutz im öffentlichen Bereich

17.1.1 Auskunftssperren für besonders gefährdete Beamtengruppen

Im Berichtszeitraum sind Gewerkschaftsvertreter auf uns zugekommen und haben auf Übergriffe auf Beschäftigte des öffentlichen Dienstes und deren Angehörige am Wohnort der Beschäftigten hingewiesen. Durch Namensschilder auf der Uniform oder am Büro der Beamten könne durch gezielte Recherche im Internet und eine sogenannte einfache Melderegisterauskunft bei einer Kommune leicht eine Verknüpfung zur Wohnadresse der Beschäftigten hergestellt werden.

Nach Angabe der Gewerkschaftsvertreter seien meist Beschäftigte des öffentlichen Dienstes von Übergriffen am Wohnort betroffen, die im Vollzugs- oder Ordnungsdienst tätig sind. Manche Bürger würden sich persönlich bei jemandem rächen wollen, der ihnen beispielsweise einen Strafzettel fürs Falschparken erteilt hat. Sobald der Name der Beamten bekannt sei, recherchieren sie auch mittels einer einfachen Melderegisterauskunft die Wohnadresse und bedrohen die Beschäftigten oder ihre Familienangehörigen.

Eine einfache Auskunft über Vor- und Familiennamen, Doktorgrad und Anschriften einzelner bestimmter Personen können gemäß § 34 Abs.1 Saarländisches Meldegesetz (MG) neben bestimmten öffentlichen Stellen auch private Antragsteller erhalten. Die einfache Melderegisterauskunft wird von Datenschützern kritisiert, weil die Auskunftserteilung nur geringen Einschränkungen unterliegt und der Meldepflichtige von wenigen gesetzlichen Ausnahmefällen abgesehen die Weitergabe seiner melderechtlichen Basisdaten an jedermann nicht verhindern kann.

Eine Ausnahme wird in § 34 Abs.1 MG benannt: „Liegen Tatsachen vor, die die Annahme rechtfertigen, dass dem Betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann, hat die Meldebehörde auf Antrag oder von Amts wegen eine Auskunftssperre im Melderegister einzutragen. Eine Melderegisterauskunft ist in diesen Fällen unzulässig, es sei denn, dass nach Anhörung des Betroffenen eine Gefahr im Sinne des Satzes 1 ausgeschlossen werden kann."

Genau diese gesetzlich vorgesehene Ausnahmemöglichkeit wurde aber von den Kommunen in der Vergangenheit bei Beamten, die einen solchen Antrag gestellt haben, abgelehnt, weil sie die Gefahr für Leben, Gesundheit oder persönliche Freiheit nicht erkannt haben. Hier sollte auch von Seiten der Kommune auf einen offeneren Umgang mit solchen Antragsersuchen hingewirkt werden. Die Kommentarliteratur führt hierzu aus, dass der Begriff der schutzwürdigen Interessen weit auszulegen und eine Gefahr mit dem Begriff der Beeinträchtigung identisch zu verwenden sei.

Eine Auskunftssperre kann jedoch nur dann ihre Wirkung entfalten, wenn die gleichen personenbezogenen Daten nicht via Internet frei recherchierbar sind.

17.1.2 Weitergabe von Verwandtschaftsverhältnissen an die Presse

In einer saarländischen Stadt wurden die verwandtschaftlichen Beziehungen sämtlicher Mitarbeiter zueinander festgestellt, in einer Liste zusammengefasst und an die Presse weitergegeben.

Hintergrund war, dass eine Oppositionspartei öffentlich den Vorwurf erhoben hatte, dass in der Stadtverwaltung Entscheidungsträger dafür sorgten, dass ihre Verwandten bei Einstellungen bevorzugt berücksichtigt und bei Beförderungen oder Höhergruppierungen besser abschnitten als andere Mitarbeiter.

Die Presse berichtete darüber und stellte der Verwaltungsspitze die Frage, ob es verwandtschaftliche Beziehungen zwischen Entscheidungsträgern der Verwaltung und Mitarbeitern gebe. Daraufhin wurde die erwähnte Liste zusammengestellt; allerdings verzichtete die Presse aus datenschutzrechtlichen Gründen auf deren Veröffentlichung.

Durch eine anonyme Eingabe hatten wir von dem Sachverhalt Kenntnis erhalten. Unsere rechtliche Überprüfung ergab, dass schon die Erhebung und somit erst recht die nachfolgende Übermittlung der verwandtschaftlichen Beziehungen mangels entsprechender Erforderlichkeit mit der einschlägigen Vorschrift im saarländischen Datenschutzgesetz über die Verarbeitung von Mitarbeiterdaten (§ 31 Saarländisches Datenschutzgesetz (SDSG)) nicht in Einklang stand.

Die Stadtverwaltung räumte auf unsere Bitte um Stellungnahme den Verstoß ein und sagte für die Zukunft zu, den Anforderungen des Datenschutzes zu genügen.

Im Hinblick darauf wurde von einer Beanstandung abgesehen.

17.2 Beschäftigtendatenschutz im nicht-öffentlichen Bereich

17.2.1 Arbeitnehmerüberwachung in einem Gastronomiebetrieb

Ein Mitarbeiter eines Gastronomiebetriebes hatte sich an die Dienststelle gewandt und behauptet, die Mitarbeiter in der Küche würden videografiert und permanent durch ihren Vorgesetzten überwacht. Die Kontrolle vor Ort ergab, dass die eingesetzte Dome-Kamera tatsächlich den nicht-öffentlich zugänglichen Arbeitsbereich der Mitarbeiter überwachte. Der Zugriff zur Kamera erfolgte über einen passwortgeschützten Remotezugang, der jederzeit vom Arbeitgeber abgerufen werden konnte.

Der Vorgesetzte wurde im Gespräch ausführlich über die Voraussetzungen einer zulässigen Videoüberwachungsmaßnahme, die den Anforderungen des BDSG entspricht und die dazu ergangene Rechtsprechung

des Bundesarbeitsgerichts informiert. Demnach dürfen Beschäftigte, außer in speziellen Einzelfällen, nicht permanent von einer Videoüberwachung erfasst werden. Da der Fokus der Kamera auf der Überwachung der Leistung und des Verhaltens der Mitarbeiter lag, die somit einem permanenten Überwachungsdruck durch ihren Arbeitgeber ausgesetzt waren, wurde die Kameraeinstellung für unzulässig erklärt.

Der Verantwortliche zeigte sich zunächst einsichtig und übermittelte uns eine Mail, in der er bestätigte, die Videokamera vom Netz genommen und keine Zugriffsmöglichkeiten mehr zu haben.

In einer Nachkontrolle mussten wir leider feststellen, dass die Kamera nach wie vor einsatzbereit und angeschlossen für Zugriffe zur Verfügung stand.

Das hierzu ergangene Ordnungswidrigkeitsverfahren wird unter Kapitel 18.2 des Tätigkeitsberichts beschrieben.

17.2.2 Telefonische Kontaktaufnahme zu ausgeschiedenen Mitarbeitern

Ein Petent, der sein Arbeitsverhältnis gekündigt hatte, beschwerte sich bei unserer Dienststelle über seinen ehemaligen Arbeitgeber.

Dieser hatte ein Callcenter damit beauftragt, Mitarbeiter, die ihr Arbeitsverhältnis gekündigt hatten, nach den Gründen zu befragen und dem Callcenter zu diesem Zweck Namen und Telefonnummern der betreffenden Personen übergeben. Ziel der Befragungsaktion sollte nach Aussage des Unternehmens sein, Ansatzpunkte für Verbesserungen im Unternehmen zu ermitteln.

Wir haben die beschriebene Datennutzung als Verstoß gegen § 32 Bundesdatenschutzgesetz (BDSG), der die Voraussetzungen einer zulässigen Datenverarbeitung von Beschäftigten regelt, bewertet. Eine Interessenabwägung zwischen dem Interesse des Unternehmens an einer Verbesserung der Arbeitsbedingungen mit den schutzwürdigen Belangen der ausgeschiedenen Mitarbeiter lässt die Maßnahme als unverhältnismäßig erscheinen.

Das Unternehmen hat dies auf unsere Nachfrage hin auch eingeräumt und als Alternative vorgeschlagen, künftig auf die Einschaltung eines Callcenters zu verzichten.

Da das Unternehmen die Aktion sofort eingestellt hat, haben wir auf die Einleitung eines Bußgeldverfahrens verzichtet.

18 Ordnungswidrigkeitsverfahren

18.1 Übersicht

Die Landesbeauftragte für Datenschutz ist zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 28a Saarländisches Datenschutzgesetz (SDSG). Im Berichtszeitraum sind durch die Behörde 29 Ordnungswidrigkeitenverfahren abgeschlossen worden.

Es handelte sich hierbei zu einem großen Teil um Verfahren zur Ahndung von Verstößen nach § 43 Abs. 1 Nr. 10 Bundesdatenschutzgesetz (BDSG). Danach handelt ordnungswidrig, wer vorsätzlich oder fahrlässig entgegen § 38 Abs. 3 S. 1 oder Abs. 4 S. 1 BDSG eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet. § 38 Abs. 3 S. 1 BDSG verpflichtet die datenverarbeitenden Stellen sowie die mit deren Leitung beauftragte Person, der Landesbeauftragten für Datenschutz auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen.

Der Gesetzgeber möchte mit der Regelung § 38 Abs. 3 und Abs. 4 BDSG eine effektive Datenschutzaufsicht erreichen, in dem die verantwortlichen Stellen zur Zusammenarbeit mit der Aufsichtsbehörde verpflichtet werden. In der Praxis der Aufsichtstätigkeit kommt es jedoch vermehrt vor, dass unsere Schreiben verzögert, erst nach wiederholtem Nachfragen beantwortet oder gar ignoriert werden. Die unverzügliche Erfüllung der Auskunftspflicht ist jedoch zwingende Voraussetzung dafür, dass das Unabhängige Datenschutzzentrum Saarland bzw. die Landesbeauftragte für Datenschutz ihre Aufgabe als Aufsichtsbehörde nach § 38 Abs. 1 BDSG effektiv wahrnehmen kann. Daher leiten wir in den genannten Fällen bereits aus generalpräventiven Gesichtspunkten ein Ordnungswidrigkeitenverfahren ein. Bemerkenswert ist, dass nach Kenntnis der Einleitung entsprechender Verfahren die geforderten Auskünfte in der Regel zeitnah nachgeholt werden.

Im Folgenden werden exemplarisch vier Verfahren dargestellt, die von unserer Behörde mit Erlass eines Bußgeldbescheides abgeschlossen wurden:

18.2 Videoüberwachung beim Pizza-Lieferdienst

Auf Grund einer anonymen Eingabe wurde die Aufsichtsbehörde im April 2013 darauf aufmerksam gemacht, dass in einer Filiale eines Pizza-Lieferdienstes mittels Videotechnik eine Überwachung der Mitarbeiter stattfinden soll. Im Rahmen des daraufhin auf der Grundlage des § 38 Abs. 1 BDSG eingeleiteten Verwaltungsverfahrens fand ein Vor-Ort-Termin in der Filiale statt. Bei diesem Termin wurde festgestellt, dass mittels einer 360-Grad-Netzwerkkamera die Mitarbeiter der Filiale überwacht wurden. Wegen der von Seiten des Unabhängigen Datenschutzzentrums geäußerten Bedenken im Hinblick auf einen datenschutzkonformen Betrieb der beschriebenen Kamera, teilte der Inhaber der Filiale im weiteren Fortgang des Verfahrens mit, dass die Kamera

vom Netzwerk entfernt wurde und somit keine Möglichkeit mehr bestehe auf die Kamera zuzugreifen. Daraufhin wurde seitens der Aufsichtsbehörde davon abgesehen weitere Maßnahmen zu treffen.

Auf Grund eines erneuten Hinweises, dass die Kamera wohl weiterhin betriebsbereit wäre und auch genutzt würde, fand im Frühjahr 2014 eine unangekündigte Prüfung in den Filialräumen statt. Dabei wurde festgestellt, dass die genannte Kamera immer noch an der im April 2013 festgestellten Stelle hing und entgegen den Angaben des Inhabers weiterhin mit dem Netzwerk verbunden war und hierüber auch mit Strom versorgt wurde und damit betriebsbereit war.

Da der Filialinhaber im geschilderten Fall bewusst wahrheitswidrig falsche Angaben gemacht hat, haben wir ein Bußgeld festgesetzt.

18.3 Darlehensabfrage über den Mieter

Immer wieder erhält die Aufsichtsbehörde Eingaben in denen vorgetragen wird, dass der Arbeitgeber, Geschäftspartner oder andere (potentielle) Vertragspartner unberechtigterweise Bonitätsauskünfte eingeholt haben sollen. Eine nicht alltägliche Variante wurde uns allerdings von einem Mieter zur Anzeige gebracht.

Mieter und Vermieter befanden sich im Streit über die Zahlung fälligen Mietzinses. Der Vermieter war Inhaber eines zu einem Konzern gehörenden Autohauses.

Da der Mieter von Beginn an keine Mietzahlungen leistete, kam beim Vermieter der Verdacht auf, dass der Mieter sich den Mietzins für das Wohnhaus von Anfang an nicht habe leisten können. Um dies für eine Strafanzeige wegen Eingehungsbetrugs nachweisen zu können, stellte der Vermieter eigene Ermittlungen an. Da der Mieter selbst ein Fahrzeug einer zum Konzern gehörenden Marke besaß, konnte der Vermieter durch die Abfrage der Fahrgestellnummer – diese war am Fahrzeug von außen ablesbar – ermitteln, dass es sich hierbei um ein Fahrzeug handelte, dass über eine dem Konzern angehörige Bank finanziert wurde.

Da der Vermieter wusste, dass bei einer Finanzierung von Fahrzeugen über die zum Konzern gehörige Bank der Darlehensnehmer Angaben zur Höhe seiner monatlichen Einkünfte machen muss, rief er in seiner Eigenschaft als Geschäftsführer des Autohauses bei der Betriebskundenhotline der Bank an und bat unter Angabe seiner Betriebsnummer um Übersendung einer Kopie des Darlehensvertrages. Der Darlehensvertrag enthielt eine Klausel, die die Bank dazu berechtigte, den Darlehensvertrag zum Zwecke der Abwicklung von Kundenanfragen im Einzelfall an die zum Konzern gehörenden Autohäuser zu übermitteln. Der Vermieter unterließ jedoch den Hinweis darauf, dass der angeforderte Darlehensvertrag nicht zur Abwicklung von Serviceleistungen gegenüber dem Darlehensnehmer angefordert wurde. Im Übrigen war der Mieter kein Kunde beim Autohaus des Vermieters, die Anforderung des Darlehensvertrages erfolgte allein aufgrund privater Motivation.

Wir werteten diesen Sachverhalt als Erschleichen der Übermittlung personenbezogener Daten durch unrichtige Angaben gemäß § 43 Abs. 2

Nr. 4 BDSG. Insbesondere das Tatbestandsmerkmal der „unrichtigen Angaben“ wurde aus unserer Sicht hier dadurch erfüllt, dass der Vermieter konkludent eine bestimmte Fehlvorstellung bei dem Sachbearbeiter der Betriebskundenhotline hervorrief und aufrechterhielt. Indem er sich als Geschäftsführer des Autohauses und damit als Handelspartner der Bank vorstellte, erweckte er konkludent den Eindruck, dass der Anruf betrieblich veranlasst sei und er die begehrten Informationen für geschäftliche Zwecke benötige. Dies wurde noch dadurch verstärkt, dass er sich den Darlehensvertrag an seine Firmenanschrift faxen ließ. Beim Mitarbeiter der Bank führte dies zu einem Irrtum über das Vorliegen eines die Übermittlung rechtfertigenden, berechtigten Interesses, denn hätte er die wahre Motivation des Handelspartners und Vermieters gekannt, so hätte er eine Übersendung des Darlehensvertrages gerade nicht veranlassen dürfen.

18.4 Bürgerbeschwerde im kommunalen Amtsblatt veröffentlicht

Wenn Bürger mit der Gemeindeverwaltung korrespondieren erwarten sie zu Recht, dass ihr Anliegen vertraulich behandelt und die geführte Kommunikation nicht veröffentlicht wird.

Anders war dies im Fall einer saarländischen Kommune. Ein Bürger hatte sich per E-Mail über die Wasserqualität in einem kommunalen Schwimmbad beschwert. In einer Antwortmail, die der Bürgermeister persönlich zeichnete, wurde sein Anliegen unter Verweis auf durchgeführte Wasserproben zurückgewiesen und in einem Postskriptum wurde der Bürger gebeten: „Beirren Sie uns nie wieder“.

Mit dieser Antwortmail wandte sich der Bürger an den Saarländischen Rundfunk. Dieser machte in einem Hörfunk-Beitrag die Wasserqualität des kommunalen Schwimmbades zum Inhalt der öffentlichen Berichterstattung und nahm den Inhalt des in der Antwortmail verwendeten Postskriptums zum Anlass um über den Umgangston des Bürgermeisters gegenüber seinen Bürgern zu diskutieren. In dem Beitrag kam auch der Bürger zu Wort, der jedoch ausdrücklich anonym bleiben wollte.

Als Reaktion auf die Berichterstattung nahm der Bürgermeister zu den Vorwürfen Stellung, indem er im amtlichen Teil des gemeindlichen Nachrichtenblattes eine kurze Stellungnahme veröffentlichte und darunter die E-Mail des Bürgers, der sich beschwert hatte, im Volltext und unter Namensnennung veröffentlichte.

Wir werteten dies als unbefugte Weitergabe von durch das Saarländische Datenschutzgesetz (SDSG) geschützten personenbezogenen Daten, die nicht offenkundig sind, entsprechend § 36 Abs. 1 Nummer 1 SDSG. In diesem Fall wurde von uns ein Bußgeld festgesetzt.

18.5 Eigene Ermittlungen des Amtsleiters

Ein weiteres Verfahren richtete sich gegen den Leiter einer saarländischen Bauaufsichtsbehörde. Diesem war aufgefallen, dass bei einer

Vielzahl von Bauanträgen für Vergnügungsstätten wiederholt dieselbe Person als Verfasser des Bauplans genannt wurde. Aufgrund eigener Ermittlungen fand der Amtsleiter heraus, dass der besagte Planverfasser hauptberuflich als Beamter in der saarländischen Landesverwaltung tätig war. Da er Zweifel daran hatte, ob der Planverfasser diese Nebentätigkeit, insbesondere im hier festgestellten Umfang habe genehmigen lassen, stellte er eine Liste mit allen Bauanträgen der vergangenen zehn Jahre zusammen, in denen diese Person als Planverfasser genannt wurde. Diese Liste übersandte er mit der Bitte um vertrauliche Behandlung per E-Mail an den Dienstvorgesetzten des Beamten. Der Dienstvorgesetzte leitete aufgrund dieser Erkenntnisse ein Disziplinarverfahren gegen den Beamten ein.

Nach unserer Auffassung war hier der Tatbestand des § 36 Abs. 1 Nr. 1 SDSG, nämlich die unbefugte Weitergabe vom saarländischen Datenschutzgesetz geschützter personenbezogener Daten, die nicht offenkundig sind, verletzt.

Eine Rechtfertigung der Weitergabe wäre hier lediglich nach § 29 Abs. 1 Saarländisches Disziplinargesetz (SDG) in Betracht gekommen, dessen Voraussetzungen hier aber nicht vorlagen. § 29 Abs. 1 SDG verlangt nämlich, dass die Vorlage von Personalakten und anderen Behördenunterlagen mit personenbezogenen Daten sowie die Erteilung von Auskünften aus diesen Akten und Unterlagen nur auf Ersuchen der mit dem Disziplinarvorgang befassten Stelle erfolgen darf. Eine Mitteilung personenbezogener Daten ohne Anregung durch die mit dem Disziplinarvorgang befasste Stelle, sozusagen auf Vorrat, ist unzulässig. Vielmehr muss zwischen den Behörden ein Vorgang der Amtshilfe stattfinden, was hier nicht der Fall war. § 29 Absatz 1 SDG bestimmt weiterhin, dass die übermittelnde Stelle zunächst versuchen muss die Einwilligung des Betroffenen - hier des Beamten - einzuholen. Auch dies war hier nicht geschehen.

Auf andere Erlaubnistatbestände, beispielsweise solche aus dem SDSG konnte sich der Amtsleiter nicht berufen, da § 29 SDG eine spezielle Sonderregelung darstellt, die Mitteilungen zwischen Dienststellen über Disziplinarvorgänge umfassend und abschließend regelt.

19 Videoüberwachung

19.1 Einführung in die Thematik

Ob Videoüberwachung unter Nachbarn, der Umgang mit Bilddaten von Kunden durch Gewerbetreibende, die Überwachung von Mitarbeitern oder der Einsatz von Drohnen und Dashcams, der thematische Bogen der Videoüberwachung ist weit gespannt und sowohl in technischer als auch rechtlicher Hinsicht durch eine große Dynamik geprägt.

Im Berichtszeitraum sind verschiedene gerichtliche Entscheidungen mit teils richtungsweisendem Charakter ergangen. So wurde durch das Urteil des Europäischen Gerichtshofs vom 11. Dezember 2014 - C-212/13 - die Anwendbarkeit der Datenschutzrichtlinie 95/46/EG auf die zweckgerichtete Videoüberwachung von öffentlichem Raum durch Privatpersonen festgestellt, was mit der bisherigen Auslegungspraxis der deutschen Aufsichtsbehörden korrespondiert. Darüber hinaus sind unter anderem das Dashcam-Urteil des Verwaltungsgerichts Ansbach vom 12. August 2014 - AN 4 K 13.01634 - und die Entscheidung des Oberverwaltungsgerichts Lüneburg vom 29. September 2014 - 11 LC 114/13 - hinsichtlich der Zulässigkeit der Videoüberwachung eines Treppenhauses zu nennen.

Neben der aufsichtsbehördlichen Sanktionierung unzulässiger Videoüberwachungsmaßnahmen wurde im Berichtszeitraum vor allem ein Schwerpunkt auf Aufklärung und präventive Beratung gelegt. Durch Informationsveranstaltungen und der Erstellung von themenspezifischen Publikationen soll erreicht werden, dass von vornherein der Einsatz von unzulässigen Überwachungsmaßnahmen vermieden wird.

19.2 Videoüberwachung im Beschäftigungsverhältnis

Immer wieder werden die Aufsichtsbehörden für den Datenschutz in Deutschland mit Fällen konfrontiert, in denen Beschäftigte eines Unternehmens per Videoüberwachung kontrolliert werden. So hat auch das Unabhängige Datenschutzzentrum des Saarlandes im Berichtszeitraum mehrere Eingaben zu dieser Thematik erhalten und musste die datenschutzrechtliche Zulässigkeit der Videoüberwachung beurteilen.

Generell ist dazu anzumerken, dass bereits im Jahr 2004 das Bundesarbeitsgericht festgestellt hat, dass eine permanente Videoüberwachung am Arbeitsplatz und der damit einhergehende permanente Überwachungsdruck in schwerwiegender Weise in das allgemeine Persönlichkeitsrecht der Arbeitnehmer eingreift. Eine „Rund-um-die-Uhr-Überwachung" von Mitarbeitern ist aufgrund dieses schwerwiegenden Eingriffs in die Persönlichkeitsrechte der Beschäftigten unzulässig (BAG Beschluss vom 14. Dezember 2004 AZ: 1 ARB 34/03).

Nur in ganz besonderen Ausnahmefällen kann eine solche Maßnahme gerechtfertigt sein. Eine permanente Videoüberwachung der Beschäftigten ist beispielsweise denkbar, wenn der Beschäftigte in einem be-

sonders gefahrträchtigen Arbeitsbereich tätig ist und der Arbeitgeber seiner Schutzpflicht nachkommen muss. In der Regel fällt die Abwägung zwischen den Interessen eines Arbeitgebers an einer Videoüberwachung und den schutzwürdigen Belangen der Beschäftigten jedoch zugunsten der Beschäftigten aus. Die Zulässigkeit ist im Einzelfall zu überprüfen.

In der Abwägung zwischen den berechtigten Interessen der Arbeitgeber und der Beschäftigten an der Durchführung einer Videoüberwachung ist insbesondere zu gewichten, ob dem Beschäftigten überhaupt ein kontrollfreier und damit unbeobachteter Arbeitsbereich zur Verfügung steht. Generell unzulässig ist eine Videoüberwachung in sensiblen Bereichen wie Umkleidekabinen, sanitäre Einrichtungen und Aufenthaltsräume. Auch eine Videoüberwachung zur reinen Leistungs- und Verhaltenskontrolle der Beschäftigten ist unzulässig.

Da eine Videoüberwachung dazu geeignet ist, das Verhalten und die Leistung der Beschäftigten zu dokumentieren, ist die Installation einer Videoüberwachung im Betrieb mitbestimmungspflichtig, soweit ein Betriebsrat im Unternehmen existiert. Bei der Installation einer Videoüberwachung im Betrieb empfehlen wir daher den Abschluss einer Betriebsvereinbarung, die eine Auswertung der Videosequenzen zur Verhaltens- und Leistungskontrolle der Belegschaft ausschließt.

Der Düsseldorfer Kreis hat aufgrund der vermehrten Eingaben zur Thematik am 26. Februar 2014 eine Orientierungshilfe zur Videoüberwachung durch nicht-öffentliche Stellen veröffentlicht. Darin wird unter anderem unter Punkt 4 auch explizit auf die Videoüberwachung von Beschäftigten eingegangen. Die Orientierungshilfe ist in unserem Internetangebot zu finden und gibt eine umfassende Hilfestellung zur Zulässigkeitsprüfung von Videoüberwachungsmaßnahmen.

19.3 Videoüberwachung in der industriellen Produktion

In einem weiteren Fall wurden wir von einem Mitarbeiter eines industriellen Produktionsbetriebes darüber informiert, dass der Eigentümer der Firma eine Videokamera zur Überwachung seiner Mitarbeiter angebracht habe. Der Bitte um Stellungnahme zur Erforderlichkeit der Videoüberwachungsmaßnahme kam der Eigentümer nicht in ausreichendem Maße nach, so dass sich zwei Mitarbeiter des Datenschutzzentrums vor Ort ein Bild der Videoüberwachungsmaßnahme machten.

Die angebrachte Netzwerkkamera war so ausgerichtet, dass sie die in der Produktionshalle tätigen Mitarbeiter permanent überwachen konnte. Die Kamera war geeignet, sowohl Ton- als auch Bildaufzeichnungen anzufertigen. Der Zugriff auf die Kamera konnte über jeden Browser erfolgen. Bei der Überprüfung vor Ort wurde festgestellt, dass auf dem PC einer Mitarbeiterin, die Zugriffsrechte zur Netzwerkkamera besaß, keine gespeicherten Videosequenzen zu finden waren. Es wurde während des Zugriffs auf die Kamera lediglich ein Livebild aus der Produktionshalle wiedergegeben, auf dem einige Mitarbeiter permanent zu sehen waren.

Als Begründung für die Installation der Kamera gab der Betreiber mehrere Szenarien an. So sollte beispielsweise der Produktionsablauf in der

Halle kontrolliert werden, damit bei Komplikationen direkt eingegriffen werden könnte. Dieses Argument war jedoch dadurch zu widerlegen, dass ständig Mitarbeiter vor Ort waren, die bei Komplikationen einschreiten konnten. Ein weiterer Grund war die Überwachung eines explosionsgefährdeten Bereichs. Allerdings war die Kamera so ausgerichtet, dass der explosionsgefährdete Bereich nicht erfasst wurde. Darüber hinaus sollte die Kamera auch der Diebstahlprävention dienen. Ein erfolgter Diebstahl, der zur Anzeige gebracht wurde, konnte uns jedoch nicht belegt werden. Als entscheidender Anlass zur Installation der Kamera wurde uns mitgeteilt, dass der Firmeninhaber während eines Kontrollganges kurz vor Schichtende festgestellt hatte, dass einige seiner Mitarbeiter bereits umgezogen auf den Feierabend gewartet haben. Aus diesem Grund eine Kamera zu installieren, die permanent alle Mitarbeiter überwacht, steht jedoch nicht im Verhältnis zum Vergehen der Mitarbeiter. Als milderes Mittel der Kontrolle hätten hier häufigere Kontrollgänge durch den Inhaber der Firma, der auch auf dem Firmengelände eine Wohnung bewohnt, völlig ausgereicht.

