UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

26. Tätigkeitsbericht

2015/2016

26. Tätigkeitsbericht

der Landesbeauftragten für Datenschutz und Informationsfreiheit

Berichtszeitraum: 2015/2016

Dem Landtag und der Landesregierung
vorgelegt am: 21. Juni 2017
(Landtagsdrucksache 16/15)

Unabhängiges Datenschutzzentrum Saarland

Die Landesbeauftragte für Datenschutz
und Informationsfreiheit

Fritz-Dobisch-Straße 12 • 66111 Saarbrücken
Postfach 10 26 31 • 66026 Saarbrücken
Telefon 0681 94781-0
Fax 0681 94781-29
E-Mail poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de
www.informationsfreiheit.saarland.de

Im Interesse einer besseren Lesbarkeit wird im Text überwiegend auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet.

Sämtliche Personenbezeichnungen gelten gleichermaßen für beiderlei Geschlecht.

Vorwort

Am 18. Oktober 2015 verstarb nach schwerer Krankheit, aber dennoch völlig überraschend die Landesbeauftragte für Datenschutz und Informationsfreiheit Judith Thieser im Alter von 60 Jahren. Ihr unerwarteter Tod löste über unsere Dienststelle hinaus große Bestürzung und Trauer aus.

Seit ihrem Amtsantritt im Mai 2010 setzte sich Judith Thieser sehr engagiert für den Datenschutz ein und trug maßgeblich dazu bei, öffentliche und nicht-öffentliche Stellen des Landes durch Aufklärung und Beratung für Fragen des Datenschutzes zu sensibilisieren.

In ihre Amtszeit fiel die Übertragung der zuvor beim Innenministerium angesiedelten Aufsicht über den Datenschutz im nicht-öffentlichen Bereich auf das Unabhängige Datenschutzzentrum Saarland und die hierdurch bedingte Neuorganisation der Dienststelle.

Ein besonderes Anliegen war es ihr, dass das Unabhängige Datenschutzzentrum nicht in erster Linie als eine Behörde wahrgenommen wird, die Datenschutzverstöße verfolgt und ahndet. Vielmehr stand für sie die Beratung in allen Fragen des Datenschutzes und der Informationsfreiheit im Vordergrund.

Großes Engagement zeigte sie auch in ihren Bemühungen, bereits Kindern und Jugendlichen einen verantwortungsvollen Umgang mit ihren Daten im Internet und den Sozialen Netzwerken zu vermitteln. Die von ihr angestoßenen Schulworkshops entwickelten sich zu einem großen Erfolg.

Mit dem Tod von Judith Thieser verlor nicht nur das Saarland eine engagierte Stimme für den Datenschutz und die Informationsfreiheit, sondern das Unabhängige Datenschutzzentrum auch eine gradlinige, aufrichtige und verständnisvolle Vorgesetzte.

Das Unabhängige Datenschutzzentrum Saarland wird die Arbeit von Judith Thieser in ihrem Sinne weiterführen und ihr ein ehrendes Andenken bewahren.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
Monika Grethel
im Namen der Mitarbeiter
des Unabhängigen Datenschutzzentrums Saarland

Einleitung

Am 16. März 2016 hat mich der Landtag des Saarlandes für die Dauer von sechs Jahren in das Amt der Landesbeauftragten für Datenschutz und Informationsfreiheit gewählt. Für das Vertrauen, das mir durch diese Wahl entgegengebracht worden ist, möchte ich mich bei allen Abgeordneten des Saarländischen Landtages bedanken. Ganz herzlich bedanken möchte ich mich an dieser Stelle auch bei meinen Mitarbeiterinnen und Mitarbeitern, die sich mit großem Engagement mit den vielschichtigen Fallgestaltungen rund um den Datenschutz und die Informationsfreiheit befasst und damit die Grundlage für den vorliegenden Tätigkeitsbericht gelegt haben.

Mit diesem Bericht gebe ich einen Überblick über die wichtigsten Fragestellungen, mit denen sich das Unabhängige Datenschutzzentrum Saarland in den Jahren 2015 und 2016 beschäftigt hat.

Obwohl das Grundrecht auf informationelle Selbstbestimmung mitunter als ein Relikt aus dem vergangenen Jahrhundert betrachtet wird, zeigt die große Vielfalt der Themen aus den verschiedensten Bereichen, dass der Datenschutz immer mehr in das Bewusstsein der Menschen rückt und alle Lebensbereiche betrifft und damit an Aktualität nichts verloren hat.

Ein Themenkomplex, der immer größere Bedeutung für unser gesamtes Leben gewinnt, ist die Digitalisierung der Gesellschaft. Durch zunehmend differenziertere Analysemöglichkeiten von großen Datenbeständen können Erkenntnisse gewonnen und Prognosen entwickelt werden, die von hohem Wert für Wirtschaft, Wissenschaft, aber auch für staatliche Stellen sind. Stichworte wie autonome Fahrzeuge, das „Internet der Dinge“ bzw. Smart Home zeigen jedoch, dass diese Themen nicht nur die Wirtschaft und den Staat betreffen, sondern dass die digitale Welt auch im Alltag der Verbraucher angekommen ist.

Die Möglichkeiten, die diese Big-Data-Anwendungen eröffnen, stellen aber gleichzeitig große Herausforderungen für die Gewährleistung des Grundrechts auf informationelle Selbstbestimmung der Bürgerinnen und Bürger dar. Diese Herausforderungen dürfen aber nicht – wie vereinzelt gefordert - dazu führen, grundlegende Absicherungen dieses Grundrechts, wie die Prinzipien der Datensparsamkeit und der Zweckbindung, zugunsten wirtschaftlicher Interessen aufzugeben. Nur wenn die Bürgerinnen und Bürger darauf vertrauen können, dass ihre persönlichen Daten geschützt werden, kann auch das notwendige Vertrauen und damit die Akzeptanz in diese Anwendungen entstehen. Angesichts der enormen technischen Entwicklungen in einer weltweit vernetzten Gesellschaft und der hiermit verbundenen Gefährdungen zeigt sich, dass die Wahrung des Rechts auf informationelle Selbstbestimmung wichtiger und notwendiger ist denn je. Daher ist es erfreulich, dass die ab Mai 2018 in allen Mitgliedstaaten der Europäischen Union geltende Datenschutzgrundverordnung diese wesentlichen Prinzipien des Datenschutzes ebenso wie die nötige Transparenz bei Datenverarbeitungsvorgängen nicht aufgegeben hat. Big-Data-Anwendungen sind deshalb so zu gestalten, dass sie ihre Funktionen möglichst frühzeitig mit anonymisierten oder pseudonymisierten Daten erfüllen können. Immer wichtiger

werden folglich technische Lösungen, die den Schutz personenbezogener Daten zum frühestmöglichen Zeitpunkt gewährleisten.

Dass das Grundrecht auf informationelle Selbstbestimmung keineswegs an Bedeutung verliert, haben im Berichtszeitraum wiederum einige Entscheidungen sowohl des Europäischen Gerichtshofs als auch des Bundesverfassungsgerichts sehr eindrucksvoll belegt. Dies gilt gerade auch in Bezug auf das in der öffentlichen Debatte kontrovers erörterte Spannungsverhältnis zwischen Sicherheit und Freiheit, in dem der Datenschutz mitunter als Hindernis für eine effektive Terrorismus- bzw. Kriminalitätsbekämpfung betrachtet wird. Es ist unzweifelhaft eine Pflicht des Staates, seine Bürgerinnen und Bürger vor Eingriffen in das Leben und die körperliche Unversehrtheit zu schützen. Es ist aber auch eine grundlegende Aufgabe des Staates, dafür zu sorgen, dass die Menschen von ihren grundrechtlich garantierten Freiheitsrechten Gebrauch machen und sich unbeobachtet und unbefangen in der Öffentlichkeit bewegen können. Daher ist der Gesetzgeber gehalten, die Schutzgüter Leib und Leben sowie Privatsphäre in einen angemessenen Ausgleich zu bringen. Die Gewährleistung der Sicherheit darf nicht zu einer Aushöhlung der Freiheitsrechte führen.

Im Bereich der Informationsfreiheit fand mit der Verabschiedung des Informationsfreiheitsgesetzes im Jahre 2006 eine Abkehr vom bislang geltenden Amtsgeheimnis hin zu einer wirksamen Informationsfreiheit statt. Damit können Bürgerinnen und Bürger auf Antrag Zugang zu amtlichen Informationen von öffentlichen Stellen des Landes erhalten. Mittlerweile geht die Entwicklung in verschiedenen Bundesländern dahin, dass eine transparente Verwaltung nicht mehr erst auf Anfragen der Bürger wartet, sondern von sich aus Informationen für den Einzelnen jederzeit abrufbar zur Verfügung stellt. Im Saarland wird dieser Weg bislang noch nicht beschritten. Der künftige saarländische Gesetzgeber sollte daher prüfen, ob ein solcher weiterer Kulturwandel beim Umgang mit Daten der Verwaltung angestoßen werden soll, um hierdurch den Bürgerinnen und Bürgern das Handeln der Verwaltung nachvollziehbarer zu machen.

Ich wünsche allen Leserinnen und Lesern bei der Lektüre dieses Tätigkeitsberichts neue interessante Einblicke in die unterschiedlichsten Fragestellungen rund um die Themen Datenschutz und Informationsfreiheit.

Saarbrücken, im Juni 2017

Monika Grethel

Die Landesbeauftragte
für Datenschutz und Informationsfreiheit

Inhaltsverzeichnis

Datenschutz

1 Überblick

1.1 Europa

Aus datenschutzrechtlicher Sicht stand der Berichtszeitraum in besonderem Maße unter dem Eindruck der Verabschiedung der Europäischen Datenschutzreform. Nach über vierjährigen Verhandlungen sind am 4. Mai 2016 sowohl die Europäische Datenschutz-Grundverordnung[1] (DS-GVO) als auch die Europäische Datenschutzrichtlinie für Polizei und Justiz[2] (JI-RL) im Amtsblatt der Europäischen Union (EU) veröffentlicht worden. Die DS-GVO ist am 24. Mai 2016 in Kraft getreten und ist ab dem 25. Mai 2018 in allen Mitgliedstaaten unmittelbar anwendbares Recht. Bis zum 6. Mai 2018 müssen die Mitgliedstaaten die zur Umsetzung der JI-RL erforderlichen Rechts- und Verwaltungsvorschriften erlassen.

Mit der Verabschiedung dieses Reformpakets ist es auf europäischer Ebene gelungen, in einem überaus komplexen Gesetzgebungsverfahren einen einheitlichen Rechtsrahmen für den Datenschutz in ganz Europa zu schaffen.

Wie bereits im vergangenen Berichtszeitraum hat sich auch in den beiden letzten Jahren wieder gezeigt, dass neben den Entscheidungen des Bundesverfassungsgerichts (BVerfG) auch der Rechtsprechung des Europäischen Gerichtshofs (EuGH) große Bedeutung für den Schutz des Grundrechts auf informationelle Selbstbestimmung zukommt.

1.1.1 Europäische Datenschutz-Grundverordnung (DS-GVO)

Mit der DS-GVO wird in Zukunft ein weitgehend einheitliches Recht bei der Verarbeitung personenbezogener Daten in der gesamten Europäischen Union gelten. Dadurch soll ein möglichst gleichmäßiges Datenschutzniveau für alle natürlichen Personen innerhalb der Union gewährleistet und die bisher bestehenden Schwierigkeiten für Unternehmen bei grenzüberschreitenden Datenverarbeitungen sollen ausgeräumt werden.

Zukünftig werden sich nicht nur die in der Europäischen Union niedergelassenen Unternehmen an die europarechtlichen Vorgaben halten müssen. Mit der Einführung des Marktortprinzips findet die DS-GVO auch auf außerhalb der EU niedergelassene verantwortliche Stellen Anwendung, wenn diese Daten verarbeiten, um entweder

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[2] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

Personen in der Union Waren oder Dienstleistungen anzubieten oder das Verhalten Betroffener zu beobachten.

Wesentliche, schon nach der aktuell noch geltenden Europäischen Datenschutzrichtlinie[3] (DSRL) zu berücksichtigende datenschutzrechtliche Grundprinzipien, wie das Verbot mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz oder die Transparenz gelten auch nach den Regelungen der DS-GVO fort.

Neuerungen gibt es bei den Betroffenenrechten in Bezug auf die Löschpflichten mit dem „Recht auf Vergessenwerden" (Art. 17 DS-GVO). Machen Betroffene einen Löschungsanspruch geltend, müssen die Stellen, die die Daten öffentlich gemacht haben, also insbesondere Internetanbieter, andere Stellen, die die Daten verarbeiten, über Löschbegehren informieren. Hierdurch soll den Betroffenen im digitalen Zeitalter eine bessere Kontrolle über ihre personenbezogenen Daten zugestanden werden.

Diesem Ziel dient auch das Recht auf Datenübertragbarkeit, das es dem Einzelnen ermöglichen soll, seine personenbezogenen Daten ohne Probleme von einem Verantwortlichen zu einem anderen zu übertragen. Da der Gesetzeswortlaut keine weitergehenden Einschränkungen zu den durch die Regelung verpflichteten verantwortlichen Stellen enthält, sind damit nicht nur allein Internetdienste Adressaten der Vorschrift.

Im Bereich des technischen und organisatorischen Datenschutzes wird der Verantwortliche stärker in die Pflicht genommen. Schon bei der Entwicklung von Produkten ist der Datenschutz sicherzustellen. So muss etwa der Verantwortliche bei der Datenverarbeitung ausdrücklich geeignete technische und organisatorische Maßnahmen, wie beispielsweise Pseudonymisierung, treffen, um die Datenschutzgrundsätze wirksam umzusetzen. Auch müssen Standardeinstellungen von Verfahren und Produkten so ausgestaltet sein, dass nur die für den jeweiligen Zweck erforderlichen Daten erhoben werden (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen).

Schließlich wird sich unter der Geltung der DS-GVO auch der Bußgeldrahmen erheblich erweitern. Bei Verstößen drohen den Unternehmen zukünftig ganz erhebliche Geldbußen von bis zu 20 Millionen Euro oder bis zu 4 % des weltweit erzielten Jahresumsatzes.

Sofern Unternehmen in mehreren Mitgliedstaaten tätig sind, ist alleiniger Ansprechpartner die Aufsichtsbehörde am Hauptsitz des Unternehmens („federführende Aufsichtsbehörde") und nicht wie bisher die jeweilige Aufsichtsbehörde am Sitz einer Niederlassung (sog. „One-Stop-Shop-Verfahren"). Die federführende Aufsichtsbehörde muss jedoch mit den anderen betroffenen Aufsichtsbehörden zusammenarbeiten und auf einen gemeinsamen Beschluss hinarbeiten. Gelingt dies nicht, wird in einem Kohärenzverfahren durch einen neu einzurichtenden Europäischen Datenschutzausschuss eine verbindliche Entscheidung getroffen. Durch dieses Verfahren wird die Rechtssicherheit für die Unternehmen gestärkt, da sie sich nicht mehr mit

[3] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

mehreren Aufsichtsbehörden mit möglicherweise unterschiedlichen Rechtsauffassungen auseinandersetzen müssen.

Zukünftig muss sich die von einem mutmaßlichen Datenschutzverstoß betroffene Person nicht mehr ausschließlich an die Aufsichtsbehörde an dem Ort wenden, an dem der für den Verstoß Verantwortliche seinen Sitz hat, sondern sie kann unabhängig vom Ort des Datenschutzverstoßes ihre Datenschutzrechte bei der Aufsichtsbehörde ihres Aufenthaltsortes geltend machen.

Insgesamt hat die DS-GVO die Aufgaben und Befugnisse der Aufsichtsbehörden erheblich erweitert, um das mit der DS-GVO verfolgte Ziel einer unionsweit einheitlichen Datenschutzpraxis durchzusetzen.

Obwohl es sich bei der DS-GVO um eine Verordnung im Sinne des Art. 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) handelt, die allgemeine Geltung hat und in allen ihren Teilen verbindlich und unmittelbar in jedem Mitgliedstaat gilt, gibt es dennoch für die nationalen Gesetzgeber aufgrund einer Reihe von Regelungspflichten und -optionen noch einen eigenen, nicht unerheblichen Handlungsspielraum. Diesen Spielraum gilt es im Sinne des Rechts auf informationelle Selbstbestimmung zu nutzen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat demensprechend mit der Entschließung „Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen" (vgl. Kapitel 25.15) die nationalen Gesetzgeber aufgefordert, Regelungen zu treffen, die das bestehende Datenschutzniveau erhalten und stärken.

Auf Bundesebene ist im Berichtszeitraum bereits ein Referentenentwurf für ein „Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU)", das auch ein Nachfolgegesetz für das Bundesdatenschutzgesetz beinhaltet, in das Anhörungsverfahren gegeben worden. Allerdings gibt dieser Entwurf erheblichen Anlass zur Kritik, da er in einigen Bereichen die nach der DS-GVO eröffneten Handlungsspielräume über das zulässige Maß ausweitet und in einigen Bereichen das bereits erreichte Datenschutzniveau absenkt. Es bleibt zu hoffen, dass bis zum Abschluss des Gesetzgebungsverfahrens die notwendigen Korrekturen noch vorgenommen werden.

Auch der saarländische Gesetzgeber wird die Zeit bis zum Stichtag am 25. Mai 2018 nutzen müssen, um die erforderlichen gesetzlichen Anpassungen vorzunehmen.

1.1.2 Europäische Datenschutzrichtlinie für Polizei und Justiz (JI-RL)

Der Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten durch die zuständigen Behörden zum Zwecke der Gefahrenabwehr und der Strafverfolgung fällt nicht unter die DS-GVO, sondern wird in einer Richtlinie, der sog. JI-RL geregelt. Diese Richtlinie, die gleichzeitig mit der DS-GVO verhandelt und verabschiedet wurde, aber in dem gesamten Reformprozess nur ein Schattendasein geführt hatte, soll erstmalig in den Bereichen Polizei und Justiz eine Datenschutz-Mindestharmonisierung innerhalb der Europäischen Union herbeiführen. Die Richtlinie lässt den Mitgliedstaaten Spielräume bei der Umsetzung in nationales Recht. Zu beachten wird aber sein, dass es sich bei den Vorgaben der Richtlinie um Mindestan-

forderungen handelt, so dass die nationalen Regelungen zwar ein höheres Schutzniveau aufweisen dürfen, eine Unterschreitung des in der Richtlinie beschriebenen Mindestniveaus indes nicht erlaubt ist.

Der saarländische Gesetzgeber wird insbesondere die polizeirechtlichen Vorschriften hinsichtlich des notwendigen Anpassungsbedarfs zu überprüfen haben und die erforderlichen gesetzgeberischen Maßnahmen ebenfalls bis Mai 2018 vornehmen müssen.

Von der JI-RL, aber auch vom Anwendungsbereich der DS-GVO nicht erfasst sind Maßnahmen für die nationale Sicherheit, also beispielsweise die Tätigkeit des Verfassungsschutzes. Um eine Rechtszersplitterung zu vermeiden, sollte sich der Gesetzgeber auch in diesen Bereichen an den Vorgaben der DS-GVO bzw. der JI-RL orientieren.

1.1.3 Von Safe Harbor zum Privacy Shield

Urteil des Europäischen Gerichtshofs zum Safe-Harbor-Abkommen

Die Europäische Datenschutzrichtlinie (DSRL) sieht vor, dass die Übermittlung personenbezogener Daten in ein Drittland, also in ein Land außerhalb der Europäischen Union, grundsätzlich nur dann zulässig ist, wenn das betreffende Drittland ein angemessenes Schutzniveau dieser Daten gewährleistet. Besteht in einem Staat kein angemessenes Datenschutzniveau, kann die EU-Kommission nach Art. 25 Abs. 6 DSRL feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau gewährleistet.

Da die USA nicht zu den Staaten gehören, in denen ein angemessenes Datenschutzniveau gewährleistet ist, hat die EU-Kommission bereits im Jahr 2000 gemeinsam mit dem US-Handelsministerium die Safe-Harbor-Grundsätze entwickelt und die sog. Angemessenheitsentscheidung nach Art. 25 DSRL getroffen. Auf der Grundlage dieses Abkommens galten Unternehmen aus den USA, die sich den Vereinbarungen dieses Abkommens unterwarfen und sich verpflichteten, die dort aufgestellten Prinzipien einzuhalten, als Unternehmen mit einem angemessenen Datenschutzniveau, so dass eine Datenübermittlung dorthin erfolgen konnte.

Dieses Safe-Harbor-Abkommen erklärte der EuGH am 6. Oktober 2015 (Az.: C-362/14) für ungültig. Der EuGH hat zur Begründung seiner Entscheidung ausgeführt, dass die Kommission vor Inkrafttreten des Safe Harbor-Abkommens nicht nur die Regelungen dieses Abkommens hätte prüfen dürfen, sondern ausführlich hätte untersuchen müssen, ob das US-amerikanische Recht tatsächlich ein angemessenes Datenschutzniveau zulässt. Schließlich stehe nach den Vereinbarungen in dem Abkommen eindeutig fest, dass den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen der USA Vorrang vor den Grundsätzen des „sicheren Hafens“ eingeräumt wird.

Ein gleichwertiges Schutzniveau in einem Drittstaat liegt nach den Ausführungen in dem Urteil dann nicht vor, wenn eine Regelung es gestattet, generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten in den Drittstaat übermittelt wurden, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken. Insbesondere sei es mit den europäischen Grundsätzen zum Schutz personenbezogener Daten nicht vereinbar, wenn Behörden generell auf elektronische Kommunikationsdaten zugreifen und eine wirksame rechtsstaatliche Kontrolle nicht gegeben ist. Zudem verletze eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des Grundrechts auf wirksamen gerichtlichen Rechtsschutz.

Darüber hinaus hat der EuGH mit diesem Urteil die Unabhängigkeit der Datenschutzaufsichtsbehörden gestärkt, indem er klar feststellt, dass die Kompetenzen und Befugnisse der nationalen Kontrollstellen durch Entscheidungen der EU-Kommission nicht tangiert werden. Da bislang im nationalen Recht ein Rechtsbehelf gegen Entscheidungen der Europäischen Kommission nicht vorgesehen ist, hat die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder mit einer Entschließung vom 20. April 2016 den Gesetzgeber aufgefordert, ein eigenständiges Klagerecht für die unabhängigen Datenschutzbehörden vorzusehen (vgl. Kapitel 25.19).

EU-US Privacy Shield

Da der EuGH das Safe-Harbor-Abkommen für ungültig erklärte, konnten sich verantwortliche Stellen nicht mehr auf diese Angemessenheitsentscheidung der EU-Kommission für ihre Datentransfers in die USA berufen. Daher bemühten sich die Kommission und die US-Regierung um eine Nachfolgeregelung, die den vom EuGH aufgezeigten Anforderungen genügt.

Am 2. Februar 2016 hat die EU-Kommission den Abschluss der Verhandlungen mit der US-Regierung über das Nachfolgeabkommen von Safe-Harbor, das sog. EU-US Privacy Shield, bekanntgegeben und am 12. Juli 2016 den Angemessenheitsbeschluss nach Art. 25 Abs. 6 DSRL, dem zufolge die Garantien für die Übermittlung von Daten auf der Grundlage des neuen EU-US Privacy Shield den Datenschutzstandards in der EU entsprechen, gefasst.

Zwar enthält diese Entscheidung Verbesserungen gegenüber dem Safe-Harbor-Abkommen; ob allerdings alle Anforderungen des EuGH an ein angemessenes Datenschutzniveau im Drittstaat erfüllt sind, ist zweifelhaft. Es ist zu erwarten, dass sich der EuGH auch mit diesem Abkommen befassen wird.

1.1.4 Personenbezug von IP-Adressen

Eine IP-Adresse ist – vereinfacht ausgedrückt – die Adresse eines Computers, mit der dieser im Internet erreichbar ist. Die IP-Adresse wird benötigt, um Daten von ihrem Absender zum vorgesehenen Empfänger transportieren zu können. Bei dem Abruf einer Website wird die IP-Adresse des abrufenden Computers an den Server übermittelt, auf dem die abgerufene Website gespeichert ist. Dieser versieht das Datenpaket mit der IP-Adresse und sendet es an den Computer, der mittels der IP-Adresse eindeutig verifiziert werden kann. Die IP-Adressen werden von Internetzugangsanbietern (Provider) an Anschlussinhaber vergeben. Man unterscheidet statische und dynamische IP-Adressen: statische IP-Adressen bleiben bei jeder Verbindung mit dem Internet gleich, dagegen werden dynamische IP-Adressen in kurzen Zeitabständen oder bei jeder Einwahl in das Internet neu vergeben. Internetzugangsanbieter speichern allerdings in der Regel für eine gewisse Zeit, welchem Anschlussinhaber sie welche dynamische IP-Adresse zuweisen, so dass auch nach der Neuvergabe einer IP-Adresse die Zuordnung einer „abgelaufenen" IP-Adresse zu einem Anschlussinhaber beim Zugangsanbieter möglich ist.

Während bei statischen IP-Adressen überwiegend davon ausgegangen wird, dass es sich bei ihnen um personenbezogene Daten handelt, war diese Frage bei dynamischen IP-Adressen bislang heftig umstritten.

Auf Vorlage des Bundesgerichtshofs (BGH) im Rahmen eines Vorabentscheidungsersuchens hat der EuGH am 19. Oktober 2016 - C-582/14 - nunmehr Klarheit bei dieser Frage geschaffen.

Anlass für dieses Verfahren ist ein Rechtsstreit in Deutschland, in dem der BGH darüber zu entscheiden hat, ob Websites des Bundes die ungekürzten IP-Adressen der zugreifenden Computer speichern dürfen, um Angriffe abzuwehren und die strafrechtliche Verfolgung von Angreifern zu ermöglichen.

Der EuGH hat die Frage nach dem Personenbezug von dynamischen IP-Adressen nunmehr dahingehend bejaht, dass die dynamische IP-Adresse des Besuchers, welche vom Betreiber einer Website im Zusammenhang mit dem Zugriff und der Nutzung der Seite gespeichert wird, für den Betreiber ein personenbezogenes Datum darstellt, sofern dieser die rechtliche Möglichkeit hat, den Besucher anhand weiterer Zusatzinformationen zu bestimmen. In Deutschland ist dies der Fall, denn Internetzugangsanbieter können durch die Gerichte verpflichtet werden, Auskunft darüber zu erteilen, welchem Internetanschlussinhaber sie zu welchem Zeitpunkt eine bestimmte dynamische IP-Adresse zugeordnet hatten.

Mit seiner zweiten Vorlagefrage wollte der BGH geklärt wissen, ob der Betreiber einer Website grundsätzlich die Möglichkeit haben muss, zur Gewährleistung der Funktionsfähigkeit der Website personenbezogene Daten der Besucher zu erheben und zu verwenden. Nach § 15 Telemediengesetz (TMG) müssen derzeit solche Daten am Ende des Nutzungsvorgangs gelöscht werden. Davon kann nur dann abgewichen werden, wenn diese Daten noch für Abrechnungszwecke benötigt werden.

Nach Auffassung des EuGH widerspricht dies jedoch dem Unionsrecht. Nach Art. 7f DSRL müsse eine Interessensabwägung möglich sein zwischen dem „berechtigten

Interesse“ des Betreibers einer Website und den Grundrechten der Nutzer. Ein solches berechtigtes Interesse an einer Speicherung über den Nutzungsvorgang hinaus kann nach Auffassung des EuGH vorliegen, wenn der Betreiber die dynamischen IP-Adressen der Nutzer vorhalten wolle, um Cyber-Attacken abzuwehren. Dieser Grundsatz werde von der deutschen Regelung im TMG eingeschränkt, da der Zweck der Aufrechterhaltung der Funktionsfähigkeit der Website danach nicht Gegenstand einer solchen Abwägung sein kann. Der BGH wird sich nunmehr abschließend mit der Frage befassen und abwägen müssen, ob die Sicherheitsargumente von Website-Betreibern oder die Persönlichkeitsrechte der Nutzer überwiegen.

1.1.5 Vorratsdatenspeicherung

Nachdem der EuGH bereits im Jahre 2014 die Europäische Richtlinie über die Vorratsdatenspeicherung (2006/24/EG) für ungültig erklärt hatte,[4] hat er im Berichtszeitraum durch ein weiteres Urteil vom 21. Dezember 2016 - C-203/15 - erneut den Bestrebungen für die anlasslose, systematische Speicherung von Telefon- und Internetverbindungsdaten aller Bürger eindeutige Grenzen gesetzt. In diesem Zusammenhang machte das Gericht deutlich, dass anlasslose und flächendeckende Überwachungsmaßnahmen gegen die in der Charta der Grundrechte der Europäischen Union gewährleisteten Grundrechte auf Achtung des Privatlebens (Art. 7) und auf Schutz personenbezogener Daten (Art. 8) verstoßen.

Anlass für das vorliegende Verfahren waren zwei Vorlagen von Gerichten aus Schweden und Großbritannien zu den dortigen nationalen gesetzlichen Vorschriften zur Vorratsdatenspeicherung. Die damit befassten Gerichte baten um Klärung, ob die jeweiligen Regelungen mit der EU-Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG), sog. ePrivacy-Richtlinie, im Lichte der Grundrechtecharta vereinbar sind.

Der Gerichtshof hat in seinem Urteil ausgeführt, dass die vertrauliche Kommunikation durch nationale Regelungen zwar eingeschränkt werden kann, er hat aber auch ausdrücklich klargestellt, dass das Unionsrecht einer nationalen Regelung entgegensteht, die eine allgemeine und unterschiedslose Speicherung von Daten vorsieht.

Die Gesamtheit der Daten, die im Rahmen einer solchen Vorratsdatenspeicherung erfasst werden können, erlauben sehr genaue Rückschlüsse auf das Privatleben der Nutzer, da private Verhaltensweisen, Lebensäußerungen, Bewegungen, Aktivitäten und Beziehungen festgehalten werden. Diese Profile sind nach Ansicht des Gerichtshofs als nicht weniger heikel zu betrachten als die eigentlichen Inhalte der Kommunikation. Das begründet ihre Schutzwürdigkeit, weshalb der damit verbundene Grundrechtseingriff als besonders schwerwiegend anzusehen sei.

Gerade der Umstand, dass die Daten ohne Information der Nutzer erhoben würden, könne bei diesen ein Gefühl der ständigen Überwachung erzeugen.

[4] Vgl. 25. Tätigkeitsbericht, 2013/2014, Kapitel 3.2.2, S. 21.

Für die Rechtfertigung eines solchen Eingriffs stellt das Gericht daher besonders hohe Anforderungen: Allein die Bekämpfung schwerer Straftaten oder eine schwerwiegende Gefahr für die öffentliche Sicherheit könne dazu herangezogen werden. Zu diesem Zweck erlaube die Richtlinie 2002/58/EG eine gezielte Vorratsspeicherung von Daten nur dann, sofern diese hinsichtlich der Art der Daten, der betroffenen Kommunikationsmittel, der betroffenen Personen und der Dauer der Speicherung auf das absolut Notwendige beschränkt sei.

Das Gericht führt weiter aus, dass eine nationale Regelung, die sich unbeschränkt auf alle Teilnehmer erstreckt und undifferenziert alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erfasst, unzulässig ist. Eine Vorratsdatenspeicherung kann nur dann europarechtskonform sein, wenn sie Beschränkungen enthält, etwa in Bezug auf einen bestimmten Zeitraum oder ein geografisches Gebiet oder einen bestimmten Personenkreis, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte.

Das Gericht betont, dass ein Zugriff auf die Vorratsdaten von Standort- und Telekommunikationsinformationen aufgrund der Schwere des Eingriffs in die Grundrechte überhaupt nur bei schwerwiegenden Verbrechen in Betracht kommen kann. Die Richter entschieden zudem, dass Behörden in der Regel nur dann Zugang zu den auf Vorrat gespeicherten Daten erhalten dürfen, wenn dies zuvor von einem Gericht oder einer anderen unabhängigen Stelle erlaubt wurde. Außerdem müssen die Daten innerhalb der EU gespeichert werden.

Das Urteil bedeutet daher, dass eine pauschale und anlasslose Vorratsdatenspeicherung nicht in Betracht kommt. Vielmehr muss der Gesetzgeber einen konkreten Anknüpfungspunkt dafür definieren, dass durch die Maßnahme eine konkrete Straftat aufgeklärt oder eine konkrete Gefahr beseitigt werden könne.

Angesichts dieser klaren Aussagen sollte der deutsche Gesetzgeber die von ihm im Jahre 2015 erneut verabschiedeten Regelungen zur Vorratsdatenspeicherung dringend überprüfen und korrigieren (vgl. hierzu Kapitel 1.2.1)

1.2 Entwicklungen in Deutschland

Auf nationaler Ebene stand vor dem Hintergrund konkreter Bedrohungen durch den internationalen Terrorismus die Sicherheitsdebatte und damit verbunden eine Verschärfung der Sicherheitsgesetze ganz besonders im Blickfeld der Gesetzgeber. Dabei scheint teilweise aus dem Blick geraten zu sein, dass neben der unzweifelhaft bestehenden Schutzpflicht des Staates gegenüber seinen Bürgern, dem Staat auch die Verpflichtung obliegt, eine angemessene Balance zwischen Sicherheit und Freiheit aufrecht zu erhalten. Bei seiner Aufgabe, immer wieder einen Ausgleich zwischen dem Interesse des Einzelnen an der Wahrung seiner von der Verfassung verbürgten Rechte und der Pflicht des Staates zum Rechtsgüterschutz herzustellen, mag der Gesetzgeber die Balance zwischen Sicherheit und Freiheit zwar neu justieren dürfen; er darf die Gewichte jedoch nicht grundlegend verschieben. Eine solche Verschiebung droht jedoch, wenn die Sicherheitsgesetzgebung zu anlasslosen und flächendeckenden Überwachungen berechtigt.

1.2.1 Wiedereinführung einer Vorratsdatenspeicherung

Die Einführung einer Vorratsdatenspeicherung von Telekommunikations-Verbindungsdaten ist sowohl in Europa als auch in Deutschland seit Jahren in der Diskussion (vgl. Kapitel 1.1.5.)

Das erste deutsche Gesetz zur Vorratsdatenspeicherung wurde vom BVerfG im Jahre 2010 für verfassungswidrig und nichtig erklärt. Am 8. April 2014 erklärte auch der EuGH die EU-Richtlinie zur Vorratsdatenspeicherung für ungültig, da sie mit der Charta der Grundrechte der Europäischen Union nicht vereinbar war. Beide Gerichte stellten klar, dass eine vorsorgliche anlasslose Speicherung von Telekommunikationsdaten die absolute Ausnahme bleiben muss, da es sich hierbei um besonders schwere Eingriffe mit großer Streubreite handelt.

Gegen Überlegungen der Bundesregierung, erneut eine gesetzliche Grundlage zur flächendeckenden Speicherung von Telekommunikationsdaten zu schaffen, wandte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9. Juni 2015 mit einer Umlaufentschließung: „Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken" (vgl. Kapitel 25.9) Dennoch verabschiedete der Bundesgesetzgeber im Oktober 2015 mit dem „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" eine Neuauflage der Vorratsdatenspeicherung.

Zwar hat der Gesetzgeber versucht, beispielsweise hinsichtlich Speicherdauer, Datensicherheit, Transparenz oder Ausgestaltung des Rechtsschutzes die verfassungsgerichtlichen Anforderungen zu erfüllen, im Kern verbleibt es dennoch bei einer flächendeckenden und verdachtslosen Speicherung der Kommunikationsdaten einer Vielzahl von Personen.

Nach dem neuerlichen Urteil des EuGH vom 21. Dezember 2016, in dem das Gericht die Unzulässigkeit einer anlasslosen Vorratsdatenspeicherung bekräftigt hat, dürfte es nunmehr höchst zweifelhaft sein, ob die bundesgesetzliche Regelung Bestand haben wird. Sofern nicht der Gesetzgeber selbst eine Korrektur der getroffenen gesetzlichen Regelung vornimmt, wird letztlich wiederum das Bundesverfassungsgericht hier für Klarheit sorgen müssen.

1.2.2 Urteil des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz

Mit Urteil vom 20. April 2016 - 1 BvR 966/09, 1 BvR 1140/09 - hat das BVerfG zahlreiche Vorschriften des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG -), das dem Bundeskriminalamt weitreichende Eingriffsbefugnisse zur Terrorismusbekämpfung einräumt, für verfassungswidrig erklärt.

Das BVerfG hat entschieden, dass die Ermächtigungen des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen zur Abwehr von Gefahren des internationalen Terrorismus zwar im Grundsatz mit den Grundrechten vereinbar ist, die

derzeitige Ausgestaltung von Befugnissen aber in verschiedener Hinsicht dem Verhältnismäßigkeitsgrundsatz nicht genügt. Die Gefahren des Terrorismus rechtfertigen weitreichende Eingriffsbefugnisse und Aufklärungsmittel nur dann, wenn diese mit rechtsstaatlichen Absicherungen versehen werden. Die Befugnisse, zumal wenn sie tief in das Privatleben eingreifen, müssen auf den Schutz gewichtiger Rechtsgüter begrenzt sein. Erforderlich sei auch immer, dass eine Gefährdung dieser Rechtsgüter konkret absehbar ist. Da die Gründe für die Verfassungswidrigkeit nicht den Kern der eingeräumten Befugnisse betreffen, gelten die beanstandeten Vorschriften überwiegend bis zum Ablauf des 30. Juni 2018 fort.

Der Bundesgesetzgeber wird daher bis zu dem genannten Zeitpunkt durch eine Änderung der beanstandeten Vorschriften des BKA-Gesetzes die verfassungsrechtlichen Vorgaben des BVerfG umsetzen müssen. Aber auch der Landesgesetzgeber wird die im Saarländischen Polizeigesetz (SPolG) enthaltenen Vorschriften zu heimlichen Überwachungsmaßnahmen unter Berücksichtigung der grundsätzlichen Anforderungen des BVerfG an die Verhältnismäßigkeit derartiger Befugnisse anpassen müssen (vgl. Kapitel 3.1).

1.3 Aus der Dienststelle

1.3.1 Zusammenarbeit mit dem Landtag

Mit Beginn der laufenden Legislaturperiode richtete der Landtag des Saarlandes einen Ausschuss für Datenschutz und Informationsfreiheit ein, in dem das Unabhängige Datenschutzzentrum den Abgeordneten des Parlaments in regelmäßigen Abständen über aktuelle Entwicklungen im Bereich des Datenschutzes und der Informationsfreiheit Bericht erstatten konnte. Die in dem Ausschuss über unsere gesetzlich vorgesehene Beteiligung an Gesetzgebungsvorhaben hinausgehende Befassung mit Fragen des Datenschutzes hat aus unserer Sicht zu einer Schärfung des Datenschutzbewusstseins der Mitglieder des Landtages geführt. Die Berichterstattungen in diesem Ausschuss boten den Abgeordneten die Gelegenheit, sich einen umfassenden Überblick über die komplexen datenschutzrechtlichen Herausforderungen unserer Zeit zu verschaffen. Da die fortschreitende Digitalisierung der Gesellschaft auch weiterhin viele datenschutzrechtliche Fragestellungen mit sich bringen wird, die von einem intensiven politischen Diskurs begleitet werden müssen, bleibt zu hoffen, dass der Ausschuss über die aktuelle Legislaturperiode hinaus Bestand haben wird.

1.3.2 Schulworkshops

Im Berichtszeitraum haben wir unsere im Schuljahr 2013/2014 gestarteten Workshops für Schülerinnen und Schüler zum Umgang mit persönlichen Daten im Internet[5] mit Erfolg fortgeführt. Bis zum Jahresende 2016 konnten mittlerweile über 7.000

[5] Vgl. hierzu 25. Tätigkeitsbericht, 2013/2014, Kapitel 15.2, S. 93.

Schülerinnen und Schüler in den sechsten Klassen der weiterführenden Schulen in der praktischen Anwendung erlernen, im Internet verantwortungsvoll mit den eigenen Daten und respektvoll mit den Daten anderer umzugehen. Die insgesamt sehr positiven Rückmeldungen seitens der Schülerinnen und Schüler sowie der Lehrer und Eltern waren allerdings immer häufiger verbunden mit der Bitte, auch für jüngere Kinder solche Unterrichtseinheiten anzubieten.

Tatsache ist, dass sich Kinder immer früher im Internet bewegen. Laut einer Umfrage des Digitalverbands Bitkom aus dem Jahre 2014 gehört das Internet für die meisten Kinder ab einem Alter von 8 Jahren zum Alltag, mit 10 Jahren sind bereits alle Kinder online. Spätestens in diesem Alter beginnt auch die Nutzung Sozialer Netzwerke.[6] Insofern ist es wichtig, die Kinder bereits bei ihren ersten Schritten im Internet zu begleiten und sie auf altersgerechte Weise zu einem eigenverantwortlichen und bewussten Umgang mit dem Internet anzuleiten. Daher haben wir uns entschlossen – wie bereits bei unseren Workshops an weiterführenden Schulen aufbauend auf einem pädagogischen Konzept des rheinland-pfälzischen Landesbeauftragten für Datenschutz und Informationsfreiheit – ab dem zweiten Schulhalbjahr 2016/2017 nunmehr auch in der vierten Klassenstufe in Grundschulen kostenlose Workshops in einem Umfang von zwei Schulstunden anzubieten (vgl. Kapitel 11.3).

1.3.3 Personalsituation

Allgemein ist in den vergangenen Jahren das Thema Datenschutz sehr viel mehr in das Bewusstsein der Menschen gerückt. Dies führt dazu, dass sich zunehmend mehr Betroffene mit Beschwerden über Unternehmen und öffentliche Stellen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten an unsere Dienststelle wenden – und das nicht nur im Bereich Videoüberwachung, obwohl in diesem Bereich die Anzahl der Beschwerden seit Jahren stetig ansteigt.

Aber auch bei den datenverarbeitenden Stellen ist eine Sensibilisierung für Fragen des Datenschutzes festzustellen, so dass den gesetzlich festgelegten Verpflichtungen, unsere Stellungnahme zu Datenverarbeitungsvorgängen einzuholen, deutlich häufiger nachgekommen wird als noch vor wenigen Jahren. Ebenso wird sowohl von öffentlichen Stellen als auch von Unternehmen bei der Einführung neuer Verfahren und bei sonstigen Datenschutzfragen eine datenschutzrechtliche Beratung durch unsere Dienststelle vermehrt in Anspruch genommen.

Darüber hinaus ist auch der Prüfungsaufwand - sei es durch neue, den Datenschutzbehörden gesetzlich festgelegte Datenschutzkontrollen bei Sicherheitsbehörden oder sei es allgemein aufgrund komplexerer technischer Verfahren - vielfach deutlich gestiegen.

Dies hat bereits jetzt zu einer erheblichen Mehrbelastung innerhalb der Dienststelle geführt.

---

[6] Vgl. https://www.bitkom.org/Presse/Presseinformation/Smartphone-und-Internet-gehoeren-fuer-Kinder-zum-Alltag.html

Darüber hinaus sind die Mitarbeiterinnen und Mitarbeiter seit der Verabschiedung der DS-GVO intensiv damit befasst, die notwendigen Vorarbeiten bis zum Inkrafttreten dieses neuen europäischen Rechtsrahmens zu leisten. Hierzu gehört neben einer Einarbeitung in die abstrakten Vorschriften der DS-GVO auch ein verstärkter Abstimmungsbedarf mit den verschiedenen Arbeitskreisen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und den Arbeitsgruppen des Düsseldorfer Kreises.

Dies alles hat dazu geführt, dass im Berichtszeitraum nahezu keine anlasslosen datenschutzrechtlichen Prüfungen durchgeführt werden konnten, obwohl gerade diese gesetzlich vorgesehene Aufgabe ein wichtiges Instrument ist, bei datenverarbeitenden Stellen eine Sensibilisierung für Fragen des Datenschutzes zu wecken. Ebenso wenig konnte der steigenden Zahl von Beratungsersuchen durch öffentliche und nicht-öffentliche Stellen, die ihre Verfahren gleichfalls den Anforderungen der DS-GVO anpassen müssen, in dem gewünschten Umfang nachgekommen werden.

Neben dem bereits dargestellten Aufgabenzuwachs werden mit Inkrafttreten der DS-GVO zahlreiche neue verpflichtend durchzuführende, auch fristgebundene Aufgaben auf das Unabhängige Datenschutzzentrum zukommen. Die DS-GVO sieht neben einer Vielzahl von Befugnissen zur Herstellung datenschutzkonformer Zustände auch umfangreiche – weit über den bisherigen gesetzlichen Rahmen hinausgehende - Beratungspflichten für die Aufsichtsbehörden vor. Von besonderem Gewicht wird auch die Zusammenarbeit mit anderen Datenschutzaufsichtsbehörden sowohl auf nationaler Ebene als auch auf europäischer Ebene sein, da diese Abstimmungsprozesse für eine einheitliche Anwendung der europäischen Regelungen in allen Mitgliedstaaten zwingend erforderlich sind. Um den gesetzlichen Anforderungen gerecht zu werden, wird daher in den kommenden Jahren eine deutliche Personalaufstockung der Dienststelle unumgänglich sein.

2 Technisch-organisatorischer Datenschutz

2.1 Auslagerung der Datenverarbeitung der Landesverwaltung an das IT-Dienstleistungszentrum

Zum 1. Januar 2016 wurde die bisherige Zentrale Datenverarbeitungsstelle des Saarlandes (ZDV-Saar), die bis dahin zum Landesamt für Zentrale Dienste gehörte, mitsamt ihren Aufgaben und den rund 150 Mitarbeitern/-innen in ein eigenständiges Landesamt für IT-Dienstleistungen überführt. Gesetzliche Grundlage hierfür bildet das Gesetz zur Errichtung eines Landesamtes für IT-Dienstleistungen vom 2. Dezember 2015. Nach dessen § 2 hat das IT-Dienstleistungszentrum (IT-DLZ) als zentraler Informations- und Kommunikationsdienstleister der Landesverwaltung unter anderem die Aufgabe, die Fachverfahren der Landesverwaltung zu betreiben. Um die mit einer solchen Zentralisierung und Professionalisierung der IT verfolgten Ziele zu gewährleisten, korrespondiert die Aufgabenzuweisung an das IT-DLZ mit einer Nutzungsverpflichtung für das Dienstleistungsangebot des IT-DLZ, indem die fachlich zuständigen Landesbehörden den Betrieb ihrer Fachverfahren auf das IT-DLZ zu übertragen haben.

Wir waren im Berichtszeitraum mit der Frage befasst, wie die mit dem Betrieb der Fachverfahren zusammenhängenden Verarbeitungen personenbezogener Daten durch das IT-DLZ datenschutzkonform ausgestaltet werden können.

Da das Gesetz zur Errichtung eines Landesamtes für IT-Dienstleistungen lediglich reine Aufgabennormen enthält, bedürfen die mit der Übertragung der Fachverfahren verbundenen Verarbeitungen personenbezogener Daten aus datenschutzrechtlicher Sicht einer eigenen rechtlichen Grundlage bzw. einer entsprechenden Befugnisnorm.

Hierbei ist zu berücksichtigen, dass bei einem Betrieb des Fachverfahrens durch das IT-DLZ die inhaltliche Verantwortung bei der zuständigen Fachbehörde verbleibt und das IT-DLZ lediglich technischer Dienstleister ist. Die für das Fachverfahren zuständige Fachbehörde entscheidet weiterhin über die Zwecke der Verarbeitung personenbezogener Daten und über inhaltliche Fragen, die den Kern der Rechtmäßigkeit der Verarbeitung wesentlich betreffen. Die Fachbehörde legt insbesondere fest, welche personenbezogenen Daten erhoben und gespeichert werden, wie lange diese aufbewahrt bzw. wann sie gelöscht werden oder an wen personenbezogene Daten weitergegeben werden (dürfen). Die Fachbehörde ist damit auch in den Fällen, in denen das IT-DLZ den Betrieb des Fachverfahrens technisch sicherstellt, weiterhin als die für die Verarbeitung verantwortliche Stelle anzusehen. Das IT-DLZ hat in Bezug auf den konkreten Datenumgang keinen Ermessens- oder Entscheidungsspielraum im Hinblick auf die Rechtmäßigkeit der Verarbeitung. Vielmehr erschöpft sich der Entscheidungsspielraum des IT-DLZ in technischen oder organisatorischen Fragestellungen, um den technischen Betrieb des Fachverfahrens zu gewährleisten bzw. entsprechend zu betreuen.

Aus datenschutzrechtlicher Sicht handelt es sich daher bei der Auslagerung des Betriebs von Fachverfahren an das IT-DLZ um rein technische Hilfs- und Unterstützungsaufgaben, die rechtlich eine Datenverarbeitung im Auftrag darstellt und die den gesetzlichen Anforderungen des § 5 SDSG genügen muss.

§ 5 Abs. 1 Verarbeitung personenbezogener Daten im Auftrag

Werden personenbezogene Daten im Auftrag einer öffentlichen Stelle verarbeitet, so bleibt sie verantwortliche Stelle im Sinne dieses Gesetzes. Die Auftragsnehmerin oder der Auftragnehmer ist unter besonderer Berücksichtigung ihrer oder seiner Eignung sorgfältig auszuwählen. Der Auftrag ist schriftlich unter Festlegung von Gegenstand und Umfang der Datenverarbeitung zu erteilen. Er muss Weisungen zur Umsetzung der Vorgaben des § 11 enthalten. Die Auftragnehmerin oder der Auftragnehmer darf personenbezogene Daten nur im Rahmen des vertraglich Festgelegten verarbeiten. Unterauftragsverhältnisse bedürfen ausdrücklicher Zustimmung. Die Auftraggeberin oder der Auftraggeber hat darauf zu achten, dass bei der Auftragnehmerin oder dem Auftragnehmer die nach § 11 Absatz 2 erforderlichen Maßnahmen getroffen sind.

Um den hohen Aufwand einer großen Zahl von Einzelvereinbarungen nach § 5 SDSG zu vermeiden, wurde mit dem zuständigen Ministerium für Finanzen und Europa eine Lösung erarbeitet, mit der eine Auftragsdatenverarbeitung gesetzlich angeordnet werden soll. Eine entsprechende Regelung soll zeitnah in das Gesetz zur Errichtung eines Landesamtes für IT-Dienstleistungen eingefügt werden.

2.2 Verbindungsverschlüsselung bei der Anbindung von externen Standorten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 27. März 2014 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“[7] folgendes festgehalten:

Die Enthüllungen von Edward Snowden haben gezeigt, dass der Zugriff auf Daten besonders einfach ist, wenn sie an Netzknoten unverschlüsselt vorliegen oder innerhalb interner Netze unverschlüsselt übertragen werden.

Diese Gefahr des unbefugten Zugriffs besteht natürlich auch bei öffentlichen Stellen des Landes. § 11 Abs. 1 S. 2 Saarländisches Datenschutzgesetz (SDSG) sieht in Bezug auf die zu ergreifenden technischen und organisatorischen Maßnahmen ausdrücklich vor, dass automatisierte Verfahren nur dann eingesetzt werden dürfen, wenn sichergestellt ist, dass keine Gefahren für das informationelle Selbstbestimmungsrecht bestehen oder diese durch Maßnahmen nach Abs. 2 verhindert werden können. Nach § 11 Abs. 2 S. 4 SDSG muss der Anbieter gewährleisten, dass personenbezogene Daten während der elektronischen Übermittlung oder ihres Transportes nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

[7] Vgl. 25. Tätigkeitsbericht, 2013/2014, Kapitel 4.2, S. 26-28.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt im Baustein „B 2.12 IT-Verkabelung“[8] die Grundlagen für eine leistungsfähige, gut abgesicherte IT-Verkabelung. Im Rahmen der Maßnahme „M 2.395 Anforderungsanalyse für die IT-Verkabelung“[9] wird ausgeführt, dass *„die Vertraulichkeit und Integrität der transportierten Daten alternativ oder ergänzend mit Hilfe von kryptographischen Verfahren geschützt werden“* kann.

Selbst wenn ein externer Standort per dedizierter Glasfaserleitung (und nicht „über das Internet“) angebunden wird, diese Anbindung jedoch unverschlüsselt erfolgt, kann ein unberechtigter Zugriff durch Dritte (beispielsweise bei physischem Zugriff auf die genutzte Netzleitung) nicht ausgeschlossen werden, auch wenn ein weitaus größerer technischer Aufwand für den potentiellen Lauscher an der Leitung erforderlich ist.

Daher fordern wir bei der Anbindung von externen Standorten spätestens bei der Übermittlung von Daten mit hohem Schutzbedarf ausdrücklich dazu auf, die Anbindung mit einer sicheren Verschlüsselung zu versehen.