Die eingesetzte Kamera unterstützte das 2-Wege-Audio-System. Sie hatte ein Mikrofon und einen Audioausgang für einen Lautsprecheranschluss. Die Möglichkeit der Tonaufzeichnung war allerdings deaktiviert. Wir haben in diesem Zusammenhang allerdings darauf hingewiesen, dass es § 201 Strafgesetzbuch (StGB) unter Strafandrohung verbietet, das nicht-öffentlich gesprochene Wort aufzuzeichnen oder abzuhören. Sofern eine Videokamera über eine solche Audiofunktion verfügt, ist sie irreversibel zu deaktivieren.

Im Rahmen der Anhörung war der Inhaber des Betriebes bereit, die Kamera zu deinstallieren und einen datenschutzkonformen Zustand herzustellen.

19.4 Videoüberwachung während einer Prüfung in der Universität des Saarlandes

Im Frühjahr 2013 erhielten wir den Anruf eines Studenten. Er informierte uns darüber, dass er gerade aus einer Prüfung an der Universität des Saarlandes komme und die Prüflinge per Videosequenz auf zwei Leinwänden im Frontbereich des Hörsaals projiziert und überwacht wurden.

Unmittelbar nach diesem Anruf fuhren zwei Mitarbeiter des Unabhängigen Datenschutzzentrum Saarland zur Universität, um sich selbst ein Bild von diesen Vorwürfen zu machen.

Ursprünglich wurde die Videoanlage installiert, um im Rahmen von E-Learning-Veranstaltungen beispielsweise einen Vortrag direkt ins Netz zu streamen oder die Aufzeichnung zu Nacharbeitszwecken zur Verfügung zu stellen. Die Anlage zu Überwachungszwecken während einer Prüfung zu benutzen war nicht Sinn und Zweck der Anlage. Gerade in Prüfungssituationen sind Studenten bereits einer besonderen Drucksituation ausgesetzt. Diese Situation zu verschärfen, indem die Studenten per Livestreaming an eine Leinwand im Frontbereich des Hörsaals projiziert werden, stellt einen unverhältnismäßigen Eingriff in das informationelle Selbstbestimmungsrecht der Studenten dar. Im Rahmen der Verhältnismäßigkeitsprüfung muss festgestellt werden, dass die Überwa-

chung der Studenten während der Prüfung mit milderen Mittel, sprich mehr Personal, durchgeführt werden kann.

Im Nachgang zu unserem Prüfbesuch wurden folgende Voraussetzungen für eine Nutzung der Videoanlage im Hörsaal festgelegt:

1. Es findet keine Videoüberwachung während einer Prüfung statt.
2. An die Eingangstüren des Hörsaals werden Schilder angebracht, die darüber informieren, dass die Videoanlage nur bei E-Learning-Veranstaltungen eingeschaltet wird.
3. Wann eine E-Learning-Veranstaltung stattfindet wird den Studenten im Vorfeld frühzeitig mitgeteilt.
4. Die Universitätsleitung wird alle Professoren und Dozenten in einem Schreiben darauf hinweisen, dass eine Videoüberwachung während einer Prüfung unzulässig ist.
5. Die Zugriffsrechte auf die Videoanlage werden derart beschränkt, dass nur der zuständige Techniker die Anlage freischalten kann.

Die Universität des Saarlandes ist unseren Forderungen gefolgt und hat einen datenschutzkonformen Zustand hergestellt.

19.5 Datenschutzrechtliche Bedingungen für den Einsatz mobiler Videokameras

Für die Frage nach der Anwendung des Bundesdatenschutzgesetzes (BDSG) im Zusammenhang mit Videoüberwachungsmaßnahmen ist es grundsätzlich unerheblich, ob stationäre Kameras oder mobile Geräte (Smartphone, portable Kameras, Drohnen[10] etc.) eingesetzt werden. Wie nachfolgend am Beispiel von Drohnen sowie Dash- und sog. Action-Cams[11] aufgezeigt wird, kann jedoch mit dem Einsatz von mobilen Kameras bzw. mit Kameras bestückten mobilen Geräten hinsichtlich der Tiefe des damit verbundenen Eingriffs in das allgemeine Persönlichkeitsrecht und der Anzahl der davon potentiell Betroffenen ein weitaus größeres Bedrohungsszenario verbunden sein, als dies bei stationären Kameras der Fall ist.

[10] Begrifflich ist dem Grunde nach, abhängig von dem Zweck der Nutzung, zwischen unbemannten Luftfahrtsystemen (UAS) und Flugmodellen zu unterscheiden. Bei gewerblicher Nutzung handelt es sich um UAS, bei der Nutzung für Zwecke des Sports und der Freizeitgestaltung kommen sog. Flugmodelle zum Einsatz. Der Begriff Drohne ist eigentlich einem militärischen Kontext vorbehalten, jedoch mittlerweile umgangssprachlich so weit verbreitet, dass im weiteren Text der Einfachheit halber nur noch von Drohne die Rede sein wird.

[11] Dashcams oder On-Board-Cams sind Kameras, die auf dem Armaturenbrett oder an der Windschutzscheibe von Autos angebracht sind und mit deren Hilfe das Verkehrsgeschehen im unmittelbaren Umfeld des Fahrzeugs aufgezeichnet wird. Sog. Action-Cams werden vereinzelt von Rad- oder Motorradfahrern eingesetzt und sind zumeist an Helmen angebracht.

19.5.1 Fliegender Eingriff in das Persönlichkeitsrecht: Gesetzliche Rahmenbedingungen für den Einsatz von mit Kameras ausgerüsteten Drohnen

In zunehmendem Maße werden Eingaben Betroffener und Anfragen von Ortspolizeibehörden an die Aufsichtsbehörde herangetragen, die den Einsatz von mit Videokameras ausgestatteten Drohnen zum Gegenstand haben.

Aufgrund einer nahezu selbstverständlichen Verfügbarkeit im Einzelhandel und zusehends fallender Preise für immer leistungsfähigere Geräte erfolgt ein Einsatz von Drohnen längst nicht mehr bloß in einem polizeilichen oder militärischen Verwendungszusammenhang. Neben gewerblichen Akteuren, die Drohnen für verschiedene Zwecke[12] einsetzen, sind es immer häufiger Privatpersonen, die solche Geräte im Rahmen ihrer Freizeitgestaltung nutzen, ohne sich oftmals über die rechtlichen Implikationen deren Einsatzes im Klaren zu sein.

Im Vergleich zum Einsatz stationärer Videoüberwachungsmaßnahmen kann der Einsatz von Drohnen mit einem ungleich größeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sein, da der potentiell überwachbare Bereich nur von den technischen Gegebenheiten des eingesetzten Geräts begrenzt wird. Mauern, Zäune oder sonstige Abtrennungen, die Dritten das Betreten des so geschützten Bereichs oder den Einblick in diesen gerade erschweren oder unmöglich machen sollen, stellen im Rahmen des Drohneneinsatzes kein Hindernis dar. Darüber hinaus ist es für Betroffene auch regelmäßig nicht ohne Weiteres möglich, den für den Drohneneinsatz Verantwortlichen zu erkennen.

An dieser Stelle sollen die Anforderungen an einen gesetzeskonformen Drohneneinsatz und die rechtlichen Handlungs- und Abwehrmöglichkeiten für Betroffene näher dargestellt werden.

Luftverkehrsrechtliche Regelungen

Während für Drohnen, die privat im Rahmen der Freizeitgestaltung eingesetzt werden, nach § 16 Abs. 1 Nr. 1 Luftverkehrsordnung (LuftVO) nur dann eine Aufstiegsgenehmigung von der zuständigen Landesluftfahrtbehörde einzuholen ist, wenn diese

- eine Gesamtmasse mit mehr als 5 Kilogramm aufweisen,
- mit Raketenantrieb, sofern der Treibsatz mehr als 20 Gramm beträgt, ausgestattet sind,
- mit Verbrennungsmotor in einer Entfernung von weniger als 1,5 Kilometern von Wohngebieten eingesetzt werden oder

[12] Beispielsweise ist der Einsatz von Drohnen zur Objektüberwachung, im Rahmen von bautechnischen Arbeiten, im Veranstaltungsmanagement oder in der Tourismuswerbung mittlerweile üblich. Perspektivisch sei in diesem Zusammenhang auch auf den beabsichtigten Einsatz von Drohnen zur Auslieferung von Paketen durch Online-Händler und Postdienstleister hingewiesen.

- in einer Entfernung von weniger als 1,5 Kilometern von der Begrenzung von Flugplätzen betrieben werden,

sind Drohnen in einem gewerblichen Zusammenhang als Luftfahrzeuge im Sinne des § 1 Abs. 2 Satz 3 Luftverkehrsgesetz (LuftVG) nach § 16 Abs. 1 Nr. 7 LuftVO grundsätzlich genehmigungspflichtig.

Die handelsübliche Drohne kann somit von Privatpersonen in einem freizeitlichen Rahmen ohne Beteiligung der Luftfahrtbehörde und ohne weitere Anforderungen an Eignung oder Zuverlässigkeit der Person des Nutzers eingesetzt werden.

Im Rahmen des gewerblichen Drohneneinsatzes erteilt die zuständige Luftfahrtbehörde[13], sofern kein Ausschlussgrund nach § 15a Abs. 3 Satz 1 Nr. 1 oder 2 LuftVO (der Betrieb der Drohne erfolgt außerhalb der Sichtweite des Steuerers oder die Gesamtmasse des Geräts beträgt mehr als 25 Kilogramm) gegeben ist, nach erfolgter Antragstellung des Nutzers und Feststellung der Unbedenklichkeit des Einsatzes nach § 16 Abs. 1 Nr. 7 und Abs. 4 LuftVO die Aufstiegsgenehmigung.

§ 16 Absatz 4 LuftVO

Die Erlaubnis wird erteilt, wenn die beabsichtigten Nutzungen nicht zu einer Gefahr für die Sicherheit des Luftverkehrs oder die öffentliche Sicherheit oder Ordnung führen können, ***insbesondere im Fall von Absatz 1 Nummer 7 die Vorschriften über den Datenschutz nicht verletzen.*** *[...]*

Nach § 16 Abs. 4 Satz 1 LuftVO sind mithin von der Luftfahrtbehörde vor der Erteilung der Aufstiegsgenehmigung auch ausdrücklich datenschutzrechtliche Belange zu prüfen.

Punkt 2.3 der „Gemeinsamen Grundsätze des Bundes und der Länder für die Erteilung der Erlaubnis zum Aufstieg von unbemannten Luftfahrtsystemen gemäß § 16 Abs. 1 Nummer 7 Luftverkehrs-Ordnung (LuftVO)" führt dazu aus, dass die im Rahmen der Antragsprüfung erfolgende Feststellung der Verletzung von Datenschutzvorschriften durch die beabsichtigte Nutzung immer die Erlaubnisversagung zum Ergebnis hat.

Die Konzeption des von der saarländischen Luftverkehrsbehörde genutzten Antragsformulars auf Erteilung einer allgemeinen Aufstiegserlaubnis für unbemannte Luftfahrtsysteme legt nahe, dass sich die datenschutzrechtliche Prüfung lediglich in der Selbstverpflichtung des Antragsstellers erschöpft, datenschutzrechtliche Bestimmungen nicht zu verletzen (dort Punkt 6. im Antragsformular). Inwiefern der Nutzer bei Antragstellung jedoch überhaupt die materiell- und formalrechtlichen Voraussetzungen für einen datenschutzkonformen Drohneneinsatz kennen kann, muss dahingestellt bleiben.

Bedauerlicherweise wurde von der saarländischen Luftfahrtbehörde der Vorschlag des Datenschutzzentrums zur Erstellung einer gemeinsamen

[13] Im Saarland ist die zuständige Luftfahrtbehörde beim Ministerium für Wirtschaft, Arbeit, Energie und Verkehr, Referat D/6, Franz-Josef-Röder-Straße 17, 66119 Saarbrücken angesiedelt.

Informationsbroschüre, welche den Antragstellern die Voraussetzungen und Pflichten im Zusammenhang mit einem datenschutzkonformen Drohneneinsatz erläutert, nicht aufgegriffen.

Datenschutzrechtliche Regelungen

Erfolgt der Einsatz der Drohne in einem **gewerblichen Kontext**, gelten die Regelungen des BDSG uneingeschränkt.

Maßgebliche Vorschrift für die datenschutzrechtliche Zulässigkeitsprüfung des Einsatzes einer mit Videokamera ausgestatteten Drohne, sofern nicht lediglich Einzelbildaufnahmen angefertigt werden, ist § 6b BDSG, welche die Videoüberwachung von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen regelt.

Für die Anwendbarkeit des § 6b BDSG kommt es darauf an, dass ein Personenbezug der von der Drohnenkamera erhobenen Bilddaten hergestellt werden kann. Da sich nach § 3 Abs. 1 BDSG der Personenbezug auf **persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person** erstreckt, können ggf. auch Aufnahmen von Grundstücken und Gebäuden als personenbezogene Informationen angesehen werden, soweit eine Zuordnung zu natürlichen Personen möglich ist. Bei Aufnahmen von Personen ist ein Personenbezug dann zu verneinen, wenn bei Einsatz von Kameras zwar Personen erkennbar sind, deren Identifizierung jedoch ausgeschlossen ist, da klare Zuordnungsmerkmale (Aussehen, Erscheinungsbild etc.) nicht oder nur sehr begrenzt wahrnehmbar sind.[14]

Die Anwendbarkeit von § 6b BDSG ist darüber hinaus nur dann gegeben, wenn beim Einsatz einer mit Kamera ausgerüsteten Drohne öffentlich zugängliche Bereiche wie Straßen und Gehwege (mit-)überwacht werden.

Eine Beobachtung könnte dann zulässig sein, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (§ 6b Abs. 1 Nr. 2 und 3 BDSG).

Ein Drohneneinsatz zur Wahrnehmung des Hausrechts wäre allenfalls im Zusammenhang mit Maßnahmen des Objektschutzes denkbar, jedoch endet dann die Überwachungsbefugnis grundsätzlich an der Grenze des vom Hausrecht umfassten Bereichs.

Zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke sind zwar verschiedene Einsatzszenarios vorstellbar, jedoch sind durch den Betreiber eben auch die schutzwürdigen Interessen Betroffener zu berücksichtigen.

Das Erstellen und Speichern von Bildaufnahmen stellt grundsätzlich einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar. Bei der gezielten Beobachtung einzelner Personen oder

[14] Dies kann z.B. beim Einsatz von Infrarotkameras oder Kameras, die so angebracht sind, dass aufgrund der großen Distanz zwischen Objekt und Objektiv eine Unterscheidung von einzelnen Personen ausgeschlossen ist, der Fall sein.

der Überwachung von Bereichen, die über Betroffene zusätzlich sensible Informationen preisgeben, wie beispielsweise bei der Überwachung von religiösen, gewerkschaftlichen oder medizinischen Einrichtungen, überwiegen grundsätzlich die schutzwürdigen Interessen Betroffener.

Bei einem Überflug über ein Festivalgelände oder bei der Aufnahme einer touristischen Attraktion dürfte ein Überwiegen schutzwürdiger Interessen Betroffener regelmäßig nicht der Fall sein, jedoch gilt es dann für den Drohnenbetreiber verschiedene weitere Erfordernisse zu beachten. So ist u.a. nach § 6b Abs. 2 BDSG auf den Umstand der Beobachtung und die dafür verantwortliche Stelle hinzuweisen. Dies ist beim Drohneneinsatz innerhalb eines von vorherein begrenzten Bereichs ggf. noch umsetzbar; wie dieser gesetzlichen Hinweispflicht aber bei einem Einsatz in nicht begrenzten Bereichen - beispielsweise im Rahmen der Drohnennutzung zur Paketzustellung - nachgekommen werden kann, bleibt unklar.

Da eine Überwachung, die eine Speicherung von Aufnahmen umfasst, nach der Entscheidung des Europäischen Gerichtshofs vom 11. Dezember 2014 zudem eine automatisierte Verarbeitung personenbezogener Daten darstellt,[15] ist ein Verfahrensverzeichnis nach § 4e in Verbindung mit § 4g Abs. 2 oder 2a BDSG zu erstellen und, sofern von der verantwortlichen Stelle kein Beauftragter für den Datenschutz bestellt ist, das Verfahren nach § 4d Abs. 1 BDSG der zuständigen Datenschutzaufsichtsbehörde vor Inbetriebnahme zu melden.

Erfolgt der Einsatz der Drohne dagegen in einem **privaten Kontext**, findet das BDSG nur unter bestimmten Voraussetzungen Anwendung.

§ 1 Abs. 2 Nr. 3 BDSG

Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch [...] nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für ***persönliche oder familiäre Tätigkeiten****.*

Ein Drohneneinsatz im Rahmen der Ausübung eines Hobbys oder zur Freizeitgestaltung stellt somit nach dem Willen des Gesetzgebers einen Bereich persönlicher Lebensführung dar, der außerhalb des datenschutzrechtlichen Regelungsregimes anzusiedeln ist. Jedoch ist diese Ausnahmeregelung restriktiv auszulegen.

Sobald z.B. eine Veröffentlichung von Aufzeichnungen im Internet stattfindet oder ein zielgerichteter Drohneneinsatz zur Beobachtung öffentlich zugänglicher Räume erfolgt, ist diese Privilegierung im Sinne des § 1 Abs. 2 Nr. 3 BDSG ausgeschlossen und das BDSG vollumfänglich anwendbar.

[15] Urteil des EuGH vom 11. Dezember 2014 - C-212/13 - Rdnr. 25.

Handlungs- und Abwehrmöglichkeiten Betroffener

Den mit dem Drohneneinsatz verbundenen Eingriff in das allgemeine Persönlichkeitsrecht[16] Betroffener kann neben der Anrufung der Datenschutzaufsichtsbehörde auch zivilrechtlich begegnet werden. Vorrangig dann, wenn die Verletzung des allgemeinen Persönlichkeitsrechts in einem Eindringen in geschützte Bereiche, wie beispielsweise das befriedete und blickgeschützte Grundstück, besteht oder eine zielgerichtete Beobachtung erkennbar stattfindet, ist die Geltendmachung eines Abwehranspruchs aus § 823 in Verbindung mit § 1004 Abs. 1 Bürgerliches Gesetzbuch (BGB) analog möglich. In diesem Zusammenhang kann auch das Recht am eigenen Bild, als besondere Ausprägung des allgemeinen Persönlichkeitsrechts, im Sinne des Kunsturhebergesetzes (KUG) tangiert sein (§§ 22, 23 KUG), sofern eine Verbreitung oder Veröffentlichung der Aufzeichnungen erfolgt.

Damit Betroffene überhaupt in die Lage versetzt werden, ihre Rechte wahrnehmen zu können, muss die Person des Drohnenführers ausfindig gemacht werden. Gestützt auf § 1 Abs. 3 Saarländisches Polizeigesetz kann eine zeitnahe Kontaktaufnahme mit dem örtlichen Ordnungsamt oder der örtlichen Polizeidienststelle mit dem Ziel der Identitätsfeststellung des Drohnenführers durch Mitarbeiter eben dieser Stellen zielführend sein.

Das Einschalten der Strafverfolgungsbehörden ist vor allem dann angezeigt, wenn durch den Drohneneinsatz die Verwirklichung von Straftatbeständen droht, wie beispielsweise bei der Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche (§ 201a Strafgesetzbuch (StGB)), mithin Bereiche der Intimsphäre[17], oder der Aufzeichnung von nichtöffentlich gesprochenem Wort (§ 201 StGB).

Fazit

- Private Drohnennutzer sollten Drohnen nur auf Freiflächen einsetzen und geschützte oder befriedete Bereiche der persönlichen Lebensgestaltung nicht oder allenfalls nach Rücksprache mit den potentiell Betroffenen überfliegen.

- Gewerbliche Drohnenführer treffen neben der luftverkehrsrechtlichen Pflicht zur Beantragung einer Aufstiegsgenehmigung bei der Luftfahrbehörde weitreichende formale Verpflichtungen nach dem BDSG. Eine Kontaktaufnahme mit der Datenschutzaufsichtsbehörde ist somit vor einem Drohneneinsatz ratsam.

- Wenn mit einer Drohne zielgerichtet in geschützte Bereiche eingedrungen wird oder gar die Verwirklichung eines Straftatbestandes droht, sollten Betroffene zur Identifikation des Drohnenführers die Ortspolizeibehörde oder die örtliche Polizeidienststelle einschalten.

- Erfolgt der Drohneneinsatz erkennbar in einem gewerblichen Kontext, kann, sofern dem Betroffenen die datenschutzrechtlich verantwortliche Stelle bekannt ist, die Luftverkehrsbehörde sowie die Da-

[16] Abgeleitet aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz.
[17] Siehe dazu im Einzelnen auch die Bundestagsdrucksache 15/2466, S. 5.

tenschutzaufsichtsbehörde involviert und gegenüber der verantwortlichen Stelle ein Auskunftsanspruch nach § 34 Abs. 1 BDSG geltend gemacht werden.

- Die Möglichkeit der Geltendmachung zivilrechtlicher Ansprüche bleibt Betroffenen jederzeit unbenommen.

19.5.2 Videoüberwachung durch Teilnehmer am Straßenverkehr

Im Berichtszeitraum wurde an das Datenschutzschutzzentrum bisher eine vergleichsweise überschaubare Anzahl an Anfragen und Eingaben im Zusammenhang mit dem Einsatz von Dash- und Action-Cams herangetragen. In allen Fällen wurde der datenschutzrechtlichen Bewertung der Aufsichtsbehörde Folge geleistet und es wurden die Geräte entfernt oder gar nicht erst in Betrieb genommen. Bemerkenswert dabei ist, dass zunehmend örtliche Polizeidienststellen den Einsatz von Kameras durch Verkehrsteilnehmer der Aufsichtsbehörde zur Kenntnis bringen.

Aufgrund der freien Verfügbarkeit solcher Kameras im Handel wird künftig mit einem Anstieg der Anzahl der Eingaben zu rechnen sein.

Datenschutzrechtliche Bewertung

Bereits mit Beschluss vom 26./27. Februar 2013[18] verlautbarte der Düsseldorfer Kreis die datenschutzrechtliche Unzulässigkeit des Einsatzes von Außenkameras an Taxis.

Aufgrund der gestiegenen Brisanz des Themas Videoüberwachung aus Fahrzeugen sah sich der Düsseldorfer Kreis auf Initiative seiner Ad-hoc-Arbeitsgruppe Videoüberwachung veranlasst, dazu eigens den Beschluss vom 25./26. Februar 2014 zu veröffentlichen.

Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)

Mittlerweile nimmt der Einsatz sog. Dashcams auch in Deutschland immer mehr zu, um, so die standardmäßige Begründung, im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können.

Die Aufsichtsbehörden des Bundes und der Länder für den Datenschutz im nichtöffentlichen Bereich machen darauf aufmerksam, dass der Einsatz solcher Kameras - jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt - datenschutzrechtlich unzulässig ist.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmauf-

[18] Siehe hierzu auch den 24. Tätigkeitsbericht des Unabhängigen Datenschutzzentrums Saarland, S. 100.

nahmen zur Dokumentation eines Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an den Regelungen des Bundesdatenschutzgesetzes zu messen. Gemäß § 6b Abs. 1 Nr. 3 und Abs. 3 des Bundesdatenschutzgesetzes (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.

Diese Voraussetzungen sind in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der Verkehrsteilnehmer überwiegen. Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dashcams zeichnen den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent auf, so dass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht sonstige Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlass- und schrankenlos mittels Kameras zu überwachen.

Das Fazit dieses Beschlusses, dass das schutzwürdige Interesse der übrigen Verkehrsteilnehmer überwiegt, erfuhr auch unlängst Bestätigung in der Entscheidung des Verwaltungsgerichts Ansbach vom 12. August 2014 - AN 4 K 13.01634. Der Entscheidung lag die Klage eines Rechtsanwalts, welcher eine Dashcam für Beweissicherungszwecke einsetzte, gegen einen Bescheid des bayerischen Landesamts für Datenschutzaufsicht (LDA) zugrunde. Das LDA verfügte in diesem Bescheid nach § 38 Abs. 5 BDSG gegenüber dem Rechtsanwalt die Einstellung der Videoüberwachung wegen entgegenstehender schutzwürdiger Interessen der übrigen Verkehrsteilnehmer und Passanten. Das Verwaltungsgericht gab der Klage zwar wegen eines Formfehlers statt, schloss sich jedoch in der Sache der datenschutzrechtlichen Bewertung der bayerischen Kollegen an.

Beweisverwertung von Aufnahmen in zivilgerichtlichen Verfahren

Die essentielle Frage, ob mithilfe von Dashcams gewonnene Aufnahmen in einem zivilgerichtlichen Verfahren überhaupt verwertbar sind, wurde wiederum zuerst von einem bayerischen Gericht beantwortet. Jedoch wurden vom Amtsgericht München dazu zwei gegensätzliche Ansichten vertreten.

Mit Urteil vom 6. Juni 2013 - 343 C 4445/13 - entschied das Gericht, dass die Aufnahmen in dem Verfahren verwertet werden dürfen, da die Abwägung der Interessen der beteiligten Parteien zugunsten der Partei

ausfiel, die das Video für ihre Beweiszwecke in das Verfahren einbrachte.

Dieses Urteil des Amtsgerichts München wurden durch die Entscheidung vom 13. August 2014 - 345 C 5551/14 - relativiert. Wohl in Kenntnis des oben angeführten Dashcam-Beschlusses des Düsseldorfer Kreises kam dort das Gericht zum Ergebnis, dass eine Verwertung der Aufnahmen ausgeschlossen sei, da ihre Erstellung zwangsläufig mit einem unzulässigen Eingriff in das informationelle Selbstbestimmungsrecht der übrigen Verkehrsteilnehmer verbunden ist. Das Interesse des Überwachenden im Bedarfsfall die Aufnahmen zur Beweisführung einzusetzen wiege nicht schwerer als der permanente und anlasslose Eingriff in das allgemeine Persönlichkeitsrecht der betroffenen Verkehrsteilnehmer.

Auch das Landgericht Heilbronn hat in seinem Urteil vom 17. Februar 2015 - I 3 S 19/14 - aus den gleichen Gründen eine Beweisverwertung von Dashcam-Aufnahmen ausgeschlossen.

Fazit

- Der Einsatz von Dash- und Actioncams im Rahmen der Ausübung eines Hobbys oder zur Freizeitgestaltung außerhalb des öffentlichen Verkehrsraums stößt im Hinblick auf § 1 Abs. 2 Nr. 3 BDSG regelmäßig nicht auf datenschutzrechtliche Bedenken. Sofern Dritte aufgenommen werden gilt dies jedoch nur, insoweit die Aufzeichnungen nicht im Internet oder auf sonstigem Wege veröffentlicht werden.

- Der Einsatz von Dash- und Actioncams im öffentlichen Verkehrsraum ist regelmäßig wegen überwiegender schutzwürdiger Interessen Betroffener unzulässig. Anderes gilt allenfalls dann, wenn schlüssig und objektiv nachvollziehbar dargelegt werden kann, dass der Cam-Einsatz im Rahmen einer persönlichen oder familiären Tätigkeit im Sinne des § 1 Abs. 2 Nr. 3 BDSG erfolgt.

- Die saarländische Datenschutzaufsichtsbehörde wird - dem oben genannten Beschluss der Düsseldorfer Kreise entsprechend - erforderlichenfalls die Einstellung einer unzulässigen Videoüberwachung durch Verkehrsteilnehmer mit Bescheid nach § 38 Abs. 5 BDSG anordnen und sich die Einleitung eines Bußgeldverfahrens nach § 43 Abs. 2 Nr. 1 BDSG vorbehalten.

- Für datenschutzrechtlich unzulässig erhobene Bildsequenzen scheidet eine prozessuale Beweisverwertung regelmäßig aus.

19.6 Voraussetzungen für die Herausgabe von Aufzeichnungen durch den Betreiber einer Videoüberwachungsmaßnahme

Ein Petent brachte der Aufsichtsbehörde zur Kenntnis, dass von einem Handelsunternehmen Aufzeichnungen der Videoüberwachungsanlage,

auf denen er abgebildet sei, seiner früheren Ehefrau zur Verfügung gestellt wurden. Vor dem Hintergrund eines bereits gerichtlich auf Grundlage des Gewaltschutzgesetzes (GewSchG) verfügten Annäherungsverbots habe diese den Kaufhausdetektiv um Zurverfügungstellung dieser Aufnahmen gebeten, um weitere Maßnahmen gegen ihren früheren Ehemann ergreifen zu können.

Das Handelsunternehmen bestätigte in seiner Stellungnahme die Herausgabe der Videoaufzeichnungen an die frühere Ehefrau des Petenten und führte weiter aus, dass diese Übermittlung von Aufzeichnungen durch den Kaufhausdetektiv nach § 28 Abs. 2 Nr. 2 a) Bundesdatenschutzgesetz (BDSG) zulässig sei.

§ 28 Abs. 2 BDSG

Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig

1. *unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,*
2. *soweit es erforderlich ist*
   a) *zur Wahrung berechtigter Interessen eines Dritten oder*
   b) *zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten*

und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.

Zudem habe sich der Kaufhausdetektiv bei der örtlichen Polizeidienststelle erkundigt, ob die Herausgabe der Aufnahmen erfolgen könne, was von einem Mitarbeiter der Polizei bestätigt worden sei.

Diese datenschutzrechtliche Bewertung des Sachverhalts hielt einer näheren rechtlichen Überprüfung nicht stand.

Da der Bereich des Verkaufsraums, in dem die Videoaufnahmen des Petenten erstellt worden sind, während der Öffnungszeiten des Einkaufsmarktes von Kunden jederzeit betreten werden konnte, war das Erheben und Verarbeiten von personenbezogenen Daten im Rahmen der Videoüberwachungsmaßnahme nach § 6b BDSG zu beurteilen.

§ 6b BDSG, als spezielle Norm für Videoüberwachungsmaßnahmen im öffentlich zugänglichen Raum verdrängt § 28 BDSG, so dass die Übermittlung - als Unterfall der Verarbeitung - von Aufnahmen nicht nach § 28 Abs. 2 Nr. 2 a) BDSG sondern allenfalls nach § 6b Abs. 3 Satz 2 BDSG zulässig sein könnte. Ein hilfsweiser Rückgriff auf § 28 BDSG zur Legitimation einer Übermittlung ist somit ausgeschlossen.

§ 6b Abs. 3 BDSG

Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der

Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

Durch § 6b Abs. 3 Satz 2 BDSG wird jedoch ausschließlich die Herausgabe von Videodaten an die Strafverfolgungsbehörden legitimiert; eine Übermittlung von Daten unmittelbar an Privatpersonen zur Verfolgung eigener Interessen ist davon nicht erfasst.

Die Herausgabe der Aufnahmen des Petenten an dessen frühere Ehefrau durch den Kaufhausdetektiv erfolgte somit datenschutzrechtlich unzulässig. Dem Handelsunternehmen wurde aufgegeben, Richtlinien hinsichtlich eines datenschutzkonformen Umgangs mit Videodaten zu erstellen und die Mitarbeiter dahingehend zu informieren. Ob die unzulässige Herausgabe als Ordnungswidrigkeit im Sinne des § 43 Abs. 2 Nr. 1 BDSG verfolgt wird, wird noch durch die Bußgeldstelle des Datenschutzzentrums geprüft.

§ 43 Abs. 2 Nr. 1 BDSG

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet.

Da vor dem Hintergrund des gerichtlich verfügten Annäherungsverbots das Verhalten des Petenten einen Straftatbestand nach § 4 GewSchG erfüllen könnte, hätte die frühere Ehefrau des Petenten mittelbar über die Strafverfolgungsbehörden die Herausgabe der Videodaten nach § 6b Abs. 3 Nr. 2 BDSG datenschutzrechtlich zulässig erwirken können.

Fazit

Eine unmittelbare Herausgabe von mithilfe einer Videoüberwachungsmaßnahme gewonnenen Aufzeichnungen an private Dritte (Kunden, Passanten etc.) zur Verfolgung ihnen gegenüber verübter Straftaten oder um diesen die Geltendmachung zivilrechtlicher Ansprüche zu ermöglichen, ist datenschutzrechtlich nicht zulässig und stellt als unzulässige Übermittlung an Dritte einen Bußgeldtatbestand nach § 43 Abs. 2 Nr. 1 BDSG dar.

19.7 Videoüberwachung durch den Inhaber eines Gastronomiebetriebs

Videoüberwachungsmaßnahmen in Gastronomiebetrieben sind im Prüfungsalltag der Aufsichtsbehörde ein altbekanntes Phänomen. Erfreulicherweise wird in der Mehrzahl der Fälle eine Stellungnahme der Aufsichtsbehörde zur (Un-)Zulässigkeit von Überwachungsmaßnahmen von den Betreibern angenommen und umgesetzt, ohne dass es weiterer Maßnahmen bedarf. Der Gastronom in diesem Fall zeigte sich jedoch von seiner beratungsresistenten Seite.

Die Videoüberwachung des gesamten Gehweges und Straßenzuges vor dem Gastronomiebetrieb und das Fehlen von Hinweisschildern wurden unserer Dienststelle durch einen Petenten, der sich als Passant einer ungerechtfertigten Videoüberwachung ausgesetzt sah, zur Kenntnis gebracht. Der Inhaber des Gastronomiebetriebes bestätigte die Überwachung des öffentlichen Verkehrsraums und führte in seiner Stellungnahme an, dass diese Überwachungsmaßnahme zum Schutz der Türsteher notwendig sei. Zudem würden die vor dem Gastronomiebetrieb geparkten Fahrzeuge der Gäste regelmäßig beschädigt. Des Weiteren wurde angeführt, dass Beeinträchtigungen der Fassade durch Graffiti, wie sie auch häufig in der Nachbarschaft zu finden seien, drohten. Bestätigungen über gestellte Strafanzeigen, Schadensmeldungen an Versicherungen o. ä., die ein berechtigtes Interesse für konkret festgelegte Zwecke im Sinne des § 6b Abs. 1 Nr. 3 Bundesdatenschutzgesetz (BDSG) objektiv nachvollziehbar zu Tage treten lassen, wurden vom Gastronomen nicht vorgelegt.

Dem Betriebsinhaber, der auch Eigentümer des Gebäudes ist, wurde von unserer Dienststelle mitgeteilt, dass die Überwachung des nahezu gesamten öffentlichen Verkehrsraums im Umfeld des Gastronomiebetriebs datenschutzrechtlich unzulässig ist. Auch ist der Schutz von Rechtsgütern Dritter, somit die Überwachung zum Schutz der an der Straße geparkten Kundenfahrzeuge, kein berechtigtes Interesse im Sinne des § 6b Abs. 1 Nr. 3 BDSG. Die Überwachung eines Toleranzbereichs von einem Meter ab der Hausfassade wäre jedoch als zulässig zu erachten, da Beschädigungen an der Hausfassade und das Anbringen von Graffiti im Umfeld des Betriebes regelmäßig anzutreffen sind; insoweit war eine abstrakte Gefährdungslage zu Lasten des Eigentums des Überwachenden anzuerkennen.

Der Betriebsinhaber zeigte sich mit dem datenschutzrechtlichen Votum der Aufsichtsbehörde nicht einverstanden und beharrte darauf, dass die bisher im Einsatz befindliche Videoüberwachung unabdingbar sei. Dementsprechend erhielt der Gastronom nach erfolgter Anhörung eine Anordnung auf Grundlage des § 38 Abs. 5 Satz 1 BDSG, mit welcher dem Inhaber die Beschränkung der Videoüberwachung auf einen Toleranzbereich von einem Meter ab der Gebäudefassade sowie die Anbringung von aussagekräftigen Hinweisschildern unter Androhung eines Zwangsgeldes[19] auferlegt wurde.

§ 38 Abs. 5 Satz 1 und 2 BDSG

Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach

[19] Das saarländische Verwaltungsvollstreckungsrecht räumt die Möglichkeit ein, die Zwangsgeldandrohung bereits mit dem zugrundeliegenden Bescheid zu verbinden und das Zwangsgeld aufschiebend bedingt festzusetzen (§ 20 Abs. 2 Saarländisches Verwaltungsvollstreckungsgesetz).

Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. […]

Der Gastronom legte überraschenderweise gegen den Bescheid der Aufsichtsbehörde keinen Rechtsbehelf ein, so dass dieser bestandskräftig wurde. Da laut Überprüfung der um Amtshilfe gebetenen Polizei die Videoüberwachung durch den Betriebsinhaber nach wie vor in dem unzulässigen Umfang betrieben wurde und auch keine Hinweisschilder angebracht waren, wurde das angedrohte Zwangsgeld fällig gestellt und ein Verfahren über eine Ordnungswidrigkeit auf Grundlage des § 43 Abs. 1 Nr. 11 BDSG eingeleitet.

§ 43 Abs. 1 Nr. 11 BDSG

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig […] einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

Da nach dem Ergebnis einer weiteren Überprüfung durch den Betreiber immer noch keine datenschutzkonformen Zustände hergestellt wurden, wurde erneut ein Zwangsgeld fällig gestellt und von der in § 38 Abs. 1 Satz 6 BDSG normierten Möglichkeit der Unterrichtung der Gewerbeaufsicht Gebrauch gemacht werden.

§ 38 Abs. 1 Satz 6 BDSG

Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie befugt, die Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten.

Erst nachdem Vollstreckungsbeamte des zuständigen Finanzamts dem Gastronomen die Beitreibung der Zwangsgeldforderungen ankündigten, teilte dieser mit, dass die Videoüberwachungsmaßnahme nunmehr entsprechend den Vorgaben des Bescheids der Aufsichtsbehörde ausgestaltet sei. Mitarbeiter des Datenschutzzentrums konnten sich im Rahmen eines Vorortttermins davon überzeugen. Bei diesem Vorortttermin kam auch zu Tage, dass seitens der Gewerbeaufsichtsbehörde ein Gewerbeuntersagungsverfahren eingeleitet wurde.

19.8 Datenschutzrechtliche Bewertung von Kameras in einer Apotheke

Mit einem übermäßigen Einsatz von Kameras in einer in räumlicher Hinsicht vergleichsweise überschaubaren Apotheke und einem in besonderem Maße um das „Wohl" seiner Mitarbeiter besorgten Apotheker, hatte sich das Datenschutzzentrum im Berichtszeitraum auseinanderzusetzen.

Ein Petent, der ausdrücklich darum bat, im Verwaltungsverfahren nicht namentlich in Erscheinung zu treten, machte unsere Dienststelle auf die

Videoüberwachung in einer Apotheke aufmerksam. Der Aufforderung des Datenschutzzentrums zur schriftlichen Stellungnahme entsprechend teilte der Bevollmächtigte des Apothekers mit, dass eine permanente Videoüberwachung im Verkaufsraum und des Betäubungsmittelschrankes im nicht öffentlich zugänglichen Vorratsraum erforderlich sei, da in den vergangenen Jahren erhebliche Inventurdifferenzen zu Tage getreten seien. Ein vor allem drogenabhängiger Personenkreis habe nach Ansicht des Apothekers verschreibungspflichtige Medikamente entwendet. Da somit ein in besonderem Maße „kriminalitätsgefährdeter Personenkreis" für das Abhandenkommen von Medikamenten verantwortlich sei, sei die Videoüberwachung somit nicht zuletzt zum Schutz der Mitarbeiter notwendig. Seit deren Anbringung sei keine nennenswerte Inventurdifferenz mehr aufgetreten. Der Apothekenleiter ließ durch seinen Bevollmächtigten noch ergänzend eine von allen Mitarbeitern unterzeichnete Erklärung übersenden, wonach alle Apothekenbeschäftigten sich mit der Videoüberwachungsmaßnahme einverstanden zeigten.

In Anbetracht dieser Schilderung war es für die Mitarbeiter des Datenschutzzentrums umso erstaunlicher, dass vor dem geschilderten Hintergrund die Strafverfolgungsbehörden nicht eingeschaltet wurden oder konkret belegt werden konnte, welche Arten von Medikamente im Einzelnen, wie z.B. Betäubungsmittel, zu welchem Zeitpunkt abhandengekommen sind. Im Rahmen eines Vorortttermins wurde von dem Apotheker entgegen seinem früheren Vorbringen nunmehr klargestellt, dass er seine Mitarbeiter für den Medikamentenschwund verantwortlich mache und diese mit der Videoüberwachung abschrecken und kontrollieren möchte. Konkrete Anhaltspunkte für ein Fehlverhalten einzelner Mitarbeiter seien jedoch nicht gegeben.

Da die angeführten Inventurdifferenzen zu einem Zeitraum festgestellt wurden, zu dem die Videoüberwachungsmaßnahme bereits im Einsatz war, ohne dass mit ihrer Hilfe die Umstände des Medikamentenschwunds geklärt, geschweige denn eine Täteridentifikation erfolgen konnte, war festzustellen, dass offensichtlich keine Abschreckungswirkung von den Kameras ausging und diese Überwachung mithin nicht geeignet war, die mit ihr verfolgten Zwecke zu erreichen.

Das Tatbestandsmerkmal der Erforderlichkeit im Sinne des § 6b Abs. 1 BDSG ist nur dann zu bejahen, wenn das festgelegte Ziel mit der Überwachung tatsächlich erreicht werden kann (Geeignetheit) und es dafür kein anderes, gleich wirksames aber mit Blick auf die informationelle Selbstbestimmung des betroffenen Personenkreises weniger einschneidende Mittel gibt (Verhältnismäßigkeit).

In Anbetracht der Inventurdifferenzen wäre insoweit eine Verkürzung der Inventurzyklen in Verbindung mit der Einführung eines elektronischen Warenwirtschaftssystem zielführender und vor allem weniger eingriffsintensiv. Bei der Bewertung der Geeignetheit der Überwachungsmaßnahme war auch der Hinweis des Apothekers von Belang, dass ihm die Zeit fehle, die Aufzeichnungen regelmäßig auszuwerten. Insoweit war fraglich, inwiefern das Abhandenkommen von Medikamenten mithilfe der Überwachungsmaßnahme überhaupt festgestellt werden kann.

Auch für die Videoüberwachung des Betäubungsmittelschranks im nicht öffentlich zugänglichen Vorratsraum, von welcher nur Beschäftigte

betroffen waren und die somit nach § 32 Abs. 1 BDSG zu beurteilen war, war das Tatbestandsmerkmal der Erforderlichkeit nicht gegeben.

§ 32 Abs. 1 BDSG

Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung ***erforderlich*** *ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.*

Das Verschließen des offenstehenden Schranks sowie die Verwahrung des Schlüssels und die Herausgabe von Betäubungsmitteln durch einen einzigen Mitarbeiter stellt eine geeignetere und im Hinblick auf die geltenden betäubungsmittelrechtlichen Aufbewahrungs- und Dokumentationsvorschriften[20] notwendige Maßnahme dar, um den Betäubungsmittelbestand vor unbefugtem Zugriff zu schützen. Begründete Verdachtsmomente gegen Beschäftigte, die eine Videoüberwachung nach § 32 Abs. 1 Satz 2 BDSG legitimiert hätten, konnten von dem Apotheker nicht dargelegt werden.

Darüber hinaus waren nach der datenschutzrechtlichen Bewertung schutzwürdige Interessen der betroffenen Kunden und Mitarbeiter schwerwiegender als das Interesse des Überwachenden an dem weiteren Betrieb der Kameras.

Im Verkaufsraum wurden im Rahmen der Videoüberwachung auch besondere personenbezogene Daten im Sinne des § 3 Abs. 9 BDSG dahingehend erhoben und verarbeitet, als aufgrund der Ausrichtung der Kameras die Übergabe der Medikamente an den Apothekenkunden aufgezeichnet wurde.

§ 3 Abs. 9 BDSG

Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

[20] § 1 Abs. 3 und §§ 13 ff Betäubungsmittel-Verschreibungsverordnung (BtMVV) sowie § 15 Betäubungsmittelgesetz (BtMG) und die dazu ergangenen Richtlinien des Bundesinstituts für Arzneimittel und Medizinprodukte über Maßnahmen zur Sicherung von Betäubungsmittelvorräten im Krankenhausbereich, in öffentlichen Apotheken, Arztpraxen sowie Alten- und Pflegeheimen.

Mittels der klar erkennbaren Umverpackungen der Arzneien konnte regelmäßig auf gesundheitliche Beeinträchtigungen von Betroffenen geschlossen werden. Zwar wird im Rahmen des Betriebs einer Apotheke zwangsläufig mit besonderen personenbezogenen Daten von Kunden, mithin Daten über deren Gesundheit, umgegangen; ein Erheben und Speichern dieser Daten mithilfe von Videokameras stellt jedoch eine neben der eigentlichen Apothekertätigkeit erfolgende automatisierte Verarbeitung von sensiblen Daten dar. Schutzwürdige Interessen der betroffenen Kunden überwogen grundsätzlich das Interesse des Apothekers an der Überwachung.

Auch standen schutzwürdige Interessen der betroffenen Mitarbeiter der Überwachung entgegen, soweit deren Arbeitsplätze permanent im Aufnahmebereich der Videokameras gelegen sind. Aufgrund der nahezu lückenlosen Überwachung des vergleichsweise überschaubaren Verkaufsraums konnten sich die Beschäftigten der Überwachung durch ihren Arbeitgeber nicht ohne Weiteres entziehen.

Die nachgereichte und von allen Mitarbeitern unterzeichnete Einwilligungserklärung stellte ebenfalls keine Legitimationsgrundlage für die Überwachung der Mitarbeiter dar. Voraussetzung für eine wirksame Einwilligung im Sinne des § 4a Abs. 1 BDSG ist u.a., dass diese auf der freien Entscheidung des Betroffenen beruht.

§ 4a Abs. 1 BDSG

Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

Da das Merkmal Freiwilligkeit nur dann zu bejahen ist, wenn die Einwilligung nicht in einer Zwangslage oder unter Druck erteilt wurde, ist bei Einwilligungserklärungen im Verhältnis zwischen Arbeitgeber und Arbeitnehmer kritisch zu hinterfragen, inwiefern der Betroffene die Verarbeitung seiner Daten sanktionslos verweigern oder ein einmal erteiltes Einverständnis folgenlos widerrufen kann. Gerade vor dem Hintergrund der im Rahmen des Verfahrens vom Apotheker angeführten Zwecke der Videoüberwachungsmaßnahme und des anscheinend belasteten Verhältnisses zwischen den Arbeitsvertragsparteien, konnte hier mithin nicht davon ausgegangen werden, dass die Arbeitnehmer vollkommen frei in ihrer Entscheidung waren.

Insgesamt war somit von einer datenschutzrechtlichen Unzulässigkeit der im Einsatz befindlichen Videoüberwachungsmaßnahme auszugehen. Der Apotheker wollte sich der Bewertung des Datenschutzzentrums jedoch nicht anschließen. Nach erfolgter Anhörung wurde die Einstellung der Videoüberwachung während der Öffnungszeiten der Apotheke auf Grundlage des § 38 Abs. 5 BDSG verfügt. Gegen den Bescheid wurde Klage eingelegt; das Klageverfahren ist bis dato nicht abgeschlossen.

19.9 Prüfungsaktion: Videoüberwachung in Clubs und Diskotheken

Das Datenschutzzentrum hat im Berichtszeitraum anlasslos eine Anzahl von Clubs und Diskotheken hinsichtlich dort eingesetzter Videoüberwachungsmaßnahmen geprüft.

Zur Vorbereitung der Prüfungen wurden die ausgewählten Stellen mithilfe eines Fragenkatalogs um Auskunft hinsichtlich der Zwecke und Ausgestaltung der Videoüberwachungsmaßnahme gebeten. Einige der angeschriebenen Betreiber waren sich nicht über das Vorhandensein einer saarländischen Datenschutzaufsichtsbehörde bewusst, denn teilweise wurden die erforderlichen Auskünfte erst nach mehrfacher Erinnerung und entsprechender Androhung, dass ein Bußgeldverfahren wegen nicht erteilter Auskunft eingeleitet wird, gegeben.

Überraschend war, dass nahezu alle angeschriebenen Stellen eine Vielzahl von Videokameras einsetzten. Von den Betreibern wurden verschiedenste Zwecksetzungen für die Überwachung der öffentlich zugänglichen Räume im Sinne des § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG) kommuniziert, wie beispielsweise der Schutz der Mitarbeiter des Sicherheitsdienstes, die Beweissicherung im Schadensfall oder bei Straftaten zu Lasten des Betreibers, als Abschreckung zur Vermeidung von Straftaten, die Wahrnehmung von Verkehrssicherungspflichten oder der Schutz der Gäste im Fall von Straftaten. Mitunter wurde von manchen Clubbetreibern angeführt, dass sie sich als verlängerten Arm der Strafverfolgungsbehörden wähnten und befürchteten, dass ein Weniger an Videoüberwachung sich sogar nachteilig auf das Verhältnis zu Polizei und Staatsanwaltschaft auswirken könnte.

Teilweise wurde zudem versucht, die Videoüberwachung rechtlich über die Allgemeinen Geschäftsbedingungen (AGB) zu legitimieren. Durch das Betreten des Clubs oder der Diskothek und der Zahlung des Eintrittsgeldes würde der Besucher die AGBs und somit die dort geregelte Videoüberwachung akzeptieren. Unabhängig davon, dass derartige Klauseln der Geschäftsbedingungen eine unangemessene Benachteiligung gemäß § 307 Abs. 1 Satz 2 Bürgerliches Gesetzbuch (BGB) darstellen können,[21] stellen diese zudem keinesfalls eine datenschutzrechtliche Legitimationsgrundlage dar.

Nach § 4 Abs. 1 BDSG kann die Videoüberwachung nur mit Einwilligung des Betroffenen oder auf gesetzlicher Grundlage erfolgen. Da das Einholen einer informierten Einwilligung im Sinne des § 4a Abs. 1 BDSG in diesem Zusammenhang ausscheidet, kann somit die Videoüberwachung öffentlich zugänglicher Bereiche nur auf § 6b BDSG gestützt werden.

In der Mehrzahl der Fälle erfolgte eine Inaugenscheinnahme der eingesetzten Videoüberwachung vor Ort. Dabei wurde von den Mitarbeitern der Aufsichtsbehörde festgestellt, dass neben Eingangs-, Kassen- und sonstigen Durchgangsbereichen teilweise auch Garderoben, Tanzflächen, Theken sowie Ruhebereiche und Lounges im Fokus der Kameras standen. Teilweise wurden zudem Parkplätze und ganze Straßenzüge überwacht.

[21] LG Koblenz, Urteil vom 19.12.2013, 3 O 205/13.

Keine einzige der festgestellten Überwachungsmaßnahmen war datenschutzrechtlich ohne Beanstandung. In keinem einzigen Fall war ein Verfahrensverzeichnis erstellt worden oder lagen sonstige schriftliche Festlegungen vor.

Hinweisschilder waren zwar zumeist angebracht, erfüllten aber nicht die Vorgaben des § 6b Abs. 2 BDSG. Die Schilder waren entweder kaum erkennbar, ließen nicht auf die für die Überwachung verantwortliche Stelle schließen oder waren so angebracht, dass der Betroffene bei Kenntnisnahme des Schildes längst den überwachten Bereich betreten hatte.

In einigen Fällen wurden von den Betreibern technische Dienstleister beauftragt, um Aufzeichnungen im Bedarfsfall auswerten zu lassen, ohne dass mit diesen ein Vertrag über eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG geschlossen wurde.

Technische und organisatorische Maßnahmen im Sinne des § 9 BDSG und der dazugehörigen Anlage waren allenfalls kursorisch und nicht revisionssicher ergriffen worden.

Hinsichtlich der im Einzelnen überwachten Bereiche ist festzuhalten, dass eine Überwachung von Parkplätzen und öffentlichem Verkehrsraum durch Club- und Diskothekenbetreiber regelmäßig datenschutzrechtlich nicht zulässig ist.

Der Einsatz von Kameras in Eingangs-, Kassen- und Durchgangsbereichen sowie im Umfeld von Garderoben kann gerade bei großen oder stark frequentierten Diskotheken und Clubs als datenschutzrechtlich zulässig erachtet werden, sofern sichergestellt ist, dass keine Mitarbeiter oder Sicherheitskräfte permanent von der Videoüberwachung betroffen sind. Gäste durchqueren diese Bereiche in aller Regel ohne längere Verweildauer, so dass schutzwürdige Interessen Betroffener der Videoüberwachung regelmäßig nicht entgegenstehen.

Anders verhält es sich mit der Überwachung von Tanzflächen, Theken sowie Ruhebereichen und Lounges. Hier überwiegt das schutzwürdige Interesse der Betroffenen, sich frei und unbeobachtet in ihrer Persönlichkeit entfalten zu können. Von den Betreibern, welche diese Bereiche überwachen, konnte auch nicht dargelegt werden, aus welchem Grund die Überwachung gerade dieser Bereiche unabdingbar sein soll. Oftmals wurde in diesem Zusammenhang angeführt, dass es in diesen Bereichen zu Tätlichkeiten oder zu Diebstahlsdelikten zu Lasten der Kunden käme. Auf Nachfrage wie häufig Fälle von Tätlichkeiten bzw. Körperverletzungen mithilfe der Kameras dokumentiert werden konnten, wurde von allen Betreibern eingestanden, dass dies bisher noch nicht eingetreten ist. Da die Ausrichtung der Videokameras zudem wegen der Nutzung von Dome-Kameras für die Betroffenen nicht erkennbar war, kann dieser Effekt auch nicht auf eine besondere Abschreckungswirkung der Kameras zurückgeführt werden.

Der Schutz von Rechtsgütern Dritter, mithin der häufig als Zweck angeführte Schutz des Eigentums der Gäste, stellt im Übrigen kein berechtigtes Interesse im Sinne des § 6b Abs. 1 Nr. 3 BDSG dar, das eine Videoüberwachung legitimieren könnte.

Oftmals war auch das Tatbestandsmerkmal der Erforderlichkeit der Überwachungsmaßnahme im Sinne des § 6b Abs. 1 BDSG zu verneinen.

Wenn aufgrund des Einsatzes von Lichteffekten (Blitzlicht-Stroboskop, Lasershows etc.) und Nebelmaschinen die Aufzeichnungen gar nicht dazu geeignet sind, überhaupt einzelne Personen erkennen zu können oder durch einfachste bauliche Maßnahmen Diebstahldelikte zu Lasten des Betreibers künftig vermieden werden können, wird die Videoüberwachung in diesen Bereichen obsolet.

Einige der Diskothekenbetreiber deaktivierten die Videoüberwachung, nachdem ihnen durch das Datenschutzzentrum im Nachgang zur Prüfung die erforderlichen Maßnahmen mitgeteilt worden sind, die im Zusammenhang mit einem datenschutzkonformen Betrieb einer Videoüberwachungsmaßnahme zu ergreifen sind. So waren von einigen Diskotheken aufgrund des großflächigen Einsatzes zahlreicher Kameras nach § 4d Abs. 5 Satz 2 Nr. 2 in Verbindung mit § 4f Abs. 1 Satz 6 BDSG betriebliche Beauftragte für den Datenschutz zu bestellen gewesen, da vor der Etablierung einer Videoüberwachungsmaßnahme eine Vorabkontrolle notwendigerweise durchzuführen war.

§ 4d Abs. 5 BDSG

Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. *besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder*

2. *die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,*

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

In einigen Fällen war es ausreichend, dass die Ausrichtung einzelner Kameras geändert und die vom BDSG vorgegebenen formalen sowie technischen und organisatorischen Maßnahmen umgesetzt wurden.

19.10 Kameraeinsatz bei der Bewirtschaftung von Parkflächen

Aufgrund eines fehlenden Hinweisschilds wurde die Aufsichtsbehörde auf die Videoüberwachungsmaßnahme an einer Schrankenanlage aufmerksam gemacht.

Die verantwortliche Stelle teilte in ihrer Stellungnahme zu dem Sachverhalt mit, dass die Überwachung der Schrankenanlage notwendig sei, um eine reibungslose Abfertigung der zufahrtsberechtigten Personen zu gewährleisten. Mit der Schranke werde der Zugang zu einem aufgrund der innenstädtischen Lage stark frequentierten Bereich kontrolliert, der sowohl der Anlieferung von Gütern für Einzelhändler diene als

auch Zufahrtsstraße für Anwohner sei. Zudem sei die Schrankenanlage häufiges Ziel teils mutwilliger Beschädigungen, welche von dem Unternehmen durch Vorlage von Videosequenzen und Bilddokumentationen umfangreich belegt werden konnte.

Die Zufahrtskontrolle betraf lediglich Kraftfahrzeuge; der überwachte Bereich war ansonsten jederzeit für Fußgänger und Radfahrer frei betret- bzw. befahrbar, so dass ein öffentlich zugänglicher Raum im Sinne des § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG) gegeben war.

Aufgrund der dokumentierten Schadensereignisse und einer hinreichenden Wahrscheinlichkeit, dass zukünftig Beschädigungen der Schrankenanlage drohen, war eine konkrete Gefährdungslage zu bejahen. Schutzwürdige Interessen Betroffener standen der Videoüberwachung auch nicht entgegen, da es sich bei dem überwachten Bereich um einen stark frequentierten Durchgangsbereich handelte, in welchem sich Betroffene allenfalls für einen kurzen Zeitraum aufhalten.