2.3 Transportverschlüsselung von Internetseiten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 27. März 2014 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“[10] die Anbieter elektronischer Kommunikationsdienste dazu aufgefordert, Maßnahmen zur sicheren Verschlüsselung beim Transport und bei der Speicherung von Daten zu treffen.

Im Rahmen einer Eingabe und anschließender Überprüfung stellten wir fest, dass eine erhebliche Anzahl der Internetauftritte öffentlicher Stellen im Saarland nicht verschlüsselt war. Über diese Internetseiten werden teilweise auch Formulare zur Kontaktaufnahme angeboten, mit denen personenbezogene Daten übertragen werden können. Diese Daten können bei einer unverschlüsselten Übertragung potentiell von unbefugten Dritten mitgelesen bzw. unbemerkt verändert werden.

Für eine datenschutzrechtliche Beurteilung sind sowohl die Datenschutzregelungen des Telemediengesetzes (TMG) als auch die Vorschriften des Saarländischen Datenschutzgesetzes (SDSG) heranzuziehen.

Gem. § 13 Abs. 7 Nr. 2a TMG haben Diensteanbieter durch technische und organisatorische Vorkehrungen sicherzustellen, dass Telemedien gegen Verletzungen des Schutzes personenbezogener Daten gesichert sind. Entsprechende Vorkehrungen müssen den Stand der Technik berücksichtigen, wobei insbesondere ein als sicher anerkanntes Verschlüsselungsverfahren angewendet werden muss.

---

8 Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b02/b02012.html

9 Vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02395.html

10 Vgl. 25. Tätigkeitsbericht, 2013/2014, Kapitel 4.2, S. 26-28.

Auch gem. § 11 Abs. 2 S. 4 SDSG muss der Anbieter gewährleisten, dass personenbezogene Daten während der elektronischen Übermittlung oder ihres Transportes nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Wir vertreten die Auffassung, dass Internetseiten öffentlicher Stellen spätestens beim Einsatz von Kontaktformularen mit einer Transportverschlüsselung zu versehen sind.

Um eine sichere und vertrauensvolle Bereitstellung von Internetangeboten zu gewährleisten, schrieben wir alle betroffenen Kommunalverwaltungen sowie die Landesverwaltung an und wiesen auf die geltende Rechtslage sowie die Entschließung der Datenschutzbeauftragten des Bundes und der Länder durch zeitnahe Einführung einer Transportverschlüsselung (SSL/TLS) hin.

Daraufhin führten fast alle Verwaltungen eine Transportverschlüsselung ein bzw. werden diese im Rahmen der Neugestaltung ihres Internetauftritts einführen. Mit den öffentlichen Stellen, bei denen noch keine Umsetzung erfolgt ist, stehen wir im Dialog, damit auch mit diesen Stellen eine sichere Kommunikation erfolgen kann.

2.4 Standard-Datenschutzmodell (SDM)

Das Standard-Datenschutzmodell (SDM)[11] stellt „eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele“ dar.

Die 92. Datenschutzkonferenz am 9. und 10. November 2016 hat das Standard-Datenschutzmodell als "Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele" zustimmend zur Kenntnis genommen. Herausgeber ist der Arbeitskreis Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. Für die Redaktion zeichnet die Unterarbeitsgruppe „Standard-Datenschutzmodell“ des Arbeitskreises Technik verantwortlich.

Das SDM befindet sich aktuell mit der Version V.1.0 in der Erprobungsphase und soll von den Aufsichtsbehörden evaluierend angewendet werden.

2.4.1 Zweck des Standard-Datenschutzmodells

Das Modell richtet sich einerseits an die für die Verarbeitung personenbezogener Daten verantwortlichen Stellen. Diese können mit dem SDM die erforderlichen Funktionen und Schutzmaßnahmen systematisch planen, umsetzen und kontinuierlich überwachen. Das Modell richtet sich andererseits an die Datenschutzbehörden, um mit einer einheitlichen Systematik zu einem transparenten, nachvollziehbaren und belastbaren Gesamturteil über ein Verfahren und dessen Komponenten zu gelangen.

Ausgangspunkt der Analyse ist die Bestimmung der für die Verarbeitung verantwortlichen Stelle oder Stellen sowie des Zwecks der Verarbeitung im Kontext der mit dem Verfahren umgesetzten oder unterstützten Geschäftsprozesse und der relevanten Rechtsgrundlagen. Erst diese rechtlich zu erzielende Bestimmtheit ermöglicht es, die

[11] Vgl. Das Standard-Datenschutzmodell, V.1.0., https://datenschutz.saarland.de/fileadmin/themen/SDM-Methode_V_1_0.pdf

Funktionalität des Verfahrens einschließlich des erforderlichen Umfangs der Verarbeitung personenbezogener Daten und der angemessenen Schutzmaßnahmen entsprechend dem Stand der Technik festzulegen.

2.4.2 Struktur des Standard-Datenschutzmodells

Das Standard-Datenschutzmodell

- überführt datenschutzrechtliche Anforderungen in einen Katalog von Gewährleistungszielen,
- gliedert die betrachteten Verfahren in die Komponenten Daten, IT-Systeme und Prozesse,
- berücksichtigt die Einordnung von Daten in drei Schutzbedarfsabstufungen,
- ergänzt diese um entsprechende Betrachtungen auf der Ebene von Prozessen und IT-Systemen und
- bietet einen hieraus systematisch abgeleiteten Katalog mit standardisierten Schutzmaßnahmen.

2.4.3 Die Gewährleistungsziele

Neben dem grundlegenden Gewährleistungsziel „Datenminimierung“ und den klassischen Gewährleistungszielen der Datensicherheit („Verfügbarkeit“, „Integrität“ und „Vertraulichkeit“) verwendet das SDM die drei auf den Schutz Betroffener ausgerichteten Gewährleistungsziele „Nichtverkettung“, „Transparenz“ und „Intervenierbarkeit“.

2.4.4 Die generischen Maßnahmen zur Umsetzung der Gewährleistungsziele

Für jede der Komponenten des SDMs (Daten, Systeme und Prozesse) werden für jedes der Gewährleistungsziele im Anhang Referenzmaßnahmen (beispielsweise die Festlegung einer geeigneten Anonymisierungsmethode) benannt und beschrieben. Für jede der Maßnahmen sind auch die Auswirkungen auf den Erreichungsgrad von anderen, von der Maßnahme nicht direkt betroffenen Gewährleistungszielen zu betrachten. So können bestimmte Einzelmaßnahmen zur Erreichung mehrerer Gewährleistungsziele beitragen.

2.4.5 Der Schutzbedarf

Jede Verarbeitung personenbezogener Daten durch eine Organisation stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Das betrifft auch solche Verarbeitungen, die aus datenschutzrechtlicher Sicht zulässig sind, also auf der Basis einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung erfolgen. Eine Organisation muss deshalb nachweisen, dass sie diesen Eingriff auf das erforderliche Maß beschränkt, die Eingriffsintensität also minimiert (siehe bspw. Art. 5 Abs. 2 und Art. 24 Abs. 1 Datenschutzgrundverordnung (DS-GVO)). Diesen Nachweis kann sie erbringen, indem sie darstellt, auf welche Weise sie die Gewährleistungsziele umsetzt.

Bei der Ermittlung des Schutzbedarfs nimmt das SDM die Perspektive des Betroffenen und dessen Grundrechtsausübung ein und unterscheidet sich daher von der

Sicht des IT-Grundschutzes. Hierbei wird zum einen die Eingriffsintensität in die Grundrechte (von Personen) durch ein Verfahren betrachtet. Maß für die Eingriffsintensität ist dabei unter anderem der durch die entsprechende Rechtsgrundlage bestimmte Zweck der Datenverarbeitung, die Schutzbedürftigkeit, die Dauer der Speicherung, sowie die Art und Anzahl möglicher Empfänger der verarbeiteten Daten. Zum anderen spielt das Gewährleistungsziel „Vertraulichkeit" eine besondere Rolle für die Bestimmung des Schutzbedarfs.

Die sich daraus ableitenden Schutzbedarfskategorien sind:

- „normal"
- „hoch"
- „sehr hoch"

2.4.6 Risikoanalyse

Neben einer Betrachtung des Eingriffs in die Grundrechte ist eine Risikoanalyse notwendig, in deren Ergebnis beurteilt werden soll, wie groß die Wahrscheinlichkeit ist, dass die betreffende Organisation trotz aller getroffenen Maßnahmen zum Schutz der Grundrechte Datenschutzvorgaben nicht einhalten wird. Aus dieser Risikoanalyse können sich zusätzliche Schutzmaßnahmen ergeben, die die aus der Eingriffsintensität resultierenden Maßnahmen ergänzen.

2.4.7 Prüfen und Beraten auf Grundlage des Standard-Datenschutzmodells

Für die Anwendung des SDM bestehen zwei Voraussetzungen: Erstens Klarheit über die sachlichen Verhältnisse, im Rahmen derer die zu betrachtende Datenverarbeitung stattfindet bzw. stattfinden soll, und zweitens eine materiell-rechtliche Beurteilung dieser Verarbeitung.

Der Kern der Anwendung des SDM besteht im Vergleich der Referenzmaßnahmen, die sich aus den betrachteten und wie oben konkretisierten Gewährleistungszielen ableiten lassen, mit den von der verantwortlichen Stelle geplanten bzw. in der Prüfung festgestellten Maßnahmen. Abweichungen sind danach zu gewichten und zu beurteilen, inwieweit sie das Erreichen der Gewährleistungsziele gefährden. In einem Prüfvorgang erlaubt die bis zu diesem Punkt geführte Analyse aus einem Verfehlen der Gewährleistungsziele auf (ggf. sanktionierbare) datenschutzrechtliche Mängel zu schließen.

2.4.8 Fazit

Das Standard-Datenschutzmodell soll als ganzheitliches Prüf- und Beratungskonzept zu einem abgestimmten, transparenten und nachvollziehbaren System der datenschutzrechtlichen Bewertung führen.

Hierbei kann das SDM sowohl die verantwortlichen Stellen bei der Verarbeitung personenbezogener Daten als auch die Aufsichtsbehörden im Rahmen ihrer Zusammenarbeit unterstützen.

Dieser Mehrwert wird nun im Rahmen der aktuell stattfindenden Erprobungsphase evaluiert.

2.5 Anti-Spy-Sticker

Webcams ermöglichen nicht nur die Videotelefonie über das Internet, sie sind auch ein wichtiger Bestandteil der heutigen Digitalkultur und in vielen Geräten wie Smartphones, Tablets, Notebooks und Smart-TVs integriert. Für Webcam-Hacker ist es ein Leichtes, unbemerkt die Kontrolle über eine Webcam zu erlangen.

Im industriellen Bereich kann durch Spionage ein wirtschaftlicher Schaden entstehen. Im privaten Bereich können Webcam-Hacker leicht in die Privatsphäre anderer eindringen und sie unbemerkt beobachten.

Im Internet kursieren zahlreiche Tools, die einen Webcam-Hack und damit eine Bespitzelung möglich machen. So ist beispielsweise ein Krimineller in die Computer von mehr als 150 Schülerinnen eingedrungen, um diese zu beobachten.[12]

Technisch gesehen ist ein Webcam-Hacker-Angriff ohne Schwierigkeiten umsetzbar, da der Angreifer nur mittels eines Trojaners in den fremden Rechner eindringen muss. Es ist ein Irrglaube anzunehmen, das leuchtende LED-Signal sei ein einfacher Indikator für die Kameraaktivität, denn ein guter Hacker kann auch dies umgehen.

Aber auch ohne Schadsoftware kann man durch fehlerhafte Webcam-Software oder die Verwendung von zu simplen Passwörtern (wie 123456) Opfer von Webcam-Hackern werden.

Eine wirksame Lösung bietet nur ein physischer Schutz, also das Abkleben der Webcam!

Um über die Gefahren bei der Nutzung von Webcams aufzuklären und vor unzulässigen Eingriffen in die Privatsphäre zu schützen, haben wir unsere Anti-Spy-Sticker konzipiert, die wir u.a. bei unseren Veranstaltungen kostenlos verteilen.

2.6 Veranstaltungsreihe „IT-Sicherheit und Datenschutz im kommunalen Umfeld – Anforderungen und Herausforderungen“

Gemeinsam mit dem Zweckverband eGo-Saar hat unsere Dienststelle die Veranstaltungsreihe „IT-Sicherheit und Datenschutz im kommunalen Umfeld – Anforderungen und Herausforderungen“ durchgeführt.

Die technologische Durchdringung und Vernetzung von Verwaltungen nimmt zu, während gleichzeitig die IT-Systeme und Infrastrukturen immer komplexer werden und die Kommunen vor neue Herausforderungen im Hinblick auf IT-Grundschutz und operativen Datenschutz stellen.

So müssen IT-Verfahren und die damit verarbeiteten Daten der Bürger mit immer höherem Aufwand gegen Angriffe von außen geschützt werden. Dies wird dadurch verschärft, dass immer wieder schwere Sicherheitslücken in IT-Systemen entdeckt werden und die Werkzeuge zur Ausnutzung dieser Verwundbarkeiten einer immer

[12] Vgl. https://www.heise.de/security/meldung/Cyber-Spanner-beobachtet-Schuelerinnen-ueber-deren-Webcams-1039630.html, aufgerufen am: 9. Februar 2017.

größer werdenden Anzahl an Angreifern zur Verfügung stehen, die diese aus der Anonymität des globalen Cyberraums für ihre Zwecke einsetzen. Diese Cyberangriffe finden täglich statt und werden zunehmend professioneller und zielgerichteter durchgeführt. Hierbei stehen verstärkt auch staatliche Stellen sowie Betreiber sog. „Kritischer Infrastrukturen" (KRITIS) im Fadenkreuz.

Im Jahre 2015 erfolgte auf das Verfahren „kfz21" der Zulassungsbehörden in Hessen und Rheinland-Pfalz über das Internetmodul „Kfz-Wunschkennzeichen" ein Hackerangriff mit der Folge, dass nahezu alle Zulassungsstellen in beiden Ländern handlungsunfähig waren. Dies zeigt sehr deutlich, dass auch kommunale Daten bzw. Informationen mittlerweile ein beliebtes Ziel krimineller Aktivitäten sind.

Zudem trägt die Kommune die Verantwortung dafür, dass bei den von ihr bzw. in ihrem Auftrag betriebenen Datenverarbeitungsprozessen technische und organisatorische Vorkehrungen getroffen werden, die innerhalb der Verwaltung, aber auch bei externen Dienstleistern und Kooperationspartnern das Recht auf informationelle Selbstbestimmung der Bürger sicherstellen.

Vor diesem Hintergrund verlangt der Gesetzgeber, dass sowohl automatisierte (Ratsinformationssysteme, Videoüberwachungsanlagen) als auch nicht-automatisierte Verfahren (Leerstandsmanagement, Personalaktenführung) so auszugestalten sind, dass sie die Verfügbarkeit, die Integrität und die Vertraulichkeit der personenbezogenen Daten gewährleisten, die Zweckbindung der Datenverarbeitung(en) sicherstellen und Verfahren zur Ausübung von Betroffenenrechten und zur Herstellung von Transparenz gegenüber dem Bürger implementieren.

Im Rahmen der Veranstaltungen wurde auf die Grundlagen und rechtlichen Rahmenbedingungen der IT-Sicherheit eingegangen und die Themen Datenschutz und Datensicherheit mittels Praxisbeispielen (z.B. Nutzung von Tabletcomputern zum Zugriff auf ein Ratsinformationssystem) erörtert.

3 Polizei

3.1 Änderungsbedarf des Saarländischen Polizeigesetzes – Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Ausgestaltung polizeilicher Ermittlungsbefugnisse

Bereits im Kapitel „Überblick" nehmen wir unter Ziffer 1.2.2 auf die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) zum Bundeskriminalamtgesetz (BKAG) Bezug (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378). In dieser Entscheidung hatte das Bundesverfassungsgericht unter anderem die Voraussetzungen für polizeiliche Ermittlungsbefugnisse auf der Grundlage des BKAG verfassungsrechtlich bewertet und dabei insbesondere die Voraussetzungen für die Durchführung von heimlichen Überwachungsmaßnahmen in grundsätzlicher Weise zusammengeführt und konkretisiert. Diese Ausführungen werfen Zweifel an der Vereinbarkeit von Regelungen im Bereich der §§ 25 bis 40 Saarländisches Polizeigesetz (SPolG) mit verfassungsrechtlichen Vorgaben auf, die eine grundsätzliche Neubewertung erforderlich machen und einen erheblichen Anpassungsbedarf des SPolG zur Folge haben. Dies gilt im besonderen Maße für die Berücksichtigung des Eingriffsgewichts von heimlichen Überwachungsmaßnahmen, der daran anknüpfenden Festlegung von Eingriffsvoraussetzungen und der Bestimmung des Adressatenkreises. Auf die einzelnen Punkte soll im Folgenden am Beispiel der Norm des § 28 SPolG näher eingegangen werden, die die zentrale Vorschrift für heimliche Überwachungsbefugnisse darstellt. Auf andere Vorschriften, beispielsweise die §§ 28a und 28b SPolG, sind die folgenden Ausführungen entsprechend übertragbar.

3.1.1 Eingriffsgewicht

Verfassungsrechtlich bedenklich ist der in § 28 Abs. 1 Nr. 1 und 2 SPolG gestattete Einsatz heimlicher Überwachungsmittel zur vorbeugenden Bekämpfung von Verbrechen und anderen gewerbs-, gewohnheits- oder bandenmäßig begangenen Straftaten. Das BVerfG hat hierzu ausgeführt, dass entsprechende Befugnisse auf Grund ihrer Dauer, ihrer Heimlichkeit und unter Nutzung moderner Technik im Einzelnen und erst recht gebündelt es ermöglichen, dass alle Äußerungen und Bewegungen der hiervon betroffenen Personen erfasst und bildlich wie akustisch festgehalten werden können. Die hiermit verbundenen Eingriffe in die Grundrechte sind von gravierendem Gewicht und dürfen nur zur Abwendung von besonders gewichtigen Rechtsgutverletzungen oder zur Verfolgung von erheblichen Straftaten gerechtfertigt werden. Diesen Anforderungen wird § 28 SPolG in der derzeitigen Ausgestaltung nur teilweise gerecht.

3.1.2 Eingriffsvoraussetzungen

Mit verfassungsrechtlichen Anforderungen nicht zu vereinbaren sind auch die Eingriffsvoraussetzungen des § 28 Abs. 1 SPolG. Die Vorschrift stellt nicht auf das Vorhandensein einer konkreten Gefahr ab, sondern verfolgt mit der Begrifflichkeit der vorbeugenden Bekämpfung von Verbrechen oder gewerbs-, gewohnheits- oder bandenmäßig bzw. in anderer Weise organisiert begangenen Taten schon im Vorfeld einer konkreten Gefahr sowohl das Ziel der Verhütung von Straftaten als auch das Ziel der Gefahrenvorsorge. Mit diesen Zielen lässt es § 28 Abs. 1 SPolG bereits ausreichen, wenn auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass eine solche Straftat begangen werden soll.

Bei Maßnahmen zur Straftatenverhütung und erst recht bei Maßnahmen zur Straftatenvorsorge verlangt das Gebot der Normenbestimmtheit zumindest eine auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützte Prognose, die auf eine konkrete Gefahr bezogen ist. Grundsätzlich gehört hierzu, dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist. (BVerfG, Urteil vom 20. April 2016, a.a.O., Rn. 164). Eine gesetzliche Formulierung, nach der die eingriffsintensive Datenerhebung zulässig ist, „*wenn Tatsachen die Annahme rechtfertigen, dass die Person Straftaten (...) begehen wird*" oder anders formuliert, wenn auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass eine bestimmte Straftat begangen werden soll (so in § 28 Abs. 1 SPolG), genügt diesen Anforderungen nach Aussage des Bundesverfassungsgerichts nicht, da sie den Behörden und Gerichten keine hinreichend bestimmten Kriterien an die Hand gibt, aber Maßnahmen eröffnet, die unverhältnismäßig weit sein können.

3.1.3 Adressaten der Maßnahmen

Verfassungsrechtliche Bedenken bestehen weiter auch im Hinblick auf die Bestimmung der Adressaten heimlicher Überwachungsmaßnahmen. Diesbezüglich nimmt § 28 Abs. 1 SPolG Bezug auf die in § 26 Abs. 2 Nr. 1 und Nr. 2 SPolG genannten Personen.

§ 26 Abs. 2 Nr. 1 SPolG erfasst zum einen solche Personen, bei denen Anhaltspunkte bestehen, dass sie künftig Straftaten begehen. Auf die obigen Ausführungen zum Erfordernis der Erkennbarkeit eines seiner Art nach konkretisierten und absehbaren Geschehens zur Bestimmung der Adressaten von Maßnahmen wird insofern Bezug genommen.

Zum anderen dürfen sich durch Verweis auf § 26 Abs. 2 Nr. 2 SPolG Ermittlungsmaßnahmen auch gegen Kontakt- und Begleitpersonen richten. Dies unter der Voraussetzung, dass Anhaltspunkte dafür bestehen, dass sie mit einer der in Nummer 1 genannten Personen bezüglich künftiger Straftaten in Verbindung stehen. Zwar ist es nicht grundsätzlich zu beanstanden, dass sich Überwachungsmaßnahmen auch gegen selbst nicht verantwortliche Personen richten; Voraussetzung jedoch ist der auf Tatsachen gestützte Nachweis, dass eine gewisse Nähebeziehung zur verantwortlichen Person gegeben ist. Die Kriterien zur Bestimmung dieser Nähebeziehung

sind in bestimmter und normenklarer Weise vorzugeben. Auch hier besteht ein entsprechender gesetzlicher Anpassungsbedarf.

3.1.4 Weiterer Anpassungsbedarf

Darüber hinaus fordert das Bundesverfassungsgericht bei der gesetzlichen Ausgestaltung heimlicher Überwachungsbefugnisse besondere Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz von Berufsgeheimnisträgern.

Es verlangt zudem die Gewährleistung einer effektiven aufsichtlichen, parlamentarischen und öffentlichen Kontrolle. Die parlamentarische und öffentliche Kontrolle soll durch entsprechende Berichtspflichten gewährleistet werden, die aufsichtliche Kontrolle durch regelmäßige Prüfungen der Landesbeauftragten für den Datenschutz, die durch vollständige Protokollpflichten flankiert werden sollen. Diese sollen sicherstellen, dass den Landesdatenschutzbeauftragten bei ihren Prüfungen Daten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält.

Schließlich fordert das Bundesverfassungsgericht die Normierung von Löschungspflichten und die Festlegung von Grenzen der Nutzung der aus heimlichen Überwachungsmaßnahmen erlangten Daten im Rahmen des ursprünglichen Erhebungszwecks und den Voraussetzungen einer zulässigen Zweckänderung.

3.2 Einsatz von Body-Cams durch die saarländische Polizei

Mit dem Ziel, Polizeibeamte künftig vor tätlichen Übergriffen besser zu schützen, sind in den vergangenen Jahren in verschiedenen Bundesländern Polizeibeamte mit Körperkameras, sog. Body-Cams, ausgestattet worden. Bei diesen Body-Cams handelt es sich um kleine Videokameras, die an der Kleidung der Polizeibeamten getragen und bei bestimmten Polizeieinsätzen aktiviert werden können.

Im Berichtszeitraum sollte auch die saarländische Polizei zur Eigensicherung der Beamten mit diesem Einsatzmittel ausgestattet werden.

3.2.1 Änderung des Saarländischen Polizeigesetzes

Während ursprünglich angedacht war, den Einsatz der Body-Cams in einem ersten Schritt als Pilotversuch auf der Grundlage der vorhandenen gesetzlichen Grundlagen einzuführen, wurde schließlich von diesen Überlegungen Abstand genommen und durch den Gesetzgeber eine Änderung des Saarländischen Polizeigesetzes (SPolG) auf den Weg gebracht.

Die im Gesetzgebungsverfahren in den Landtag eingebrachte und letztlich unverändert verabschiedete Regelung des § 27 Abs. 3 SPolG enthält neben der Befugnis,

Daten durch eine offene Anfertigung von Bild- und Tonaufzeichnungen zur Abwehr einer konkreten Gefahrensituation zu erheben, auch die Regelung, dass durch eine sog. Vorabaufnahme (sog. Pre-Recording-Funktion) bereits im Vorfeld einer Gefahrensituation Aufnahmen angefertigt werden können.

§ 27 Abs. 3 SPolG

Die Vollzugspolizei kann in öffentlich zugänglichen Räumen personenbezogene Daten kurzzeitig speichern (Vorabaufnahme) und durch die offene Anfertigung von Bild-und Tonaufzeichnungen erheben, soweit dies zum Schutz von Polizeivollzugsbeamtinnen oder Polizeivollzugsbeamten oder Dritten zur Abwehr einer konkreten Gefahr erforderlich ist. Auf Maßnahmen nach Satz 1 ist durch Schilder oder in sonstiger geeigneter Form hinzuweisen.

In § 27 Abs. 6 SPolG ist zudem bestimmt, dass die im Rahmen einer solchen Maßnahme getätigten Aufzeichnungen, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung erforderlich sind, unverzüglich zu löschen sind.

Obwohl in der öffentlichen Diskussion im Wesentlichen nur von einer Befugnis zum Einsatz von am Körper getragenen Kameras die Rede war, ermächtigt die neue Befugnisnorm allgemein zur Anfertigung von Bild- und Tonaufnahmen zum Schutz von Polizeibeamtinnen und -beamten, so dass hierdurch nicht nur der Einsatz von Body-Cams, sondern beispielsweise auch ein Technikeinsatz in oder aus Fahrzeugen ermöglicht wird.

Im Rahmen des parlamentarischen Anhörungsverfahrens hatte unsere Dienststelle die Möglichkeit, zu dem Gesetzesvorhaben Stellung zu nehmen.

Wenn auch das gesetzgeberische Anliegen, Polizeibeamte vor Übergriffen zu schützen, durchaus nachvollziehbar und begrüßenswert ist, war die Umsetzung des Vorhabens unter datenschutzrechtlichen Gesichtspunkten an verschiedenen Stellen kritikwürdig.

Bedenken bestanden insbesondere hinsichtlich der Bestimmtheit und Klarheit der Regelung zur sog. Pre-Recording-Funktion, der Verhältnismäßigkeit der gesetzlich geforderten Gefahrenlage sowie der Löschfristen.