Der verantwortlichen Stelle wurde die Anbringung von Schildern aufgegeben, die sowohl auf den Umstand der Videoüberwachung als auch auf die dafür verantwortliche Stelle hinweisen. Im Hinblick auf das Datensparsamkeitsgebot wurde zudem die Neuausrichtung der Kameras veranlasst, so dass der von den Kameras erfasste Bereich nunmehr auf das notwendige Minimum beschränkt ist.

Im weiteren Verfahren bat das Unternehmen die Aufsichtsbehörde um Mitteilung, unter welchen Voraussetzungen die Videoüberwachung von Parkflächen zulässig ist.

Eine Videoüberwachung von Zufahrtsschranken und Kassenautomaten kann, sofern eine Gefährdungslage durch Nachweis bereits eingetretener Schadensereignisse belegt oder das Drohen einer solchen objektiv nachvollziehbar begründet werden kann, datenschutzrechtlich zulässig sein. Eine anlasslose und permanente Überwachung der Parkflächen ist dahingegen regelmäßig als datenschutzrechtlich unzulässig zu bewerten. Laut den Ausführungen des Betreibers solle die Überwachung vorrangig dem Schutz der Fahrzeuge der Kunden vor Beeinträchtigungen dienen. Jedoch ist der Schutz von Rechtsgütern Dritter regelmäßig kein berechtigtes Interesse im Sinne des § 6b Abs. 1 Nr. 3 BDSG.

Allenfalls denkbar wäre beispielsweise die Einrichtung bestimmter videoüberwachter Bereiche für Dauerparker, unter der Voraussetzung, dass diese ihr Einverständnis in die Überwachung der Stellplätze erklären.

Nach bisherigem Kenntnisstand verfolgte das Unternehmen die projektierte Videoüberwachung der Stellflächen nicht weiter.

Automatisierte Kennzeichenerfassung

Ende Oktober 2014 wurde das Thema automatisierte Kennzeichenerfassung durch Parkhaus- und Campingplatzbetreiber von den Medien aufgegriffen.

Unter automatisierter Kennzeichenerfassung sind Systeme der kameragestützten Erfassung von Kfz-Kennzeichen zu verstehen. Dabei wird das erfasste Kfz-Kennzeichen mit Datum und Uhrzeit der Ein- und Ausfahrt

verknüpft, um für die Dauer des Parkvorgangs gespeichert zu werden. Ziel ist es, eine sekundengenaue Abrechnung der Park- oder Aufenthaltsdauer zu ermöglichen und Betrugsversuche zu Lasten des Betreibers zu vermeiden oder Betrugsfällen beweissicher begegnen zu können. Fahrzeuginsassen oder sonstige Personen werden dabei regelmäßig nicht erfasst.

Im Nachgang zu den Presseveröffentlichungen wurden Parkhaus- und Campingplatzbetreiber im Saarland um Auskunft gebeten, ob Verfahren der automatisierten Kennzeichenerfassung eingesetzt werden. Bis dato ist noch kein solches Unternehmen in Erscheinung getreten, welches ein derartiges Verfahren im Saarland betreibt. Im Rahmen dieser Überprüfung wurden auch Unternehmen befragt, die Parkraum im Saarland bewirtschaften ohne ihren Sitz im Saarland zu haben.

Eine einzelfallbezogene datenschutzrechtliche Bewertung dieses Sachverhalts ist durch das Datenschutzzentrum bisher nicht erfolgt. Abhängig von der Ausgestaltung des Verfahrens - Aufzeichnen einer Videosequenz oder einer Einzelbildaufnahme - kann rechtliche Grundlage für den Umgang mit Kundendaten von Kurzzeitparkenden § 6b BDSG oder § 28 BDSG sein. Für Dauerparkendende wiederum ist als Legitimationsgrundlage allenfalls eine informierte Einwilligung des betroffenen Fahrzeughalters im Sinne des § 4 Abs. 1 in Verbindung mit § 4a BDSG heranzuziehen.

Fazit

- Eine Videoüberwachung von Parkflächen ist ohne Einwilligung der Betroffenen regelmäßig datenschutzrechtlich unzulässig. Die Videoüberwachung von Schrankenanlagen und Kassenautomaten kann beim Vorliegen einer Gefährdungslage datenschutzrechtlich zulässig erfolgen. Jedoch sind dabei durch die überwachende Stelle alle im Zusammenhang mit der Videoüberwachung notwendigen Maßnahmen und rechtlichen Erfordernisse - wie beispielsweise die Anbringung eines Hinweisschilds im Sinne des § 6b Abs. 2 BDSG – umzusetzen.

- Eine automatisierte Kennzeichenerfassung kann unter Berücksichtigung der spezifischen Gegebenheiten des Einzelfalls als datenschutzrechtlich zulässig erachtet werden.

19.11 Wildkameras

Der Wald ist ein Bereich, welcher der Erholung der Menschen dient und einen unersetzbaren Lebensraum für Pflanzen und Tiere bietet. Diesen gilt es, von äußeren Einflüssen möglichst frei zu halten. Die moderne Überwachungstechnik hat nunmehr auch Einzug in diesen Bereich gehalten. Jäger setzen – gerade auch im Bereich von Kirrungen - vermehrt auf den Einsatz von Tierbeobachtungskameras, was einerseits auf den eklatanten Preisverfall entsprechender Geräte zurückzuführen ist, andererseits im Gegensatz zur Beobachtung vor Ort eine enorme Zeitersparnis mit sich bringt.

Grundsätzlich geregelt ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) und die Verarbeitung und Nutzung der durch eine solche Videoüberwachung erhobenen Daten in § 6b Bundesdatenschutzgesetz (BDSG).

Bei Waldgebieten handelt es sich um einen öffentlich zugänglichen Raum i. S. d. Bundesdatenschutzgesetzes (BDSG), da gemäß § 25 des Waldgesetzes für das Saarland (LWaldG) das Betreten des Waldes zum Zweck der naturverträglichen Erholung jedermann gestattet ist.

Von Seiten der Jägerschaft wird in Bezug auf Kirrungen unter Verweis auf das Saarländische Jagdgesetz (SJG)[22] hingegen die Ansicht vertreten, dass diese keine öffentlich zugänglichen Bereiche im Sinne des BDSG seien, da es sich hierbei um mit einem Betretungsverbot behaftete besondere jagdliche Einrichtungen handele. Kirrungen als nicht öffentlich zugängliche Bereiche zu qualifizieren, vermag indes nicht zu überzeugen, da es regelmäßig an der Erkennbarkeit des Betretungsverbotes für den Waldbesucher fehlt. Sollen Teile des öffentlich zugänglichen Waldgebietes nicht öffentlich zugänglich sein, so ist erforderlich, dass die Ausdehnung dieses Bereichs in Breite, Länge und Höhe für den Waldbesucher erkennbar wird. Nicht die Kontrollbefugnis des Berechtigten ist maßgeblich, sondern vielmehr dessen nach außen sichtbar gemachter Wille, den Zutritt zu beschränken und diesen Bereich klar als nicht öffentlich zugänglich zu kennzeichnen, etwa durch bauliche Abgrenzungen oder durch Beschilderungen; hieran fehlt es bei Kirrungen regelmäßig.

Eine Videoüberwachung nach § 6b Absatz 1 BDSG kann zulässig sein zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke. Der Zweck der Videoüberwachung muss vor Inbetriebnahme bei der verantwortlichen Stelle dokumentiert werden und diese Dokumentation der Aufsichtsbehörde nachgewiesen werden können. Voraussetzung hierbei ist, dass die Videoüberwachung erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Dem Persönlichkeitsrecht des Betroffenen, z. B. eines Spaziergängers oder Wanderers, der von der Kamera erfasst wird, ist in diesem Zusammenhang ein hoher Stellenwert einzuräumen. Da der Wald ein Bereich ist, der der Erholung des Menschen dient und in dem man sich unbeobachtet bewegen können sollte, sind Wildkameras daher in der Regel unzulässig.

Der Einsatz einer Wildkamera kann lediglich dann erforderlich sein, wenn es, um das berechtigte Interesse verfolgen zu können, keine objektiv zumutbare Alternative gibt. Da dieses Erforderlichkeitsgebot sowohl in räumlicher als auch in zeitlicher Hinsicht gilt, ist die Überwachung auf einen für den Beobachtungszusammenhang erforderlichen Zeitraum zu beschränken.

Im Rahmen der Interessenabwägung ist zu berücksichtigen, dass die Intensität des Eingriffs in das informationelle Selbstbestimmungsrecht der Betroffenen auch davon abhängt, wie wahrscheinlich es ist, dass diese überhaupt zum Objekt der Überwachung werden. In diesem Zusammenhang spielt u. a. eine entscheidende Rolle, in welcher Entfernung eine Kamera zu einem Waldweg angebracht ist und ob die Kame-

[22] Insbesondere § 23 Abs. 3 SJG, wonach das Betreten besonderer jagdlicher Einrichtungen nur mit Erlaubnis des Grundeigentümers oder des Jagdausübungsberechtigten zulässig ist.

ra beispielsweise durch eine schräge Anbringung nur den Nahbereich erfasst.

Auch ist auf den Umstand der Videoüberwachung im Sinne des § 6b Abs. 2 BDSG durch geeignete Maßnahmen hinzuweisen. Dazu gehört, dass Anlagenbetreiber unter Angabe von Namen und Anschrift darüber informieren müssen, durch wen und in welchen Waldstücken (z.B. Reviernummer und –bezeichnung) Tierbeobachtungskameras eingesetzt werden. Dies ist zweimal jährlich ortsüblich (Amts- oder Gemeindeblatt) bekanntzugeben und zusätzlich durch entsprechende Piktogramme an den Wanderkarten in den betroffenen Waldarealen kenntlich zu machen. Alternativ besteht die Möglichkeit, durch gut sichtbare Hinweisschilder in der unmittelbaren Umgebung von Tierbeobachtungskameras auf diese hinzuweisen.

Da Videoüberwachungen mittels Digitaltechnik gemäß § 4d BDSG der Meldepflicht unterliegen, hat das Unabhängige Datenschutzzentrum ein Formular für die Meldung von Tierbeobachtungskameras erstellt, das auf der Internetseite der Aufsichtsbehörde zum Abruf bereit steht.

Im Berichtszeitraum sind der Aufsichtsbehörde in etwa 50 Wildkameras gemeldet worden. Es ist anzunehmen, dass die Anzahl der tatsächlich sich im Einsatz befindlichen Anlagen jedoch um ein Vielfaches höher ist.

Das Unabhängige Datenschutzzentrum behält sich vor, bei Zuwiderhandlungen aufsichtsbehördliche Maßnahmen einzuleiten.

20 Handel und Gewerbe

20.1 Aufsichtsbehördliche Anordnung der Bestellung eines Beauftragten für den Datenschutz

Durch mehrere Eingaben im Berichtszeitraum wurde das Datenschutzzentrum auf den Betreiber eines webbasierten Firmenverzeichnisses aufmerksam.

Tenor der Eingaben war, dass der Betreiber auf Löschungs- oder Änderungsersuchen der Petenten nicht reagierte. So begehrten Petenten die Löschung von veralteten Verzeichniseinträgen, da die dort aufgeführten Unternehmen nicht mehr existierten und die angegebenen Telefonnummern zwischenzeitlich an Privatpersonen vergeben waren. Diese erhielten dann an das frühere Unternehmen gerichtete telefonische Anfragen. Auch waren einige Gewerbetreibende, deren private und geschäftliche Adressen und Kontaktdaten übereinstimmten, mit der Veröffentlichung ihrer Kontaktdaten im Internet nicht einverstanden.

In seiner Stellungnahme teilte der Betreiber der Webseite mit, dass sich eine zeitnahe Reaktion auf die große Anzahl an Auskunftsersuchen sowie Änderungs- und Löschungsbegehren, die er tagtäglich erhalte, aufgrund der wenigen Mitarbeiter seines Unternehmens schwierig gestalte, aber eine dahingehende Optimierung der Geschäftsprozesse erfolgen werde.

Weiterhin teilte der Betreiber mit, dass er seiner Ansicht nach keine personenbezogenen Daten erhebe oder verarbeite, da über die Webseite ausschließlich Adressen und Kontaktdaten von Unternehmen recherchiert werden können. Im Übrigen sei ein Beauftragter für den Datenschutz im Sinne des § 4f Bundesdatenschutzgesetz (BDSG) für das Unternehmen nicht bestellt worden.

Entgegen dessen Auffassung wurden durch den Betreiber im Rahmen des Betriebs der Webseite personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG erhoben und verarbeitet.

§ 3 Abs. 1 BDSG

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Zielsetzung des BDSG ist zwar ausdrücklich der Schutz des informationellen Selbstbestimmungsrechts natürlicher Personen, jedoch können bei einer Einzelfirma oder bei einem Einzelkaufmann gewerbliche Informationen und personenbezogene Daten des Inhabers deckungsgleich sein. Darüber hinaus können beispielsweise auch von dem Na-

men einer „Ein-Mann-GmbH“ Rückschlüsse auf den dahinter stehenden Gesellschafter gezogen werden.[23]

Somit war davon auszugehen, dass eine unbestimmte Anzahl der insgesamt im Rahmen des Betriebs der Webseite erhobenen und verarbeiteten Daten zwangsläufig als personenbezogene Daten anzusehen waren. Für die Fragestellung, ob das BDSG in diesem Zusammenhang Anwendung findet, ist mithin nicht entscheidend wie groß der Anteil personenbezogener Daten an der Gesamtmenge der Firmendaten ist; ausschlaggebend für die Bewertung ist allein, dass überhaupt personenbezogene Daten erhoben und verarbeitet werden.

Die im Rahmen des Betriebs der Webseite erfolgende geschäftsmäßige Erhebung und Speicherung von Daten zum Zweck der Übermittlung war nach § 29 Abs. 1 BDSG grundsätzlich datenschutzrechtlich nicht zu beanstanden, jedoch ergibt sich aus dem geschäftsmäßigen Umgang mit personenbezogenen Daten nach § 29 BDSG auch die Verpflichtung, das Verfahren der automatisierten Verarbeitung personenbezogener Daten nach § 4d Abs. 1 in Verbindung mit Abs. 4 Nr. 1 BDSG der Aufsichtsbehörde zu melden und für das Unternehmen nach § 4f Abs. 1 Satz 6 BDSG einen Beauftragten für den Datenschutz zu bestellen.

§ 4d Abs. 1 bis 4 BDSG

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

*1. **zum Zweck der Übermittlung**,*

2. zum Zweck der anonymisierten Übermittlung oder

3. für Zwecke der Markt- oder Meinungsforschung

[23] Beschluss des OVG Lüneburg vom 15.05.2009, 10 ME 385/08, Rdnr. 20 und Urteil des EuGH vom 9.11.2010, C-92/09- und C-93/09-.

gespeichert werden.

§ 4f Abs. 1 Satz 6 BDSG

Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder ***personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung,*** *der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.*

Trotz entsprechender Aufforderung wurde von der verantwortlichen Stelle weder das Verfahren im Sinne der Vorschrift gemeldet noch die Bestellung eines Beauftragten für den Datenschutz nachgewiesen, so dass schließlich gegenüber dem Betreiber der Webseite eine Anordnung auf Grundlage des § 38 Abs. 5 Satz 1 BDSG erlassen wurde.

§ 38 Abs. 5 Satz 1 BDSG

Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder ***technischer oder organisatorischer Mängel*** *anordnen.*

Die Nichtbestellung eines betrieblichen Beauftragten für den Datenschutz verstößt nicht nur gegen die sich aus § 4f Abs. 1 Satz 6 BDSG ergebende gesetzliche Pflicht, sondern stellt auch einen **organisatorischen Mangel** im Sinne des § 9 BDSG dar. Der Begriff umfasst dabei auch personelle Maßnahmen.

§ 9 BDSG

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die Anordnung der Bestellung eines Datenschutzbeauftragten scheint für eine verantwortliche Stelle, die ohnehin lediglich einige wenige Mitarbeiter beschäftigt, im Hinblick auf den in Satz 2 der Vorschrift normierten Verhältnismäßigkeitsgrundsatz auf den ersten Blick unverhältnismäßig zu sein, jedoch spielen Faktoren wie die mit der Bestellung verbundenen Kosten, die Unternehmensgröße oder die Art der betroffenen Daten, mit denen umgegangen wird, bei der Betrachtung eben keine Rolle, wenn die Voraussetzungen des § 4f Abs. 1 Satz 6 BDSG für die Bestellung eines Datenschutzbeauftragten vorliegen.

Der Betreiber der Webseite hat gegen die aufsichtsbehördliche Anordnung keinen Rechtsbehelf eingelegt, so dass der Bescheid bestands-

kräftig wurde. Erst nachdem ein Zwangsgeld fällig gestellt wurde, wurde seitens des Betreibers ein Beauftragter für den Datenschutz bestellt, welcher sodann auch das Verfahren im Sinne des § 4 Abs. 1 in Verbindung mit Abs. 4 BDSG meldete.

Da sowohl die nicht erfolgte Meldung des Verfahrens als auch die nicht erfolgte Bestellung eines Beauftragten für den Datenschutz sowie die Zuwiderhandlung gegen eine vollziehbare Anordnung nach § 38 Abs. 5 Satz 1 BDSG Bußgeldtatbestände darstellen, wurde auch die Bußgeldstelle des Datenschutzzentrums eingeschaltet.

20.2 Umgang mit Kundendaten in Franchisesystemen

Vor dem Hintergrund des dem Datenschutzrecht innewohnenden Transparenzgebots sollte es eigentlich selbstverständlich sein, dass verantwortliche Stellen, die personenbezogene Daten von Kunden erheben und verarbeiten, die Betroffenen vollumfänglich über den jeweiligen Zweck des Datenumgangs und insbesondere eventuelle Empfänger der Daten informieren. Dass dieses Transparenzgebot mitunter nur unzureichend Beachtung findet, trat im Zusammenhang mit der datenschutzrechtlichen Bewertung des Umgangs mit Kundendaten durch verantwortliche Stellen eines Franchisenetzwerks zu Tage.

Das deutsche Datenschutzrecht kennt kein Konzernprivileg. Insofern ist in einem Verbund von rechtlich selbstständigen Unternehmen jedes Einzelne als verantwortliche Stelle im Sinne des Datenschutzrechts zu betrachten, unabhängig davon, dass in einem Konzernverbund Weisungsstrukturen und Abhängigkeiten institutionalisiert sind. Personenbezogene Daten, mit denen die einzelnen Konzernunternehmen umgehen, wie beispielsweise Daten von Kunden oder Mitarbeitern, dürfen nicht anlasslos in diesem Verbund zirkulieren; es bedarf vielmehr einer datenschutzrechtlichen Grundlage, die eine zweckspezifische Übermittlung von personenbezogenen Daten legitimiert.

Dies gilt genauso für den Umgang mit personenbezogenen Daten in Vertriebssystemen wie Franchisenetzwerken. Franchisegeber und -nehmer als rechtlich selbstständige Akteure sind für sich genommen verantwortliche Stellen im Sinne des § 3 Abs. 7 BDSG und bleiben im Verhältnis zueinander Dritte im Sinne des § 3 Abs. 8 Satz 2 BDSG. Jedoch steht aufgrund der asymmetrischen Verteilung struktureller Entscheidungskompetenzen in einem Franchisesystem vorrangig der Franchisegeber für die Herstellung datenschutzkonformer Zustände in der Verantwortung.

Ein Franchiseverhältnis ist dadurch gekennzeichnet, dass der Franchisegeber im Rahmen der Zurverfügungstellung eines einheitlich gestalteten Geschäftskonzepts dem Franchisenehmer während der gesamten Dauer seiner unternehmerischen Tätigkeit vor allem hinsichtlich des vertriebenen Produkts bzw. der vertriebenen Dienstleistung, aber auch flankierend (z.B. in Bezug auf betriebswirtschaftliche, logistische oder marketingspezifische Aspekte) Beratung und Unterstützung zukommen lässt. Gleichzeitig behält sich der Systemgeber regelmäßig Kontroll- und Weisungsrechte sowie die Zahlung von fixen oder umsatzbasierten Entgelten vor. Durch einen einheitlich gestalteten Marktauftritt wird bei Kunden außerdem der Eindruck erzeugt, dass es sich bei den lokalen

Franchisenehmern um Betriebsstätten bzw. Niederlassungen eines einzigen Unternehmens handelt.

Im Franchisesystem ist ein umfangreicher Datenaustausch zwischen Systemgeber und –nehmer mitunter vitale Voraussetzung für das Funktionieren des Systems. Für die Erstellung betriebswirtschaftlicher Kennzahlen und Benchmarks oder die Abwicklung einer zentralen Warenbeschaffung sind jedoch regelmäßig keine personenbezogenen Daten von Kunden des Systemnehmers erforderlich. In Bezug auf qualitätssichernde Maßnahmen sowie Maßnahmen der externen Revision oder der Marktanalyse durch den Systemgeber wird eine Übermittlung von Daten, die keinen Personenbezug mehr aufweisen, üblicherweise ausreichend sein.

Für spezifische Zwecke kann eine institutionalisierte Zurverfügungstellung von personenbezogenen Daten der Kunden jedoch zur Aufgabenwahrnehmung der beteiligten Akteure notwendig sein, beispielsweise wenn das Marketing und eine personalisierte Werbeansprache nur durch den Franchisegeber erfolgt oder dieser die Warenauslieferung zentral abwickelt. Hierbei gilt es das Datensparsamkeitsgebots zu beachten, so dass ausschließlich die Kundendaten zur Verfügung zu stellen sind, die für die Aufgabenwahrnehmung erforderlich sind.

Daneben kann auch die Bereitstellung einer IT-Infrastruktur durch den Systemgeber denkbar sein.

Im zugrundeliegenden Sachverhalt wurde den Franchisenehmern die Nutzung einer webbasierten Anwendung verpflichtend vorgegeben, mit deren Hilfe nahezu die Gesamtheit ihrer administrativen Prozesse abgebildet wird. Im Rahmen der vom Franchisegeber entwickelten und administrierten Anwendung wurde zwangsläufig mit Kundendaten der Franchisenehmer umgegangen; diese Kundendaten wurden zudem auf Servern des Franchisegebers gespeichert und von diesem zur Erstellung nicht personenbezogener betriebswirtschaftlicher Kennzahlen und zur Entgeltabrechnungskontrolle herangezogen. Im Übrigen wurden durch den Systemgeber keine Aufgaben zentral für alle Stellen des Netzwerks wahrgenommen, die eine Weitergabe von Kundendaten erforderlich gemacht hätten.

Während die Systemnehmer aufgrund des mit dem Kunden bestehenden Vertragsverhältnisses dessen Daten nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG datenschutzrechtlich zulässig erheben und verarbeiten, bedurfte die Weitergabe von Kundendaten im Zusammenhang mit dem Einsatz der vorgeschriebenen Anwendung einer datenschutzrechtlichen Legitimationsgrundlage.

Da die Kunden der Franchisenehmer in dem zugrundeliegenden Fall weder über die Datenübermittlung an den Franchisegeber informiert wurden, geschweige denn in diese eingewilligt hatten, war fraglich, auf welcher Grundlage diese Weitergabe zulässig erfolgt sein sollte.

Der Systemgeber positionierte sich dahingehend, dass eine undifferenzierte Übermittlung von Kundendaten innerhalb des Franchisesystems grundsätzlich nicht zu beanstanden sei und die Kunden auch ohne weitere Hinweise die beteiligten Akteure des Systems ausmachen könnten. Im Übrigen wäre die Übermittlung durch die Franchisenehmer aber auch nach § 28 Abs. 1 Satz 1 Nr. 1 und 2 sowie nach § 28 Abs. 2 Satz 2 Nr. 2 Bst. a BDSG datenschutzrechtlich legitimiert. Jedoch wurde seitens

des Franchisegebers auch ausdrücklich darauf hingewiesen, dass neben der Erstellung nicht personenbezogener Kennzahlen und der Entgeltabrechnungskontrolle ausdrücklich keine Nutzung der auf den Servern gespeicherten Kundendaten erfolge und ein Zugriff auf die Daten somit nicht stattfinde.

§ 28 Abs. 1 Nr. 1 und 2 BDSG

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 […]*

§ 28 Abs. 2 Nr. 2 a) BDSG

Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig soweit es erforderlich ist, zur Wahrung berechtigter Interessen eines Dritten […]

Diese Auffassung des Franchisegebers hielt einer näheren Prüfung nicht stand. Vor dem Hintergrund, dass eine personenbezogene Nutzung der im Rahmen der Anwendung auf dessen Servern gespeicherten Kundendaten ausdrücklich nicht erfolgen sollte, war deren Übermittlung an den Franchisegeber mithin nicht erforderlich im Sinne des § 28 BDSG. Daneben standen aufgrund der betroffenen Datenkategorien, des spezifischen Verwendungszusammenhangs und der fehlenden Transparenz gegenüber den betroffenen Kunden der Franchisenehmer schutzwürdige Interessen der Übermittlung entgegen.

Um die zugrundeliegende Anwendung im Franchisesystem doch noch datenschutzkonform einsetzen zu können, bot sich folgender Maßnahmenkatalog an:

- Abschluss eines Vertrages über eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG mit dem Franchisenehmer als Auftraggeber und dem Franchisegeber als Auftragnehmer

  Die Franchisenehmer würden somit datenschutzrechtlich vollumfänglich verantwortlich für und verfügungsberechtigt über die personenbezogenen Daten ihrer Kunden bleiben. Jedoch gilt in diesem Zusammenhang zu beachten, dass der Franchisenehmer als Auftraggeber im Auftragsdatenverarbeitungsverhältnis den Auftragnehmer nach § 11 Abs. 2 Satz 1 BDSG **auswählen kann**. Dementsprechend würde beispielsweise eine über den Franchisevertrag erfolgende vertragsrechtliche Verpflichtung der Systemnehmer, den

Systemgeber als Auftragsdatenverarbeiter auszuwählen, dem Regelungsgehalt des § 11 BDSG zuwiderlaufen.

- (Flankierende) Einholung einer informierten Einwilligung des Kunden im Sinne des § 4a BDSG

  Für den Fall, dass ein Franchisenehmer aus spezifischen Gründen mit dem Franchisegeber keinen Vertrag über eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG abzuschließen wünscht, kann die Übermittlung von Kundendaten über die Einholung einer informierten Einwilligung im Sinne des § 4a BDSG der betroffenen Kunden erfolgen. Dazu sind die Kunden unter anderem über die betroffenen Datenkategorien, die Identität des Empfängers und den Zweck der Übermittlung zu informieren. Hier gilt jedoch zu bedenken, dass die Abgabe der Einwilligung absolut freiwillig erfolgen muss und dementsprechend mit einer hohen Verweigerungsquote bzw. mit Widerrufen der abgegebenen Einwilligung zu rechnen ist.

- Übermittlung anonymisierter Daten für Zwecke des Franchisegebers

  Für den Fall, dass schließlich der Abschluss eines Auftragsdatenverarbeitungsvertrags von einem Franchisenehmer ausgeschlossen wird und eine Einwilligung des Kunden in die Übermittlung seiner Daten an den Franchisegeber nicht erteilt wird, bleibt als einzige Möglichkeit wiederum nur die Weitergabe anonymisierter Daten.

Trotz anfänglichem Widerstand konnte sich der Systemgeber dem datenschutzrechtlichen Votum der Aufsichtsbehörde anschließen. Eine datenschutzkonforme Ausgestaltung des Franchisesystems ist zurzeit im Gange.

Gleichzeitig wurde der Sachverhalt an die Bußgeldstelle des Datenschutzzentrums abgegeben, da durch die unzulässige Datenübermittlung ein Verstoß gegen § 43 Abs. 2 Nr. 1 BDSG im Raum stand. Das diesbezügliche Ordnungswidrigkeitenverfahren ist bis dato noch nicht abgeschlossen.

20.3 Fallstricke bei der Nutzung personenbezogener Daten für Werbezwecke

Eine Petentin wandte sich im Berichtszeitraum an die Aufsichtsbehörde, da ihr von einem Fitnessstudio, dessen Angebot sich speziell an Senioren richtete, unverlangt ein Werbeschreiben zugesandt wurde. Weil sie in keiner Beziehung zu dem Fitnessstudio stand, adressierte sie an das Unternehmen ein Auskunftsersuchen nach § 34 Bundesdatenschutzgesetz (BDSG), um die Herkunft ihrer Adressdaten zu erfahren.

§ 34 Abs. 1 BDSG

Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. *die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,*

2. *den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und*

3. *den Zweck der Speicherung.*

Der Betroffene soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, ist Auskunft über die Herkunft und die Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind. Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

Das Auskunftsersuchen der Petentin blieb allerdings unbeantwortet.

Nach unserer Aufforderung zur Stellungnahme machte der Bevollmächtigte des Unternehmens die nebulöse Angabe, dass die Adressdaten der Petentin aus öffentlich zugänglichen Verzeichnissen entnommen worden wären und ihr Auskunftsersuchen nach § 34 BDSG bei der verantwortlichen Stelle nicht zugegangen sei.

Die Petentin erwiderte auf diese Stellungnahme des Unternehmens, dass die Entnahme ihrer Adressdaten aus einem Rufnummernverzeichnis ausgeschlossen sei, da sie bei ihrem Telekommunikationsanbieter keine Veröffentlichung der Daten im Sinne des § 104 Telekommunikationsgesetz (TKG) beantragt habe.

§ 104 TKG

Teilnehmer können mit ihrem Namen, ihrer Anschrift und zusätzlichen Angaben wie Beruf, Branche und Art des Anschlusses in öffentliche gedruckte oder elektronische Verzeichnisse eingetragen werden, soweit sie dies beantragen. Dabei können die Teilnehmer bestimmen, welche Angaben in den Verzeichnissen veröffentlicht werden sollen. Auf Verlangen des Teilnehmers dürfen Mitbenutzer eingetragen werden, soweit diese damit einverstanden sind.

Zudem sei in dem Werbeanschreiben des Fitnessstudios ihr zweiter Vorname genannt, weshalb sie davon ausgehe, dass die Daten von der Meldebehörde ihres Wohnortes stammten.

Nach Aufforderung zur Konkretisierung der ersten Stellungnahme bestätigte der Bevollmächtigte des Studiobetreibers, dass die Angaben von der Meldebehörde übermittelt worden seien.

Die Meldebehörde teilte wiederum auf Nachfrage mit, dass der Studiobetreiber – vor dem Hintergrund der Zielgruppe des Fitnessstudios - um Übermittlung von Adressbeständen der Einwohner zwischen dem 55. und 80. Lebensjahr gebeten habe, mit dem Ziel, diesen ein Werbeschreiben postalisch zukommen zu lassen. Diesem Ersuchen sei entsprochen worden, so dass von der Meldebehörde ein Bestand von 2.000 Namen und Anschriften an das Unternehmen übermittelt worden sei. Auch eine Nachbargemeinde übermittelte auf Nachfrage des Be-

treibers Namen und Anschriften von 1.200 Bürgern an diesen. Die Übermittlung des Geburtsdatums oder weiterer Daten sei ausdrücklich nicht erfolgt.

Fraglich war in diesem Zusammenhang somit, inwiefern die Erhebung und Nutzung der personenbezogenen Daten der Petentin für Werbezwecke durch den Studiobetreiber datenschutzrechtlich zulässig erfolgt ist.

Da eine Einwilligung in die Erhebung und Nutzung ihrer personenbezogenen Daten für Werbezwecke außer Rede stand, könnte diese aber möglicherweise nach § 28 Abs. 3 Satz 2 Nr. 1 BDSG zulässig erfolgt sein.

§ 28 Abs. 3 Satz 2 Nr. 1 BDSG

Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

1. *für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Absatz 1 Satz 1 Nummer 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren* ***Verzeichnissen*** *erhoben hat […]*

Dies bedeutet, dass Vorname, Name und Anschrift als **Listendaten** im Sinne des § 28 Abs. 3 Satz 2 BDSG für eine Werbeansprache der Einwohner einer Gemeinde, die das 55. Lebensjahr vollendet haben, durch den Studiobetreiber datenschutzrechtlich zulässig genutzt werden dürfen, wenn die Daten aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen stammen. Einschränkend hierzu gilt, dass nach § 28 Abs. 3 Satz 6 BDSG keine schutzwürdigen Interessen der Betroffenen entgegenstehen dürfen.

Die Frage, ob das Melderegister als öffentliches Register ein allgemein zugängliches Verzeichnis im Sinne der Vorschrift darstellt, wird in der datenschutzrechtlichen Kommentarliteratur unterschiedlich beantwortet. Jedoch lassen selbst die Stimmen, die die Meinung vertreten, dass das Melderegister ein allgemein zugängliches Verzeichnis im Sinne des § 28 Abs. 3 Satz 2 Nr. 1 BDSG darstellt, dies nur für eine voraussetzungslose **einfache Melderegisterauskunft** nach § 21 Abs. 1 Melderechtsrahmengesetz (MRRG) bzw. im konkreten Fall nach § 34 Abs. 1 Meldegesetz (MG) gelten.

Entgegen einer einfachen Melderegisterauskunft, die ohne Geltendmachung eines berechtigten Interesses erteilt werden kann und ausschließlich Vor- und Nachnamen, Doktorgrad sowie die Anschrift des Betroffenen umfasst, ist der Informationsgehalt von nach Altersgesichtspunkten vorsortierten Adressdaten eben ungleich größer.

Im Hinblick auf den Regelungsgehalt des zum 1. November 2015 in Kraft tretenden § 44 Abs. 3 Nr. 2 Bundesmeldegesetz (BMG), wird zu-

dem der Wille des Bundesgesetzgebers erkennbar, dass das Melderegister eben keine voraussetzungslose Bezugsquelle für Adressdaten für werbewillige Unternehmen sein soll.

Entsprechend dieser Vorschrift ist eine Erhebung von Adressdaten durch private Stellen und ihre anschließende Nutzung für Werbezwecke von der Einwilligung des Betroffenen abhängig zu machen.

§ 44 Abs. 3 BMG

Die Erteilung einer einfachen Melderegisterauskunft ist nur zulässig, wenn

1. *die Identität der Person, über die eine Auskunft begehrt wird, auf Grund der in der Anfrage mitgeteilten Angaben über den Familiennamen, den früheren Namen, die Vornamen, das Geburtsdatum, das Geschlecht oder eine Anschrift eindeutig festgestellt werden kann, und*

2. *die Auskunft verlangende Person oder Stelle erklärt, die Daten nicht zu verwenden für Zwecke*

   a) *der Werbung oder*

   b) *des Adresshandels,*

es sei denn, die betroffene Person hat in die Übermittlung für jeweils diesen Zweck ausdrücklich eingewilligt.

Die Erhebung von Adressdaten mit dem Zweck der Werbeansprache der Betroffenen war darüber hinaus auch vor dem Hintergrund als unzulässig zu bewerten, als schutzwürdige Interessen der Betroffenen einer späteren Nutzung für Werbezwecke im Sinne des § 28 Abs. 3 Satz 6 BDSG entgegenstanden.

Wenn im Zusammenhang mit der Zusammenstellung der Adressdaten Einzelheiten zu Tage treten, die über den Informationsgehalt der reinen Listendaten hinausgehen, können schutzwürdige Interessen der weiteren Verwendung entgegenstehen. Da sich gerade im Hinblick auf die oben geschilderte alters- und wohnortbezogene Eingrenzung von Adressdaten und Zusatzwissen über lokale Gegebenheiten beispielsweise auf die Unterbringung eines Betroffenen in einem Alters- und Pflegeheim schließen ließ, standen eben schutzwürdige Interessen der Betroffenen der Nutzung der Adressdaten entgegen.

Dies wurde der verantwortlichen Stelle kommuniziert mit der Aufforderung, die somit datenschutzrechtlich unzulässig erhobenen Adressdaten zu löschen.

Darüber hinaus wurde ein Bußgeldverfahren eingeleitet, da das Werbeschreiben keinen Hinweis auf das Widerspruchsrecht nach § 28 Abs. 4 Satz 1 BDSG enthielt und das Fehlen eines solchen Hinweises nach § 43 Abs. 1 Nr. 3 BDSG einen Bußgeldtatbestand darstellt.

§ 28 Abs. 4 Satz 1 und 2 BDSG

Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig. ***Der Betroffene ist bei der Ansprache zum Zweck der Werbung*** *oder der Markt- oder Meinungsforschung und in den Fällen des Absatzes 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses* ***über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten*** *[...].*

20.4 Abfotografieren von Schülerfahrausweisen

Das unangekündigte Abfotografieren des Schülerfahrausweises ihrer Tochter führte dazu, dass sich eine Petentin im Berichtszeitraum an die Aufsichtsbehörde wandte.

Beim Einsteigen in den Schulbus sei die Tochter ohne weitere Information dazu angehalten worden, ihren Fahrausweis abfotografieren zu lassen. Auf dem Fahrausweis war neben dem Lichtbild des Ausweisinhabers und dessen Name noch eine Abo- bzw. Zeitkartennummer zu finden. Eine spätere Rückfrage der Mutter beim Busunternehmen hatte zum Ergebnis, dass Zweck der Maßnahme die Überprüfung der fahrgastbezogenen Auslastung bestimmter Buslinien im Ausbildungsverkehr sei. Dazu sei ein Verkehrsgutachter von dem Busunternehmen beauftragt worden, dessen Mitarbeiter die Bilddokumentationen anfertigten.

Laut Stellungnahme des Busunternehmens wurde die bereits der Petentin kommunizierte Zwecksetzung bestätigt. Anlass dafür sei, dass die Verteilung der nach § 45a Personenbeförderungsgesetz gewährten Ausgleichsmittel mit der tatsächlichen Beförderungsleistung im Ausbildungsverkehr in Relation gesetzt werden soll, um gegebenenfalls eine für das Unternehmen günstigere Verteilungsquote zu erreichen. Neben dem von den Mitarbeitern des beauftragten Verkehrsgutachters erhobenen Bild des Fahrausweises würde auch die Uhrzeit des Einstiegs in den Bus dokumentiert. Relevant für die bildgestützte Fahrgasterhebung seien jedoch ausschließlich Fahrkartenart und Abo- bzw. Zeitkartenummer; Bild und Name des Kunden seien in diesem Zusammenhang lediglich „Beifang" gewesen. Nach abgeschlossener Auswertung der Bilddaten hinsichtlich der relevanten Daten wäre dem Busunternehmen durch den Verkehrsgutachter die linienbezogene Auslastung im Ausbildungsverkehr dargestellt worden.

Eine Bilddokumentation sei aufgrund der ungünstigen Umgebungsbedingungen (häufiger Fahrgastwechsel und zeitweise kurze Verweildauer der Fahrgäste im Fahrzeug) zielführender als ein einfaches Notieren der relevanten Daten, da durch die im Vergleich dazu kürzere Dauer des Erhebungsvorgangs eine größere Genauigkeit und geringere Fehlerquote erreicht würde.

Unabhängig davon, dass unter Beachtung des Datensparsamkeitsgebots eine Erhebung und Speicherung der in diesem Zusammenhang nicht erforderlichen Daten, wie Name und Bild des Ausweisinhabers,

datenschutzrechtlich nicht zulässig erfolgte, hätte eine Datenerhebung und -verarbeitung der Fahrkartenart und der Abo- bzw. Zeitkartennummer in diesem Kontext durchaus im berechtigten Interesse des Busunternehmens im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) erfolgen können. Jedoch wurden von dem verantwortlichen Busunternehmen verschiedene datenschutzrechtliche Vorgaben und Erfordernisse nicht beachtet.

Da der Datenumgang durch den Verkehrsgutachter im Auftrag und für Zwecke des Busunternehmens erfolgte, war dieses verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG und die Ausführung des Projekts durch den Auftragnehmer rechtlich als Auftragsdatenverarbeitung im Sinne des § 11 BDSG abzubilden.

Im Rahmen einer Auftragsdatenverarbeitung sind nach § 11 Abs. 2 Satz 2 BDSG spezifische Erfordernisse zu berücksichtigen, die in einem schriftlichen Vertrag festzulegen sind. Eine schriftliche Vereinbarung im Sinne der Vorschrift wurde jedoch nicht abgeschlossen.

Da es sich hierbei auch um eine automatisierte Verarbeitung von personenbezogenen Daten handelte, war zudem ein Verfahrensverzeichnis nach § 4e BDSG zu erstellen. Ein solches existierte aber auch nicht.

Weiterhin wurde der dem Datenschutzrecht immanente Grundsatz der Transparenz nicht beachtet. Nach § 4 Abs. 3 BDSG sind Betroffene unter anderem bereits zum Zeitpunkt der Datenerhebung über die Identität der verantwortlichen Stelle, die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und ggf. die Kategorien von Empfängern zu unterrichten.

Da eine einzelfallbezogene Information der betroffenen Kunden vor Beginn der Maßnahme hier ausgeschlossen war, hätte die notwendige Transparenz beispielsweise dergestalt hergestellt werden können, dass vorab ein Hinweis auf die geplante Durchführung der Maßnahme in einem lokalen Printmedium ergangen und zum Zeitpunkt der Datenerhebung im Bus ein Hinweiszettel mit den erforderlichen Informationen ausgehändigt worden wäre.

Das verantwortliche Busunternehmen teilte im Laufe des Verfahrens mit, dass der Auftrag an den Verkehrsgutachter noch vor Abschluss des Projekts storniert und die bereits erhobenen personenbezogenen Daten beim Auftragnehmer durch diesen gelöscht wurden.

21 Auskunfteien

21.1 Allgemeines Anfragerecht bei Auskunfteien

Im Berichtszeitraum wandte sich ein Petent an die Aufsichtsbehörde mit dem Vorwurf, eine Auskunftei habe in ungerechtfertigter Weise Auskunft über seine Person erteilt.

Unter einer Auskunftei ist ein privatwirtschaftliches Unternehmen zu verstehen, welches sich zum Zweck gesetzt hat, wirtschaftsrelevante Daten über Privatpersonen und Unternehmen an ihre Geschäftspartner (auf Anfrage) mitzuteilen. Zu diesen Daten bei Privatpersonen gehören insbesondere Kontaktdaten (Name, Vorname, postalische Anschrift, Geburtsdatum, etc.), Familienstand, Tätigkeit, Beurteilung der Finanzlage, Immobilienbesitz, Beteiligungen, Bankverbindungen, welche personenbezogene Daten darstellen.

Im Rahmen einer Selbstauskunft habe der Petent festgestellt, dass eine Kreditanstalt des öffentlichen Rechts, mit der der Petent vor einiger Zeit ein zwischenzeitlich beendetes Geschäftsverhältnis unterhielt, über seine Person eine Anfrage bei der Auskunftei gestellt habe. Der Auskunftei wurde die Vertragsbeendigung seinerzeit auf ausdrücklichen Wunsch des Petenten auch mitgeteilt. Aus Sicht des Petenten bestand insofern keine Berechtigung der Kreditanstalt diese Anfrage durchzuführen, zumal parallel hierzu zusätzlich ein Scorewert ermittelt und an die Bank als Antragsteller übermittelt worden sei. Da er weder in einer aktuellen Geschäftsbeziehung mit der Bank stehe noch seine ausdrückliche Einwilligung in die Abfrage erteilt habe, bat er die Aufsichtsbehörde um datenschutzrechtliche Überprüfung der Angelegenheit.

Bei der Bank handelte es sich um eine öffentliche Stelle i. S. d. § 2 Abs. 1 SDSG. Da sie als öffentlich-rechtliches Unternehmen am Wettbewerb teilnimmt, gelten für sie gemäß § 2 Abs. 2 SDSG nur der zweite Teil sowie § 7 Abs. 1 und §§ 9, 30 bis 32 SDSG. Mit Ausnahme der Vorschriften über die Aufsichtsbehörde sind im Übrigen die für nicht öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes (BDSG) einschließlich der Straf- und Bußgeldvorschriften anwendbar. Die Zuständigkeit der Aufsichtsbehörde war somit gegeben.

Vor diesem Hintergrund wurde die Kreditanstalt zur umfassenden Stellungnahme aufgefordert, inwiefern durch diese eine Anfrage bezüglich eines ehemaligen Kunden eingereicht wurde und aufgrund welchen Tatbestandes bzw. welcher Rechtsgrundlage diese Anfrage getätigt wurde.

Der Datenschutzbeauftragte der Kreditanstalt teilte mit, dass der Auskunft ein Schreiben des ehemaligen Bankkunden vorausging. Da eine Rückantwort aufgrund der nicht zu entziffernden Anschrift ausgeschlossen war, wurde durch einen Mitarbeiter des Unternehmens eine Auskunft eingeholt, um die aktuelle Anschrift des Petenten zu ermitteln. Man habe im Interesse des Kunden handeln wollen, ohne sich über die Sensibilität bzw. datenschutzrechtliche Zulässigkeit des Abrufs im Kla-

ren zu sein. Im Rahmen des Tagesgeschäfts sei dem Mitarbeiter dieser Fehler unterlaufen, was aus Unternehmenssicht jedoch einen Einzelfall darstellt. Der Datenschutzbeauftragte habe dies zum Anlass genommen, den einzelnen Mitarbeiter als auch den gesamten Fachbereich auf die rechtliche Situation hinzuweisen und entsprechend zu sensibilisieren.

Grundsätzlich ist die Übermittlung personenbezogener Daten durch die Auskunftei dann zulässig, wenn ein Vertragspartner der Auskunftei ein berechtigtes Interesse glaubhaft darlegen kann und im Gegenzug kein Grund zu der Annahme besteht, dass ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung besteht (§ 29 Abs. 1 Nr. 1 BDSG). Ein berechtigtes Interesse ist dann anzunehmen, wenn der Vertragspartner durch eine bevorstehende Entscheidung ein finanzielles Risiko eingehen würde (z. B. Warenversand auf Rechnung, Kreditgewährung, etc.). Eine Bonitätsanfrage an die Auskunftei ist in solchen Fällen zulässig.

Nicht zulässig hingegen ist die Auskunft für andere Zwecke, z. B. wenn ein Vertragspartner wie geschildert die Anschrift eines Kunden ermitteln möchte, um mit diesem in Schriftverkehr zu treten. In solchen Fällen ist anzunehmen, dass das Interesse des Betroffenen an der Geheimhaltung seiner personenbezogenen (wirtschaftsrelevanten) Daten das Informationsinteresse des Vertragspartners überwiegt.

§ 29 Abs. 2 S. 5 BDSG verpflichtet die Auskunftei zur stichprobenhaften Überprüfung des berechtigten Interesses der Antragsteller. Eine lückenlose Kontrolle findet dabei jedoch nicht statt.

Grundsätzlich hat aber auch jeder das Recht, sich selbst über die zu seiner Person bei einer Auskunftei gespeicherten Daten zu informieren. Von Gesetzes wegen ist jede Auskunftei dazu verpflichtet, einmal im Jahr Verbrauchern eine kostenlose Auskunft über gespeicherte Daten zu erteilen (§ 34 Abs. 8 BDSG). Da die Datenbestände bei Auskunfteien erfahrungsgemäß nicht zwingend aktuell und fehlerfrei sind, haben Betroffene nach § 35 BDSG einen Anspruch auf Berichtigung, Löschung oder Sperrung von unrichtigen Daten.

22 Umwelt

22.1 Katasterverwaltung: Ablösung von Altverfahren durch ALKIS

Das Landesamt für Vermessung, Geoinformation und Landentwicklung verarbeitet die Daten des Liegenschaftskatasters mit einem Verfahren, dessen grundlegende Entwicklung bereits mehr als 40 Jahre zurück liegt. Es handelt sich dabei um eine großrechnerbasierte Eigenentwicklung, die in Zusammenarbeit mit der ZDV-Saar ständig aktualisiert und modernisiert wurde. Da jedoch die Großrechnertechnologie in absehbarer Zeit bei der ZDV-Saar nicht mehr vorgehalten wird, war es unumgänglich ein neues Verfahren einzuführen.

Bereits 2006 wurde beschlossen, die Liegenschaftsverwaltung neu zu strukturieren. Dabei fiel auch der Entschluss, sich dem bundesweit eingesetzten AAA-Modell[24] anzuschließen. Die Daten des Liegenschaftskatasters werden mit der Komponente ALKIS (Amtliches Liegenschaftskatasterinformationssystem) verarbeitet. Da in diesem Teil des AAA-Modells personenbezogene Daten verarbeitet werden, wurde das Datenschutzzentrum gemäß § 7 Abs. 2 Saarländisches Datenschutzgesetz (SDSG) Ende 2013 über die Verfahrensumstellung informiert.

---

[24] AAA-(AFIS-ALKIS-ATKIS-)Modell

Die Vermessungs- und Katasterverwaltungen der Bundesländer haben die Aufgabe, raumbezogene Basisdaten (Geobasisdaten) für Verwaltung, Wirtschaft und private Nutzer zu liefern, und zwar zunehmend in digitaler Form.

Geobasisdaten werden derzeit in folgenden Datenbeständen bereitgestellt:

- Das Amtliche Topographisch-Kartographische Informationssystem (ATKIS®) beschreibt die Oberfläche der Erde mit Digitalen Landschafts- und Geländemodellen.
- Die Automatisierte Liegenschaftskarte ALK und das Automatisierte Liegenschaftsbuch ALB enthalten die Daten des Liegenschaftskatasters. Diese beiden Informationssysteme werden zukünftig integriert im Amtlichen Liegenschaftskatasterinformationssystem (ALKIS®) geführt. Darüber hinaus wurde eine Harmonisierung mit ATKIS® vorgenommen.
- Da die Festpunkte weder originär zur ALK noch zu ATKIS® gehören, wird deren Modellierung nunmehr in einem eigenen Amtlichen Festpunktinformationssystem (AFIS®) durch einen eigenen Objektartenkatalog vorgenommen.

Überregionale Nutzer und GIS-Industrie fordern im Hinblick auf die Inhalte und die Strukturierung der Geobasisdaten sowie aus Gründen der Wirtschaftlichkeit die Festlegung eines bundesweit einheitlichen Grunddatenbestandes.

Das AAA®-Modell soll dazu dienen, die Grunddatenbestände von ATKIS®, ALKIS® und AFIS® zu einem Grunddatenbestand der Geodaten des amtlichen Vermessungswesens zusammenzuführen. Unter der Überschrift Dokumentation zur Modellierung der Geoinformationen des amtlichen Vermessungswesens werden die AdV-Projekte AFIS®, ALKIS® und ATKIS® mit ihren länderübergreifend festgelegten Eigenschaften in durchgängiger Form gemeinsam beschrieben und miteinander in Beziehung gebracht.

Die Umstellung berührt im Wesentlichen die technischen Komponenten (Umstellung von Großrechner auf Server), die Datenhaltung (von ADABAS auf Oracle) und die Verarbeitungsprogramme selbst. Am Umfang und Inhalt der Daten wird es keine Änderungen geben. Die Überprüfung in technisch-organisatorischer Sicht ergab keine Beanstandungen. Auch die Verarbeitung der Daten erfolgt wie im bisherigen Umfang, sodass es keiner erneuten Prüfung bedarf.

Der Online-Zugriff auf die Daten des Liegenschaftskatasters im Digitalen Rissarchiv erfolgt in Zukunft über die neue Anwendung DIRI-Web. Über diese Anwendung können zugelassene Nutzer, z. B. öffentlich bestellte Vermessungsingenieure zur Bearbeitung ihrer Aufträge alle, die Lage von Flurstückgrenzen bestimmenden Vermessungsinformationen online recherchieren und abrufen. Diese Abrufe werden anhand einer Vorgangsnummer erfasst und protokolliert.

Im neuen Verfahren ALKIS wird der Kreis der Zugriffsberechtigten, der im Saarländischen Vermessungs- und Katastergesetz in Verbindung mit der Katasterinhalts- und Datenübermittlungsverordnung gesetzlich festgelegt ist, nicht erweitert. Personenbezogene Daten werden nur in dem Umfang zur Verfügung gestellt, wie die Kenntnis der Daten zur Erfüllung der Aufgaben der Zugriffsberechtigten erforderlich ist.

Die Migration der Datenbestände und der Umstieg auf ALKIS ist für das 1. Quartal 2015 geplant und wird von uns datenschutzrechtlich begleitet.

23 Versicherungen

23.1 Einwilligungs- und Schweigepflichtentbindung in der Versicherungswirtschaft

Die obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich haben in Zusammenarbeit mit dem Gesamtverband der Deutschen Versicherungswirtschaft e. V. eine Einwilligungs- und Schweigepflichtentbindungserklärung entwickelt, die im Beschluss des Düsseldorfer Kreises vom 17. Januar 2012 als datenschutzgerechte Lösung von den Versicherungsunternehmen übernommen werden sollte.

Eine solche Einwilligungserklärung war notwendig, da die Regelungen des Versicherungsvertragsgesetzes, des Bundesdatenschutzgesetzes sowie anderer Datenschutzvorschriften keine ausreichenden Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen enthalten.

Die Versicherungen waren also aufgefordert, die bisherigen Einwilligungstexte kurzfristig durch neue, der Mustererklärung entsprechende, zu ersetzen.

Im Einzelnen wird auf die Ausführungen zu Kapitel 23.9 Einwilligungs- und Schweigepflichtentbindungserklärung im 24. Tätigkeitsbericht (2011/2012) des Unabhängigen Datenschutzzentrums Saarland verwiesen, insbesondere auch auf die Anwendungshinweise.

In der Folge informierten die betroffenen Unternehmen ihre Versicherungsnehmer über die wesentlichen Inhalte zur Einwilligungs- und Schweigepflichtentbindungserklärung ergänzend zu bereits bestehenden Regelungen in den Versicherungsvertragsverhältnissen.

In den Zuständigkeitsbereich der saarländischen Aufsichtsbehörde fallen die im Saarland ansässigen Versicherungsunternehmen. Diese haben ihre Kunden schriftlich auf die neuen Regelungen zur Einwilligungs- und Schweigepflichtentbindungserklärung hingewiesen. Darin enthalten war auch ein Hinweis, die vollständige Einwilligungs- und Schweigepflichtentbindungserklärung im Internet abzurufen oder postalisch zugesendet zu bekommen, womit die Versicherungen den wesentlichen Forderungen der Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich nachgekommen sind.

Im Zuge dieser Benachrichtigungen erreichten die Landesdatenschutzbeauftragte aus dem gesamten Bundesgebiet Beschwerden von Versicherungsnehmern, die eine Benachteiligung in datenschutzrechtlicher Hinsicht befürchteten. Insbesondere ging es bei den Beschwerden darum, dass die Versicherungen zusätzliche Vertragsbedingungen einseitig, also ohne Einwilligung der Betroffenen, mitteilte.

Im Hinblick auf etwaige Bedenken sei darauf hingewiesen, dass durch die „neue" Einwilligungs- und Schweigepflichtentbindungserklärung eine Anhebung des Datenschutzniveaus zu Gunsten der Versicherten erreicht werden konnte.

23.2 Informationsweitergabe durch eine Versicherung an die Polizei

Zu Beginn des Kalenderjahres 2014 erreichte die Aufsichtsbehörde die Eingabe eines Versicherungsnehmers einer im Saarland ansässigen Versicherungsgesellschaft. Grundlegend ging es dabei um die Frage nach der datenschutzrechtlichen Zulässigkeit hinsichtlich einer auf telefonischer Nachfrage erfolgten Weitergabe personenbezogener Daten an Dritte zur Strafverfolgung.

Der Petent schilderte den Sachverhalt, wonach seine Ehefrau in einem Parkhaus einen Autounfall verursachte und aufgrund einer situationsbezogenen Fehleinschätzung den Unfallort ohne weiteres Zutun verließ. Ein Zeuge teilte den Sachverhalt der Polizei mit und erstattete Anzeige wegen Unfallflucht. Im Rahmen einer polizeilichen Vernehmung machte der Petent von seinem Zeugnisverweigerungsrecht Gebrauch. Der Petent teilte dies und die Tatsache, dass die Ehefrau das Fahrzeug am Unfalltag gesteuert hatte, dem Versicherungsunternehmen im Zuge der Schadensregulierung mit. Der polizeilichen Ermittlungsakte war zu entnehmen, dass die Polizei telefonisch Kontakt mit dem Versicherer aufgenommen hatte und dem Beamten die Unfallbeschreibung des Petenten auszugsweise mitgeteilt wurde.