Nach den Ausführungen in der Gesetzesbegründung soll durch die Formulierung *„Die Vollzugspolizei kann (…) personenbezogene Daten kurzzeitig speichern (Vorabaufnahme)"* ermöglicht werden, dass eine Bildaufzeichnung für einen definierten Zeitraum bereits vor einer manuellen Aufzeichnungsauslösung verfügbar gehalten und diese erst bei manueller Auslösung der Aufzeichnung endgültig gespeichert wird.

Diese Funktion soll es den Polizeibeamten ermöglichen, das Entstehen einer Gefahrensituation zu dokumentierten. Allerdings wird diese Funktionsweise durch die Formulierung im Gesetzestext nicht hinreichend deutlich beschrieben.

Ebenso lässt sich auch nur der Gesetzesbegründung entnehmen, dass im Rahmen der Vorabaufnahme im Gegensatz zur nachfolgenden Aufnahme nur Bild- und nicht auch Tonaufnahmen zulässig sind.

Schließlich wäre aus Gründen der Rechtsklarheit auch eine Konkretisierung des Begriffs „kurzzeitig“ erforderlich gewesen, da nicht eindeutig ist, ob es sich hierbei um eine Speicherdauer von einem Zeitraum von wenigen Sekunden oder mehreren Minuten handelt.

Hinsichtlich der Gefahrenlage, die die Polizeibeamten zur Aktivierung der Videoaufnahmen berechtigen soll, hatten wir vor dem Hintergrund des ausdrücklichen gesetzgeberischen Ziels, Polizeivollzugsbeamte sowie auch Dritte vor gewalttätigen Übergriffen zu schützen, gefordert, den Gesetzeswortlaut diesem Ziel anzupassen und Aufnahmen nur bei einer konkreten Gefahr für Leib und Leben zuzulassen. Die im Gesetz gewählte Formulierung gibt hingegen keinen Hinweis auf das zu schützende Gut und lässt demnach Aufnahmen schon bei konkreten Gefahren für jedes polizeiliche Schutzgut (z.B. Ehre, Eigentum) zu. Damit können bereits drohende niedrigschwellige Verstöße gegen die öffentliche Sicherheit und Ordnung zur Aktivierung der Aufzeichnungen berechtigen. Angesichts des mit der Anfertigung von Ton- und Bildaufnahmen verbundenen erheblichen Eingriffs in das Recht auf informationelle Selbstbestimmung bestehen gegen diese weite Eingriffsbefugnis ernstliche Zweifel hinsichtlich der Angemessenheit und damit ihrer Verhältnismäßigkeit.

Zweifelhaft ist auch, ob die - den Grundrechtseingriff vertiefende - Befugnis zur Anfertigung von Tonaufnahmen ein geeignetes und erforderliches, mithin verhältnismäßiges Mittel zum Schutz der Polizeibeamten darstellt. Denn es ist nicht erkennbar, dass potentielle Angreifer durch zusätzliche Tonaufnahmen eher vor Übergriffen auf die Beamten abgehalten werden als durch das Anfertigen bloßer Bildaufnahmen. Es spricht hier vielmehr einiges dafür, dass dieses Mittel lediglich der Dokumentation beleidigender Äußerungen gegenüber den Beamtinnen und Beamten und damit repressiven Zwecken dienen soll. Dies entspricht jedoch nicht dem gesetzgeberischen Zweck, die Polizeibeamten vor Übergriffen zu schützen.

Um nicht nur den Polizeibeamten, sondern auch den von der Maßnahme Betroffenen eine Überprüfung der Rechtmäßigkeit der Maßnahme zu erlauben, wäre eine angemessen lange Aufbewahrungsdauer der Aufnahmen erforderlich. Die gesetzlich vorgesehene unverzügliche Löschung der Aufnahmen wird hingegen den Betroffenen im Regelfall keinen nachträglichen Zugriff auf die Aufnahmen erlauben.

In unserer Stellungnahme zu dem Gesetzentwurf wiesen wir zudem darauf hin, dass der Einsatz von Body-Cams von einer wissenschaftlichen Evaluation zur Klärung der Frage, ob der Einsatz von Body-Cams tatsächlich ein wirksames Mittel zur Verhinderung von Gewalt gegen Polizeibeamten darstellt, begleitet werden sollte.

Am 18. Mai 2016 hat der Landtag das Gesetz – wie oben erwähnt – unverändert verabschiedet.

3.2.2 Errichtungsanordnung

Kurz nach Inkrafttreten der Änderungen des Saarländischen Polizeigesetzes wurden für die Polizeiinspektionen Saarbrücken – St. Johann, Neunkirchen und Lebach für eine erste Erprobungsphase insgesamt 15 Body-Cams angeschafft und unsere

Dienststelle wurde vor dem Einsatz und dem Erlass der Errichtungsanordnung entsprechend den gesetzlichen Vorgaben beteiligt.

Im Rahmen der Anhörung wirkten wir insbesondere in den folgenden Bereichen auf Konkretisierungen in der Errichtungsanordnung hin:

Wie bereits oben ausgeführt, lässt das Gesetz durch die Verwendung des Begriffs „kurzzeitig" offen, wie lange der Zeitraum des sog. Pre-Recordings, also der Vorabaufnahme, zulässigerweise sein darf. Die Errichtungsanordnung sah hierzu ebenfalls keine Konkretisierung vor. Wir konnten uns mit dem Landespolizeipräsidium darauf einigen, dass eine Dauer von nicht mehr als 30 Sekunden als Höchstfrist für die Pre-Recording-Funktion in der Errichtungsanordnung festgelegt wird.

Ein aus unserer Sicht weiterer wichtiger Punkt war die Umsetzung der Transparenzerfordernisse des Gesetzes. Da es sich nach den gesetzlichen Voraussetzungen um eine offene Überwachung handelt, muss nicht nur der Beginn der Aufnahme mitgeteilt werden, sondern der Betrieb der laufenden Kamera muss für die Betroffenen erkennbar sein. Allein die Kennzeichnung der Beamten mit einer Weste ist hierfür nicht ausreichend. Hier war unsere Forderung, dass die Errichtungsanordnung konkrete Vorgaben dazu machen sollte, wie die Kennzeichnung durch die Polizeivollzugsbeamten vor Ort umzusetzen ist. Es konnte erreicht werden, dass die Erkennbarkeit der Body-Cam führenden Beamten nun nicht nur durch Funktionswesten mit einem hinweisenden Aufdruck "Videodokumentation" auf Brust und Rücken gewährleistet wird, sondern zusätzlich der konkrete Einsatz dem Betroffenen durch optische Signalisierung mittels roter LED, durch zusätzliche akustische Signalisierung der Aufzeichnung bei Beginn und Ende und mittels der Ausrichtung des an der Kamera angebrachten LCDs nach vorn erkennbar zu machen ist. Insbesondere diese zusätzlichen Transparenzmaßnahmen sollen dem polizeilichen Gegenüber die Möglichkeit eröffnen zu erkennen, ob und wann eine Aufnahme stattfindet.

Die Auslösung der Aufzeichnung erfolgt manuell durch den die Kamera führenden Polizeivollzugsbeamten und kann nicht durch andere Personen, beispielsweise in der Einsatzzentrale, fernausgelöst werden. Die angeschafften Body-Cams verfügen über keine Schnittstelle zur Daten-Fernübertragung. Aus diesem Grund ist auch eine Übertragung des Livebildes an die Einsatzzentrale nicht möglich.

Die Speicherung der Aufnahmen erfolgt zunächst ausschließlich auf der Kameraeinheit in verschlüsselter Weise. Nach Rückkehr zur Dienststelle werden die Aufzeichnungen mit Hilfe einer Bearbeitungs-, Verwaltungs- und Archivierungssoftware auf einen Auswerterechner übertragen, gespeichert und von den Kameraeinheiten gelöscht. Die aufgezeichneten Videosequenzen sind dort unverzüglich auszuwerten und Bildmaterial, das für eine Verfolgung von Straftaten oder von Ordnungswidrigkeiten von erheblicher Bedeutung irrelevant ist, ist zu löschen.

Die bereits erwähnte Bearbeitungs-, Verwaltungs- und Archivierungssoftware bildet die einzige Schnittstelle zur einzelnen Kameraeinheit. Vor der Verausgabung einer Kameraeinheit an den Polizeivollzugsbeamten wird die einzelne Body-Cam mit dem Bearbeitungs-, Verwaltungs- und Archivierungsprogramm an den Auswerterechner gekoppelt. Hierbei wird eine vorgegebene Kamerakonfiguration aufgespielt, die die technischen Einstellungen der Kamera verbindlich und für den die Kamera führenden

Polizeivollzugsbeamten unveränderbar festlegt. Ab diesem Zeitpunkt ist auch ein Zugriff auf den Speicherbereich der Kamera nicht mehr ohne die Verwaltungssoftware möglich.

Die Ausgabe der Kamerasysteme erfolgt ausschließlich durch die Dienstgruppenleitung. Diese hat auch zu gewährleisten, dass die einzelnen Geräte entsprechend den Vorgaben der Errichtungsanordnung vorkonfiguriert bzw. eingestellt sind und dass der Body-Cam-Einsatz nachvollziehbar dokumentiert wird. Ein Export von Aufnahmen, beispielsweise zur Übernahme als Beweismittel in das polizeiliche Vorgangsbearbeitungssystem ist ebenso wie eine Löschung von Aufnahmen nur durch die Dienstgruppenleitung möglich.

3.3 POLADIS Zentral

Im September 2014 übersandte uns das Ministerium für Inneres und Sport eine umfassend überarbeitete Errichtungsanordnung (EAO) zum Verfahren POLADIS (Polizeiliches Anwenderorientiertes Dokumentations- und Informationssystem) verbunden mit der Bitte um Wahrnehmung unserer Beteiligungsrechte. Grund hierfür waren aus Sicht des Landespolizeipräsidiums (LPP) festgestellte Fortschreibungsbedarfe der EAO hinsichtlich Zweck der Datei, Ausgestaltung der Suchfunktion, Ausweitung der Zugriffsberechtigungen und Änderungen / Anpassungen der technischen und organisatorischen Maßnahmen aufgrund einer zentralisierten Datenhaltung im Landesbetrieb für Daten und Information (LDI) in Rheinland-Pfalz.

Nach einer ersten Sichtung der neben der EAO teils bereits vorgelegten, teils von uns eingeforderten, sehr umfangreichen Verfahrensunterlagen (u.a. Berechtigungsmatrix, Screenshots zu bestimmten Eingabemasken der Anwender, die Dienstanweisung über Aufgaben, Organisation und Einsatz des Wach- und Streifendienstes, des Ermittlungs- und Servicedienstes und des Kriminaldienstes der Polizeiinspektionen) sowie diverser Anträge verschiedener Organisationseinheiten des LPP auf Ausweitung ihrer Zugriffsberechtigungen wurden in einer ersten Besprechung mit dem LPP grundsätzliche Fragestellungen erörtert und weitere für eine datenschutzrechtliche Freigabe notwendige Klärungsbedarfe formuliert:

- Ein wichtiger Punkt war dabei die in POLADIS vorgesehenen Such- und Recherchemöglichkeiten und die damit verbundenen Zugriffsoptionen. Nach § 11 Abs. 2 Nr. 3 Saarländisches Datenschutzgesetz (SDSG) ist durch technische und organisatorische Maßnahmen zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen und dass diese Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle). Im Falle von POLADIS ist vorgesehen, dass über drei Berechtigungsstufen der Umfang der Such- und Zugriffsmöglichkeit je Nutzer gesteuert werden kann. In der ersten Berechtigungsstufe (sog. Aliasbereich) erfasst die Suche nur die Vorgänge der eigenen Dienststelle. Die zweite und dritte Stufe ermöglichen hingegen eine landesweite Suche über alle beim LPP geführten Vorgänge

und differenzieren lediglich im Hinblick auf den Umfang der zugriffsberechtigten Datenfelder. Während in der zweiten Stufe der Zugriff nur auf einen Katalog von Grunddaten (z.B. Vorname, Name, Geburtsdatum, Status des Betroffenen wie Zeuge oder Beschuldigter, Vorgangsnummer und sachbearbeitende Dienststelle) je Verfahren begrenzt ist, ermöglicht die dritte Berechtigungsebene einen landesweiten, umfassenden und vollständigen Zugriff auf alle in POLADIS hinterlegten Daten. Hierzu gehören sämtliche Vorgangssachbearbeitungsdaten (z.B. Vermerke zum Tathergang, Zeugenvernehmung u.ä.) als auch Vorgangsverwaltungsdaten, die zum Suchzeitpunkt gespeichert sind. Solche tiefgreifenden Zugriffsberechtigungen sind insbesondere unter dem Aspekt der Erforderlichkeit zu prüfen. Hierbei war von Bedeutung, für welche Fälle der Anwender einer bestimmten Organisationseinheit tatsächlich zuständig ist und weshalb im Rahmen einer landesweiten Suchmöglichkeit Erkenntnisse wie Vorname, Name, Geburtsdatum, Status, Vorgangsnummer und sachbearbeitende Dienststelle nicht ausreichen. Hierbei sollten auch Alternativen, wie die Freischaltung eines temporären Zugriffs auf einen konkreten Vorgang oder die Kontaktaufnahme mit der sachbearbeitenden Dienststelle geprüft werden.

- Ein weiterer Punkt war die Einbindung des Landesbetriebs für Daten und Information Rheinland-Pfalz (LDI). Hierzu existiert seit 2005 eine Kooperationsvereinbarung über den Betrieb, die Entwicklung und die Pflege von Komponenten im polizeilichen Informations- und Kommunikationstechnik (IuK) - Bereich zwischen dem Ministerium für Inneres und Sport des Saarlandes und dem LDI. Da in dieser Vereinbarung keine datenschutzrechtlichen Fragestellungen, insbesondere mit Blick auf eine datenschutzrechtliche Verantwortlichkeit und Auftragskontrolle, enthalten waren, verlangten wir zusätzlich die Vereinbarung von Regelungen zu einer Datenverarbeitung im Auftrag entsprechend § 5 SDSG.
- Weitere klärungsbedürftige Fragestellungen ergaben sich aus technisch-organisatorischer Sicht bzgl. der Protokollierung von Anlass und Zweck von Suchabfragen, sowie im Hinblick auf die Berücksichtigung von Zweckbindung und Löschfristen beim Export von Daten aus POLADIS heraus.

Im Januar 2015 wurde uns als Anlage zur Kooperationsvereinbarung eine datenschutzrechtliche Vereinbarung des LPP als Auftraggeber und des LDI als Auftragnehmer nach § 5 SDSG zur weiteren Prüfung vorgelegt. Diese berücksichtigt nunmehr sämtliche nach dem SDSG zu beachtenden Regelungen, wie beispielsweise zur Wahrung des Datengeheimnisses, zur Durchsetzung der Kontrollrechte der Landesbeauftragten für Datenschutz oder zur Umsetzung von Datensicherungsmaßnahmen, und entspricht im Wesentlichen dem von uns auch auf unserer Internetseite zur Verfügung gestellten Mustervertrag zur Auftragsdatenverarbeitung.

Noch vor Abschluss des Beteiligungsverfahrens ergaben sich im weiteren Verlauf des Jahres 2015 aus Sicht des LPP weitere, neue Fortschreibungsbedarfe der EAO, da für weitere Organisationseinheiten und Funktionsträger der Bedarf gesehen wurde, landesweite Zugriffsberechtigungen in der höchsten Berechtigungsstufe 3 zu vergeben.

Zu Beginn des Jahres 2016 wurde uns sodann unter Berücksichtigung der hinzugekommenen Fortschreibungsbedarfe eine überarbeitete EAO sowie auch eine entsprechend überarbeitete Berechtigungsmatrix zur neuerlichen Prüfung übersandt. Im Rahmen eines weiteren Besprechungstermins in unserer Dienststelle wurde nach Prüfung der vorgetragenen Bedarfe unter Berücksichtigung der hierzu gegebenen Begründung unser datenschutzrechtliches Votum zur konkreten Ausgestaltung der Zugriffsberechtigungen für die einzelnen Organisationseinheiten mitgeteilt. Im Nachgang zu diesem Erörterungstermin haben wir unsere Rechtsauffassung zu den einzelnen Fortschreibungsbedarfen der Zugriffsberechtigungen nochmals schriftlich dargelegt sowie auch konkrete Vorschläge zu technischen Lösungen unterbreitet.

3.3.1 Zugriffsberechtigungen der Dienststellen Operative Telekommunikationsüberwachung (TKÜ) und IT-Forensik

Aufgabe der beiden Dienststellen ist die Auswertung der IT bzw. der TKÜ in konkreten strafrechtlichen Ermittlungsverfahren. Hierzu ist es nach unserer Auffassung zur Aufgabenerfüllung ausreichend, dass der Zugriff auf die (einzelnen) Vorgänge beschränkt wird, die entsprechende Auswertungen zum Gegenstand haben und für die ein konkreter Auswertungsauftrag vorliegt.

Um einen vorgangsbezogenen Einzelzugriff zu realisieren, haben wir nach Rücksprache mit den technisch Verantwortlichen für POLADIS ein sog. Deep-Linking-Verfahren vorgeschlagen. Dahinter steht die Generierung eines speziellen Links, der ein sog. Accesstoken (temporäre Sicherheitsreferenzen eines Nutzers, mit denen sich dieser gegenüber einem System authentifiziert) enthält, über das direkt auf die Inhalte des entsprechenden Vorgangs zugegriffen werden kann. Das Vorhalten einer Suchmöglichkeit erübrigt sich dadurch. Nach Abschluss des Auswertungsauftrags kann der Deep-Link invalidiert werden.

Das von uns vorgeschlagene Deep-Link-Verfahren wurde seitens des LPP aufgegriffen und ein entsprechender technischer Lösungsansatz erarbeitet.

Im Juni 2016 war das Deep-Link-Verfahren für Auswertefälle der IT-Dienststelle implementiert, so dass nur die Mitarbeiter dieser Fachdienststelle durch Anklicken des Link auf den konkreten Vorgang zugreifen können.

3.3.2 Zugriffsberechtigungen des Bereichs Qualitätsmanagement/Controlling

In Bezug auf die genannte Organisationseinheit Qualitätsmanagement / Controlling wurde seitens des LPP dargelegt, dass die Beschränkung des Zugriffs auf einzelne Vorgänge wegen des Spektrums an unterschiedlichen Untersuchungsaufträgen durch die Behördenleitung sowie auch das Ministerium für Inneres und Sport mit der Folge des Bedarfs an sehr unterschiedlichen Daten nicht zielführend sei.

Für konkrete Projekt- und Untersuchungsaufträge haben wir daher einem landesweiten, aber nur temporären Lesezugriff zugestimmt.

3.3.3 Zugriffsberechtigungen der Direktions- und Abteilungsleitung der Direktion LPP 2

Für die Direktions- und Abteilungsleitung wurde seitens des LPP das Erfordernis eines landesweiten Zugriffs gesehen. Für eine standardisierte bzw. temporäre landesweite Zugriffsmöglichkeit sahen wir indes keine Erforderlichkeit. Der Zugriff der Direktionsleitung (und Stellvertreter) war daher auf die der eigenen Direktion zugeordneten Abteilungen und Dezernate zu beschränken. Ebenso ist der Zugriff der Abteilungsleitung (und Stellvertreter) auf die dem eigenen Verantwortungsbereich zugeordneten Dezernate zu beschränken.

3.3.4 Zugriffsberechtigungen der Leitung des Kriminaldauerdienstes (KDD)

Das LPP führte aus, dass die Dienstgruppenleiter des KDD außerhalb der allgemeinen Dienstzeit die Zentralstellenfunktion i.S.d. § 13 Bundeskriminalamtgesetz (BKAG) wahrnehmen. Vor allem außerhalb der allgemeinen Dienstzeit würden Erkenntnisanfragen und Unterstützungsersuchen anderer Länderpolizeien gestellt, die einen kurzfristigen Zugriff auf einen Ermittlungsvorgang erforderlich machten.

Einem standardisierten landesweiten Zugriff wurde vor diesem Hintergrund zugestimmt.

3.3.5 Zugriffsberechtigungen der Dienststelle Alkohol/Drogen

Für die Dienststelle Alkohol/Drogen, die als zentrale Stelle des Landes für die Erkennung und Koordinierung der Alkohol- und Drogenerkennung im Straßenverkehr fungiert, war ein standardisierter landesweiter Lesezugriff gefordert worden. Dies wurde von uns aus datenschutzrechtlicher Sicht kritisch bewertet.

Wir waren der Auffassung, dass ein unbefugter Zugriff auf POLADIS-Vorgänge, die in keinem Zusammenhang mit alkohol- bzw. drogenrelevanten Vorgängen im Straßenverkehr stehen, bereits auf technischer Ebene ausgeschlossen werden muss. Wir schlugen als technische Lösung vor, dass mittels vorgegebener Selektionskriterien die jeweils für die Dienstelle relevanten POLADIS-Vorgänge, hier im Kontext von Alkohol und Drogen, über die zu jedem POLADIS-Vorgang vorgehalten Metadaten (z.B. Ereignis-, Gegenstands- und Sachdaten) automatisiert ausgefiltert werden. In einem zweiten Schritt, der ebenfalls automatisiert ablaufen sollte, sollte den jeweiligen Dienststellen bzw. Mitarbeitern dann nur auf diese vorselektierten POLADIS-Vorgänge lesender Zugriff gewährt werden. Auch für den zweiten Schritt, nämlich die Zugriffsgewährung auf einzelne konkrete POLADIS-Vorgänge, bestehe nach unserem Dafürhalten mit der bereits implementierten Deep-Link-Lösung prinzipiell eine taugliche technische Lösung.

Im weiteren Verlauf beauftragte die Behördenleitung des LPP die Dienststelle Programmentwicklung / Datenbankauswertung mit der Programmierung einer technischen Lösung. Von der Berechtigungsvergabe „Landesweite Vorgangssuche“ und

„Dienststellenübergreifender Lesezugriff auf Vorgangsdaten“ wurde daher seitens des LPP Abstand genommen und die Berechtigungsmatrix entsprechend angepasst.

3.3.6 Zugriffsberechtigungen der Dienststelle Verkehrsunfallanalyse

Für die Dienststelle zur Durchführung der zentralen Verkehrsunfallanalyse war ebenfalls ein standardisierter landesweiter Lesezugriff gefordert worden.

Auch hier wurde die Dienststelle Programmentwicklung / Datenbankauswertung, nachdem wir datenschutzrechtliche Bedenken geltend gemacht und einen technischen Lösungsvorschlag unterbreitet hatten, mit der Programmierung einer entsprechenden technischen Umsetzung beauftragt. Das LPP teilte hierzu mit, dass die entwickelte Software für einen Zeitraum von drei Wochen durch die Dienststelle Verkehrsunfallanalyse getestet worden sei und im Ergebnis die fachlichen Bedarfe der Dienststelle abdecken konnte.

Einer Berechtigungsvergabe „Landesweite Vorgangssuche“ und „Dienststellenübergreifender Lesezugriff auf Vorgangsdaten“ bedurfte es mithin für die Dienststelle Verkehrsunfallanalyse nicht mehr. Die Berechtigungsmatrix wurde demzufolge angepasst. Aus hiesiger Sicht bestanden keine Einwände, die durch das LPP erarbeitete technische Lösung in den Produktivbetrieb zu übernehmen.

3.3.7 Zugriffsberechtigungen der Dienststelle Rechtsangelegenheiten

Einen standardisierten oder auch temporären landesweiten Zugriff hielten wir in Anbetracht des Aufgabenbereichs der Dienststelle Rechtsangelegenheiten für zu weitgehend. Nach unserer Auffassung war, wie auch bei den Dienststellen Operative Telekommunikationsüberwachung und IT-Forensik, ein vorgangsbezogener Einzelfallzugriff für die Aufgaben der Dienststelle ausreichend. Maßgebend hierfür war auch die im Rahmen einer Eingabe durch diese Dienststelle vertretene Rechtsauffassung zur Zulässigkeit der Datenerhebung von Dritten aus polizeilichen Informationssystemen sowie auch deren Datenübermittlung aufgrund beamtenrechtlicher Streitigkeiten (siehe hierzu auch Verwaltungsgericht des Saarlandes, Urteil vom 7. Oktober 2015 - 1 K 63/14 - und Oberverwaltungsgericht des Saarlandes, Beschluss vom 29. September 2016 - 2 A 210/15).

3.3.8 Fazit

Das Verfahren wurde im Dezember 2016 gemäß § 7 Abs. 2 Satz 1 SDSG durch das zuständige Ministerium für Inneres und Sport freigegeben.

In der Gesamtschau stellte sich das Verfahren aufgrund der erheblichen Fortschreibungsbedarfe sowie der hieraus resultierenden Änderungs- und Anpassungsbedarfe sowohl für die Vertreter des LPP als auch unsere Mitarbeiter als sehr arbeitsintensiv

dar. Aus hiesiger Sicht kann jedoch gesagt werden, dass in konstruktiver Zusammenarbeit die Anwendung des Verfahrens datenschutzgerecht sowie auch für die Anwender bedarfskonform angepasst werden konnte.

3.4 Automatisierter Abgleich personenbezogener Daten mit dem Datenbestand in POLADIS und POLIS

Im Rahmen unserer Beteiligungsrechte wurde uns durch das Ministerium für Inneres und Sport im August 2014 die Errichtungsanordnung (EAO) „Automatisierter Abgleich personenbezogener Daten mit dem Datenbestand in POLADIS und POLIS (AutoPers-GRD)“ zur datenschutzrechtlichen Bewertung übersandt.

Die Datei soll der vorbeugenden Bekämpfung von Straftaten dienen, indem in ihr gespeicherte personenbezogene Daten mit den Datenbeständen des Polizeilichen Informations- und Fahndungssystems (POLIS) und des Polizeilichen Anwenderorientierten Dokumentations- und Informationssystems (POLADIS) abgeglichen werden. Erfasst werden sollten sowohl Störer i.S.v. § 26 Abs. 1 Nr. 1 Saarländisches Polizeigesetz (SPolG) und relevante Personen gemäß § 26 Abs. 2 Nr. 1 und 2 SPolG als auch Personen gemäß § 2 Antiterrordateigesetz (ATDG) und § 2 Rechtsextremismusdateigesetz (RED-G).

In der Praxis soll dem Anwender eine Ergebnismaske mit allen in der Datei AutoPers-GRD gespeicherten Personen angezeigt werden. Personen, bei deren Datensätze sich Veränderungen ergeben haben, sollen für die Sachbearbeitung farblich gekennzeichnet werden. Erst durch Anklicken der farblich markierten Person werden die Datensätze des durchgeführten automatisierten Datenabgleichs mit POLIS und POLADIS angezeigt. Nach entsprechender Prüfung durch die Sachbearbeitung können die Änderungen durch Aktivierung „Bearbeitung abgeschlossen“ übernommen werden.

Datenführende und damit auch datenschutzrechtlich verantwortliche Stelle für die Zulässigkeit der Speicherung, sonstige Verarbeitung sowie Einhaltung und Prüfung der Löschfristen soll das Dezernat Auswertung und Analyse des Landespolizeipräsidiums (LPP) sein. Die Zugriffsrechte sollten somit auf den mit der Aufgabe betrauten Personenkreis eingeschränkt werden. Die Löschung soll automatisiert bei Wegfall der Speichervoraussetzungen oder mit Ablauf des Löschdatums erfolgen.

Wir teilten dem LPP nach entsprechender Prüfung der EAO unsere Bedenken, die der beabsichtigen Verarbeitung personenbezogener Daten in AutoPers-GRD entgegenstanden, mit nachfolgender Begründung mit:

In der Datei AutoPers-GRD sollen Daten von Personen, die die Voraussetzungen des § 2 ATDG bzw. § 2 RED-G erfüllen, gespeichert werden, um mit den Datenbeständen in POLADIS und POLIS einen automatisierten Datenabgleich durchzuführen.

Rechtgrundlage für diese Speicherung sollte nach Vorstellung des LPP das ATDG bzw. das RED-G sein. Diese Auffassung wurde von uns jedoch nicht geteilt. Denn nach § 2 Hs. 1 ATDG sind die beteiligten Behörden verpflichtet, ATD-relevante Daten in der Antiterrordatei zu speichern. Ebenso führt § 2 Hs. 1 des RED-G aus, dass die beteiligten Behörden verpflichtet sind, RED-relevante Daten in der Datei nach § 1

RED-G, nämlich einer gemeinsamen standardisierten zentralen Datei, zu speichern. Eine Speicherung in der Datei AutoPers-GRD ist daher weder auf der Grundlage des ATDG noch des RED-G möglich. Auch die in den genannten Gesetzen expliziten Regelungen zur weiteren Verwendung von Daten, welche sich auf konkrete Fälle beziehen, laufen einer Speicherung in der Datei AutoPers-GRD zuwider.

Wir baten daher um entsprechende Streichung in den Ziffern „Inhalt der Datei", „Zweck der Datei" und „betroffener Personenkreis und Löschfristen" sowie auch um entsprechende Anpassung der weiteren Ziffern der EAO.

Darüber hinaus baten wir auch um Erläuterung, inwieweit technisch sichergestellt ist, dass bei Neuanlage eines Personendatensatzes zwingend die Rechtsgrundlage hierfür in einem systemseitig vorgegebenen Eingabefeld zu benennen ist, um hierdurch dem Transparenzgebot und der Kontrollmöglichkeit Rechnung zu tragen.

Im November 2015 wurde uns sodann eine überarbeitete EAO übersandt, die unseren rechtlichen Einwänden zur Speicherung von Personen auf der Grundlage des ATDG bzw. RED-G außerhalb der ATD bzw. RED vollumfänglich Rechnung trug. Die Datenerhebung als Datenverarbeitung findet nun mithin ausschließlich auf der Grundlage und unter den Voraussetzungen des SPolG statt.

Des Weiteren war unter dem Aspekt der Neuanlage von Personendatensätzen aus dem für die Anwendung erstellten Benutzerhandbuch ersichtlich, dass für die Speicherung einer Person zuvor Anlass, Rechtsgrundlage für die Speicherung, Speicherdauer und Prüffrist in der Anwendung einzugeben sind. Aus datenschutzrechtlicher Sicht ist es uns auch ein Anliegen, nicht nur vom betroffenen Anwender datenschutzkonformes Handeln einzufordern, sondern ihn auch durch entsprechende praxisnahe Maßnahmen in die Lage zu versetzen, dieser Forderung gerecht zu werden. Das uns vorgelegte Benutzerhandbuch ist hierfür aus unserer Sicht ein positives Beispiel.

Das Verfahren wurde im Dezember 2015 durch das Ministerium für Inneres und Sport freigegeben.

3.5 Elektronischer Lichtbildabgleich

Zu Beginn des Jahres 2015 bat uns das Ministerium für Inneres und Sport zum Einsatz des Verfahrens eLBA um Wahrnehmung unserer Beteiligungsrechte nach § 7 Abs. 2 Saarländisches Datenschutzgesetz (SDSG) und übersandte uns gleichzeitig die erforderliche Errichtungsanordnung (EAO) sowie weitere das Verfahren beschreibende Anlagen.

Die Vollzugspolizei des Saarlandes hat nach §§ 1 Abs. 2 i.V.m. 85 Abs. 1 Saarländisches Polizeigesetz (SPolG) sowie § 163 Abs. 1 Strafprozessordnung (StPO) Straftaten zu erforschen. Die Polizei kann im Rahmen ihrer Ermittlungen Zeugen gemäß § 163 Abs. 3 StPO vernehmen. Zu diesem Zweck kann sie die betreffenden Personen vorladen. Insbesondere die Vorlage von Lichtbildern des Verdächtigen und anderer Personen gegenüber Zeugen zur Ermittlung eines noch unbekannten Tatverdächtigen, sogenannte Wahllichtbildvorlage, ist aus polizeilicher Sicht ein geeignetes Mittel zur Ermittlung von Beschuldigten wie auch zum Ausschluss Unbeteiligter. Das Verfahren

eLBA ermöglicht die Zusammenstellung von Lichtbildern zur Wahllichtbildvorlage, aber auch die Zusammenstellung von Lichtbildern für Einsatzkräfte im Zusammenhang mit der Durchführung von Fahndungsmaßnahmen oder Observationen. Die benötigten Lichtbilder werden manuell aus dem Verfahren POLIS oder dem beim BKA geführten zentralen Informationssystem INPOL-Zentral extrahiert und im entsprechenden Verfahrensmodul, z.B. „Wahllichtbildvorlage", gespeichert.

Nach Prüfung der vorgelegten Unterlagen setzten wir uns im Rahmen des Abstimmungsprozesses zunächst mit dem behördlichen Datenschutzbeauftragten des Landespolizeipräsidiums ins Benehmen. Hinsichtlich des betroffenen Personenkreises wurden auch Personen aufgeführt, die sich freiwillig erkennungsdienstlich behandeln ließen. Es war jedoch unklar, inwieweit diesem Personenkreis bei Abgabe der Einverständniserklärung auch transparent war, dass die personenbezogenen Daten aus der erkennungsdienstlichen Behandlung auch zum Zwecke der Strafverfolgung – z.B. als Lichtbildvorlage im Rahmen eines anderen konkreten Strafverfahrens - genutzt werden können. In der Folge wurde dieser Personenkreis ersatzlos gestrichen.

Weiterhin erschienen die Ausführungen zu den Löschfristen sämtlicher Datenarten nach hiesiger Auffassung zu wenig spezifiziert. Die Ziffer „Löschfristen" wurde daher seitens des LPP dahingehend überarbeitet, dass nunmehr sämtliche Datenarten (Personen-, Fall- und Verwaltungsdaten) sowie die aus POLIS oder INPOL-Zentral importierten Daten automatisiert nach 30 Tagen gelöscht werden.

Im April 2015 haben wir dem Ministerium für Inneres und Sport zum überarbeiteten Stand der EAO berichtet und gleichzeitig mitgeteilt, dass gegen die nunmehr vorliegende Fassung der EAO keine datenschutzrechtlichen Bedenken bestehen.

Das Verfahren wurde nach Mitteilung des Ministeriums für Inneres und Sport am 20. April 2015 freigegeben.

3.6 Polizeilicher Informations- und Analyseverbund

Auf Beschluss der Innenministerkonferenz wurde der Polizeiliche Informations- und Analyseverbund (PIAV) eingeführt. Bei PIAV bzw. der Anwendung PIAV-Operativ Zentral handelt es sich um eine sogenannte Verbundanwendung, ein gemeinsam genutztes IT-Verfahren der Länderpolizeien, der Bundespolizei (BPol), des Zolls und des Bundeskriminalamtes (BKA). Das Verfahren dient einer zeitnahen Bereitstellung von Personen-, Fall- und Sachdaten der Kriminalitätsbekämpfung aus den Systemen der oben genannten Teilnehmer, um so länderübergreifend operative und strategische Kriminalitätsanalysen zu ermöglichen.

Im Saarland gewährleistet die landesseitige Informationsplattform „PIAV-Operativ Saarland" den direkten Datenaustausch mit dem Verbundsystem. Das polizeiliche anwenderorientierte Dokumentations- und Informationssystem POLADIS dient hierbei als Quellsystem für PIAV-Operativ Saarland, da in POLADIS alle polizeilichen Informationen, insbesondere solche zu strafrechtlichen Vorgängen, gespeichert werden.

Aus POLADIS werden auch Daten in das saarländische Fallbearbeitungssystem KRISTAL (Kriminalpolizeiliches System zur täter-/tatorientierten Analyse und Lagedarstellung) überführt. KRISTAL dient der Erforschung, Ermittlung und Aufklärung von Verbrechen und Vergehen, die serien-, banden-, gewerbsmäßig oder organisiert im Saarland begangen werden, und Straftaten von erheblicher Bedeutung sowie Straftaten im Bereich der politisch motivierten Kriminalität. Es unterstützt die Polizei im Rahmen vorbeugender Verbrechensbekämpfung sowie bei der Durchführung spurenintensiver Ermittlungen und bietet so auch die Möglichkeit, Tatzusammenhänge zeitnah zu erkennen und darzustellen. Hinsichtlich seiner Auswerte- und Analysefunktionen sowie deren technischer Umsetzung ist PIAV-Operativ Saarland ähnlich wie KRISTAL ausgestaltet. Datenschutzrechtlich bedeutsam ist bei derartigen Systemen, dass verschiedenste Informationen wie Texte, Bilder und Lebenssachverhalte zügig recherchiert und verknüpft werden können. Insbesondere steht auch eine grafische Darstellung komplexer Sachverhalte systemseitig zur Verfügung[13]. Auch KRISTAL soll nach bisheriger Planung zukünftig für die Anwendung PIAV-Operativ Saarland neben POLADIS als Quellsystem dienen.

Im Saarland wurde für die Befüllung von PIAV-Operativ Saarland als auch für den anschließenden Datentransfer nach PIAV-Operativ Zentral eigens eine Projektgruppe PIAV Saarland eingerichtet. Zunächst prüfen Sachbearbeiter dieser Projektgruppe als PIAV-relevant gekennzeichnete Daten sowohl unter fachlichen Gesichtspunkten als auch danach, ob deren Speicherung nach den Vorschriften der Strafprozessordnung (StPO) oder des Saarländischen Polizeigesetzes (SPolG) zulässig ist. Erst dann werden die überprüften Daten in PIAV-Operativ Saarland überführt. Für den anschließenden Datentransfer in PIAV-Operativ Zentral, welches beim BKA geführt wird, sind die Vorschriften des § 35 SPolG i.V.m. § 13 Bundeskriminalamtgesetz zu beachten.

In den PIAV-Anwendungen soll sukzessive für jeden Deliktsbereich (z.B. Waffen/Sprengstoffkriminalität, Rauschgiftkriminalität u.a.) eine eigene Datei eingerichtet werden.

Das Verfahren PIAV-Operativ Saarland befindet sich noch im Abstimmungsprozess mit unserer Dienststelle.

[13] Vgl. 23. Tätigkeitsbericht, 2009/2010, Kapitel 4.3, S. 28-30.

4 Verfassungsschutz

4.1 Prüfung der Antiterrordatei (ATD) und Rechtsextremismus-Datei (RED) beim Landesamt für Verfassungsschutz

Gemäß § 10 Abs. 2 Antiterrordateigesetz (ATDG) und § 11 Abs. 2 Rechtsextremismus-Datei-Gesetz (RED-G) sind die Bundesbeauftragte für Datenschutz und die Landesbeauftragten für Datenschutz im Rahmen ihrer jeweiligen örtlichen Zuständigkeiten verpflichtet, mindestens alle zwei Jahre die Durchführung des Datenschutzes in der Antiterrordatei (ATD) und der Rechtsextremismus-Datei (RED) zu kontrollieren. Bereits im 25. Tätigkeitsbericht[14] hatten wir über die Prüfung der ATD beim Landespolizeipräsidium berichtet. Im Berichtszeitraum stand nun die Prüfung beim Landesamt für Verfassungsschutz (LfV) an.

Bezugnehmend auf die vorgenannte gesetzlich vorgeschriebene Prüfpflicht haben wir im April 2015 gegenüber dem LfV die beabsichtigte Prüfung der ATD und RED angekündigt und gleichzeitig darum gebeten, uns im Rahmen einer Informationsveranstaltung zunächst die Grundzüge der Datenverarbeitung durch das LfV in der ATD als auch in der RED, sowie etwaige Datenübermittlungen, Art und Umfang der Zugriffsmöglichkeiten und Zugriffsberechtigungen, den Umgang mit Suchabfragen und auch ggf. besondere Datensicherheitsaspekte näher zu erläutern. Zeitgleich mit unserer Prüfankündigung baten wir das LfV auch darum, für die Durchführung unserer Prüfung, die im Zeitraum vom 1. Mai 2014 bis 30. April 2015 angefallenen Protokolldaten der im LfV auf die ATD und die RED zugriffsberechtigten Personen beim Bundeskriminalamt (BKA) anzufordern.

In der Auftaktveranstaltung erläuterte das LfV zunächst die verschiedenen Datenverarbeitungsphasen näher. Basis für die Befüllung der beiden Dateien ist das sogenannte Nachrichtendienstliche Informationssystem - NADIS, eine Verbunddatei der Verfassungsschutzbehörden des Bundes und der Länder, die auf der Grundlage des § 6 Bundesverfassungsschutzgesetz (BVerfSchG) geführt wird und die der Erfüllung der gegenseitigen Unterrichtungspflichten im Hinblick auf Informationsgewinn, Erkenntnisgewinn und Auswertung dient. Die Befüllung der ATD und RED aus NADIS heraus erfolgt ausschließlich automatisiert über eine gesondert für jede Datei eingerichtete Schnittstelle. Voraussetzung hierfür ist, dass zuvor die Speicherrelevanz und die Voraussetzungen zur Einspeicherung in die ATD / RED nach § 2 ATDG bzw. § 2 RED-G positiv festgestellt wurde.

Die Nutzung von ATD / RED durch die zugriffsberechtigten Mitarbeiter beim LfV erfolgt über eine Volltextsuche, die grundsätzlich den gesamten Datenbestand aller einspeichernden Behörden erschließt. Wegen der gesetzlichen Vorgaben erfolgt der Zugriff jedoch zweistufig. Während über die Volltextsuche alle in der Datei hinterlegten Daten indexiert und recherchierbar sind, erfolgt im Trefferfall in einem ersten

[14] Vgl. 25. Tätigkeitsbericht, 2013/2014, Kapitel 7.2, S. 51-55.

Schritt zunächst nur die Anzeige der sog. Grunddaten des Treffers. Zu den Grunddaten zählen im Wesentlichen die Daten, die der Identifizierung einer Person dienen (siehe § 3 Abs. 1 Nr. 1 lit. a ATDG / RED-G). Die Sicht auf die erweiterten Grunddaten, die in § 3 Abs. 1 Nr. 1 lit. b ATDG / REDG-G abschließend aufgezählt sind, bedarf dann einer gesonderten Erkenntnisanfrage an die einspeichernde / verantwortliche Behörde, die sodann nach rechtlicher Prüfung, ob die Voraussetzungen einer datenschutzrechtlichen Übermittlungsbefugnis gegeben sind, den Datensatz für die anfragende Behörde freigeben soll. Die Erkenntnisanfragen und das Freigabeverfahren erfolgen IT-gestützt über die jeweiligen Nutzeroberflächen der ATD / RED. Jede Erkenntnisanfrage und die damit korrespondierende Freigabe durch die einspeichernde Behörde wird auf dem Protokollserver beim BKA protokolliert.

Schwerpunkt der an die Auftaktveranstaltung anschließenden Vor-Ort-Kontrolle der ATD / RED war die Überprüfung der Nachvollziehbarkeit der durch das LfV als ATD / RED - relevant eingestuften Personen unter Berücksichtigung des Aktenrückhalts sowie die weitere Nutzung der beiden Dateien.

Die Erkenntnisse, die seitens der zuständigen Mitarbeiter des LfV in die ATD / RED gespeichert werden, sind im dort geführten Aktenrückhalt dokumentiert. Da das LfV in diesem Bereich keine Personen-, sondern Sachakten führt, finden sich bewertungsrelevante Informationen häufig an mehreren Stellen. Dies erschwert die datenschutzrechtliche Überprüfung, weil beiden Dateien ein personenbezogener und nicht sachbezogener Ansatz zugrunde liegt und damit ein Auffinden der in der Akte geführten Erkenntnisgrundlagen nur mittels des in den entsprechenden Datensätzen hinterlegten Aktenzeichens nicht unmittelbar möglich ist. Um trotzdem die Nachvollziehbarkeit zu gewährleisten, wird bei Änderungen in der RED – in der ATD wird dies analog gehandhabt – durch das hiesige LfV ein individuelles, tagesbezogenes Aktenzeichen, vergleichbar einer Tagebuchnummer, vergeben, das eine Zuordnung zum Aktenrückhalt vereinfacht. Durch diese Form der Einzeldokumentation wird nicht nur den bestehenden Dokumentationspflichten Rechnung getragen, sondern auch eine möglichst einfache Nachvollziehbarkeit jeder Änderung gewährleistet.

Bei der Durchsicht der Protokolldaten war uns aufgefallen, dass in einigen Fällen entgegen § 9 Abs. 1 ATDG / § 10 Abs. 1 RED-G eine Protokollierung des Zugriffszwecks unter Angabe des Abfragegrundes „Sonstiges" nicht hinreichend präzisiert war. Um den Anlass der Suchanfrage hinreichend genau nachvollziehen zu können, hielten wir es für notwendig, die Anwender des LfV darauf hinzuweisen, dass der Abfragegrund „Sonstiges" nur in Ausnahmefällen verwendet werden dürfe und für diese Fälle Vorgaben hinsichtlich der Bestimmtheit der Präzisierung zu machen seien. Das LfV hat uns im Nachgang hierzu mitgeteilt, dass die Mitarbeiter umgehend schriftlich angehalten wurden, eine Präzisierung in einem entsprechenden Texteingabefeld bei der Durchführung von Suchanfragen vorzunehmen und ansonsten die Auswahl „sonstiger Abfragegrund" nur in Ausnahmefällen zu verwenden.

Ein besonderes Augenmerk bei unserer Prüfung galt schließlich den Kontaktpersonen. Nach der Entscheidung des Bundesverfassungsgerichts (Urteil vom 24. April 2013 – 1 BvR 1215/07) und den daran anschließenden Anpassungen durch das Gesetz zur Änderung des Antiterrordateigesetztes und anderer Gesetze (ATDGuaÄndG) durften Kontaktpersonen sowie zu ihnen gesetzlich genau aufgeführte Datenarten

zur Identifizierung und Kontaktaufnahme nur noch als erweiterte Grunddaten zu einer Hauptperson gespeichert werden und nicht mehr wie vorher als eigenständiger Personendatensatz. Dies hatte zur Folge, dass Kontaktpersonen nun nicht mehr unmittelbar über die Suche zugänglich sind, sondern es zu ihrer Kenntnisnahme einer Erkenntnisanfrage an die einspeichernde Behörde bedarf.

Es stellte sich daher die Frage, ob aufgrund der Gesetzesänderung eine Bereinigung des Datenbestandes hinsichtlich seinerzeit als Kontaktpersonen gespeicherten Personen stattgefunden hatte. Hierzu legte das LfV dar, dass im Quellsystem NADIS keine Kontaktpersonen gespeichert wurden und aufgrund der ausschließlich automatisierten Schnittstellenbefüllung somit auch keine Kontaktpersonen in die ATD / RED überführt wurden.

Gemäß § 28 Abs. 1 Saarländisches Datenschutzgesetz (SDSG) sind die öffentlichen Stellen verpflichtet, die Landesbeauftragte für Datenschutz und deren Beauftragte bei der Erfüllung ihrer Aufgaben zu unterstützen. Dabei ist insbesondere Auskunft auf Fragen zu erteilen sowie Einsicht in alle Vorgänge und Aufzeichnungen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Das Landesamt für Verfassungsschutz ist dieser Verpflichtung in vorbildlicher Weise nachgekommen. Während der gesamten Prüfung haben die jeweiligen Vertreter des LfV konstruktiv mit uns zusammengearbeitet.

5 Justiz

5.1 Jugendarrestvollzugsgesetz

Die Verhängung von Jugendarrest ist gemäß § 13 Jugendgerichtsgesetz (JGG) die Anordnung eines sog. Zuchtmittels, mit dem eine Straftat eines Jugendlichen geahndet werden kann, wenn eine Jugendstrafe nicht geboten ist, dem Jugendlichen aber eindringlich zum Bewusstsein gebracht werden muss, dass er für das von ihm begangene Unrecht einzustehen hat. Dieses Zuchtmittel hat nicht die Rechtswirkungen einer Strafe und kann gemäß § 16 Abs. 4 JGG höchstens vier Wochen betragen.

Zum Vollzug des Jugendarrests sieht § 90 JGG lediglich vor, dass dieser erzieherisch gestaltet werden muss und in Jugendarrestanstalten oder Freizeitarreträumen der Landesjustizverwaltung vollzogen wird. Die Ausgestaltung des Vollzugs des Jugendarrests erfolgte bislang auf der Grundlage einer Rechtsverordnung des Bundes (Jugendarrestvollzugsordnung - JAVollzO). Da aber der Vollzug des Jugendarrests Maßnahmen mit sich bringt, die in die Grundrechte der Jugendlichen und Heranwachsenden eingreifen, bedarf es einer gesetzlichen Grundlage, die die jeweiligen Eingriffsvoraussetzungen in hinreichend bestimmter Weise normiert.

Mit dem Gesetz über den Vollzug des Jugendarrests (Saarländisches Jugendarrestvollzugsgesetz – SJAVollzG) sollten die hierfür erforderlichen Regelungen geschaffen und darüber hinaus wesentliche Vorgaben zur Gestaltung des Vollzugs getroffen werden. Zu den im Gesetzentwurf enthaltenen datenschutzrechtlichen Vorschriften wurde unserer Dienststelle durch das zuständige Ministerium der Justiz bereits frühzeitig Gelegenheit zur Stellungnahme gegeben. Einige unserer Verbesserungsvorschläge sind bereits in den in den Landtag eingebrachten Gesetzentwurf eingeflossen. Die Punkte, hinsichtlich derer mit dem Ministerium keine übereinstimmende Auffassung herbeigeführt werden konnte, blieben leider auch nach Durchführung des parlamentarischen Anhörungsverfahrens unverändert.

Insgesamt entsprechen die gesetzlichen Regelungen zum Umgang mit personenbezogenen Daten in weiten Teilen den Vorschriften, die in den Strafvollzugsgesetzen enthalten sind. Dies gilt auch für die in § 37 Abs. 7 SJAVollzG geregelte Befugnis zur erkennungsdienstlichen Behandlung der Arrestierten.

§ 37 Abs. 7 SJAVollzG

Soweit es zur Sicherung des Vollzugs, zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt oder zur Identitätsfeststellung erforderlich ist, sind mit Kenntnis der Gefangenen zulässig:

1. *die Abnahme von Finger- und Handflächenabdrücken,*
2. *die Aufnahme von Lichtbildern,*
3. *die Feststellung äußerlicher körperlicher Merkmale,*
4. *die elektronische Erfassung biometrischer Merkmale und*
5. *Messungen.*

Bei den dargestellten erkennungsdienstlichen Maßnahmen handelt es sich um intensive Eingriffe in das informationelle Selbstbestimmungsrecht der Jugendlichen bzw. Heranwachsenden. Nach der Gesetzesbegründung dienen die Maßnahmen zum einen der Erleichterung der Fahndung und des Wiederaufgreifens flüchtiger Arrestierter sowie zum anderen der Überprüfung der Identität von Arrestierten zur Aufrechterhaltung der Sicherheit und Ordnung.

Angesichts des Umstandes, dass es sich bei dem Jugendarrest nicht um eine Strafe, sondern um ein Zuchtmittel mit einer Dauer von zwei Tagen bis maximal vier Wochen handelt und dem Staat gegenüber den Jugendlichen nach der Zielsetzung des Gesetzes eine besondere Fürsorgepflicht obliegt, bestehen erhebliche Zweifel an der Erforderlichkeit solch eingriffsintensiver Maßnahmen. Es ist nicht ersichtlich, dass bei der relativ kurzen Arrestdauer eine erhebliche Fluchtgefahr besteht. Auch ist nicht erkennbar, dass es bei diesen kurzen Aufenthaltsdauern zu Identitätstäuschungen durch die Jugendlichen kommen wird, die nur mittels erkennungsdienstlicher Maßnahmen erkannt werden können. Daher wurde vorgeschlagen, diese Regelung zu streichen, zumindest aber dahingehend zu ändern, dass eine routinemäßige erkennungsdienstliche Behandlung aller Arrestierten ausgeschlossen wird. Eine solche Behandlung kann allenfalls im Einzelfall nach vorheriger Prüfung der Notwendigkeit der Maßnahme dem Verhältnismäßigkeitsgrundsatz genügen.

Zweifel bestehen auch an der Verhältnismäßigkeit der Aufbewahrungsdauer der im Rahmen der erkennungsdienstlichen Behandlung erhobenen Daten. § 37 Abs. 8 S. 3 SJAVollzG sieht hierzu vor, dass diese Daten spätestens sechs Monate nach Entlassung der Arrestierten oder deren Verlegung in eine andere Anstalt zu löschen sind. Da der Erhebungszweck, nämlich die Fahndung und Wiederergreifung flüchtiger Arrestierter und die Aufrechterhaltung der Sicherheit und Ordnung in der Anstalt, mit der Entlassung aus dem Arrest entfällt, ist kein rechtlicher Grund für eine weitere Speicherung ersichtlich, so dass nach hiesiger Auffassung eine unverzügliche Vernichtung der genannten Daten nach der Entlassung bzw. Verlegung des Arrestierten geboten wäre.