Das Versicherungsunternehmen teilte auf Nachfrage der Aufsichtsbehörde mit, dass das Auskunftsersuchen bzw. die Übermittlung personenbezogener Daten in hiesigem Fall gemäß §§ 28 Abs. 2 Bundesdatenschutzgesetz (BDSG) i. V. m. 161a Strafprozessordnung (StPO) legitimiert sei. Nach § 28 Abs. 2 Buchst. b BDSG ist eine Datenübermittlung zulässig, soweit sie zur Verfolgung von Straftaten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Da ein Ermittlungsverfahren wegen unerlaubten Entfernens vom Unfallort anhängig sei, diene die Auskunft schließlich der Verfolgung einer Straftat. Da der ermittelnde Beamte telefonisch und nicht wie im Regelfall schriftlich oder per Fax Auskunft darüber verlangte, ob aus der Schadensakte die Person hervorgehe, die zum Zeitpunkt des Unfalls Fahrer des in Rede stehenden KFZ sei, erfolgte eine Identifikation des Anrufenden dergestalt, dass neben der Namensnennung des Gesprächspartners sowie einer Abfrage der entsprechenden behördlichen Dienststelle auch eine Identifikation der Telefonnummer ablief, indem die angezeigte Nummer mit der im Internet abrufbaren Rufnummer der dortigen Polizeibehörde abgeglichen wurde. So sei aus Sicht des Versicherungsunternehmens eine Datenübermittlung an unbefugte Personen ausgeschlossen.

Aus Sicht der Aufsichtsbehörde kann die Legitimation des Anrufenden entgegen der Auffassung der Versicherung im Rahmen eines Telefonats nicht zweifelsfrei geklärt werden, da eine Identifizierung des Anrufers anhand der angezeigten Telefonnummer ebenso wenig geeignet bzw.

als ausreichend zu erachten ist wie die Abfrage des Namens des Gesprächspartners und der behördlichen Dienststelle. Des Weiteren wurde in diesem Zusammenhang auf die mangelnde Berücksichtigung interner Datenschutzrichtlinien des Versicherungsunternehmens hingewiesen, da u. a. die Vorgabe, dass vor Erteilung einer telefonischen Auskunft eine Abwägung der schützenswerten Interessen zu erfolgen hat, zumindest teilweise missachtet wurde. Dies wog umso schwerer, da dem Petent gemäß § 52 Abs. 1 Nr. 2 StPO ein Zeugnisverweigerungsrecht zu stand und er von diesem gegenüber der Ermittlungsbehörde auch Gebrauch machte. Im Rahmen eines Telefonats konnte eine datenschutzrechtlich einwandfreie Abwägung der schützenswerten Interessen jedenfalls nicht stattfinden und fand auch nicht statt.

Aus diesen Erwägungen heraus ist von Ermittlungsbehörden grundsätzlich zu fordern, dass diese unter Darlegung des berechtigten Interesses eine schriftliche Anfrage an die verantwortliche Stelle – hier das Versicherungsunternehmen – richten. Insbesondere kann durch ein Fax zeitnah und in datenschutzrechtlich unbedenklicher Weise die Identität und die Legitimation des Anrufers geklärt werden. In Zweifelsfällen sollte die verantwortliche Stelle gegenüber der Polizei oder Staatsanwaltschaft auf einer förmlichen Anordnung bestehen.

Abschließend wurde das Versicherungsunternehmen vor dem Hintergrund einer drohenden Geldbuße im Falle einer rechtswidrigen Datenübermittlung an Dritte auf die Notwendigkeit der Sensibilisierung der Mitarbeiter und eine restriktive Handhabung hinsichtlich des Umgangs bei entsprechenden telefonischen Anfragen hingewiesen.

24 Sonstiges

24.1 Strafantrag wegen Amtsanmaßung gegen einen selbstständigen Datenschutzbeauftragten

Im Alltagsgeschäft der Datenschutzaufsichtsbehörde spielen nicht bloß rein datenschutzrechtliche Fragestellungen eine Rolle. Der Fall eines selbstständigen Datenschutzbeauftragten, der in seiner Aufgabenwahrnehmung weit über das Ziel hinausgeschossen ist, beschäftigte die Aufsichtsbehörde im Berichtszeitraum.

Durch den Anruf eines sehr erbosten Einzelhändlers, der das seines Erachtens ungerechtfertigte und ungewöhnliche Vorgehen eines angeblichen Mitarbeiters der Aufsichtsbehörde thematisierte, wurde die Aufsichtsbehörde auf die Tätigkeit eines selbstständigen Datenschutzbeauftragten aufmerksam. Der Anrufer erklärte, er habe hinsichtlich der in seinem Laden angebrachten Videoüberwachungsmaßnahme und wegen des Impressums seiner Webseite mehrfach E-Mails von einem Mitarbeiter der Datenschutzaufsicht erhalten, in denen Bußgelder und Abmahnungen angedroht würden.

Da das Datenschutzzentrum bislang mit dem Ladeninhaber nicht in Kontakt gestanden hatte, geschweige denn ein Verwaltungsverfahren gegen diesen führte, wurde der Ladeninhaber um Zurverfügungstellung der besagten E-Mails gebeten. Aus diesen ging hervor, dass ein selbstständiger Datenschutzbeauftragter diese E-Mails an den Ladeninhaber adressierte und darin, entsprechend der Schilderung des Ladeninhabers, Bußgelder androhte. Zudem vermittelte der Verfasser der E-Mails durch seine Wortwahl bewusst den Eindruck, dass er im Auftrag einer staatlichen Stelle handele und dieser vorgesetzten Stelle Meldung über das Verhalten des Ladeninhabers erstatten müsse.

Auf Grundlage dieser E-Mails wurde der Vorgang wegen Verdachts der Amtsanmaßung an die Staatsanwaltschaft weitergegeben.

§ 132 Strafgesetzbuch

Amtsanmaßung

Wer unbefugt sich mit der Ausübung eines öffentlichen Amtes befasst oder eine Handlung vornimmt, welche nur kraft eines öffentlichen Amtes vorgenommen werden darf, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Die Staatsanwaltschaft folgte der rechtlichen Bewertung des Sachverhalts durch das Datenschutzzentrum und beantragte im Hinblick auf die im Raum stehende Amtsanmaßung den Erlass eines Strafbefehls.

Das zuständige Amtsgericht beraumte die Hauptverhandlung an, um dem Datenschutzbeauftragten Gelegenheit zur Stellungnahme zu geben. Das Gericht sah jedoch abschließend den Tatvorwurf der Amtsanmaßung bestätigt und verurteilte den Datenschutzbeauftragten zu einer

Geldstrafe. Der selbstständige Datenschutzbeauftragte legte gegen dieses Urteil Berufung ein, über die bislang noch nicht entschieden worden ist.

25 Aus der Dienststelle

25.1 Zusammenarbeit mit dem Landtag

Im Berichtszeitraum haben wir an 17 Sitzungen des Ausschusses für Datenschutz und Informationsfreiheit teilgenommen, aktuelle Themen vorgetragen und den Abgeordneten die datenschutzrechtlichen Positionen zu aktuellen politischen Fragestellungen erläutert.

Zu den Themen der Ausschusssitzungen gehörten sowohl die zusammenfassende Darstellung des letzten Tätigkeitsberichtes als auch der Vortrag über die jeweils aktuellen Entschließungen der halbjährlich tagenden Datenschutzkonferenz und der Konferenz der Informationsfreiheitsbeauftragten.

Darüber hinaus haben wir unter anderem zu folgenden datenschutzrechtlichen Themen berichtet:

- Abfragen von Kontendaten durch Finanz- und Sozialbehörden im Saarland
- die rechtliche Würdigung der Selbstauskunftsbögen der gesetzlichen Krankenkassen
- die datenschutzrechtliche Würdigung der Fragebögen bei Einschulungsuntersuchungen im Saarland
- die Datenschutzregelungen im neuen Bundesmeldegesetz den Einsatz und die Zulässigkeit von Wildkameras in saarländischen Wäldern
- datenschutzrechtliche Gesichtspunkte der Verpflichtung saarländischer Kassenärzte nur noch online abrechnen zu dürfen
- Bericht zu den Schülerworkshops des Unabhängigen Datenschutzzentrums
- Zulässigkeit der Fahndung in sozialen Netzwerken - insbesondere in Facebook
- Stellungnahme zum Pressebericht der millionenfachen Ausforschung von Zugangsdaten von privaten Anwendern und Behörden durch Hacker
- Bericht über den europäischen Datenschutztag
- Meldepflicht für Videokameras zur Verkehrsüberwachung oder Verbrechensbekämpfung in den saarländischen Kommunen
- Datensicherheit und Datenschutz bei mobilen Endgeräten
- Bericht zum Stand der EU-Datenschutzgrundverordnung

- Datenschutzrechtliche Bedenken gegen die geplante PKW-Maut

- Videoüberwachung am Arbeitsplatz

In weiteren sieben Sitzungen anderer Landtagsausschüsse war der Ausschuss für Datenschutz und Informationsfreiheit hinzugezogen. Hierbei ging es in einigen Fällen insbesondere um Anhörungen zu verschiedenen Gesetzgebungsverfahren sowie aktuelle politische Themen im Land.

Im Rahmen dieser Hinzuziehung konnten wir auch mit dem Ausschuss für Justiz, Verfassungs- und Rechtsfragen sowie Wahlprüfung das Institut für Rechtsinformatik an der Universität des Saarlandes besuchen und wurden über den Werdegang des Institutes in den letzten 25 Jahren und die dortige Arbeit unter neuer Leitung informiert.

25.2 Zusammenarbeit mit anderen Stellen

25.2.1 Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK)

Die Datenschutzkonferenz ist ein freiwilliger Zusammenschluss der Bundesbeauftragten und der Landesbeauftragten für Datenschutz. Die Konferenz trifft sich zweimal im Jahr, der Vorsitz wechselt jährlich. Im Berichtszeitraum hatte im Jahr 2013 das Bundesland Bremen den Vorsitz und im Jahre 2014 das Bundesland Hamburg.

In der Konferenz werden zu aktuellen Datenschutzfragen politische Forderungen diskutiert und als Entschließungen formuliert, die anschließend veröffentlicht und an die für die Thematik jeweils zuständigen Ministerien versandt werden.

Die im Berichtszeitraum verabschiedeten Entschließungen sind auf der Homepage der Dienststelle veröffentlicht:

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. Januar 2013:

- Beschäftigtendatenschutz nicht abbauen, sondern stärken!

Entschließungen der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13. und 14. März 2013 in Bremerhaven:

- Pseudonymisierung von Krebsregisterdaten verbessern

- Europa muss den Datenschutz stärken

- Soziale Netzwerke brauchen Leitplanken - Datenschutzbeauftragte legen Orientierungshilfe vor

- Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. September 2013:

- Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen

Entschließungen der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 1. und 2. Oktober 2013 in Bremen:

- Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!
- Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages
- Stärkung des Datenschutzes im Sozial- und Gesundheitswesen
- Sichere elektronische Kommunikation

Entschließungen der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. März 2014 in Hamburg:

- Beschäftigtendatenschutzgesetz jetzt!
- Entschließung zur Struktur der künftigen Datenschutzaufsicht in Europa (siehe auch Europa in diesem TB)
- Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke - Strenge Regeln erforderlich!
- Biometrische Gesichtserkennung durch Internetdienste - Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!
- Entschließung: Gewährleistung der Menschenrechte bei der elektrischen Kommunikation
- Anlage zur Entschließung: Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

Entschließungen der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014 in Hamburg:

- Effektive Kontrolle der Nachrichtendienste herstellen!
- Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar
- Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen
- Datenschutz im Kraftfahrzeug
- Marktmacht und informationelle Selbstbestimmung

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014:

- Keine PKW-Maut auf Kosten des Datenschutzes!

Düsseldorfer Kreis

Der Düsseldorfer Kreis ist ein privilegierter Arbeitskreis der Datenschutzkonferenz mit eigenen Beschlüssen aus dem Bereich des Bundesdatenschutzgesetzes mit sechs Unterarbeitskreisen. Der Vorsitz wird vom Landesbeauftragten für Datenschutz Nordrhein-Westfalen geführt.

Ziel des Düsseldorfer Kreises ist die bundesweit einheitliche Auslegung des geltenden Rechts im nicht-öffentlichen Bereich in wesentlichen Fragen des Datenschutzes 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. Hier die Themen der wichtigsten Entscheidungen:

Beschlüsse aus dem Jahr 2013:

- Datenübermittlung in Drittstaaten erfordert zwei Stufen
- Videoüberwachung in und an Taxis

Beschlüsse aus dem Jahr 2014:

- Smartes Fernsehen nur mit smartem Datenschutz
- Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)
- Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden

Orientierungshilfen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschließt darüber hinaus in unregelmäßigen Abständen Orientierungshilfen zu verschiedenen Themen, die jeweils von unterschiedlichen und teils mehreren Arbeitskreisen in bundesweiten Tagungen erarbeitet und vorbereitet werden. Den vollen Text der Orientierungshilfen finden Sie auf unserer Homepage, unter: *www.datenschutz.saarland.de*

Im Berichtszeitraum sind neu veröffentlicht worden:

Orientierungshilfe Soziale Netzwerke

Ziel dieser Orientierungshilfe ist es, neben der Konkretisierung der gesetzlichen Mindeststandards auch Best-Practice-Ansätze aufzuzeigen. Sie reflektiert das Verständnis der Datenschutzbeauftragten und Aufsichtsbehörden bei der Verwendung sozialer Netzwerke zur Erfüllung eigener Aufgaben oder Geschäftszwecke.

Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter

Die Orientierungshilfe richtet sich an Entwickler und Anbieter mobiler Applikationen (Apps). Sie zeigt datenschutzrechtliche und technische Anforderungen auf und macht diese anhand plakativer Beispiele verständlich.

Orientierungshilfe – Cloud Computing

Die Datenschutzbeauftragten des Bundes und der Länder beschäftigen sich bereits seit längerer Zeit mit der Thematik des Cloud Computing. Da das Thema weiter an Aktualität gewonnen hat, wurde von den Arbeitskreisen Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises die Orientierungshilfe erarbeitet. Der Schwerpunkt liegt dabei auf Hinweisen bei der Nutzung von Cloud-Computing Diensten durch datenverarbeitende Stellen.

In diesem Tätigkeitsbericht finden Sie auch unter dem Kapitel Technisch-organisatorischer Datenschutz eine Zusammenfassung für den Praktiker.

Orientierungshilfe zur "Einholung von Selbstauskünften bei Mietinteressenten"

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten zum Teil sehr umfangreiche persönliche Angaben, auf deren Basis sie ihre Entscheidung über den Vertragsabschluss treffen. An der Beantwortung solcher Selbstauskünfte muss der Vermieter jedoch ein berechtigtes Interesse haben und es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Die Aufsichtsbehörden für den Datenschutz haben in der Orientierungshilfe die wichtigsten Grundsätze aufgezeigt.

Orientierungshilfe der Datenschutzaufsichtsbehörden für den Umgang mit Verhaltensregeln nach § 38a BDSG

Verhaltensregeln dienen dem präventiven Datenschutz und der regulierten Selbstregulierung der Wirtschaft. Für den Umgang mit datenschutzrechtlichen Verhaltensregeln (auch CoC - Code of Conduct ge-

nannt) gilt § 38a BDSG, der die Regelung in Art. 27 der Europäischen Datenschutzrichtlinie (95/46/EG) in nationales Recht umsetzt.

Verhaltensregeln können gesetzliche Regeln nicht ersetzen oder verdrängen, sollen aber diese konkretisieren (Durchführung) und im Hinblick auf den Datenschutz verbessern (Förderung). Kommt es trotz positiver Überprüfung einer Aufsichtsbehörde (Anerkennung) zu einem Widerspruch zwischen gesetzlicher Regelung und Verhaltensregel geht das Gesetz vor.

Um die Voraussetzungen dafür zu schaffen, die Wirtschaft zu motivieren, sich datenschutzrechtliche Verhaltensregeln zu geben, die im Interesse aller zu mehr Rechtssicherheit führen können, haben die Aufsichtsbehörden die Orientierungshilfe erstellt.

Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen"

Die seitens des Gesetzgebers vorgegebenen Anforderungen an den datenschutzkonformen Betrieb einer Videoüberwachungsmaßnahme machen vor deren Einsatz somit teils komplexe Vorüberlegungen erforderlich. Zudem sind flankierende technische und organisatorische Maßnahmen umzusetzen.

Die Orientierungshilfe soll darüber informieren, unter welchen Voraussetzungen eine Videoüberwachung zulässig ist und welche gesetzlichen Vorgaben dabei einzuhalten sind.

Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke

Der Düsseldorfer Kreis hat eine Ad-hoc-Arbeitsgruppe „Werbung und Adresshandel" unter Leitung des Bayerischen Landesamts für Datenschutzaufsicht eingerichtet und diese mit der Erarbeitung von Anwendungshinweisen zu den BDSG-Regelungen für den werblichen Umgang mit personenbezogenen Daten beauftragt. In mehreren Sitzungen wurden Anwendungshinweise formuliert, die in diesem Dokument abgedruckt und als beschlossen anzusehen sind.

Orientierungshilfe Krankenhausinformationssysteme in der zweiten Fassung

Diese Orientierungshilfe soll es Betreibern und Herstellern von Krankenhausinformationssystemen erleichtern, den gesetzlichen Anforderungen und den gerechtfertigten Erwartungen der Patienten im komplexen System Krankenhaus gerecht zu werden.

Mit der vorliegenden, überarbeiteten Fassung der Orientierungshilfe werden keine neuen Themenbereiche erschlossen oder die Anforderungen der Ursprungsfassung revidiert. Vielmehr soll den Herstellern und Betreibern von Krankenhausinformationssystemen eine für die Praxis besser handhabbare Handreichung für die datenschutzgerechte Gestaltung und Nutzung von Krankenhausinformationssystemen geboten werden.

Datenschutzrechtliche Leitlinien mit Mindestanforderungen für die Ausgestaltung und den Betrieb von Arztbewertungsportalen im Internet

Mangels bestehender bereichsspezifischer Regelungen zur Ausgestaltung und zum Betrieb von Bewertungsportalen müssen die einzuhaltenden Anforderungen des Datenschutzes aus den allgemeinen Bestimmungen der §§ 27 ff. BDSG sowie der in diesem Zusammenhang ergangenen Rechtsprechung abgeleitet werden.

Mit der vorliegenden Handreichung werden die aus Sicht der Datenschutzaufsicht grundsätzlich zu beachtenden Mindestvoraussetzungen für eine datenschutzgerechte Errichtung und den Betrieb derartiger Bewertungsportale zusammengefasst und konkretisiert. Die Darstellung soll den Portalbetreibern, den Nutzern und den Bewerteten eine allgemeine Orientierung für den in diesem Zusammenhang regelmäßig zur Verfügung stehenden Gestaltungsspielraum geben. Unabhängig davon obliegt die datenschutzrechtlich verbindliche Bewertung einzelner Bewertungsportale auch weiterhin der im Einzelfall zuständigen Datenschutzaufsicht.

25.2.2 Zusammenarbeit in der Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder

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

Die Konferenz selbst tagt grundsätzlich 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.

Im Jahr 2013 tagte die Konferenz der Informationsfreiheitsbeauftragten unter dem Vorsitz des Informationsfreiheitsbeauftragten aus Thüringen und im Jahre 2014 lag der Vorsitz bei Hamburg.

In den Bundesländern Bayern, Baden-Württemberg, Hessen und Niedersachsen und Sachsen gibt es bisher kein Gesetz zur Informationsfreiheit und damit auch keine Beauftragten (Im Saarland ist das Informationsfreiheitsgesetz des Landes im Jahre 2006 verabschiedet worden und in Kraft getreten)

In der Anlage sind die Entschließungen der Informationsfreiheitsbeauftragten aus dem Berichtszeitraum beigefügt.

Hier die Themen:

26. Konferenz der Informationsfreiheitsbeauftragten vom 28. Juni 2013

- "Open Data stärkt die Informationsfreiheit - sie ist eine Investition in die Zukunft!"

- "Transparenz bei Sicherheitsbehörden"
- "Verbraucher durch mehr Transparenz im Lebensmittelbereich schützen - Veröffentlichungspflichten für Hygieneverstöße jetzt nachbessern!"

27. Konferenz der Informationsfreiheitsbeauftragten vom 28. November 2013

- Forderungen für die neue Legislaturperiode: Informationsrechte der Bürgerinnen und Bürger stärken!

28. Konferenz der Informationsfreiheitsbeauftragten vom 17. Juni 2014

- Das Urheberrecht dient nicht der Geheimhaltung
- Keine Flucht ins Privatrecht
- Informationsfreiheit nicht Privaten überlassen

29. Konferenz der Informationsfreiheitsbeauftragten vom 9. Dezember 2014

- Transparenz bei Ermittlungsmethoden
- Unabhängige Informationsfreiheitsaufsicht unabdingbar
- Open Data als Standard

25.2.3 Zusammenarbeit auf Landesebene

Auf Landesebene findet ein regelmäßiger Erfahrungsaustausch mit dem Arbeitskreis Datenschutz von BEST - Beratungsstelle für sozialverträgliche Technologiegestaltung e.V. der Arbeitskammer.

Ebenso sind wir in der Arbeitsgemeinschaft Medienkompetenz vernetzt.

Ständige Mitglieder sind:

- das Landesinstitut für Pädagogik und Medien (LPM),
- das Landesinstitut für Präventives Handeln (LPH),
- das Landespolizeipräsidium,
- das Unabhängige Datenschutzzentrum (UDZ),
- die Landesmedienanstalt Saarland (LMS),
- der Jugendserver-Saar sowie
- die Europäische EDV-Akademie des Rechts (EEAR).

Die Arbeitsgemeinschaft hat im Jahr 2014 auch den 1. Saarländischen Medientag ausgerichtet.

25.3 Öffentlichkeitsarbeit

Die Öffentlichkeitsarbeit ist im Berichtszeitraum weiter ausgebaut worden. Dies ist unabdingbar, da nur durch Information über die Gefahren für die Privatsphäre ein möglichst hoher Schutz erreicht werden kann.

In Zeiten der Digitalisierung des Alltages und der Vernetzung im Internet besteht die Notwendigkeit über aktuelle datenschutzrechtliche Themen breit zu informieren da vielen Menschen die Risiken unbekannt sind.

Der Schwerpunkt lag im Berichtszeitraum im Schulbereich mit den Workshops für Schüler zum Thema: „Datenverantwortung und Datenschutz"

Angesichts der zunehmenden Nutzung von Web 2.0-Angeboten wie Facebook, Google+, Twitter, Wikis, usw. geht es darum, junge Menschen möglichst frühzeitig das Basiswissen zum Thema Privatsphäre zu vermitteln.

Wir konnten unsere Workshops auch in den Schulleiterbesprechungen im Landkreis Merzig, St. Wendel und im Saarpfalz-Kreis vorstellen.

Die Workshops werden an den 6. Klassen der weiterführenden Schulen angeboten.

Vom Oktober 2013 bis zum Dezember 2014 konnten wir in 135 Schulklassen die Grundlagen zum Datenschutz vermitteln. Einen ausführlichen Bericht zu diesem Thema können Sie in dem Bereich Schule und Bildung in diesem Tätigkeitsbericht nachlesen.

25.3.1 Vorträge

Ein Mitarbeiter hält regelmäßig Vorträge an der Verwaltungsschule, auch an der Sparkassenakademie finden jährlich Vorträge zu aktuellen datenschutzrechtlichen Themen statt.

Darüber hinaus haben wir an einer Vielzahl von Veranstaltungen zu unterschiedlichen Themen vortragen dürfen.

So haben wir in weiteren 20 Veranstaltungen vor Eltern, Lehrern, Organisationen und saarländischen Einrichtungen neben allgemeinen Datenschutzthemen und Vorstellungen des Unabhängigen Datenschutzzentrums folgende Vorträge halten:

- Facebook und Co - wo bleibt der Datenschutz
- Fachtagung für Staatsanwälte und Strafrichter zum Thema Telemedien
- Datenschutz in Medien und im Bereich Bildung

- Sichere Wege im Internet
- Daten in der Wolke
- Datenschutz bei Smartphones und Tablets
- Videoüberwachung im öffentlichen Raum
- Smart(er) fernsehen
- Alles was Recht ist; Datenschutz in der Schule
- Datenschutz bei Gesundheitsdaten

25.3.2 Fortbildungen für Unternehmen zusammen mit der IHK

Durch die Unterstützung seitens der IHK konnten wir auch drei gemeinsame Veranstaltungen für Unternehmen und deren betriebliche Datenschutzbeauftragte im Berichtszeitraum anbieten:

- Datenschutzkonforme Ausgestaltung der Internetseiten – datenschutzrechtliche Anforderungen an Telemedien,
- Betrieblicher Datenschutzbeauftragter und seine Aufgaben,
- Datensicherheit im Betrieb – „die Hacker kommen".

25.3.3 Umbau der Homepage zum Informationsmedium

Zur Unterstützung der Öffentlichkeitsarbeit unserer Dienststelle wurde die Webseite des Unabhängigen Datenschutzzentrums optisch und inhaltlich überarbeitet sowie technisch modernisiert. Das Herz der neuen Webseite bildet das freie Content-Management-Framework Typo3, das wegen seiner Flexibilität, seines Funktionsumfangs und seiner Erweiterbarkeit die erste Wahl war.

Aus Datenschutz- und Datensicherheitsgründen ist die Webseite jetzt nur noch über https, also mittels Transportverschlüsselung, erreichbar. Alle Besucher werden bei Aufruf der Webseite automatisch auf die verschlüsselte Variante umgeleitet.

Neue Wege sind wir bei den Kommunikationsmöglichkeiten mit unserer Dienststelle über die Webseite gegangen. Wie die anderen Datenschutzbeauftragten (Bund und Länder) auch, bieten wir ein Kontaktformular auf unserer Webseite an, mit dem Besucher der Webseite unmittelbar mit uns in Kontakt treten können. Neu ist jedoch, dass wir – um die Hürden für die Besucher so gering wie möglich zu halten und gleichzeitig auch sensibelste Eingaben der Nutzer gegen unbefugte Kenntnisnahme Dritter zu schützen – das Kontaktformular um eine Möglichkeit zur asymmetrischen Verschlüsselung ergänzt haben. Das bedeutet, dass die Eingaben des Nutzers noch vor dem Absenden im Browser auf dem Gerät des Nutzers mit dem öffentlichen PGP-Schlüssel

unserer Dienststelle verschlüsselt werden und dann erst - zusätzlich mittels Transportverschlüsselung gesichert - auf den Weg gebracht werden um so den größtmöglichen Schutz der Eingaben des Besuchers zu gewährleisten. So asymmetrisch verschlüsselte Nachrichten können nur von unserer Dienststelle gelesen werden, was bei einer reinen Transportverschlüsselung nicht in jedem Fall gewährleistet ist. Da die asymmetrische Verschlüsselung der Eingaben jedoch nicht von älteren Browsern unterstützt wird, prüft das System bereits beim Aufruf des Kontaktformulars ob eine verschlüsselte Kommunikation im Endgerät des Nutzers technisch möglich ist und informiert den Nutzer bei Bedarf durch eine Ampellogik (rot, gelb, grün) und aussagekräftige Hinweise.

25.3.4 Flyer, Poster und Merkblätter

Im Berichtszeitraum wurden versucht durch verschiedene Flyer und Poster zu unterschiedlichen Themen auf die Datenschutz- und Datensicherheitsthemen aufmerksam zu machen.

Beispielhaft sei hier verwiesen auf ein Poster für Schüler, dass an alle weiterführenden Schulen versandt wurde, und eine Weihnachtsgrußkarte die auf Datensicherheitsthemen hinwies und eine zusätzliche Karte mit Hinweisen zur Browsersicherheit beinhaltete.

Im Berichtszeitraum wurden auch die Merkblätter

- zum datenschutzkonformen Einsatz von Tierbeobachtungskameras in saarländischen Wäldern und das
- Merkblatt zur Videoüberwachung durch nicht öffentliche Stellen vorgestellt.

25.3.5 Tätigkeitsbericht

Ein wesentlicher Teil unserer Öffentlichkeitsarbeit ist auch dieser Tätigkeitsbericht, der sowohl der Sensibilisierung der Allgemeinheit aber auch dem Vorbeugen vor weiteren Verstößen dient.

Nur wer weiß was datenschutzrechtlich zulässig ist, kann sein Verhalten auch darauf einstellen.

Nur wer weiß, dass er sich vor Angriffen seiner Privatsphäre schützen kann, findet auch die richtigen Werkzeuge hierzu.

26 Beschlüsse des Düsseldorfer Kreises

26.1 Videoüberwachung in und an Taxis

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 26./27. Februar 2013)

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 § 6 b 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.

26.2 Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

Beschluss der Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich (Düsseldorfer Kreis am 11./12. September 2013)

Bei Datenübermittlungen in einen Drittstaat, also einen Staat außerhalb des Europäischen Wirtschaftsraums, sind Datenschutzfragen auf zwei Stufen zu prüfen:

Auf der ersten Stufe ist es erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (z.B. §§ 28 und 32 Bundesdatenschutzgesetz (BDSG)) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Abs. 1 BDSG zulässig sein muss (vgl. § 3 Abs. 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfungs-

maßstab in der Regel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, bei sensitiven Daten ist § 28 Abs. 6 ff. BDSG zu beachten.

Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4c BDSG vorliegen.

Die Datenübermittlung ist nur zulässig, wenn auf beiden Stufen ein positives Prüfungsergebnis vorliegt.

26.3 Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“

Beschluss der Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich (Düsseldorfer Kreis am 27. Januar 2014)

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten zum Teil sehr umfangreiche persönliche Angaben, auf deren Basis sie ihre Entscheidung über den Vertragsabschluss treffen. An der Beantwortung solcher Selbstauskünfte muss der Vermieter jedoch ein berechtigtes Interesse haben und es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Die legitimerweise zu stellenden Fragen basieren folglich auf einer Abwägung der Interessen des Vermieters gegenüber dem Recht des Mietinteressenten auf informationelle Selbstbestimmung.

Die Orientierungshilfe "Einholung von Selbstauskünften bei Mietinteressenten" zeigt die wichtigsten Grundsätze auf. Für häufige Fallgestaltungen wird – ohne Anspruch auf Vollständigkeit – dargestellt, was zulässig ist.

26.4 Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden

Beschluss der Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich (Düsseldorfer Kreis am 25./26. Februar 2014)

I. Ausgangslage

Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen.

Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.

Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbraucher in den achtsamen Umgang mit ihren Daten zu fördern.

Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.

Der Ruf nach einem Audit hat im Zuge der Diskussion um den Europäischen Rechtsrahmen weiteren Auftrieb erhalten. Initiativen auf Landesebene und nunmehr auch auf Bundesebene haben dieses Anliegen aufgegriffen.

II. Erprobung von Modellen, Anforderungen

Die Gesetzgeber haben bisher lediglich einzelne Teilregelungen zu Zertifizierungen getroffen.

Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in Eigener Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten.

Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und organisatorische Vorkehrungen für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.

Dazu gehören im Kern folgende, von Zertifizierungsdiensten zu bearbeitende Strukturelemente:

- Prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,

- beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),

- für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,

- Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,

- Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,

- den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne weiteres dem Zertifikat entnehmen können,

- Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,

- Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

III. Abstimmung im Düsseldorfer Kreis

Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen.

Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Beratungsersuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.

26.5 Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 25./26. Februar 2014)

Mittlerweile nimmt der Einsatz sog. Dashcams auch in Deutschland immer mehr zu, um, so die standardmäßige Begründung, im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können.

Die Aufsichtsbehörden des Bundes und der Länder für den Datenschutz im nicht-öffentlichen Bereich machen darauf aufmerksam, dass der Einsatz solcher Kameras - jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt - datenschutzrechtlich unzulässig ist.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an den Regelungen des Bundesdatenschutzgesetzes zu messen. Gemäß § 6b Abs. 1 Nr. 3 und Abs. 3 des Bundesdatenschutzgesetzes (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.

Diese Voraussetzungen sind in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der Verkehrsteilnehmer überwiegen. Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dashcams zeichnen den Verkehr sowie Personen, die sich in

der Nähe einer Straße aufhalten, ohne Anlass und permanent auf, so dass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht sonstige Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlass- und schrankenlos mittels Kameras zu überwachen.

26.6 Smartes Fernsehen nur mit smartem Datenschutz

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis im Mai 2014)

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals u. a. die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauern ist es somit möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internet-Dienste an. Für die Zuschauer ist aufgrund der Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich handelt.

Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus datenschutzrechtlicher Sicht sind die folgenden Anforderungen zu beachten:

1. Die anonyme Nutzung von Fernsehangeboten muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.

2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als Telemedien den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:

    - Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.

    - Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und –verwendung informiert werden.

    - Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat. Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z.B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.

    - Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammen geführt werden.

3. Beachtung des Prinzips „privacy by default“: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z. B. die Red-Button-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.

4. Smart-TV-Geräte, die HbbTV- Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Diese Position wird von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt.

27 Internationale Konferenz der Datenschutzbeauftragten

27.1 Entschließung zu Big Data

36. Konferenz vom 13. – 16. Oktober 2014, in Balaclava

Es wird häufig anerkannt, dass die Möglichkeit zur Speicherung und Analyse riesige Mengen von Daten sich für die Gesellschaft als vorteilhaft erweisen kann. So kann Big Data z.B. genutzt werden, um die Ausbreitung von Epidemien vorherzusagen, gravierende Nebenwirkungen von Medikamenten aufzudecken und die Verschmutzung in großen Städten zu bekämpfen. Einige dieser Nutzungen beinhalten keine Verwendung personenbezogener Daten; Big Data kann jedoch auch in einer Art genutzt werden, die zu gravierenden Besorgnissen in Bezug auf die Privatsphäre des Individuums und auf Bürgerrechte, den Schutz gegen Diskriminierungen und Beschränkungen des Rechts auf Gleichbehandlung führt.

Big Data bedingt einen neuen Blick auf Daten, mit dem Informationen sichtbar werden, die vorher nur schwer zu gewinnen oder in anderer Weise verschleiert waren. Big Data beinhaltet in großem Ausmaß die Wiederverwendung von Daten. Der Wert der Daten kann mit der Möglichkeit verbunden sein, Vorhersagen über zukünftige Handlungen oder Ereignisse zu treffen. Big Data kann als Herausforderung für wesentliche Grundsätze des Schutzes der Privatsphäre, insbesondere für die Prinzipien der Zweckbindung und der Datenminimierung angesehen werden. Der Schutz, den diese Datenschutzprinzipien gewähren, ist wichtiger als je zuvor in einer Zeit, in der ein zunehmendes Ausmaß von Daten über jedermann gesammelt wird. Die Prinzipien stellen das Fundament für Schutzmaßnahmen dar gegen eine extensive Profilbildung in einer immer weiter zunehmenden Reihe von neuen Zusammenhängen. Eine Verwässerung grundlegender Datenschutzprinzipien in Kombination mit einer extensiveren Nutzung von Big Data wird sich aller Voraussicht nach nachteilig auf den Schutz der Privatsphäre und anderer Grundrechte auswirken.

Mitglieder der Internationalen Konferenz und andere Interessenvertreter wie z.B. die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (IWGDPT, auch bekannt als "Berlin Group") haben sich mit Fragen des Datenschutzes und des Schutzes der Privatsphäre im Zusammenhang mit Big Data auseinandergesetzt. Datenschutzbedenken im Hinblick auf die Nutzung von Profilbildung sind von der Internationalen Konferenz in der Uruguayer Erklärung von 2012 und in der Warschauer Erklärung zur Profilbildung von 2013 aufgeworfen worden. Um weitere Anstrengungen zur Reduzierung von Risiken bei der Verwendung von Big Data zu befördern, fordert die 36. Internationale Konferenz der Datenschutzbeauftragten alle Parteien auf, die Big Data verwenden,

- Den Grundsatz der Zweckbindung zu respektieren.

- Das Ausmaß der Datenerhebung und -speicherung auf das für den beabsichtigten, rechtmäßigen Zweck notwendige Maß zu beschränken.

- Eine rechtsgültige Einwilligung von den Betroffenen im Zusammenhang mit der Nutzung personenbezogener Daten für Zwecke der Analyse und Profilbildung einzuholen, wo dies angemessen ist.

- Transparent zu machen, welche Daten erhoben werden, wie die Daten verarbeitet werden, für welche Zwecke sie genutzt werden und ob die Daten an Dritte übermittelt werden oder nicht.

- Den Betroffenen angemessene Auskunft über die über sie gespeicherten Daten und über Informationen und sie betreffende Entscheidungen zu geben. Betroffene sollen auch über die Quellen der verschiedenen personenbezogenen Daten informiert werden und, wo dies angemessen ist, berechtigt sein, ihre Daten zu berichtigen und effektive Werkzeuge zu deren Kontrolle zu erhalten.

- Wo dies angemessen ist, den Betroffenen Auskunft über die wichtigen Faktoren und Kriterien für Entscheidungen (Algorithmen) zu gewähren, die als Basis für die Entwicklung des Profils genutzt wurden. Solche Informationen sollten in einem klaren und verständlichen Format dargestellt werden.

- Eine Vorabkontrolle (Privacy Impact Assessment) ist durchzuführen, besonders, wenn die Analyse von Big Data eine neue oder unerwartete Nutzung personenbezogener Daten beinhaltet.

- Big Data-Technologien nach den Prinzipien des "Privacy by Design" zu entwickeln und zu nutzen.

- Zu prüfen, wo die Nutzung anonymisierter Daten den Schutz der Privatsphäre verbessern kann. Anonymisierung kann bei der Bewältigung der Risiken für die Privatsphäre helfen, die mit Big Data-Analysen zusammenhängen, aber nur, wenn die Anonymisierung angemessen entwickelt und gehandhabt wird. Über die optimale Lösung zur Anonymisierung der Daten sollte fallweise entschieden werden, möglicherweise durch Kombination verschiedener Techniken.

- Bei der Weitergabe oder Publikation pseudonymisierter oder in anderer Weise indirekt identifizierbarer Datensätze große Vorsicht walten zu lassen und in Übereinstimmung mit dem anwendbaren Datenschutzrecht zu handeln. Wenn die Daten hinreichend Details enthalten, mit anderen Datensätzen verknüpft werden können oder personenbezogene Daten enthalten, sollte der Zugang beschränkt und kontrolliert werden.

- Nachzuweisen, dass Entscheidungen über die Nutzung von Big Data fair, transparent und verantwortlich sind. Im Zusammenhang mit der Nutzung von Daten für Profilbildungs-

zwecke erfordern sowohl die Profile als auch die zugrundeliegenden Algorithmen ständige Überprüfung. Dies verlangt regelmäßige Untersuchungen, um nachzuweisen, ob die Ergebnisse der Profilbildung verantwortlich, fair und ethisch und vereinbar und proportional zu den Zwecken sind, für die die Profile genutzt werden. Ungerechtigkeiten für Betroffene aufgrund vollautomatischer falsch-positiver oder falsch-negativer Ergebnisse sollten vermieden werden und es sollte stets eine manuelle Überprüfung von Ergebnissen mit signifikanten Auswirkungen auf Betroffene verfügbar sein.

27.2 Erklärung zum Internet der Dinge

Balaclava - 14. Oktober 2014

Das Internet der Dinge wird bleiben. Immer mehr Gegenstände sind mit dem Internet verbunden und in der Lage, miteinander zu kommunizieren, manchmal ohne dass die Nutzenden dies bemerken. Diese Gegenstände können unser Leben sehr viel einfacher machen. Zum Beispiel bei der Gesundheitsversorgung, beim Transport oder der Energieversorgung können die verbundenen Gegenstände die Art und Weise verändern, mit der wir etwas erledigen. Das Internet der Dinge kann allerdings auch intime Details über das Handeln und die Bewegungen der Eigentümer von Gegenständen mithilfe der in ihnen enthaltenen Sensoren offenbaren.

Selbstbestimmung ist ein unveräußerliches Recht aller Menschen. Die persönliche Entwicklung sollte nicht dadurch festgelegt werden, was Unternehmen und Regierungen über den Einzelnen wissen. Die Ausbreitung des Internets der Dinge vergrößert allerdings das Risiko, dass dies geschehen wird. Die versammelten Beauftragten für Datenschutz und Privatsphäre haben deshalb die Möglichkeiten des Internets der Dinge und seine Konsequenzen während der 36. Internationalen Datenschutzkonferenz diskutiert, die in Balaclava, Mauritius am 13./14. Oktober 2014 stattfand. Vier Redner, die sowohl den wirtschaftlichen Sektor als auch die Wissenschaft repräsentierten, stellten den Beauftragten die positiven Veränderungen wie auch die Risiken vor, die das Internet der Dinge in unser tägliches Leben bringen kann. Die Redner gaben außerdem einen Überblick darüber, was getan werden muss, um den weiteren Schutz unserer personenbezogenen Daten wie auch unseres Privatlebens sicherzustellen.

Die anschließende Diskussion führte zu den folgenden Empfehlungen:

- Die beim Internet der Dinge verwendeten Sensoren erzeugen Daten in hoher Quantität, Qualität und Sensitivität. Dies bedeutet, dass sehr viel weiterreichende und sensitivere Folgerungen gezogen werden können und die Herstellung eines Personenbezugs wahrscheinlicher ist als dessen Vermeidung. Angesichts der Tatsache, dass die Personenbeziehbarkeit und der Datenschutz im Zusammenhang mit “Big Data” an sich schon eine große Herausforderung sind, ist es deutlich, dass Datenmengen, die von Gegenständen im Internet der Dinge gewonnen werden, diese Herausforderungen um

ein Vielfaches vergrößern. Deshalb sollten solche Daten als personenbezogen angesehen werden.

- Obwohl für viele Unternehmen das Geschäftsmodell noch unbekannt ist, liegt der Wert des Internets der Dinge eindeutig nicht nur in den Geräten selbst. Das finanzielle Interesse liegt in den neuen Diensten im Zusammenhang mit dem Internet der Dinge und in den Daten.

- Jeder, der heute lebt, wird erkennen, dass Konnektivität allgegenwärtig ist. Dies mag noch mehr der Fall sein für die junge und zukünftige Generation, die sich keine Welt ohne Vernetzung vorstellen können. Es sollte aber nicht allein ihre Aufgabe sein, ob ihre Daten geschützt werden oder nicht. Es ist eine gemeinsame Verantwortung aller Handelnden in der Gesellschaft, damit das Vertrauen in vernetzte Systeme aufrechterhalten werden kann. Dafür ist Transparenz von entscheidender Bedeutung: Wer Dienstleistungen im Internet der Dinge anbietet, sollte klar sagen, welche Daten er sammelt, für welche Zwecke und wie lange diese Daten gespeichert werden. Er sollte Überraschungen für Verbraucher ausschließen. Beim Kauf von Gegenständen des Internets der Dinge oder entsprechender Programme sollte eine angemessene ausreichende und verständliche Information zur Verfügung stehen. Gegenwärtige Datenschutzerklärungen vermitteln nicht immer die Information in einer klaren, verständlichen Weise. Einwilligungen, die auf der Basis solcher Datenschutzerklärungen erteilt werden, können kaum als informierte Einwilligungen angesehen werden. Unternehmen müssen ihre Herangehensweise grundlegend verändern, damit Datenschutzerklärungen nicht länger in erster Linie dem Zweck dienen, sie vor Klagen zu schützen.

- Die Datenverarbeitung beginnt in dem Moment der Datenerhebung. Alle Schutzmaßnahmen sollten ab diesem Zeitpunkt greifen. Wir ermutigen zur Entwicklung von Technologien, die neue Wege der Einbeziehung von Datenschutz und Verbraucherschutz von Anfang an ermöglichen. "Privacy by Design and Default" sollte nicht länger als etwas Abseitiges betrachtet werden. Beide Prinzipien sollten ein wesentliches Verkaufsargument für innovative Technologien werden.

- Das Internet der Dinge wirft auch wesentliche Sicherheitsrisiken auf, die beherrscht werden müssen. Eine einfache Firewall reicht längst nicht mehr aus. Ein Weg, um das Risiko für Betroffene zu begrenzen, liegt darin, dass man die Datenverarbeitung auf das Endgerät selbst beschränkt (lokale Verarbeitung). Wenn dies nicht möglich ist, sollten Unternehmen Ende-zu-Ende Verschlüsselung vorsehen, um die Daten vor ungerechtfertigter Einwirkung oder Manipulation zu schützen.

- Die Datenschutz- und Privatsphäre-Behörden werden weiterhin die Entwicklungen beim Internet der Dinge beobachten. Sie machen es sich zur Aufgabe, die Befolgung der Datenschutzgesetze in ihren jeweiligen Ländern sicherzustellen, ebenso wie die Einhaltung der international akzeptierten

Prinzipien. Wenn Rechtsverstöße festgestellt werden, werden sie angemessene Sanktionsmaßnahmen ergreifen, entweder einseitig oder durch internationale Zusammenarbeit.

- Angesichts der Herausforderungen, denen sich die Entwickler im Internet der Dinge, die Datenschutzbehörden und die Betroffenen gegenübersehen, sollten sich alle Beteiligten an einer starken, aktiven und konstruktiven Debatte zu den Konsequenzen des Internets der Dinge und der aus ihm gewonnen großen Datenmenge beteiligen, um das Bewusstsein für die zu treffenden Entscheidungen zu erhöhen.

28 Informationsfreiheitsgesetz

28.1 Informationszugang zu Akten des Ministeriums der Justiz

Ein Petent beantragte Informationszugang nach dem Saarländischen Informationsfreiheitsgesetz (SIFG) zu Akten, die über ihn beim Ministerium der Justiz geführt werden. Es handelte sich um Vorgänge, die sich mit der Ausübung des Rechts auf Leitung und Aufsicht durch das Justizministerium (§ 147 Gerichtsverfassungsgesetz (GVG)) über die Staatsanwaltschaft Saarbrücken, sowie mit der Ausübung der Dienstaufsicht (§ 13 Abs. 1 Nr. 1 Saarländisches Ausführungsgesetz zum GVG (SAG GVG)) über die Gerichte befassten. Das Ministerium lehnte den Antrag im Wesentlichen mit der Begründung ab, die Ausübung der Aufsicht über die Staatsanwaltschaft sei nicht Verwaltungstätigkeit, sondern vielmehr dem Bereich der Rechtsprechung zuzuordnen. Daher könne das SIFG schon keine Anwendung finden. Außerdem seien die Regelungen der Strafprozessordnung (StPO) als anwendungsvorrangige, abschließende Spezialvorschriften anzusehen sind. Ein Informationszugang wurde daher abgelehnt.

Der Petent legte daraufhin Widerspruch ein und bat uns, parallel zur Durchführung des Vorverfahrens, um Stellungnahme. Wir teilten sowohl dem Petenten als auch dem Ministerium der Justiz unsere Rechtsauffassung mit, nämlich, dass ein Zugang zu den begehrten Informationen zu gewähren sei.

Die vom Ministerium der Justiz vorgebrachten Argumente griffen unserer Auffassung nach im Ergebnis nicht durch. Entsprechend der Rechtsprechung des Bundesverwaltungsgerichts unterfällt die Aufsichtstätigkeit des Justizministeriums dem Bereich der öffentlichen Verwaltung und nicht der Judikative, mit der Folge, dass der Anwendungsbereich des SIFG hier eröffnet ist. Denn anders als der Bereich der Judikative deren Ziel die Rechtsfindung, Rechtsverwirklichung und Rechtsdurchsetzung ist, geht es bei der Aufsicht über die Staatsanwaltschaft darum die parlamentarische Verantwortung zu sichern. Und genau diesen Zweck, nämlich die Transparenz staatlichen Handelns zu gewährleisten, verfolgt auch das SIFG.

Auch konnten wir keinen Vorrang der Akteneinsichtsrechte nach §§ 147 Abs. 1 und 475 StPO erkennen. Nach unserer Auffassung fehlte es bereits an vergleichbaren, im Ausschließlichkeitsverhältnis stehenden Sachverhalten, da über die Akteneinsichtsgesuche nach StPO andere Stellen entscheiden als die Stelle, gegen die sich der vorliegende Informationsfreiheitsantrag richtete.

Nach Ablehnung des Widerspruchs durch das Ministerium der Justiz reichte der Petent Klage beim Verwaltungsgericht ein. Mit dem Urteil wurde ihm jedoch nur teilweise Zugang zu den begehrten Informationen gewährt.

Das Gericht bewertete die Berichtsvorgänge der Staatsanwaltschaft als materiell der Strafrechtspflege zuzuordnende Dokumente und nicht als

andere allgemeine Verwaltungsangelegenheiten. Die Fertigung der Berichte sei eine der Staatsanwaltschaft zugewiesene Aufgabe. Sie könne diese Aufgabe allein auf der Grundlage ihrer als Einrichtung der Strafrechtspflege gewonnenen Informationen wahrnehmen. Durch die Berichte solle die Landesjustizverwaltung in die Lage versetzt werden, den wesentlichen Gegenstand der Berichtssachen zu beurteilen und die ihr von Gesetzes wegen obliegende Aufsichts- und Leitungsfunktion wahr zu nehmen. Ein Akteneinsichtsrecht nach § 1 Satz 1 SIFG scheide aus, weil dem SIFG die abschließenden Regelungen der StPO zur Akteneinsicht vorgehen.

Zu den Akten, eine Dienstaufsichtsbeschwerde bzw. eine Zwangsvollstreckungsmaßnahme betreffend, erhält der Kläger Informationszugang, da es sich hierbei um Verwaltungsvorgänge handelt und Ausschlussgründe nicht geltend gemacht wurden.

Leider wurde das Verfahren durch den Kläger nicht weiterverfolgt. Wir hätten eine Entscheidung des Oberverwaltungsgerichts des Saarlandes begrüßt, da wir weiterhin der Ansicht sind, dass grundsätzlich auf der Grundlage des (S)IFG ein Zugang zu Berichtsakten beim Ministerium der Justiz besteht. Mittlerweile gibt es auch in der juristischen Literatur Stimmen, die im Ergebnis unsere Ansicht teilen (z.B. *Rixecker* in „Verborgene Räume der Strafaktenführung", Festschrift für Klaus Tolksdorf, 2014, Seite 365ff.).

28.2 Informationszugang zu einem Erschließungsvertrag

Ein großes Handelsunternehmen plante an seinem Stammsitz in einer saarländischen Kleinstadt umfangreiche Erweiterungsmaßnahmen. Auf der Basis eines Bebauungsplanes hatte die Stadt mit dem Handelsunternehmen einen Erschließungsvertrag geschlossen. Der Antrag eines Bürgers auf Informationszugang zu diesem Erschließungsvertrag wurde von der Stadt anfänglich weder beschieden noch wurde Informationszugang gewährt.

Der Bürger wandte sich mit einer Eingabe an uns. Anlässlich eines Termins bei der zuständigen unteren Bauaufsicht der Stadt erhielten wir Einblick in den Erschließungsvertrag. Es waren keinerlei Ausschlussgründe erkennbar und wir empfahlen, dem Antrag auf Informationszugang stattzugeben. Der für die Bearbeitung zuständigen Bauamtsleiter ließ allerdings erkennen, dass er dennoch den Antrag ablehnen werde. Im ablehnenden Bescheid waren die Ablehnungsgründe auf 35 Seiten dargestellt. Die Anwendbarkeit der Informationsfreiheitsgesetze auf Kommunen wurde grundsätzlich verneint. Als Ablehnungsgründe wurden unter anderem genannt:

- die Sperrwirkung des Kommunalrechts und weiterer öffentlich-rechtlicher Spezialvorschriften,

- wegen des gebotenen Schutzes der gemeindlichen städtebaulichen und verkehrlichen Entwicklungsinteressen,

- wegen des Schutzes der gemeindlichen Funktion, die in den kommunal verfassungsrechtlichen Organen manifestiert sind,

- wegen des gebotenen Schutzes der Standortinteressen des/der Unternehmen und der Gemeinde,

Das Unabhängige Datenschutzzentrum verfasste hierzu eine rechtliche Bewertung, in der die Ablehnungsgründe allesamt widerlegt wurden und stellte sie dem Antragsteller zur Verfügung. Diese wurde dann zur Basis des Widerspruchs, den der Antragsteller beim zuständigen Kreisrechtsausschuss einlegte.

Der Kreisrechtsausschuss gab dem Widerspruch in vollem Umfang statt und verpflichtete die Stadt, Zugang zum Erschließungsvertrag zu gewähren.

Damit wurde dargelegt, dass das Saarländische Informationsfreiheitsgesetz (SIFG) grundsätzlich auf Kommunen anwendbar ist. Weder im ablehnenden Bescheid der Kreisstadt noch vor dem Kreisrechtsausschuss wurden Gründe nach dem IFG substantiell angeführt, die dem Antragsteller den Zugang zum Erschließungsvertrag verwehren konnten. Insbesondere wurden durch das Handelsunternehmen auch keine schutzwürdigen Interessen vorgebracht.

Der Vorgang zeigt, dass es sich durchaus lohnen kann, das Recht auf Informationszugang zu verfolgen.

28.3 Anspruch auf Akteneinsicht in Disziplinarverfahren

Im Berichtszeitraum trat ein Petent, dessen Antrag auf Akteneinsicht im Zusammenhang mit einem Disziplinarverfahren gegen Beamte einer saarländischen Gemeinde abgelehnt wurde, an die Aufsichtsbehörde heran.

Aus Sicht der Aufsichtsbehörde stellte sich zunächst die Frage, ob der Petent als Betroffener einen Auskunftsanspruch über die zu seiner Person gespeicherten Daten nach den Regelungen des § 20 Saarländisches Datenschutzgesetz (SDSG) oder einen allgemeinen Informationsanspruch nach dem Saarländischen Informationsfreiheitsgesetz (SIFG) geltend machen wollte. Da der Petent daraufhin mitteilte, dass er Dienstaufsichtsbeschwerde bei einer Gemeinde gegen dessen Beschäftigte eingelegt hatte, demnach also keine eigene Betroffenheit vorlag, war der Anspruch auf der Grundlage des SIFG zu prüfen.

Diese Vorschrift räumt jedem einen voraussetzungslosen Anspruch gegenüber den Behörden des Landes, der Gemeinden und Gemeindeverbände auf Zugang zu amtlichen Informationen ein.

Dieser grundsätzliche Informationsanspruch wiederum wird durch die Ausnahmetatbestände gemäß § 1 S. 1 SIFG i. V. m. §§ 3 bis 6 und 9 Abs. 3 Informationsfreiheitsgesetz des Bundes (IFG-Bund) sowie § 2 SIFG eingeschränkt. Vorliegend war zu prüfen, ob der Schutz personenbezogener Daten i. S. d. § 5 IFG-Bund dem Informationsinteresse des Antragstellers entgegen stand.

Dabei ist im Rahmen der Prüfung der Informationsgewährung gemäß § 5 Abs. 1 S. 1 IFG-Bund eine Rechtsabwägung zwischen den Interessen des Beschwerdeführers und dem schutzwürdigen Interesse des Dritten, hier der Beschäftigten, am Ausschluss des Informationszugangs durch-

zuführen. Gemäß § 5 Abs. 2 IFG-Bund überwiegt das Interesse des Antragstellers nicht bei Informationen aus Unterlagen, soweit sie mit dem Dienst- oder Amtsverhältnis des Dritten in Zusammenhang stehen. Der Gesetzgeber geht davon aus, dass auch Akten aus Disziplinarverfahren, Arbeitsgerichtsprozessen und Beamtenrechtsprozessen geschützt sind. Hier war davon auszugehen, dass sowohl Akten aus dem Dienstaufsichtsverfahren als auch die Akten eines Disziplinarverfahrens durch § 5 Abs. 2 IFG-Bund geschützt sind und somit dem Informationsanspruch des Petenten entzogen waren.

Abschließend wurde dem Petenten mitgeteilt, dass ein Anspruch auf Zugang zu den gewünschten Informationen nach den Vorschriften der Informationsfreiheitsgesetze nicht bestand.

28.4 Informationszugang zu Telefonlisten

Der Informationszugang zu Telefonlisten von Behörden wird häufig begehrt, da die „Kunden" bestimmter Einrichtungen (Jobcenter, Finanzämter, etc.) gerne den direkten Kontakt zur zuständigen Stelle suchen und nicht mit einem Call-Center sprechen möchten. Bislang ist uns kein Fall bekannt geworden, dass Telefonlisten von saarländischen Behörden nicht herausgegeben wurden.

Es zeigt sich jedoch in der Rechtsprechung, dass ein Anspruch auf Informationszugang zu Telefonlisten nicht allgemein besteht.

Den Entscheidungen liegen geringfügig abweichende Sachverhalte zugrunde. Zum einen waren die Antragsteller Anwälte und begehrten Zugang zu Telefonlisten der Bearbeiter mit Außenkontakten (VG Aachen, 8 K 532/11 v. 17.7.2013; VG Gießen, 4 K 2911/13 v. 24.2.2014). Zum andern waren es Bürger, die eine komplette Telefonliste erhalten wollten (VG Ansbach, AN 4 K 13.01194 v.27.5.2014).

Im ersten Fall wurden dem Informationszugang entsprochen, im zweiten nicht. Nachfolgend eine Zusammenfassung der Begründungen:

Fall 1:

Bei den streitigen Telefonnummern handelt es sich um amtliche Informationen. § 2 Nr. 1 IFG-Bund enthält keine Einschränkung des Informationszugangs auf einen konkreten Verwaltungsvorgang.