Schließlich erscheint auch die für die Videoüberwachung des Gebäudes und des Geländes der Arrestanstalt vorgesehene Frist zur Speicherung von sieben Tagen 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 worden sind, nicht mehr erforderlich sind. Zweck der Speicherung ist es nach Absatz 2, 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 eine unzulässige Datensammlung auf Vorrat dar.

5.2 Gefangeneneinkauf in der Justizvollzugsanstalt

Im Berichtsjahr 2016 erhielten wir mehrere Eingaben von in der Justizvollzugsanstalt Saarbrücken (JVA) inhaftierten Personen, die sich bei der Durchführung der Gefangeneneinkäufe in ihrem Recht auf informationelle Selbstbestimmung verletzt sahen. Sämtlichen Eingaben war gemein, dass die Gefangenen sich dagegen wandten, dass ihr Vor-, Familien- und Geburtsname bei Bestellungen an die Lieferfirmen übermittelt wurden.

Gemäß § 107 Abs. 1 S. 1 Saarländisches Strafvollzugsgesetz (SLStVollzG) ist das Übermitteln von nach § 106 SLStVollzG durch die Anstalt erhobenen personenbezogenen Daten nur dann zulässig, wenn es für den Vollzug erforderlich ist. Nach hiesiger Auffassung war die Übermittlung der Namen von Gefangenen an Lieferfirmen zur Abwicklung eines Einkaufs jedoch als nicht erforderlich anzusehen und hatte daher zu unterbleiben.

Im Rahmen unserer datenschutzrechtlichen Prüfung der JVA Saarbrücken im Jahre 2012[15] wurde uns von dieser ein datenschutzkonform ausgestaltetes Verfahren vorgestellt, bei dem die Lieferfirmen keine Kenntnis über die personenbezogenen Daten der Inhaftierten erhielten.

Wir haben daher aufgrund der ersten Eingabe die Anstaltsleitung um Stellungnahme gebeten. Mit Verwunderung, insbesondere auch unter dem Aspekt der zur Sicherstellung des Datenschutzes bei wesentlichen Änderungen eines Verfahrens nach § 7 Abs. 2 S. 4 Saarländisches Datenschutzgesetz (SDSG) gesetzlich festgelegten Vorgehensweise, haben wir daher zur Kenntnis genommen, dass seit Oktober 2014 sämtliche Daten des Einkaufsscheins an die Lieferfirma übermittelt wurden. Der Einkaufsschein enthielt neben Daten wie Buchnummer des Gefangenen und zur Verfügung stehendem Geldbetrag auch Vor- und Nachname des Gefangenen. Da aber die JVA in ihrer Stellungnahme im Februar 2016 darlegte, dass nach erneuter Überprüfung der Durchführung des Gefangeneneinkaufs nunmehr auf die Übermittlung der Einkaufsscheine verzichtet werde, war aus hiesiger Sicht ein datenschutzkonformes Verfahren wiederhergestellt.

Im Mai 2016 jedoch erhielten wir eine weitere Eingabe eines Gefangenen, der sich darüber beschwerte, dass die Einkaufsscheine mit den Angaben zu Familienname, Geburtsname und Vorname der Gefangenen im Rahmen des Gefangeneneinkaufs an die Lieferfirmen übermittelt würden.

Auf erneute Nachfrage wurde uns seitens der JVA bestätigt, dass nach wie vor die Namen der Käufer an die Lieferfirma übermittelt würden. Es handele sich aber nur um einen einzigen Mitarbeiter dieser Firma, der die Einkaufsscheine unmittelbar in der JVA entgegennehme. Zudem sei dieser Mitarbeiter auf das Datengeheimnis verpflichtet.

Wir haben daher erneut gegenüber der Anstaltsleitung ausdrücklich dargelegt, dass dies für die rechtliche Bewertung nicht maßgeblich sei, da keine Rechtsgrundlage für diese Datenübermittlung an eine nicht-öffentliche Stelle gegeben ist. Insbesondere

[15] Vgl. 24. Tätigkeitsbericht, 2011/2012, Kapitel 5.1, S. 29-34.

stellt auch die Verpflichtung auf das Datengeheimnis gemäß § 6 SDSG keine Rechtsgrundlage für eine Datenübermittlung an die verpflichtete Person dar. Vielmehr setzt diese Vorschrift voraus, dass die verpflichtete Person rechtmäßig Zugang zu den personenbezogenen Daten hat. Gleichzeitig haben wir unter Hinweis auf § 28 Abs. 1 SDSG die Anstaltsleitung der JVA um Stellungnahme zu dem Sachverhalt gebeten sowie auch mit gleicher Post das hiesige Ministerium der Justiz nachrichtlich beteiligt.

Ein Vertreter des Ministeriums kündigte zunächst an, dass der Ablauf des Gefangeneneinkaufs neu geregelt werde. Die in Rede stehenden Einkaufscheine sollten künftig statt der vollständigen Namensgebung nur noch die Initialen enthalten, um Verwechslungen ausschließen zu können.

Im Juli 2016 teilte die JVA sodann mit, dass das Verfahren des Gefangeneneinkaufs insoweit angepasst wurde, als dass die für den Gefangeneneinkauf zur Verfügung stehenden Partnerfirmen nunmehr lediglich pseudonymisierte Bestellscheine, also ohne erkennbare personenbezogene Daten, zur Zusammenstellung der Bestellungen erhalten. Auf den Einkaufsscheinen würden künftig nur noch die Buchnummer, Unterbringungsort und zur Verfügung stehender Geldbetrag des Gefangenen sowie dessen Initialen stehen. Von einem Versand der Einkaufsscheine an die Lieferfirmen wird gänzlich abgesehen. Die Einkaufsscheine stehen nur noch den die bestellten Waren ausgebenden Abteilungsbeamten der JVA zur Erfüllung ihrer Aufgaben zur Verfügung.

Die nunmehr beschriebene Verfahrensweise begegnete keinen datenschutzrechtlichen Bedenken. Wir teilten dies der JVA unter nachrichtlicher Beteiligung des Ministeriums der Justiz noch im gleichen Monat mit und baten im Interesse der Betroffenen um eine möglichst zeitnahe Umsetzung des Verfahrens sowie um entsprechende Mitteilung an unsere Dienststelle.

Zur gleichen Zeit etwa wurden wir mit einer erneuten Eingabe befasst, die sich auf die Bestellung bestimmter Gegenstände oder Geräte der Unterhaltungselektronik bezog. Ausweislich des der Eingabe beigefügten Formulars der JVA Saarbrücken zur Beantragung der Genehmigung dieser Gegenstände oder Geräte wurde vom Gefangenen das schriftliche Einverständnis zur Weitergabe seiner personenbezogenen Daten an die Lieferfirma verlangt, verbunden mit dem ausdrücklichen Hinweis, dass ohne entsprechendes Einverständnis eine Bestellung ausgeschlossen sei.

Mit Blick auf die nunmehr abgestimmte Verfahrensweise zum Gefangeneneinkauf fragten wir daher an, ob diese auch für die Bestellung bestimmter Gegenstände oder Geräte der Unterhaltungselektronik künftig gelten soll. Wir erhielten daraufhin die Mitteilung, dass der Einkauf dieser Gegenstände oder Geräte ebenfalls zeitnah neuorganisiert werden solle und nach der Umstellung der mit uns abgestimmten Verfahrensweise entsprechen werde.

Im September 2016 wurden wir sodann in Kenntnis gesetzt, dass die technischen und organisatorischen Maßnahmen abgeschlossen seien und das mit uns abgestimmte Verfahren ab Oktober 2016 eingesetzt werde.

5.3 Fehlerhafte Kontopfändung nach automatisiertem Kontoabruf

Ein Petent aus einem anderen Bundesland wandte sich an unsere Dienststelle, nachdem sein Konto aufgrund einer Verwechslung mit einer im Saarland gemeldeten Person mit dem gleichen Vor- und Nachnamen sowie dem gleichen Geburtsdatum gepfändet worden war.

Der Gläubiger der dieser Pfändung zugrundeliegenden vollstreckbaren Forderung hatte dem zuständigen Gerichtsvollzieher mit dem üblichen Auftragsformular u.a. den Auftrag erteilt, gem. § 802l Zivilprozessordnung (ZPO) beim Bundeszentralamt für Steuern (BZSt) eine Auskunft über das Bestehen eines Kontos oder Depots des Schuldners einzuholen, um hierauf zum Zwecke der Zwangsvollstreckung zugreifen zu können.

Nach § 93b Abs. 2 Abgabenordnung (AO) darf das BZSt auf Ersuchen berechtigter Stellen, zu denen auch Gerichtsvollzieher gehören, einzelne Daten aus einer durch die Kreditinstitute gemäß § 24c Kreditwesengesetz (KWG) zu führenden Datei abrufen. § 24c Abs. 1 KWG verpflichtet die Kreditinstitute in einer separaten Datenbank bestimmte Stammdaten der bei ihnen geführten Konten und Depots, u.a. den Namen des Inhabers und den Tag der Geburt, zu speichern. Im Ergebnis eines Kontoabrufs erscheinen somit bei Kontoinhabern nur Vorname, Name und Geburtsdatum. Die auf dem Kontoabrufersuchen anzugebende Anschrift des Kontoinhabers wird nicht in die Anfrage einbezogen. Die Verantwortung für die Zulässigkeit des Datenabrufs und der Datenübermittlung trägt der ersuchende Gerichtsvollzieher.

In dem von dem Petenten geschilderten Fall sind dem Gerichtsvollzieher durch das BZSt mehrere Datensätze über Personen mit den gleichen Namen und Geburtsdaten wie denjenigen Daten des Petenten übermittelt worden. Aus den übermittelten Datensätzen war nicht erkennbar, welcher Datensatz den richtigen Schuldner betraf. Der Gerichtsvollzieher leitete daher alle Datensätze an den Gläubiger weiter, der sodann die Zwangsvollstreckung gegen die falsche Person einleitete.

Nach Prüfung des Sachverhalts konnte dem Gerichtsvollzieher kein Vorwurf wegen unzulässiger Datenerhebung oder -übermittlung gemacht werden. Obwohl er sein Auskunftsersuchen an das BZSt unter Angabe auch der Anschrift des Schuldners der Forderung stellte, wurde – wie dargelegt - die Anschrift nicht in die Abfrage durch das BZSt einbezogen. Dieses kann vielmehr nur auf die Daten zugreifen, die die Kreditinstitute gemäß § 24c Abs. 1 KWG zu speichern verpflichtet sind. Im Ergebnis des Kontoabrufs erscheinen in Bezug auf die Kontoinhaber daher nur Name und Geburtsdatum. Weitere Identifizierungsmerkmale in Bezug auf den Kontoinhaber, wie bspw. die Wohnanschrift oder der Geburtsort, sind in der von den Kreditinstituten zu führenden Datei nicht enthalten.

Weitere Ermittlungen bezüglich des richtigen Schuldners durfte der Gerichtsvollzieher nicht anstellen, vielmehr war er – da es keine eindeutigen Hinweise darauf gab, dass es sich bei den mitgeteilten Konten um andere als die des Schuldners handelte – verpflichtet, die ihm übermittelte Liste an den Gläubiger weiterzuleiten (LG Würzburg, Beschluss vom 29. Juli 2014 – 3 T 773/14).

Es oblag daher dem Gläubiger, sorgfältig zu prüfen, gegen wen er die Vollstreckung einleitet.

Festzustellen ist, dass es bei derartigen Konstellationen durchaus zu Personenverwechselungen kommen kann, da die durch den Kontoabruf erlangten Daten nicht immer eine eindeutige Identifizierung des Schuldners zulassen.

Nach Auskunft des in der vorliegenden Angelegenheit tätig gewordenen Gerichtsvollziehers sowie des zuständigen Amtsgerichts ist diese Problematik bekannt und wurde auf Bundesebene bereits diskutiert. Eine Lösung dürfte nur durch eine Änderung des § 24c KWG herbeigeführt werden, indem die Banken verpflichtet werden, neben dem Namen und dem Geburtsdatum als weiteres Identifizierungsmerkmal zumindest den Geburtsort oder ggf. die aktuelle Wohnanschrift zu speichern.

6 Verkehr

6.1 Beachtung von Löschfristen durch die Führerscheinstelle

Sachverhalt

Auf die Eingabe eines Petenten hin hatten wir folgenden Sachverhalt zu bewerten:

Im Rahmen einer Polizeistreife wurde der Petent dabei beobachtet, wie er mit einem Motorrad zwei Lichtzeichenanlagen mit überhöhter Geschwindigkeit bei Rot überfuhr. Im Zuge der daraufhin eingeleiteten Verfolgung missachtete der Petent eine weitere Lichtzeichenanlage und die Anhalteanweisungen der Polizei.

Nachdem der Petent gestellt werden konnte, stellte der Polizeibeamte während der Aufnahme des Vorfalls beim Petenten unterschiedliche Auffall- und Ausfallerscheinungen fest, die ihn dazu veranlassten, zunächst einen Atemalkoholtest durchzuführen. Da dieser Atemalkoholtest negativ verlief, wurde wegen Verdachts des Drogenkonsums die Entnahme einer Blutprobe angeordnet, mit der sich der Petent im Folgenden dann auch einverstanden erklärte. Die immunchemische Voruntersuchung des Blutes des Petenten verlief negativ. In einer sich daran anschließenden toxikologischen Begutachtung der Blutprobe wurde bestätigt, dass weder Alkohol noch zentralnervös wirksame Medikamente, Drogen oder deren Stoffwechselprodukte im Blut des Petenten nachgewiesen werden konnten. Zur Erklärung der von dem Polizeibeamten festgestellten Ausfall- und Auffallerscheinungen wurde in dem Gutachten über Arzneimittel und Drogen, die sich nur ausnahmsweise ohne gezielte Informationen im Blut nachweisen ließen, sehr rasch aus dem Körper wieder eliminierte Wirksubstanzen, „Nachwirkungen" von Drogen bzw. Arzneimittelkonsum, ohne dass die Wirksubstanzen noch feststellbar sind oder andere körperliche oder geistige Mängel, etwa im Zusammenhang mit Erkrankungen verschiedenster Art spekuliert. Es wurde jedoch darauf hingewiesen, dass sich aus den bisher vorliegenden Unterlagen keine gezielten Hinweise hierfür ergeben. Die Staatsanwaltschaft stellte daraufhin das Ermittlungsverfahren gegen den Petenten wegen Trunkenheit im Verkehr und wegen Straßenverkehrsgefährdung nach § 170 Abs. 2 Strafprozessordnung (StPO) ein und gab das Verfahren unter Übersendung der gesamten Ermittlungsakte an das Landesverwaltungsamt – Zentrale Bußgeldbehörde - als zuständige Verwaltungsbehörde zur Verfolgung als Ordnungswidrigkeit ab.

Das Verkehrsverhalten des Petenten wurde in der Folgezeit durch das Landesverwaltungsamt als vier Verkehrszuwiderhandlungen nach dem Ordnungswidrigkeitengesetz (OWiG) verfolgt, die jeweils Rechtskraft erlangten und zusammen mit 13 Punkten im Verkehrszentralregister geführt wurden. Es handelte sich ausweislich eines nicht näher datierten Auszugs aus dem Verkehrszentralregister um zwei Verstöße wegen Missachtung des Rotlichts einer Lichtzeichenanlage, um einen Verstoß wegen Missachtung des Rotlichts einer Lichtzeichenanlage unter gleichzeitiger Gefährdung Anderer und um einen Verstoß wegen Nichtbefolgens des Haltgebots eines Polizei-

beamten. Gleichzeitig übersandte das Landesverwaltungsamt die gesamte Ermittlungsakte mit der Bitte um Prüfung der Fahreignung an die für den Petenten zuständige Führerscheinstelle.

Ab Eingang der Akte bei der Führerscheinstelle wurde der weitere Fortgang des Verfahrens nur unzureichend und lückenhaft in der Akte dokumentiert. Jedenfalls wurde gegenüber dem Petenten eine Verwarnung nach dem damaligen § 4 Abs. 3 S. 1 Nr. 1 Straßenverkehrsgesetz (StVG) ausgesprochen. Danach hat die Fahrerlaubnisbehörde gegenüber den Inhabern einer Fahrerlaubnis, bei denen sich unter Anwendung des im StVG geregelten Punktesystems zwischen acht und 13 Punkten ergeben, den Betroffenen schriftlich darüber zu unterrichten, ihn zu verwarnen und ihn auf die Möglichkeit der Teilnahme an einem Aufbauseminar hinzuweisen. Von dieser freiwilligen Möglichkeit der Teilnahme an einem Aufbauseminar hat der Petent in der Folge dann auch Gebrauch gemacht.

Zeitgleich wurde ein Konsilbefund zu den Auffall- und Ausfallerscheinungen erstellt, der lediglich psychosomatische Beschwerden diagnostizierte. Wer diesen Konsilbefund veranlasste und auf welcher Rechtsgrundlage dies erfolgte, konnte der Akte nicht entnommen werden.

Darüber hinaus ergaben sich aus der Akte keine Hinweise darauf, dass weitere verwaltungsbehördliche Entscheidungen durch die Führerscheinstelle getroffen wurden. Insbesondere sah man offensichtlich kein Erfordernis zur Einholung weiterer Gutachten oder Zeugnisse eines Fach- oder Amtsarztes, eines Gutachtens einer amtlich anerkannten Begutachtungsstelle für Fahreignung oder eines amtlichen anerkannten Sachverständigen oder Prüfers für den Kraftfahrzeugverkehr mit dem Ziel der Feststellung der Eignung oder Mängel hinsichtlich der Befähigung des Petenten zum Führen von Kraftfahrzeugen.

Mittlerweile war der Petent umgezogen und eine andere Führerscheinstelle für ihn örtlich zuständig. Gegenüber der neuen Führerscheinstelle machte der Petent ca. drei Jahre nach dem oben geschilderten Vorfall einen Auskunftsanspruch geltend und bat um Löschung der ihn betreffenden personenbezogenen Daten aus diesem Vorfall. Nachdem der nun zuständigen Führerscheinstelle der entsprechende Vorgang von der alten Führerscheinstelle übersandt wurde, lehnte man das Löschungsersuchen des Petenten unter Verweis auf eine 10-jährige Speicherfrist ab.

Der Petent hatte sich daraufhin an unsere Dienststelle gewandt. Die Führerscheinstelle wurde in der Folge um Stellungnahme zu Umfang und Dauer der Aufbewahrung der Unterlagen gebeten. Zur Begründung wurde darin ausgeführt, dass sich aus § 2 Abs. 9 StVG eine Befugnis zur Aufbewahrung der vorgenannten Unterlagen für eine Dauer von 10 Jahren ergebe. Darüber hinaus wurde mitgeteilt, dass aus Sicht der Behörde zum Zeitpunkt des rechtsmedizinischen Gutachtens eigentlich weitere Maßnahmen hätten ergriffen werden müssen, diese aber zum jetzigen Zeitpunkt nicht mehr „zielführend bzw. sehr aufwändig" seien. Daher wurde wiederholt darauf hingewiesen, dass zurzeit von einer erneuten Einleitung eines Überprüfungsverfahrens abgesehen werde, da seit dem Vorfall bereits drei Jahre vergangen seien, die Unterlagen aber weiter aufbewahrt würden um sie *„im Falle neuer Erkenntnisse, die im Zusammenhang mit den zurückliegenden Auffälligkeiten stehen, (...) diese (...) in der Gesamtsicht"* mit heranzuziehen.

Rechtliche Würdigung

Mit Ausnahme des Auszugs aus der Führerscheindatei und den Bescheinigungen über die Teilnahme an einem Fahreignungsseminar waren nach hiesiger Auffassung die weiteren, vorher genannten Unterlagen, die aus dem Ermittlungsverfahren gegen den Petenten stammen, und der Konsilbefund unverzüglich zu löschen, da ihre Speicherung unzulässig war. Die Speicherung war deshalb unzulässig, da die Unterlagen schon gar nicht hätten an die nach dem Umzug des Petenten zuständige Führerscheinstelle übermittelt werden dürfen und die Unterlagen auch nicht zur Erfüllung der Aufgaben der Behörde erforderlich waren.

Die Pflicht zur Löschung ergibt sich aus § 21 Abs. 3 lit. a Saarländisches Datenschutzgesetz (SDSG), wonach personenbezogene Daten zu löschen sind, wenn ihre Speicherung unzulässig ist. Die Speicherung personenbezogener Daten ist nur dann zulässig, wenn diese zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich sind (§ 13 Abs. 1 S. 1 SDSG). Die Daten dürfen dabei nur für die Zwecke verarbeitet werden, für die sie erhoben bzw. erstmals gespeichert worden sind (§ 13 Abs. 1 S. 2 und 3 SDSG).

Die Voraussetzungen einer datenschutzrechtlich zulässigen Speicherung der oben genannten Unterlagen waren im vorliegenden Fall nicht gegeben, da es an der von § 13 Abs. 1 S. 1 SDSG verlangten Erforderlichkeit zur Aufgabenerfüllung fehlte. Die Erforderlichkeit ist zu bejahen, wenn eine Aufgabe ohne die hier relevanten Unterlagen nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann. Nicht ausreichend ist, dass die Kenntnis der Informationen für Erfüllung der Aufgabe lediglich geeignet oder zweckmäßig sind. Der Erforderlichkeitsgrundsatz gilt dabei nicht nur in qualitativer- bzw. quantitativer Hinsicht, sondern begrenzt die Befugnis zur Datenverarbeitung auch in zeitlicher Sicht. Erforderlich ist die Speicherung, Veränderung oder Nutzung personenbezogener Daten erst dann und nur so lange, wie die Aufgabe aktuell ist, d.h. ihre Erfüllung ansteht. Dies war hier nicht mehr der Fall.

Die für den vorliegenden Sachverhalt zu Grunde zu legende Aufgabe besteht in der Anwendung des StVG durch die Führerscheinstelle und die sich hieraus ergebenden Befugnisse zur Überprüfung der Eignung und Befähigung des Fahrerlaubnisinhabers nach § 2 Abs. 8 StVG. Danach ist für ein Tätigwerden der Fahrerlaubnisbehörden das Vorliegen tatsächlicher Anhaltspunkte notwendig, die Bedenken gegen die Eignung oder Befähigung des Fahrerlaubnisinhabers begründen. Bestehen diese tatsächlichen Anhaltspunkte nicht oder nicht mehr, so sind die zum Zwecke der Eignungsprüfung erhobenen und gespeicherten personenbezogenen Daten zu löschen.

So war es im vorliegenden Fall. Die streitgegenständlichen Unterlagen mit personenbezogenen Daten des Petenten wurden der ursprünglich zuständigen Führerscheinstelle vom Landesverwaltungsamt zu dem Zweck übermittelt, die Fahreignung und -befähigung des Petenten in einem konkreten Verwaltungsverfahren zu überprüfen. Offensichtlich sah die damals zuständige Behörde aber die von § 2 Abs. 8 StVG geforderten tatsächlichen Anhaltspunkte als nicht gegeben an, denn aus der Akte ergeben sich keine Anhaltspunkte dafür, dass eine Anordnung zur Beibringung eines Gutachtens oder Zeugnisse gegenüber dem Petenten erlassen wurde oder gar, dass eine Änderung, eine Entziehung, ein Widerruf, eine Aberkennung oder eine Rücknahme der Fahrerlaubnis des Petenten erfolgt ist. Spätestens in dem Zeitpunkt, in

dem die Behörde sich dazu entschloss, das gegen den Petenten eingeleitete Überprüfungsverfahren nicht weiter zu betreiben, wäre sie verpflichtet gewesen, die hierfür gespeicherten Daten zu löschen. Dabei ist es unerheblich, ob der Abschluss des Verfahrens in den Akten vermerkt wurde, da ein solcher Vermerk rein deklaratorische Funktion hat. Allein aus der Tatsache, dass vom Eingang der Mitteilung über die Durchführung eines Fahreignungsseminars bis zur Übersendung der Akte an die nun zuständige Führerscheinstelle fast zwei Jahre vergangen sind und in dieser Zeit keine verwaltungsbehördlichen Maßnahmen oder Entscheidungen durch die Führerscheinstelle getroffen wurden, wird ersichtlich, dass das Überprüfungsverfahren faktisch eingestellt war. Zwar reicht für eine solche Annahme noch nicht jede Untätigkeit aus, denn der Fahrerlaubnisbehörde muss es in einem engen zeitlichen Rahmen gestattet sein, erst Erkenntnisse über die fahreignungsrelevanten Eigenschaften eines Fahrerlaubnisinhabers zunächst zu sammeln, das weitere Verhalten des Betroffenen zu beobachten und schließlich nach einer Würdigung sämtlicher in diesem begrenzten Zeitraum gewonnenen Erkenntnisse über mögliche Beeinträchtigungen der Fahreignung des Betroffenen zu entscheiden (VGH Baden-Württemberg, Urteil vom 28. Oktober 2014 - 10 S 475/04). Ein Zeitraum von zwei Jahren überschreitet diesen engen zeitlichen Rahmen jedoch um ein Vielfaches.

Somit war die weitere Speicherung der streitgegenständlichen Unterlagen mit den personenbezogenen Daten des Petenten bereits durch die ursprüngliche Führerscheinstelle unzulässig. Aus der Unzulässigkeit der Speicherung folgte ebenso die Unzulässigkeit der Übermittlung der personenbezogenen Daten und die sich hieran anschließende Speicherung durch die nach dem Umzug des Petenten zuständige Führerscheinstelle.

Die Speicherung durch die neue Führerscheinstelle war aber auch unabhängig von der rechtswidrigen Übermittlung der personenbezogenen Daten unzulässig. Denn im Rahmen der gegenüber unserer Dienststelle abgegebenen Stellungnahme wurde seitens der Behörde wiederholt darauf hingewiesen, dass „zur Zeit [sic] von einer erneuten Einleitung eines Überprüfungsverfahrens abgesehen wird". Damit wird deutlich, dass die Behörde in den bis dahin vorliegenden Informationen keine ausreichenden, von § 2 Abs. 8 StVG verlangten tatsächlichen Anhaltspunkte erkennen konnte. Damit konnten die vorliegenden Informationen für ein Überprüfungsverfahren nicht erforderlich im datenschutzrechtlichen Sinne sein, zumal ein solches Überprüfungsverfahren zum Zeitpunkt unseres Tätigwerdens überhaupt nicht existent war. Dass die Informationen im „Falle neuer Erkenntnisse, die im Zusammenhang mit den zurückliegenden Auffälligkeiten stehen" von Relevanz sein können, ist rein spekulativer Natur und berechtigte nach unserer Auffassung nicht dazu, die personenbezogenen Daten des Petenten weiterhin aufzubewahren. Mit der Entscheidung ein erneutes Überprüfungsverfahren nicht durchzuführen, wären somit die streitgegenständlichen personenbezogenen Daten des Petenten zu löschen gewesen.

Der Vollständigkeit halber wiesen wir auch darauf hin, dass § 2 Abs. 9 StVG und § 12 StVG hier ebenfalls keine rechtliche Grundlage bietet, da diese beiden Vorschriften auf den vorliegenden Sachverhalt keine Anwendung fanden. § 2 Abs. 9 StVG betrifft inhaltlich schon nur solche Unterlagen (Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse), die auf der Grundlage von § 2 Abs. 7 und 8 StVG

erhoben wurden. Die hier relevanten Unterlagen wurden jedoch nicht von der Fahrerlaubnisbehörde zur Prüfung der Eignung und Befähigung des Petenten erhoben, weil tatsächliche Anhaltspunkte für das Fehlen der Eignung / Befähigung vorlagen. Sie sollten vielmehr dem Nachweis der tatsächlichen Anhaltspunkte dienen, auf Grund derer dann weitere Unterlagen (Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse) hätten eingeholt werden können. In diesem Zusammenhang ist auch darauf hinzuweisen, dass § 2 Abs. 9 StVG keine 10-jährige Speicherbefugnis enthält, sondern verlangt, dass die dort genannten Unterlagen spätestens nach 10 Jahren zu löschen sind. Dies bedeutet, dass im Einzelfall auch erheblich kürzere Aufbewahrungsfristen aus § 2 Abs. 9 StVG gefolgert werden müssen.

§ 2 Abs. 12 StVG findet hingegen schon deswegen keine Anwendung, weil die hier streitgegenständlichen Unterlagen der Fahrerlaubnisbehörde nicht von der Polizei übermittelt wurden, sondern aus einem Ordnungswidrigkeitsverfahren stammen, das beim Landesverwaltungsamt geführt wurde. Darüber hinaus bringt § 2 Abs. 12 StVG aber auch den bereits genannten Erforderlichkeitsgrundsatz zum Ausdruck, wonach solche Daten, die für ein konkretes Eignungsüberprüfungsverfahren nicht erforderlich sind, unverzüglich zu löschen sind.

Ergebnis

Wir haben der Führerscheinstelle und dem Petenten unsere Rechtauffassung mitgeteilt. Von der Behörde wurde uns mitgeteilt, man werde unsere Rechtauffassung prüfen und uns über das Ergebnis benachrichtigen. Zum Redaktionsschluss des vorliegenden Tätigkeitsberichts steht diese Beantwortung noch aus.

6.2 Stationäre Geschwindigkeitsmessanlagen

In immer mehr saarländischen Kommunen kommen Anlagen zur stationären Geschwindigkeitsmessung zum Einsatz. Dabei werden die datenschutzrechtlichen Implikationen, die mit dem Betrieb einer solchen Anlage einhergehen, oft nicht erkannt. So konnten wir im Berichtszeitraum bei allen geprüften Kommunen datenschutzrechtliche Mängel feststellen.

So muss zunächst darauf geachtet werden, dass vor der Inbetriebnahme eines Verfahrens zur Verkehrsüberwachung und anschließenden Fallbearbeitung nach § 46 Abs. 1 OWiG i.V.m. § 490 StPO eine Errichtungsanordnung zu erstellen ist.

§ 490 StPO Errichtungsanordnung für automatisierte Dateien

Die speichernde Stelle legt für jede automatisierte Datei in einer Errichtungsanordnung mindestens fest:

1. *die Bezeichnung der Datei,*
2. *die Rechtsgrundlage und den Zweck der Datei,*
3. *den Personenkreis, über den Daten in der Datei verarbeitet werden,*
4. *die Art der zu verarbeitenden Daten,*

5. *die Anlieferung oder Eingabe der zu verarbeitenden Daten,*
6. *die Voraussetzungen, unter denen in der Datei verarbeitete Daten an welche Empfänger und in welchem Verfahren übermittelt werden,*
7. *Prüffristen und Speicherungsdauer.*

Dies gilt nicht für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.

Diese Errichtungsanordnung erfüllt eine Doppelfunktion. Zum einen legt sie als Verwaltungsvorschrift für den Sachbearbeiter der Kommune verbindlich fest, wie mit der Datei und den darin enthaltenen personenbezogenen Daten umzugehen ist. Zum anderen soll die Errichtungsanordnung den Datenschutzbeauftragten die Wahrnehmung ihrer Kontroll- und Beratungsbefugnisse erleichtern.

Soweit sich die Kommune beim Betrieb des Verfahrens eines Dritten bedient, ist auf den Abschluss eines Vertrags zur Auftragsdatenverarbeitung zu achten (§ 5 SDSG). Insbesondere wenn es sich um private Dritte handelt, ist darauf zu achten, dass der Inhalt des Vertrages den Anforderungen des § 5 Abs. 3 SDSG genügt. In den Fällen der Einschaltung eines privaten Dritten ist der Vertrag im Übrigen der Landesbeauftragten für Datenschutz vorab vorzulegen. Eine solche Einschaltung von privaten Dritten ist in vielerlei Hinsicht denkbar. Dies reicht von Anbietern, die neben dem technischen Betrieb der Blitzsäulen auch die entsprechende Aufbereitung und nachfolgende Zurverfügungstellung von Blitzerfotos anbieten, über Anbieter von externen (Cloud-)Speicherlösungen bis hin zu Anbietern von gehosteten Softwarelösungen (Software as a Service) zur Fallbearbeitung.

Ein besonderes Augenmerk gilt aus materiellrechtlicher Sicht auch den oft viel zu langen Speicherfristen. Insbesondere in den sog. Verwarngeldfällen, in denen dem Fahrzeugführer ein Verwarngeldangebot gemacht wird und dieses innerhalb einer bestimmten Frist beglichen wird, hielten wir eine Speicherung der personenbezogenen Daten über einen längeren Zeitraum als vier Wochen für nicht mehr erforderlich. Denn mit der Bezahlung des Verwarngeldes ist das stillschweigende Einverständnis des Betroffenen gegeben und die Verwarnung wirksam. Sodann kann die Tat nicht mehr nach § 56 Abs. 4 OWiG verfolgt werden und es mangelt mithin an der Erforderlichkeit der weiteren Datenspeicherung.

6.3 Kontrollmaßnahmen im Zusammenhang mit einer Brückensperrung

Für großes mediales Interesse sorgte im Frühjahr 2016 die Vollsperrung der Fechinger Talbrücke der Bundesautobahn 6 (BAB 6). Im Rahmen einer turnusmäßigen Brückenprüfung waren bauartbedingte statische Defizite festgestellt worden. Nachdem erste Verstärkungen an der Autobahnbrücke durchgeführt worden waren, wurde die Brücke im Frühsommer wieder für Fahrzeuge mit einem Gesamtgewicht von weniger als 3,5 t freigegeben. Seit dem 31. Oktober 2016 kann die Brücke auch wieder von Fahrzeugen über 3,5 t Gewicht befahren werden.

Videoüberwachung der automatischen Wiegeanlage

Im Zeitraum der Teilöffnung der Brücke für PKW wurden zur Überwachung der Einhaltung des Befahrungsverbots für LKW an den Autobahnanschlussstellen Saarbrücken-Fechingen und St. Ingbert-West jeweils eine automatische Wiegevorrichtung installiert, die verhindern sollten, dass LKW mit einem Gewicht von über 3,5 t die Brücke befahren. Hierzu wurde an den beiden Anschlussstellen rund um die Uhr Personal postiert, das den Betrieb der Wiegevorrichtung und Schrankenanlage sicherstellen und gegebenenfalls LKW mit mehr als 3,5 t von der Autobahn leiten sollte.

Zur Unterstützung des Personals vor Ort wurde seitens des Landesbetriebes für Straßenbau (LfS) angefragt, ob und unter welchen Voraussetzungen eine Videoüberwachung der Wiegestation und des etwa 1 km langen Einfahrbereichs zulässig sein kann. Nach den Plänen des LfS sollten alle Fahrzeuge mit Kennzeichen erfasst und die Aufnahmen für einen Monat gespeichert werden.

Zweck für die Videoüberwachung seien Verkehrssicherheitsgründe sowie die Überprüfung der Funktionalität der Wiegevorrichtung. Sobald ein LKW in die Wiegevorrichtung einfährt, der das zulässige Gewicht überschreitet, schließen sich die Schranken, wodurch eine Weiterfahrt des LKW verhindert werden soll. In einem solchen Fall müsse unverzüglich Kontrollpersonal zur Brücke, um den LKW abzuleiten und anschließend die Strecke wieder freizugeben. Des Weiteren müsse das Kontrollpersonal auch bei Versagen der Technik direkt eingreifen.

Wir wiesen darauf hin, dass grundsätzlich keine rechtliche Grundlage für eine Aufzeichnung von Videobildern des öffentlichen Verkehrsraum bestehe. Nach unserer Auffassung rechtfertigten die vorgetragenen Zwecke im Rahmen des § 34 Abs. 1 Nr. 2 SDSG lediglich ein Live-Monitoring in den neben der Wiegestation aufgestellten Kontrollcontainern. Hierdurch werde das Kontrollpersonal in die Lage versetzt, den Bereich der Wiegevorrichtung zu überblicken und bei Störungen unverzüglich eingreifen zu können. Eine darüberhinausgehende Speicherung sei nicht erforderlich.

Überwachung des Nachtfahrverbots

Bedingt durch die Sperrung der Fechinger Talbrücke für den Schwerlastverkehr waren großräumige Umleitungen für LKW über 3,5 t erforderlich geworden, was insbesondere nachts zu erheblichen Lärmbelästigungen für die Anwohner an einer Umleitungsstrecke geführt hatte. Daher wurde auf dieser Strecke ein Nachtfahrverbot für LKW angeordnet, von dem jedoch Anlieger ausgenommen waren.

Zur Überwachung der Einhaltung des Nachtfahrverbots beabsichtigte das Landespolizeipräsidium, LPP 13 – Zentrale Verkehrspolizeiliche Dienste, bei sämtlichen LKW auf dieser Umleitungsstrecke, der Flughafenstraße L108, Fotos der Fahrer und der Kennzeichen während der Nachtzeiten anzufertigen und dann im nachfolgenden Verfahren zu prüfen, ob diese als Anlieger vom Nachtfahrverbot ausgenommen waren. Wir hielten diese Praxis für datenschutzrechtlich unzulässig, was wir der Leitung des LPP 13 auch mitgeteilt haben.

Nach unserer Auffassung war eine Erhebung und Speicherung personenbezogener Daten mittels Anfertigung von Lichtbildern von Fahrzeugkennzeichen und -führern

zum Zwecke der Überwachung des Nachtfahrverbots auf der L108 unzulässig. Eine entsprechende Erfassung der personenbezogenen Daten wäre nur in den Fällen zulässig, in denen im Einzelfall der Anfangsverdacht einer Ordnungswidrigkeit gem. §§ 41, 49 StVO, 24 StVG wegen Verstoß gegen das Vorschriftszeichen 253 der StVO angenommen werden konnte.

Nach § 53 Abs. 1 OWiG haben Behörden und Beamte des Polizeidienstes nach pflichtgemäßem Ermessen Ordnungswidrigkeiten zu erforschen. Die Erforschungspflicht beginnt mit dem Vorliegen des Anfangsverdachts einer Ordnungswidrigkeit i.S. zureichender tatsächlicher Anhaltspunkte gem. § 152 Abs. 2 StPO. Ein Anfangsverdacht liegt vor, wenn auf der Grundlage konkreter Tatsachen eine gewisse Wahrscheinlichkeit besteht, dass nach kriminalistischer Erfahrung eine verfolgbare (tatbestandliche, rechtswidrige und vorwerfbare) Ordnungswidrigkeit gegeben ist. Auch wenn die Anforderungen an den Anfangsverdacht relativ gering sind, so muss das Wahrscheinlichkeitsurteil trotzdem auf konkreten tatsächlichen Erkenntnissen beruhen. Statistisch gewonnenes Wissen der Häufung von Ordnungswidrigkeiten in bestimmten Lebenszusammenhängen und/oder Örtlichkeiten genügen hingegen nicht für die Bejahung eines Anfangsverdachts, sondern stellen lediglich Vermutungen ohne Bezug zu einem konkreten Geschehen dar, die es nicht rechtfertigen, jemandem die Begehung einer Ordnungswidrigkeit zur Last zu legen.

Dass solche tatsächlichen Anhaltspunkte hier feststellbar waren, darf bezweifelt werden. Das Vorschriftzeichen 253 (Verbot eines Fahrzeugs mit einem Gewicht von mehr als 3,5 t) galt nicht für Anlieger, da ein entsprechendes Zusatzzeichen an jeder Zufahrt zur Umleitungsstrecke angebracht war. Eine verfolgbare Ordnungswidrigkeit kann daher nur vorgelegen haben, wenn zu einer Zeit zwischen 22.00 und 6.00 Uhr ein Fahrzeug mit mehr als 3,5 t festgestellt wurde und dabei der auf tatsächlichen Anhaltspunkten gegründete Verdacht vorlag, dass der Fahrzeugführer nicht Anlieger im Sinne der StVO ist. Woraus sich solche tatsächlichen Anhaltspunkte hier ergeben haben sollen, war für uns nicht ersichtlich. Offensichtlich ist, dass ein ausländisches oder ortsfremdes Fahrzeugkennzeichen allein keinen Anfangsverdacht begründen kann. Anlieger sind alle Bewohner (Anwohner) oder Nutzungsberechtigte von Grundstücken an einer Verkehrsfläche, die Zugang oder -fahrt zu den Grundstücken ermöglicht. Anlieger sind in diesem Zusammenhang alle Personen, die mit Grundstückseigentümern oder Bewohnern in Beziehung treten wollen. Dies kann sowohl Liefer- oder Kundenverkehr sein, ebenso wie private Besucher eines Anwohners. Hierbei ist zu berücksichtigen, dass die L 108 nicht nur eine Verbindungsstraße zum Flughafen Saarbrücken darstellt, sondern die BAB 6 mit den Ortsteilen der Gemeinde Mandelbachtal verbindet und den dort ansässigen Betrieben und Bewohnern den Zugang zum überörtlichen Straßennetz ermöglicht. Die hiermit einhergehende Erweiterung möglicher Anfahrtsziele erschwert die Feststellung der (Nicht-)Berechtigung zur Straßennutzung. Denn ein berechtigtes Anliegen kann sich nicht nur auf solche Grundstücke beziehen, die an der L 108 gelegen sind, sondern auch auf jede/s/n beliebige/n Grundstück / Firma / Anwohner im gesamten Mandelbachtal. Auf solche Ungewissheiten und daraus folgende Mutmaßungen kann ein Verdacht i.S. von § 152 Abs. 2 StPO jedenfalls nicht gestützt werden.

Schließlich war auch zu bedenken, dass die Anliegereigenschaft nicht an den Halter des Kraftfahrzeugs anknüpft, sondern an den Fahrzeugführer, sodass bereits aus diesem Grund die Einbeziehung des Fahrzeugkennzeichens und daraus schlussfolgernd die Herkunft des Fahrzeughalters an Hand des Kennzeichens ungeeignet für die Frage der Anliegereigenschaft ist.

Wenn - wie im vorliegenden Fall - nur allgemeine, auf eine Ordnungswidrigkeit hindeutende Umstände vorliegen, wäre es nach hiesiger Auffassung erforderlich gewesen, die Sach- und Rechtslage zunächst vor Ort durch eine formlose informatorische Befragung des Fahrzeugführers abzuklären. Nur bei einem konkreten Verdacht gegen einen bestimmten Fahrzeugführer wäre dann die Erhebung und Speicherung der Personalien und ggfls. des Fahrzeugkennzeichens erforderlich und damit als datenschutzrechtlich zulässig zu werten gewesen.

6.4 Beabsichtigte Videoüberwachung an einem Industriehafen

Im Dezember 2015 wurden wir um eine datenschutzrechtliche Beratung hinsichtlich einer möglichen Ausgestaltung einer Videoüberwachung an einem von einem landeseigenen Unternehmen betriebenen Industriehafen gebeten.

Um uns hinsichtlich der datenschutzrechtlichen Aspekte wie Erforderlichkeit, betroffener Personenkreis und Überwachungsbereiche einen Eindruck verschaffen zu können, wurde ein Vororttermin vereinbart. Im Rahmen dieses Termins wurde uns dargelegt, dass durch die beabsichtigte Videoüberwachungsmaßnahme zum einen der Schutz von Personen im Bereich des Hafenbeckens sowie der Schutz des Eigentums, hier der Kaimauer, erreicht und zum anderen eine Zufahrtskontrolle des Schiffsverkehrs zum Hafen gewährleistet werden soll. In unserer datenschutzrechtlichen Bewertung haben wir dargelegt, dass Videoüberwachungsmaßnahmen grundsätzlich einen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellen und daher nur aufgrund einer bereichsspezifischen Rechtsgrundlage eingesetzt werden können. Sind in den für einen Bereich geltenden spezialgesetzlichen Vorschriften keine konkreten Normen zur Durchführung von Videoüberwachungsmaßnahmen enthalten, können die in den Datenschutzgesetzen des Bundes und der Länder enthaltenen Vorschriften zur Durchführung von Videoüberwachungsmaßnahmen herangezogen werden.

Weder in den für die Bundeswasserstraße Saar geltenden Gesetzen, dem Wasserhaushaltsgesetz (WHG), dem Bundeswasserstraßengesetz (WaStrG), dem Saarländischen Wassergesetz (SWG) noch den jeweiligen Rechtsverordnungen der Binnenschifffahrtsstraßen-Ordnung (BinSchStrO) sowie auch der für Häfen im Saarland geltenden Hafenverordnung (HafenO-SL) sind einschlägige Rechtsvorschriften zur Ausgestaltung von Videoüberwachungsmaßnahmen enthalten.

Mithin war zunächst zu prüfen welche datenschutzrechtlichen Bestimmungen auf die Hafenbetriebe Saarland Anwendung finden. Die Hafenbetriebe Saarland sind zu 100 % im Besitz des Landes und gemäß § 28 Abs. 8 SWG i.V.m. § 1 Abs. 1 und § 3 Abs. 3 HafenO-SL mit dem Vollzug der Hafenverordnung beauftragt und handeln insoweit öffentlich-rechtlich.

Demnach finden nach § 2 Abs. 1 S. 1 bis 3 Saarländisches Datenschutzgesetz (SDSG) die Vorschriften des SDSG auf die Hafenbetriebe Saarland Anwendung, so dass Videoüberwachungsmaßnahmen nur auf der Grundlage von § 34 SDSG durchgeführt werden können.

Nach § 34 Abs. 1 Nr. 1 SDSG ist die Beobachtung öffentlich zugänglicher Bereiche mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie in Wahrnehmung des Hausrechts der verantwortlichen Stelle zum Zweck des Schutzes von Personen, des Eigentums oder des Besitzes oder der Kontrolle von Zugangsberechtigungen erforderlich ist.

Für die Gefährdung der vorgenannten Rechtsgüter müssen konkrete Anhaltspunkte bestehen. Es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Videoüberwachung darf nur durch die Leitung der verantwortlichen Stelle angeordnet werden.

Dabei sind der Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung zu dokumentieren. Zu den einzelnen möglichen Überwachungsbereichen haben wir Nachstehendes ausgeführt:

Kaimauer

Es wurde vorgetragen, dass gehäuft Beschädigungen an der Kaimauer festzustellen sind. § 34 Abs. 1 Nr. 1 SDSG eröffnet dem Hafenbetreiber in Wahrnehmung seines Hausrechts zum Schutz seines Eigentums oder Besitzes entsprechende Möglichkeiten zur Videoüberwachung. Konkrete Anhaltspunkte für das Vorliegen einer entsprechenden Gefährdungssituation wurden dokumentiert. Hinsichtlich des möglichen Aufzeichnungsbereiches in Abwägung mit schutzwürdigen Interessen von Betroffenen wurde von uns die Erfassung der Kaimauer, als auch ein Ein-Meter-Bereich auf der Kaimauer in den Uferdamm hineinragend, in äquivalenter Anwendung hierzu ergangener Rechtsprechung als zulässig erachtet. Für die Interessenabwägung war insbesondere von Belang, dass an einem Teil der Kaimauer ein öffentlicher Fahrradweg vorbeiführte. Bei Einhaltung des zuvor erwähnten Ein-Meter-Bereiches würden die auf dem Uferdamm entlangfahrenden Radfahrer oder Spaziergänger in der Regel nämlich nicht mit dem ganzen Körper, sondern nur Teile hiervon, und vor allem auch nur kurzzeitig von der Kamera erfasst. Mit Blick auf den ebenso möglichen betroffenen Personenkreis von Anglern ist festzustellen, dass das Angeln nach § 10 Nr. 4 HafenO-SL ohne Erlaubnis verboten ist. Soweit keine Erlaubnis des Hafenunternehmers erteilt wird, verhält sich der Betroffene ordnungswidrig nach § 46 Abs. 1 lit. c) HafenO-SL. Sollten hingegen Erlaubnisse nach § 10 HafenO-SL erteilt werden, die ein dauerhaftes Verweilen in dem zuvor beschriebenen Ein-Meter-Bereich gestatten, müsste der Aufzeichnungsbereich auf die Kaimauer begrenzt werden.

Hafenbecken

Es wurde uns dargelegt, dass das Hafenbecken zum Schutz von Personen mit Videotechnik überwacht werden soll. Eine Videoüberwachungsmaßnahme muss für den

beabsichtigten Zweck, hier zum Schutz von Personen, auch eine geeignete Maßnahme darstellen. Zur Erreichung des Schutzzwecks von Personen ist daher ein sogenanntes Kameramonitoring zu implementieren. Ein Kameramonitoring muss so ausgestaltet sein, dass, wenn wie hier eine Gefahr für Leib und Leben der Betroffenen verhindert oder minimiert werden soll, auch unmittelbar, etwa durch einen den Kameramonitor überwachenden Sicherheitsdienst Rettungskräfte wie Feuerwehr, Wasserschutzpolizei und/oder Notarzt herbeigerufen werden können. Eine reine Aufzeichnung liefert allenfalls Beweismaterial für den Hergang des Geschehens, erfüllt aber nicht den vorgenannten Schutzzweck.

Zufahrtskontrolle zum Hafen

Bei der Zufahrtskontrolle ist insbesondere zu beachten, dass auf diese Maßnahme möglichst frühzeitig in einer für den Schiffverkehr geeigneten Weise hinzuweisen ist. Die Größe der Hinweisschilder wird sich daher für diesen Bereich mit Blick auf die Erkennbarkeit nach der im Schiffsverkehr üblichen Beschilderungsgröße richten müssen. Für Nachtfahrten sollten die Schilder beleuchtet oder mit fluoreszierender Schrift und Einfassung ausgestaltet sein.

Überwachung öffentlich zugänglicher Freiflächen

Eine Videoüberwachung ist nur zulässig, soweit sie erforderlich ist. Sofern der Zweck also auch durch weniger in die Rechte der Betroffenen eingreifende Mittel erreicht werden kann, sind diese vorzuziehen. Eine Nichtbenutzung von Freiflächen kann z.B. auch durch eine Umfriedung (Zaun, Mauer) erreicht werden. Die Überwachung öffentlich zugänglicher Freiflächen wird daher in Ermangelung der Erforderlichkeit als auch im Rahmen der Interessensabwägung grundsätzlich als unzulässig zu bewerten sein.

Abschließend haben wir ausführlich auf die erforderlichen Hinweispflichten nach § 34 Abs. 2 SDSG sowie deren Ausgestaltung und bei Aufzeichnungen auf die Maximalspeicherdauer von 24 Stunden gemäß § 34 Abs. 4 SDSG hingewiesen. Ebenso haben wir ausführlich dargelegt, in welcher Form unsere Dienststelle vor der beabsichtigten Installation einer Videoüberwachungsanlage zu beteiligen ist und welche weiteren erforderlichen Unterlagen hier vorzulegen sind.

7 Steuern

7.1 Automatisierter Zugriff des Rechnungshofes auf die Fördermitteldatenbank

Durch das Gesetz über die Einrichtung einer Fördermitteldatenbank im Saarland vom 2. April 2003 (SFöDG) wurde die rechtliche Grundlage für die Führung einer Fördermitteldatenbank geschaffen. Mit dieser Datenbank werden im Bereich der Finanzverwaltung Fördermittel aus dem Landeshaushalt, nach dem Kommunalfinanzausgleichsgesetz und Zuwendungen des Bundes oder der Europäischen Union erfasst und verwaltet. Hinterlegt werden dabei Antragsteller, Förderprojekte und die Überwachung der zweckgebundenen Fördermittel.

In § 2 Abs. 2 SFöDG ist vorgesehen, dass dem Rechnungshof auf dessen Verlangen für Zwecke der Finanzkontrolle die erforderlichen Daten aus der Fördermitteldatenbank zu übermitteln sind. Dies geschah bisher dergestalt, dass halbjährlich Auszüge für sämtliche Projekte aus der Fördermitteldatenbank in Form einer Excel-Tabelle vom Ministerium für Finanzen und Europa an den Rechnungshof übermittelt wurden. Dieses Vorgehen sollte dahingehend geändert werden, dass dem Rechnungshof ein Zugriffsrecht in Form eines Leserechts auf die gesamte Fördermitteldatenbank eingeräumt würde, mit der Folge, dass die halbjährliche Übermittlung der Excel-Tabellen entbehrlich würde.

Das Ministerium für Finanzen und Europa bat uns um datenschutzrechtliche Bewertung, ob und unter welchen Bedingungen es zulässig sei, dass dem Rechnungshof ein ständiger und insbesondere automatisierter Zugriff auf die Fördermitteldatenbank gewährt werde. Wir bewerteten die Zurverfügungstellung eines solchen Zugangs als Bereithalten eines automatisierten Abrufverfahrens für das es jedoch an der von § 10 Abs. 1 SDSG verlangten bundes- bzw. landesrechtlichen Regelung fehlte.