Telefonlisten kommen einem Organisationsplan gleich. Name, Titel, akademischer Grad, Berufs- und Funktionsbezeichnung, Büroanschrift und Bürotelekommunikationsnummer von Behördenmitarbeitern sind vom Informationszugang nicht ausgeschlossen, soweit sie Ausdruck und Folge der amtlichen Tätigkeit sind und kein Ausnahmetatbestand erfüllt ist. Der Ausnahmetatbestand des § 5 Abs. 1 IFG-Bund gilt nicht für Amtsträger, soweit es um die Weitergabe von Daten geht, die sich auf ihre Amtsträgerfunktion beziehen (§ 5 Abs. 4 IFG-Bund).

Fall 2:

Es werden Zweifel gehegt, ob Telefonlisten amtliche Informationen sind, da der Zugang zu amtlichen Informationen nur im Rahmen eines konkreten Vorgangs zu gewähren ist (lt. Gesetzesbegründung). Telefonlisten seien keinem konkreten Vorgang zugeordnet.

Selbst wenn man annehmen würde, dass es sich um amtliche Informationen handeln würde, gelte der Ausnahmetatbestand des § 5 Absatz 1 IFG-Bund (Schutz personenbezogener Daten) und es sei eine Interessenabwägung vorzunehmen. Ein Fall des § 5 Abs. 4 IFG-Bund liege nicht vor, da der Bezug zu einem konkreten Vorgang fehle. Der Gesetzgeber habe den Begriff „Bearbeiter" gewählt um die Beschäftigung mit einem Vorgang zu implizieren.

Diese Entscheidungen machen es uns nicht leichter, Empfehlungen allgemeiner Art zu geben. Sie zeigen uns, dass die Gerichte in der Betrachtung selbst gleichartiger Sachverhalte zu unterschiedlichen Ergebnissen kommen können. Im Resultat ergibt sich für uns die Notwendigkeit, jede Anfrage einer Einzelfallbetrachtung zu unterziehen, um zu einer ausgewogenen Entscheidung zu gelangen.

29 Entschließungen der IFK

29.1 Für einen effektiven presserechtlichen Auskunftsanspruch gegenüber allen Behörden – auch des Bundes

27. Juni 2013

Das Bundesverwaltungsgericht hat mit Urteil vom 20. Februar 2013 entschieden, dass die Pressegesetze der Länder keine Verpflichtung von Bundesbehörden zur Auskunftserteilung an Journalistinnen und Journalisten begründen. Die Gesetzgebungskompetenz für den presserechtlichen Auskunftsanspruch gegenüber Bundesbehörden liege danach beim Bund. Eine entsprechende Auskunftsverpflichtung existiert bislang nicht. Das Bundesverwaltungsgericht sieht einen unmittelbar aus der Garantie der Pressefreiheit abgeleiteten „Minimalstandard von Auskunftspflichten" und einen einklagbaren, ebenfalls unmittelbar aus Art. 5 Abs. 1 Satz 2 GG abgeleiteten Rechtsanspruch auf Auskunft, soweit dem nicht berechtigte schutzwürdige Vertraulichkeitsinteressen von Privatpersonen oder öffentlichen Stellen entgegenstehen. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland begrüßt die Entscheidung des Bundesverwaltungsgerichtes insofern, als damit der Auskunftsanspruch von Journalistinnen und Journalisten grundrechtlich abgeleitet und abgesichert wird.

Aus Sicht der Konferenz gilt es - unabhängig von der kontrovers diskutierten Regelungszuständigkeit - die notwendigen gesetzlichen Grundlagen für eine effektive journalistische Recherche herzustellen, die eine zeitnahe, aktuelle und profunde Berichterstattung ohne abschreckende Kostenhürden möglich machen. Das Urteil, das einen unscharfen, beliebig interpretierbaren Minimalstandard mit unklaren Grenzen und Beschränkungsmöglichkeiten zugesteht, darf hier jedenfalls nicht das letzte Wort sein! Bundesbehörden müssen denselben Auskunftspflichten unterliegen wie Landesbehörden.

29.2 Open Data stärkt die Informationsfreiheit – sie ist eine Investition in die Zukunft!

27. Juni 2013

Die gesellschaftlichen Erwartungen an einen transparenten Staat gehen inzwischen weit über das bisherige Recht der Bürgerinnen und Bürger, einen Antrag auf Informationszugang zu stellen, hinaus. Open Data – also die aktive Bereitstellung öffentlicher Informationen im Internet – wird auf den ersten Portalen bereits praktiziert. Zahlreiche Projekte befinden sich im Aufbau. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland begrüßt diese Entwicklungen ausdrücklich und formuliert in einem Positionspapier wesentliche Anforderungen an eine moderne Transparenz-gesetzgebung.

Die Konferenz hält Regelungen in den Informationsfreiheits- und Transparenzgesetzen für erforderlich. Diese müssen um geeignete Instrumente zur Veröffentlichung von Informationen ergänzt werden. Datenbestände öffentlicher Stellen dürfen grundsätzlich nicht durch Urheberrecht oder Nutzungsbeschränkungen blockiert werden. Um Urheberrechten Dritter Rechnung zu tragen, sollten öffentliche Stellen mit diesen die Einräumung der Nutzungsrechte vertraglich vereinbaren.

29.3 Transparenz bei Sicherheitsbehörden

27. Juni 2013

Im Zusammenhang mit den Enthüllungen der umfassenden und anlasslosen Überwachungsmaßnahmen des US-amerikanischen und des britischen Geheimdienstes wurde bekannt, dass auch ein großer Teil des Kommunikationsverhaltens der Bürgerinnen und Bürger in Deutschland ohne ihr Wissen von diesen Geheimdiensten überwacht worden ist.

Die Konferenz der Informationsfreiheitsbeauftragten fordert die Verantwortlichen in Deutschland und Europa auf, für Transparenz auf nationaler und internationaler Ebene zu sorgen. Das Vertrauen der Bevölkerung kann nur zurückgewonnen werden, wenn die Aufgaben und Befugnisse der Sicherheitsbehörden völkerrechtlich festgelegt und deren tatsächliche Arbeitsweisen nachvollziehbar sind.

Zweifellos verfügen die Nachrichtendienste über Informationen, die nicht offengelegt werden dürfen. Gleichwohl hält die Konferenz die pauschale Ausnahme der Nachrichtendienste des Bundes und der Länder vom Anwendungsbereich der Informationsfreiheits- und Transparenzgesetze für nicht hinnehmbar und erwartet von den Gesetzgebern entsprechende Verbesserungen.

Darüber hinaus bedürfen die weit gefassten Ausnahmeregelungen für Sicherheitsbelange in den Informationsfreiheits- und Transparenzgesetzen einer Überprüfung und Einschränkung.

Die Informationsfreiheitsbeauftragten unterstützen die Verbesserung der Transparenz der nachrichtendienstlichen Aktivitäten gegenüber den Parlamenten und schließlich die Stärkung der parlamentarischen Kontrollgremien.

29.4 Verbraucher durch mehr Transparenz im Lebensmittelbereich schützen – Veröffentlichungspflichten für Hygieneverstöße jetzt nachbessern!

27. Juni 2013

Mit der Reform des Verbraucherinformationsrechts zum 1. September 2012 hat der Gesetzgeber als Reaktion auf die Lebensmittelskandale der letzten Jahre mit § 40 Abs. 1a Lebensmittel- und Futtermittelgesetzbuch (LFGB) eine Rechtsgrundlage für die Veröffentlichung von Hygieneverstößen durch die zuständigen Behörden geschaffen. Schon

im damaligen Gesetzgebungsverfahren hatte die Konferenz der Informationsfreiheitsbeauftragten darauf hingewiesen, dass die Vorschrift zu undifferenziert sei.

Nachdem zahlreiche Bundesländer begonnen hatten, Verbraucherinnen und Verbraucher auf eigens dafür geschaffenen Internetplattformen über entsprechende Hygieneverstöße zu informieren, sind die Veröffentlichungen durch eine Reihe von verwaltungsgerichtlichen Entscheidungen in Baden-Württemberg, Bayern, Berlin, Nordrhein-Westfalen und Rheinland-Pfalz gestoppt worden. Nach Auffassung der Gerichte greift § 40 Abs. 1a LFGB unter anderem deshalb unverhältnismäßig in die Rechte der betroffenen Unternehmen ein, weil die Vorschrift schon bei geringen Verstößen eine Veröffentlichung zulasse und keine Grenzen für die Dauer der Veröffentlichung vorsehe.

Die Informationsfreiheitsbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, dringend die lebensmittelrechtlichen Vorschriften über die Information der Öffentlichkeit zu überarbeiten und wie vom Bundesrat angeregt im Fachdialog mit den Ländern ein Transparenzsystem zu schaffen, das in eine rechtskonforme und effektive Gesamtkonzeption eingebunden wird. Nach der Rechtsprechung sind als Kriterien für eine Neuregelung der Veröffentlichungspflicht im Sinne des § 40 Abs. 1a LFGB insbesondere die Schwere des Rechtsverstoßes, eine behördliche Hinweispflicht auf die Tatsache und den Zeitpunkt der Mängelbeseitigung, Löschungspflichten sowie Ermessens- und Härtefallregelungen in Erwägung zu ziehen.

Umfassende Transparenz bei der Lebensmittelsicherheit darf nicht als Belastung für die Betriebe verstanden werden. Vielmehr ist dies der einzige Weg, das Vertrauen von Verbraucherinnen und Verbrauchern in die Qualität der Lebensmittel langfristig herzustellen und zu wahren.

29.5 Forderungen für die neue Legislaturperiode: Informationsrechte der Bürgerinnen und Bürger stärken!

28. November 2013

Der freie Zugang der Bürgerinnen und Bürger der Bundesrepublik Deutschland zu den Informationen der öffentlichen Stellen muss auch in Deutschland ein fester Bestandteil der verfassungsrechtlich garantierten Rechte werden. Transparenz ist eine wesentliche Grundlage für eine funktionierende freiheitlich demokratische Gesellschaft. Sie ist der Nährboden für gegenseitiges Vertrauen zwischen staatlichen Stellen und den Bürgerinnen und Bürgern.

Es reicht nicht aus, dass Informationen nur auf konkreten Antrag hin herauszugeben sind. In Zukunft sollten öffentliche und private Stellen, die öffentliche Aufgaben wahrnehmen, verpflichtet sein, Informationen von sich aus zur Verfügung zu stellen. Auf diese Weise wird der Zugang zu Informationen für alle erleichtert und der Aufwand der Informationserteilung reduziert.

Die Bundesrepublik Deutschland muss jetzt die nötigen gesetzlichen Regelungen für ein modernes Transparenzrecht schaffen, um mit den

internationalen Entwicklungen Schritt zu halten und die Chancen der Transparenz wahrzunehmen.

Die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder fordert daher alle Beteiligten in Bund und in den Ländern auf, sich für die Stärkung der Transparenz auf nationaler, europäischer und internationaler Ebene einzusetzen.

Sie fordert insbesondere:

- den Anspruch auf freien Zugang zu amtlichen Informationen endlich in alle Verfassungen aufzunehmen,

- einen gesetzlich geregelten effektiven Schutz von Whistleblowern, die über Rechtsverstöße im öffentlichen und nichtöffentlichen Bereich berichten,

- ein einheitliches Informationsrecht zu schaffen, das die Regelungen des Informationsfreiheitsgesetzes, des Umweltinformationsgesetzes und des Verbraucherinformationsgesetzes in einem Gesetz zusammenfasst,

- dass das Informationsfreiheitsrecht im Sinne eines Transparenzgesetzes mit umfassenden Veröffentlichungspflichten nach den Open-Data-Grundsätzen weiterentwickelt wird,

- aus der vom Bundestag in Auftrag gegebenen Evaluation des Bundesinformationsfreiheitsgesetzes die notwendigen Konsequenzen zu ziehen und die Ausnahmeregelungen auf das verfassungsrechtlich zwingend gebotene Maß zu beschränken,

- die Bereichsausnahme für die Nachrichtendienste abzuschaffen, die entsprechende Ausnahmeregelung auf konkrete Sicherheitsbelange zu beschränken und den Umgang mit Verschluss-Sachen gesetzlich in der Weise zu regeln, dass die Klassifizierung von Unterlagen als geheimhaltungsbedürftig regelmäßig von einer unabhängigen Instanz überprüft, beschränkt und aufgehoben werden kann,

- Transparenz der Kooperationen auch zwischen privaten und wissenschaftlichen Einrichtungen sicherzustellen, die im Rahmen der Wahrnehmung öffentlicher Aufgaben für staatliche Stellen tätig sind. Dies gilt auch und insbesondere für Sicherheitsbehörden,

- die Berliner Erklärung der 8. Internationalen Konferenz der Informationsfreiheitsbeauftragten zur Stärkung der Transparenz auf nationaler und internationaler Ebene vom 20. September 2013, insbesondere die Anerkennung eines Menschenrechts auf Informationszugang im Rahmen der Vereinten Nationen, den Beitritt der Bundesrepublik zur Open Government Partnership und zur Tromsö-Konvention des Europarats (Konvention des Europarates über den Zugang zu amtlichen Dokumenten) umzusetzen.

Die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder bietet ihre Unterstützung an.

29.6 Das Urheberrecht dient nicht der Geheimhaltung!

17. Juni 2014

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland betrachtet mit Sorge die Entwicklung, dass sich auskunftspflichtige Stellen zur Ablehnung von Anfragen auf das Urheberrecht oder andere Rechte des „Geistigen Eigentums" berufen. Das Urheberrecht darf nicht dazu eingesetzt werden, staatliche Informationen zurück zu halten.

Amtliche Vermerke sind in aller Regel nicht urheberrechtlich geschützt. Gedankliche Inhalte können in ihrer politischen, wirtschaftlichen oder gesellschaftlichen Aussage nicht über das Urheberrecht monopolisiert werden, sondern müssen vielmehr Gegenstand der freien geistigen Auseinandersetzung bleiben. Mit Steuermitteln finanzierte und für die Erfüllung einer öffentlichen Aufgabe erstellte Vermerke dürfen nicht unter Berufung auf Rechte des „Geistigen Eigentums" zurückgehalten werden. Hintergrund insbesondere des urheberrechtlichen Schutzes ist die Garantie einer angemessenen Vergütung der Urheber. Diese ist aber nicht bedroht, wenn Werke betroffen sind, die in Erfüllung dienstlicher Pflichten erstellt wurden.

Nur in Ausnahmefällen kann es sein, dass von Dritten für staatliche Stellen erstellte Gutachten tatsächlich dem Urheberrecht unterfallen und die Dritten schutzbedürftig sind. Wer mit der Verwaltung Verträge schließt, muss wissen, dass diese an gesetzliche Transparenzpflichten gebunden ist, die sich nicht abbedingen lassen. Wo dies nicht bereits gesetzlich vorgeschrieben ist, sollen sich die staatlichen Stellen in solchen Fällen das Recht an einer Herausgabe einräumen lassen. Soweit diese Stellen einem Informationsfreiheitsgesetz unterliegen, ist es ihre Pflicht, dafür Sorge zu tragen, dass Rechte Dritter nicht einem gesetzlichen Informationszugang entgegenstehen. Was mit staatlichen Mitteln für die Verwaltung von staatlichen Stellen oder Dritten hergestellt wird, muss grundsätzlich zugänglich sein.

29.7 Keine Flucht vor der Informationsfreiheit ins Privatrecht!

17. Juni 2014

Es ist für weite Bereiche der Rechtsordnung anerkannt, dass der Staat sich nicht durch Wahl einer privaten Rechtsform seiner verfassungsrechtlichen Bindungen entledigen kann. Für das Recht aller Bürgerinnen und Bürger, sich voraussetzungslos über staatliches oder kommunales Handeln zu informieren, gilt dies leider nicht in gleichem Maße. Entscheidet sich der Staat für eine formale Privatisierung und erledigt eine öffentliche Aufgabe durch eine juristische Person des Privatrechts, so ist diese nach vielen Informationsfreiheitsgesetzen nicht direkt auskunftsverpflichtet. Informationszugang muss für alle Unterlagen gelten, die im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen. Dabei darf es nicht darauf ankommen, ob die Aufgaben durch Behörden oder durch Private, an denen die öffentliche Hand mehrheitlich beteiligt ist,

wahrgenommen werden. Ebenso wenig kommt es auf die Rechtsform an, in der jeweils gehandelt wird.

Da häufig gerade die Bereiche privatisiert werden, die über große Finanzvolumina verfügen, ist hier die Herstellung von Transparenz hinsichtlich der Verwendung öffentlicher Steuermittel besonders wichtig. Bereits 2003 hatten die Informationsfreiheitsbeauftragten die Gesetzgeber im Bund und in den Ländern dazu aufgerufen, die Herstellung von Transparenz nicht davon abhängig zu machen, in welcher Form die öffentliche Aufgabe erledigt wird. Leider ist diese Forderung längst nicht überall umgesetzt worden. Es gilt weiterhin: Für die Auskunftsverpflichtung sollte allein entscheidend sein, ob es sich um eine staatliche oder kommunale Aufgabe, insbesondere eine der Grundversorgung handelt. Bei der Erfüllung öffentlicher Aufgaben müssen Ansprüche auf Auskunft auch direkt gegenüber den Unternehmen geschaffen werden.

29.8 Informationsfreiheit nicht Privaten überlassen

Die Anwendung der Informationsfreiheitsgesetze darf nicht von der Rechtsform abhängen, in der öffentliche Aufgaben erledigt werden. Eine Flucht vor der Informationsfreiheit in das Privatrecht ist mit einem modernen Staatsverständnis nicht zu vereinbaren. Informationsfreiheit nicht Privaten überlassen!

17. Juni 2014

Öffentliche Stellen vertreten vielfach die Auffassung, staatliche Transparenz könne durch die Bereitstellung amtlicher Informationen auf von Privaten nach deren Regularien betriebenen Plattformen wie Facebook, Twitter etc. hergestellt werden. Auch wenn derartige Internetdienstanbieter einen großen Nutzerkreis erreichen, stehen kommerzielle Interessen der Betreiber vielfach einem bedingungslosen und freien Informationszugang entgegen.

Öffentlichkeit ist gekennzeichnet durch voraussetzungslose, für ausnahmslos alle Menschen bestehende Zugangsmöglichkeiten. Sie kann deshalb nicht durch die Bereitstellung von Inhalten auf Internetseiten und -diensten hergestellt werden, die zum Beispiel ausschließlich durch allgemeine Geschäftsbedingungen Privater geregelt sind, nur Mitgliedern offen stehen oder keinen unbeobachteten Zugang gewähren. Staatliche Transparenz darf nicht durch die Offenbarung personenbezogener Daten erkauft werden.

Nur die Veröffentlichung auf von öffentlichen Stellen steuerbaren und der Allgemeinheit kostenfrei und anonym zugänglichen Kanälen genügt den Anforderungen der Herstellung staatlicher Transparenz. Die Konferenz der Informationsfreiheitsbeauftragten fordert, die Veröffentlichung amtlicher Informationen auf ausschließlich von den öffentlichen Stellen selbst gesteuerten Veröffentlichungsmedien vorzunehmen. Eine Steuerung und Kontrolle in diesem Sinne kann beispielsweise auch durch Einzelverträge mit Privaten geschehen. Der im Hamburger Transparenzgesetz formulierte Grundsatz, wonach der Zugang zum Informationsregister kostenlos und anonym ist, sollte in alle Informationsfreiheits- und Transparenzgesetze aufgenommen werden.

29.9 Mehr Transparenz bei technischen Ermittlungsmethoden – Vertrauen in den Rechtsstaat stärken!

9. Dezember 2014

In den vergangenen Jahren wurden die Ermittlungsbefugnisse für Polizeien, Strafverfolgungsbehörden und Nachrichtendienste kontinuierlich ausgeweitet. Ihnen steht ein beträchtliches Instrumentarium unterschiedlich eingriffsintensiver technischer Maßnahmen zur Verfügung, wie zum Beispiel Funkzellenabfragen, Einsatz von IMSI-Catchern, Telekommunikationsüberwachung und Verkehrsdatenerhebung. Im Rahmen der Erweiterung wurden in die Landespolizeigesetze und die Strafprozessordnung Berichterstattungspflichten aufgenommen. Dadurch sollte garantiert werden, dass die Gesellschaft sich der Auswirkungen dieser neuen Maßnahmen bewusst ist.

Eine kritische Überprüfung der Berichtspflichten zeigt, dass eine Transparenz der Auswirkungen solcher Ermittlungsmaßnahmen nicht erreicht wird. Die Berichterstattungspflichten sind nicht nur uneinheitlich geregelt: Zum Teil fehlen für einige Maßnahmen wie zum Beispiel die Bestandsdatenabfrage Berichtspflichten vollständig, zum Teil lassen die bestehenden Berichtspflichten keine hinlänglichen Erkenntnisse über das Ausmaß der Überwachung und insbesondere die Zahl der Betroffenen zu. Die Berichte über Funkzellenabfragen zu Strafverfolgungszwecken lassen etwa nicht erkennen, dass von einer einzelnen gerichtlichen Anordnung tausende Bürgerinnen und Bürger betroffen sein können, die keinen Anlass für die Erhebung ihrer Daten gegeben haben. Das Bundesverfassungsgericht verlangt in seinem Urteil zur Vorratsdatenspeicherung aber gerade, dass der Gesetzgeber eine „Überwachungsgesamtrechnung“ betreibt und beim Erlass neuer Überwachungsregelungen berücksichtigt. Nur so könne verhindert werden, dass die Freiheitswahrnehmung der Bürger total erfasst und registriert wird, denn dies verstieße gegen die verfassungsrechtliche Identität Deutschlands. Deshalb ist es jedenfalls erforderlich, nicht nur die theoretisch bestehenden, vom Gesetz erlaubten Überwachungsmöglichkeiten in den Blick zu nehmen, sondern gerade auch das konkrete Ausmaß ihres Einsatzes sichtbar zu machen.

Auf der Grundlage der gegenwärtig veröffentlichten Statistiken und zum Teil schmalen Berichtspflichten ist es nicht möglich, die gesamtgesellschaftlichen Auswirkungen aller Maßnahmen differenziert zu erfassen. Die Konferenz der Informationsfreiheitsbeauftragten fordert die Gesetzgeber in Bund und Ländern daher auf, die bestehenden Verpflichtungen zur Erstellung und Veröffentlichung von Statistiken auf alle Maßnahmen im Rahmen verdeckter Ermittlungsmethoden auszudehnen und sie durch die Angabe der Anzahl der Betroffenen so aussagekräftig zu gestalten, dass sich der Effekt auf die Bevölkerung klar erkennen lässt.

Darüber hinaus muss eine gesetzliche Veröffentlichungspflicht für die Berichte der Bundesnetzagentur zur Bestandsdatenabfrage festgeschrieben werden.

Eine besondere Bedeutung kommt der Transparenz der Nachrichtendienste zu. Erforderlich ist die Verschärfung bestehender bzw. Schaffung neuer Berichtspflichten gegenüber parlamentarischen Kontroll-

gremien und Datenschutzbeauftragten und die Verpflichtung zur Aufnahme aussagekräftiger statistischer Angaben zu Überwachungsmaßnahmen in die Verfassungsschutzberichte von Bund und Ländern. Geboten ist insbesondere eine Berichterstattung für den gesamten Bereich der strategischen Auslands-Telekommunikationsüberwachung.

Die Transparenz beim Einsatz staatlicher, insbesondere geheimer Ermittlungsmethoden ist neben den datenschutzrechtlichen Anforderungen eine wesentliche Voraussetzung für eine effiziente demokratische Kontrolle sowie die Beurteilung der Angemessenheit des staatlichen Eingriffshandelns und damit eine unabdingbare Wissensgrundlage für das Vertrauen der Bürgerinnen und Bürger in ihren Rechtsstaat.

29.10 Open Data muss in Deutschland Standard werden!

9. Dezember 2014

Die Bundesregierung hat mit der Digitalen Agenda 2014 - 2017, der Digitalen Verwaltung 2020 und dem nationalen Aktionsplan zur Umsetzung der G8 Open-Data-Charta wesentliche Regierungsprogramme zur Etablierung von E- und Open-Government sowie zur Digitalisierung der Verwaltung auf den Weg gebracht. Die Regierungsprogramme sehen aus informationsfreiheitsrechtlicher Sicht u.a. die Einführung einer gesetzlichen Open-Data-Regelung, die Schaffung von Open-Data-Ansprechpartnern in den Behörden, die Einführung der elektronischen Verwaltungsakte und eine verstärkte Zusammenarbeit mit den Ländern vor.

Die Konferenz der Informationsfreiheitsbeauftragten betont in diesem Zusammenhang das Erfordernis weitgehender gesetzlicher Veröffentlichungspflichten und die Übertragung der Aufgabe des Open-Data-Ansprechpartners auf behördliche Informationsfreiheitsbeauftragte.

Insbesondere bei Planung und Einführung der eAkte sind Aspekte der Informationsfreiheit und des Datenschutzes frühestmöglich im Anforderungskatalog abzubilden. Schon bei Anlage einer Akte sollten personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse und sonstige Beschränkungen vor einer weiteren Verwendung markiert werden, so dass sie automatisiert ersetzt oder hervorgehoben werden können. Dies erleichtert eine nachfolgende Weitergabe und Weiterverwendung erheblich und unterstützt die aktenführenden Stellen bei der effizienten Bearbeitung von IFG-Anträgen.

Es gilt jetzt, die Regierungsprogramme zügig in die Tat umzusetzen, damit Open Data in Deutschland zum Standard werden kann. Die Konferenz fordert die Länder und den Bund auf, soweit noch nicht geschehen, mit dieser Zielsetzung E- und Open-Government-Strategien gemeinsam zu entwickeln.

29.11 Umfassende und effektive Informationsfreiheitsaufsicht unabdingbar!

9. Dezember 2014

Mit den Informationsfreiheitsgesetzen des Bundes und der Länder wurde der Bundes- bzw. den Landesbeauftragten für Informationsfreiheit die Aufgabe eines „außergerichtlichen Streitschlichters" im Bereich des allgemeinen Informationsfreiheitsrechts übertragen. Sie kontrollieren die Anwendung der Informationsfreiheitsgesetze, vermitteln in Streitfällen und wirken auf die Einhaltung des geltenden Rechts hin. Im Bund sowie in den meisten Bundesländern verfügen die Informationsfreiheitsbeauftragten jedoch nur über eine eingeschränkte Kontroll- und Beratungskompetenz. Sie überwachen nur die Einhaltung des allgemeinen Informationsfreiheitsrechts, nicht jedoch der besonderen Informationszugangs-rechte, wie z.B. nach dem Umwelt- oder dem Verbraucherinformationsrecht.

Diese Situation ist unbefriedigend. Bürgerinnen und Bürger erwarten, dass ihr Informationsanliegen von den Informationsfreiheitsbeauftragten umfassend geprüft wird. Mangels umfassender Kontroll- und Beratungszuständigkeit ist dies jedoch zu häufig nicht der Fall, sodass es im Umwelt- und im Verbraucherinformationsrecht an einer unabhängigen Aufsichtsbehörde fehlt.

Auch die wissenschaftlichen Evaluierungsberichte zum Informationsfreiheitsgesetz des Bundes und einiger Länder haben sich dafür ausgesprochen, den Informationsfreiheitsbeauftragten zusätzlich die Kontrollkompetenzen für das besondere Informationsfreiheitsrecht zu übertragen. Im Bereich des Datenschutzes sind die Beauftragten bereits für das besondere Datenschutzrecht zuständig. Dieser Standard muss auch in der Informationsfreiheit hergestellt werden.

Die Konferenz der Informationsfreiheitsbeauftragten fordert daher die Gesetzgeber in Bund und Ländern auf, die Kontroll- und Beratungskompetenzen der Informationsfreiheits-beauftragten um das Umwelt- und das Verbraucherinformationsrecht – wo dies noch nicht geschehen ist - zu erweitern und die Informationsfreiheitsbeauftragten mit ausreichenden personellen und sachlichen Mitteln auszustatten, damit sie ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen können. Nur so ist gesichert, dass Bürgerinnen und Bürger bei der Ausübung ihrer Informationsrechte umfassend beraten werden und die Einhaltung der verschiedenen Informationsgesetze unabhängig kontrolliert wird.

30 Stichwortverzeichnis

UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

Fritz-Dobisch-Straße 12
66111 Saarbrücken
Telefon 0681/94781 0
Telefax 0681/94781 29
E-Mail poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de
www.informationsfreiheit.saarland.de