Nach § 10 Abs. 1 Saarländisches Datenschutzgesetz (SDSG) ist die Einrichtung eines automatisierten Abrufverfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, nur zulässig, soweit dies durch Bundes- oder Landesrecht bestimmt ist. Da die Norm begrifflich nur auf die Einrichtung des Verfahrens abstellt, handelt es sich um einen Regelungsvorbehalt, der auf Seiten der verantwortlichen Stelle zu beachten ist und der keine Aussage über die datenschutzrechtliche Zulässigkeit eines Abrufs im Einzelfall trifft.

Dementsprechend sahen wir auch in § 95 Abs. 3 Landeshaushaltsordnung keine Bestimmung im vorgenannten Sinne und damit keine Befugnis zur Einrichtung eines solchen Verfahrens. Zwar ist dort geregelt, dass die dem Rechnungshof gegenüber bestehende Auskunftspflicht sich auch auf den automatisierten Abruf der beim Auskunftspflichtigen elektronisch gespeicherten Daten erstreckt. § 95 Abs. 3 LHO gestat-

tet damit jedoch nach hiesiger Auffassung nicht die Einrichtung eines automatisierten Abrufverfahrens im Sinne des § 10 Abs. 1 SDSG, sondern setzt das Bestehen eines solchen automatisierten Abrufverfahrens voraus.

Mit dem Rechnungshof und dem Ministerium für Finanzen und Europa konnte hinsichtlich des Erfordernisses einer gesetzlichen Regelung zur Rechtfertigung des ständigen Zugriffs auf die Fördermitteldatenbank Einvernehmen erzielt werden. Es wurde vereinbart, dass dem Gesetzgeber eine Änderung des SFöDG vorgeschlagen wird, um den automatisierten Zugriff zu regeln. Die neue Formulierung des § 2 Abs. 2 SFöDG wurde mit uns abgestimmt und die Änderung trat zum 1. Dezember 2015 in Kraft:

Dem Rechnungshof steht der für die Erfüllung seiner Aufgaben erforderliche automatisierte Zugriff auf die in der Fördermitteldatenbank gemäß § 3 Absatz 1 Satz 2 enthaltenen Daten zu. Er bedient sich dabei der in der Fördermitteldatenbank eingerichteten technischen Zugriffs- und Auswertemöglichkeiten.

7.2 Verlagerung der steuerlichen Verfahren zur Zentralen Datenverarbeitung der Finanzverwaltung (ZDFin) nach Koblenz

Bereits 2014 wurde zwischen den Ländern Rheinland-Pfalz und Saarland ein Staatsvertrag zur Kooperation im Bereich des Betriebs von IT-Systemen geschlossen. Betroffen von dieser Maßnahme war in erster Linie der Großrechnerbetrieb der damaligen Zentralen Datenverarbeitungsstelle des Saarlandes (ZDV-Saar, heute: Landesamt für IT-Dienstleistungen). Aus Kostengründen wurden Großrechner und die dazu notwendige Infrastruktur im Saarland nicht mehr ersetzt und die entsprechende Rechnerleistung in Rheinland-Pfalz angemietet. Somit wurde es notwendig, dass die komplette Anwendung der steuerlichen Verfahren nach Rheinland-Pfalz migriert wurde.

Nach § 20 Abs. 2 Finanzverwaltungsgesetz ist es erlaubt, die automationsgesteuerte Verarbeitung der Steuerverfahren auf ein anderes Land zu übertragen:

Die für die Finanzverwaltung zuständigen obersten Landesbehörden können technische Hilfstätigkeiten durch automatische Einrichtungen der Finanzbehörden des Bundes, eines anderen Landes oder anderer Verwaltungsträger verrichten lassen. Das Bundesministerium der Finanzen kann technische Hilfstätigkeiten durch automatische Einrichtungen der Finanzbehörden eines Landes oder anderer Verwaltungsträger verrichten lassen. In diesen Fällen ist sicherzustellen, dass die technischen Hilfstätigkeiten entsprechend den fachlichen Weisungen der für die Finanzverwaltung zuständigen obersten Behörde oder der von ihr bestimmten Finanzbehörde der Gebietskörperschaft verrichtet werden, die die Aufgabenwahrnehmung übertragen hat.

Die Verlagerung zur ZDFin wurde in enger Abstimmung mit unserem zuständigen Referat für den Bereich Steuer sowie dem Technik-Referat durch die ZDV-Saar vorbereitet und in 2015 abgeschlossen.

8 Kommunales

8.1 Beanstandung einer Videoüberwachungsanlage an einer religiösen Stätte

Bereits in unserem 24. Tätigkeitsbericht[16] hatten wir über die Demontage einer unzulässig verdeckt ausgestalteten Videoüberwachungsmaßnahme durch eine saarländische Kommune informiert. Seinerzeit hatten wir die in Rede stehende Kommune ausführlich auf die Beteiligungspflichten nach § 7 Abs. 2 Saarländisches Datenschutzgesetz (SDSG), Transparenzerfordernisse sowie über die Voraussetzungen für eine nach § 34 SDSG zulässige Videoüberwachung hingewiesen.

Im Juni 2015 wurde unsere Dienststelle dann durch eine Eingabe darauf aufmerksam gemacht, dass dieselbe Kommune erneut im Bereich dieser religiösen Stätte eine Videoüberwachungsanlage installiert hatte. Wir haben diese Eingabe zum Anlass genommen, um uns vor Ort zunächst selbst ein Bild von der vom Petenten vorgetragenen Videoüberwachungsmaßnahme zu machen. Aufgrund der bei dieser Begehung gewonnenen Erkenntnisse über die Art der eingesetzten Videoüberwachungsanlage war davon auszugehen, dass es sich nicht lediglich um eine – datenschutzrechtlich irrelevante – Attrappe, sondern um eine in Betrieb befindliche Echtanlage zur Videoüberwachung handelte, deren Überwachungsbereiche mit hoher Wahrscheinlichkeit unzulässig ausgestaltet waren. Auch die Transparenzhinweise entsprachen nicht den gesetzlichen Vorgaben.

Wir sahen uns daher veranlasst, die verantwortliche Kommune unverzüglich aufzusuchen, um die tatsächlichen Verhältnisse im Rahmen einer Ad-hoc-Kontrolle gemeinsam mit den Verantwortlichen festzustellen. In unserem Gespräch mit dem Bürgermeister wurde eingeräumt, dass es sich um eine in Betrieb befindliche Videoüberwachungsanlage handele. In Anbetracht der ausgebliebenen Beteiligung unserer Dienststelle sowie aufgrund der bei der vorausgegangenen Begehung gewonnenen Erkenntnisse zu Art und Umfang der Videoüberwachung, haben wir das sofortige Abschalten der Kameras bis zur Herstellung eines ordnungsgemäßen Abstimmungsprozesses gefordert. Die anschließende Sichtung der aktuellen Live-Bilder der Kamera sowie der gespeicherten Aufzeichnungen bestätigte unsere Vermutung einer unzulässigen Ausgestaltung des Erfassungsbereiches. Konkret wurden Teile eines überdachten Gebetsbereiches, große Teile eines Versammlungsvorplatzes sowie nahezu der gesamte Innenraum der zum Areal gehörenden Kapelle überwacht. Hinsichtlich der Aufzeichnungsdauer war festzustellen, dass die zulässige Höchstdauer von 24 Stunden deutlich überschritten wurde. Sodann wurde die Kameraüberwachung in unserem Beisein eingestellt.

Das Erstellen und Speichern von Bildaufnahmen stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar. Bei der gezielten Beobachtung einzelner Personen oder der Überwachung von Bereichen, die über Betroffene

[16] Vgl. 24. Tätigkeitsbericht, 2011/2012, Kapitel 9.1.1, S. 54f.

zusätzlich sensible Informationen preisgeben, wie bei der Überwachung von religiösen Einrichtungen, in denen Menschen beispielweise im stillen Gebet verweilen, sind die schutzwürdigen Interessen Betroffener besonders zu berücksichtigen.

Hinzu kam vorliegend, dass durch unzureichend ausgestaltete Transparenzmaßnahmen, völlig ungenügend festgelegte Löschfristen und die unterlassene Beteiligung unserer Dienststelle datenschutzrechtliche Vorgaben in signifikantem Maße missachtet wurden.

Dies zusammengenommen stellte in der Gesamtschau einen Verstoß gegen Vorschriften des SDSG dar, der nicht unerheblich war. Stellt die Landesbeauftragte für Datenschutz erhebliche Verstöße gegen Vorschriften über den Datenschutz fest, beanstandet sie dies gemäß § 27 Abs. 1 S. 3 Nr. 2 SDSG bei den Gemeinden und Gemeindeverbänden gegenüber dem vertretungsberechtigten Organ und fordert zur Stellungnahme innerhalb einer von ihr zu bestimmenden Frist auf. Sie unterrichtet nach § 27 Abs. 1 S. 4 SDSG gleichzeitig auch die zuständige Aufsichtsbehörde.

Daher wurde eine entsprechende förmliche Beanstandung gegenüber der betreffenden Gemeinde ausgesprochen und die zuständige Aufsichtsbehörde, das Landesverwaltungsamt, hierüber unterrichtet. Inwieweit das Landesverwaltungsamt auf unsere Unterrichtung hin tätig geworden ist, entzieht sich indes unserer Kenntnis.

Im weiteren Verlauf des Verfahrens erfolgte sodann die gesetzlich vorgesehene Beteiligung unserer Dienststelle. Im Rahmen dieser Beteiligung wurde gemeinsam mit der Kommune die Videoüberwachung datenschutzkonform ausgestaltet. Die Überwachungsbereiche wurden unter Wahrung der schutzwürdigen Interessen der Betroffen völlig neu justiert, deutlich verkleinert und bestimmte Bereiche systemtechnisch ausgeblendet. Die erforderliche Beschilderung wurde gesetzeskonform erneuert und die Speicherdauer auf 24 Stunden begrenzt.

8.2 Heimliche Überwachung von Mitarbeitern im öffentlichen Dienst

Die Beauftragung einer Detektei mit dem Ziel der Überwachung von im öffentlichen Dienst einer Kommune beschäftigten Mitarbeitern zur Aufklärung des Verdachts von Arbeitszeitbetrug und Diebstahl von kommunalem Eigentum gab im Berichtszeitraum Anlass, sich mit der Zulässigkeit einer solchen Überwachungsmaßnahme auf der Grundlage des Saarländischen Datenschutzgesetzes zu beschäftigen. Denn anders als § 32 Abs. 1 S. 2 Bundesdatenschutzgesetz (BDSG), der die Verarbeitung personenbezogener Daten zur Aufdeckung von Straftaten unter bestimmten weiteren Voraussetzungen gestattet, fehlt es im für öffentliche Stellen des Landes anwendbaren § 31 SDSG an einer ausdrücklichen Befugnis der Verarbeitung personenbezogener Daten von Mitarbeitern zu repressiven Zwecken.

Entsprechend sahen wir § 31 SDSG nicht als ausreichende Rechtsgrundlage für die Observierung von Mitarbeitern im öffentlichen Dienst einer saarländischen Kommune zu repressiven Zwecken, unabhängig davon, ob diese Überwachung während der Arbeitszeit oder in der Freizeit des überwachten Arbeitnehmers erfolgt.

Denn nach § 31 SDSG dürfen personenbezogene Daten von Mitarbeitern nur verarbeitet werden, wenn diese zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen erforderlich sind. Eine auf § 31 Abs. 1 S. 1 SDSG gestützte Observation von Mitarbeitern im öffentlichen Dienst zu repressiven Zwecken, um ein (vermutetes) Fehlverhalten der Mitarbeiter aufzudecken, ist von den Tatbestandsvoraussetzungen nicht gedeckt.

§ 31 Abs. 1 S. 1 SDSG, der inhaltlich an § 32 Abs. 1 S. 1 BDSG angelehnt ist, gestattet ebenso wie die gleichlautende Formulierung des § 95 Abs. 3 S. 1 Saarländisches Beamtengesetz nur solche Datenverarbeitungen, die mit einem der genannten Zwecke in unmittelbarem Zusammenhang stehen. Die Notwendigkeit, d.h. das Erfordernis der Datenerhebung bzw. -verarbeitung, müssen sich unmittelbar aus dem Gegenleistungsverhältnis zwischen Arbeitgeber und Arbeitnehmer ergeben und damit der Zweckbestimmung des Beschäftigungsverhältnisses zuzuordnen sein. An diesem Unmittelbarkeitszusammenhang fehlt es bei der Durchführung von (heimlichen) Überwachungsmaßnahmen zur Aufdeckung eines (vermuteten) Fehlverhaltens, da diese primär dazu dienen, Informationen zu sammeln und Verdachtsmomente zu bestätigen, um möglicherweise später, gestützt auf die gewonnenen Erkenntnisse, Maßnahmen im Dienst- und Arbeitsverhältnis ergreifen zu können und damit nicht unmittelbar der Abwicklung des Arbeitsvertrags dienen.

Eine hingegen weite Auslegung der Tatbestandsvoraussetzungen mit dem Ziel auch personenbezogene Daten des Mitarbeiters zu repressiven Zwecken verarbeiten zu dürfen, wäre mit verfassungsrechtlichen Vorgaben an das Bestimmtheitsgebot nicht zu vereinbaren. Die Anforderungen der Normenbestimmtheit und Normenklarheit hat zwar in erster Linie der Gesetzgeber zu beachten. Aber auch die Träger öffentlicher Verwaltung und die sie kontrollierenden Gerichte müssen diese Anforderungen insofern beachten, als ein staatlicher Eingriff nicht auf eine Rechtsgrundlage gestützt werden darf, die dem Bestimmtheitsgebot nicht entspricht (vgl. BVerfG, Stattgebender Kammerbeschluss vom 23. Februar 2007 – 1 BvR 2368/06 –, Rn. 48).

Im Kontext von Eingriffen in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) soll das Gebot sicherstellen, dass der Betroffene sich auf mögliche belastende Maßnahmen einstellen kann, dass die gesetzesausführende Verwaltung für ihr Verhalten steuernde und begrenzende Handlungsmaßstäbe vorfindet und dass die Gerichte die Rechtskontrolle durchführen können. Der Anlass, der Zweck und die Grenzen des Eingriffs müssen daher in der Ermächtigung bereichsspezifisch, präzise und normenklar festgelegt werden (vgl. BVerfG, Beschluss vom 3. März 2004 – 1 BvF 3/92 –, BVerfGE 110, 33 Rn. 102).

Die konkreten Anforderungen an die Bestimmtheit und Klarheit der Ermächtigung richten sich nach der Art und der Schwere des Eingriffs. Bei Ermächtigungen zu Überwachungsmaßnahmen verlangt das Bestimmtheitsgebot zwar nicht, dass die konkrete Maßnahme vorhersehbar ist, wohl aber, dass die betroffene Person erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist (vgl. BVerfG, Beschluss vom 3. März 2004 – 1 BvF 3/92 –, BVerfGE 110, 33 Rn. 104). Gerade längerfristige Observationsmaßnahmen vermitteln schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung. Dies gilt erst recht, wenn dabei technische Mittel zum Einsatz kommen

oder unbeteiligte Dritte miterfasst werden, weshalb aus verfassungsrechtlicher Sicht die Normierung konkreter Voraussetzungen unerlässlich ist.

Die Regelung des § 31 SDSG lässt, anders als § 32 Abs. 1 S. 2 BDSG, hingegen völlig offen, bei welchen Anlässen (Straftat, Ordnungswidrigkeit, Nichtbefolgen einer Weisung des Arbeitgebers) und unter welchen Voraussetzungen, insbesondere im Hinblick auf den Verdachtsgrad und etwaige Dokumentationspflichten, eine Überwachung von Mitarbeitern zulässig ist. Würde man die Vorschrift als Erlaubnisgrundlage für eine Observation heranziehen, so wären Anlass, Umfang und Grenzen einer solchen Maßnahme einseitig in das Ermessen der Verwaltung gestellt.

Auf obigen verfassungsrechtlichen Erwägungen beruhen auch die Regelungen in § 163f der Strafprozessordnung, wonach eine längerfristige Observation (mit einer durchgehenden Dauer von mehr als 24 Stunden oder an mehr als zwei Tagen) nur unter bestimmten Voraussetzungen zulässig ist und nur durch das Gericht, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen angeordnet werden darf. Der Landesgesetzgeber hat mit § 28 des Saarländischen Polizeigesetzes ebenfalls eine ähnliche Regelung geschaffen. Danach handelt es sich unter anderem bei der längerfristigen Observation (planmäßig angelegte Beobachtung einer Person, die durchgehend länger als 24 Stunden oder über einen Zeitraum von mehr als einer Woche durchgeführt wird, (Abs. 2 Nr. 1)) und beim verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen sowie zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes (Abs. 2 Nr. 2) um besondere Mittel der verdeckten Datenerhebung, die nur unter bestimmten Voraussetzungen zulässig sind (Abs. 1 und 3). Diese besonderen Formen der Erhebung personenbezogener Daten dürfen nur durch die Vollzugspolizei durchgeführt werden. Die längerfristige Observation bedarf dabei grundsätzlich einer richterlichen Anordnung. Nur bei Gefahr im Verzug kann die Anordnung auch durch den Behördenleiter erteilt werden, muss dann aber innerhalb von drei Tagen vom Amtsgericht bestätigt werden. Beide Vorschriften sehen zudem Vorgaben zum Schutz unbeteiligter Dritter vor.

Andere Rechtsgrundlagen als § 31 Abs. 1 S. 1 SDSG für eine Überwachung von Mitarbeitern einer Kommune kommen nicht in Betracht. § 31 Abs. 1 S. 1 SDSG ist in Bezug auf die Datenverarbeitung bei Dienst- und Arbeitsverhältnissen im öffentlichen Dienst abschließend („Daten von […] Beschäftigten dürfen nur verarbeitet werden …", § 31 Abs. 1 S. 1 SDSG). Eine Überwachung von Mitarbeitern zu repressiven Zwecken war daher nach unserer Auffassung hier unzulässig. Eine Einschaltung der Staatsanwaltschaft wäre nach unserer Auffassung hier das richtige Mittel gewesen.

8.3 Outsourcing von Druck, Adressierung und Kuvertierung behördlicher Schreiben

Bereits im 25. Tätigkeitsbericht[17] hatte sich die Landesbeauftragte zur Zulässigkeit des Outsourcings von Druck, Adressierung und Kuvertierung von kommunalen Abgabenbescheiden geäußert. Anlass war damals die Beauftragung eines Lettershops

[17] Vgl. 25. Tätigkeitsbericht, 2013/2014, Kapitel 8.3, S. 63f.

durch eine saarländische Kommune. An unserer diesbezüglichen Rechtsauffassung, dass ein entsprechendes Outsourcing im Anwendungsbereich des § 30 Abgabenordnung (AO) unzulässig ist, halten wir weiterhin fest. Gleichwohl spielt diese Thematik aber auch in anderen Bereichen außerhalb des Steuerrechts eine immer größere Rolle.

Im Berichtszeitraum sind mehrere saarländische Kommunen mit der Bitte um datenschutzrechtliche Bewertung eines geplanten Outsourcings von Druck, Adressierung und Kuvertierung behördlicher Schreiben an uns herangetreten.

Datenschutzrechtlich ist das Outsourcing von Druck, Adressierung und Kuvertierung behördlicher Schreiben grundsätzlich als Auftragsdatenverarbeitung (ADV) zu qualifizieren und damit an den Voraussetzungen des § 5 SDSG zu messen, unabhängig davon, ob es sich bei dem Dienstleister um einen kleinen Lettershop, eine regional tätige Druckerei oder einen internationalen Postkonzern handelt. In jedem Fall ist der Abschluss eines ADV-Vertrages nach § 5 SDSG erforderlich, um die datenschutzrechtlichen Vorgaben sicherzustellen. Die Landesbeauftragte ist hierüber zu unterrichten.

Datenschutzrechtlich problematisch stellte sich im Berichtszeitraum insbesondere die Nutzung des sog. ePOSTBRIEFES mit klassischer Zustellung bzw. der sog. ePOSTBUSINESSBOX, beides Produkte des Konzerns Deutsche Post AG, dar. Die hierfür vorgegebenen Vertragsformulare und -unterlagen der Deutschen Post AG zur Auftragsdatenverarbeitung sahen bisher die spezifischen, für öffentliche Stellen im Saarland geltenden Anforderungen des § 5 Abs. 3 SDSG nicht vor, sondern orientierten sich ausschließlich an den Vorgaben des § 11 BDSG. Wir mussten den betroffenen Kommunen daher mitteilen, dass eine datenschutzkonforme Nutzung der ePOSTBUSINESSBOX bisher für öffentliche Stellen im Saarland nicht möglich war.

Die Deutsche Post AG hat hierauf reagiert und bietet nun nach Abstimmung mit unserer Dienststelle für Kunden, die dem Anwendungsbereich des SDSG unterfallen, einen auf die saarländische Rechtslage angepassten Auftragsdatenverarbeitungsvertrag an. So ist in dem Vertrag nun entsprechend § 5 Abs. 3 S. 1 SDSG eine Kontrollbefugnis der Landesbeauftragten für Datenschutz vorgesehen. Zudem wurde das Verfahren in Bezug auf Unterauftragsverhältnisse angepasst, sodass nun sichergestellt ist, dass Unterauftragsverhältnisse nicht ohne ausdrückliche Zustimmung der verantwortlichen Stelle zustande kommen, wie dies § 5 Abs. 1 S. 6 SDSG verlangt, gleichzeitig auf Seiten der Deutschen Post AG aber die für den Betrieb des Angebotes notwendige Flexibilität und Homogenität gewahrt bleibt.

Gleichwohl ist nochmals ausdrücklich darauf hinzuweisen, dass in jedem Fall und unabhängig von dem eingesetzten Dienstleister, die Kommune vor der Beauftragung eines Unternehmens die Landesbeauftragte für Datenschutz hierüber zu unterrichten hat und den Vertragsentwurf zur Prüfung der Vorgaben des § 5 Abs. 1 und 3 SDSG vorzulegen hat. Es ist daher für Kommunen sinnvoll, gerade auch bei der Einschaltung von Dienstleistern das Beratungsangebot der Landesbeauftragten frühzeitig in Anspruch zu nehmen.

8.4 Einbau und Betrieb "intelligenter" Wasserzähler

Im Berichtszeitraum haben wir Beschwerden darüber erhalten, dass immer mehr Stadtwerke und Zweckverbände dazu übergehen, bisherige "analoge" Wasserzähler durch sog. "intelligente" Wasserzähler zu ersetzen.

Bei den uns bekannten sog. "intelligenten" Wasserzählern handelt es sich um elektronische Ultraschall-Wasserzähler, die mit einer unidirektionalen Funk-Sendeeinheit ausgestattet sind. Über diese Schnittstelle sendet der Zähler im 16 Sekunden-Takt die jeweilige Zählernummer, den tagesaktuellen Verbrauchsstand, den Verbrauchsstand des Vormonatsletzten, eventuelle Fehlermeldungen (Leckage, Rohrbruch, Rückwärts, Trocken oder Defekt), die durchschnittliche Temperatur des Wassers und der Umgebung des Vormonats sowie die Einsatzzeit des Wasserzählers in Stunden. Das Datenpaket wird dabei kryptographisch gesichert. Geräte mit ähnlichen Funktionen kommen auch im Bereich der Fernwärmeversorgung zum Einsatz.

Der Versorger kann diese Datenpakete im Vorbeifahren empfangen und so ohne Mitwirkung und ohne Kenntnis der Kunden die Zählerstände erfassen. Die Versorger machen hiervon zum Zwecke der Verbrauchsabrechnung, aber auch zur Sicherung der Trinkwasserhygiene und des Netzmanagements Gebrauch.

Das Saarländische Datenschutzgesetz regelt in § 32 SDSG die datenschutzrechtlichen Rahmenbedingungen für den Einsatz solcher Fernmessdienste durch Stadtwerke und kommunale Zweckverbände.

§ 32 Fernmessen und Fernwirken

(1) Öffentliche Stellen dürfen ferngesteuerte Messungen oder Beobachtungen (Fernmessdienste) in Wohnungen oder Geschäftsräumen nur vornehmen, wenn die oder der Betroffene zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes unterrichtet worden ist und nach der Unterrichtung schriftlich eingewilligt hat. Entsprechendes gilt, soweit eine Übertragungseinrichtung dazu dienen soll, in Wohnungen oder Geschäftsräumen andere Wirkungen auszulösen (Fernwirkdienste). Die Einrichtung von Fernmess- und Fernwirkdiensten ist nur zulässig, wenn die oder der Betroffene erkennen kann, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist; dies gilt nicht für Fernmess- und Fernwirkdienste der Versorgungsunternehmen. Die oder der Betroffene kann ihre oder seine Einwilligung jederzeit widerrufen, soweit dies mit der Zweckbestimmung des Dienstes vereinbar ist. Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) Eine Leistung, der Abschluss oder die Abwicklung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, dass die oder der Betroffene nach Absatz 1 S. 1 oder 2 einwilligt. Verweigert oder widerruft sie oder er ihre oder seine Einwilligung, so dürfen ihr oder ihm keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen.

(3) Soweit im Rahmen von Fernmess- oder Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet werden. Dies gilt nicht, wenn ein Gesetz die anderweitige Verarbeitung dieser Daten zulässt oder wenn diese Daten zur Abwehr erheblicher Nachteile für das Gemeinwohl

oder unmittelbar drohender Gefahren für Leben, Gesundheit oder persönliche Freiheit anderer erforderlich sind. Die Daten sind zu löschen, sobald sie zur Erfüllung dieser Zwecke nicht mehr benötigt werden.

Für öffentliche Stellen im Saarland ist der Einsatz solcher Zähler folglich dann zulässig, wenn der Betroffene vorher über den Verwendungszweck sowie Art, Umfang und Zeitraum des Einsatzes unterrichtet wurde und nach der Unterrichtung schriftlich eingewilligt hat. Diese Einwilligung ist jederzeit widerruflich. Hierdurch soll die Freiwilligkeit des Einsatzes sichergestellt werden. Der Einbau und der Betrieb von intelligenten Zählern gegen den Willen des Betroffenen ist somit nicht möglich.

Schließlich ist darauf hinzuweisen, dass dem Betroffenen bei Verweigerung der Einwilligung oder im Falle des späteren Widerrufs keine Nachteile entstehen dürfen, die über die unmittelbaren Folgekosten hinausgehen. Nach Absatz 2 S. 1 besteht ein Junktimverbot, die vertragliche Leistung, den Abschluss oder die Abwicklung des Vertragsverhältnisses von der Einwilligung des Betroffenen zur Einrichtung der Dienste abhängig zu machen. Damit soll die Entscheidungsfreiheit des Betroffenen soweit wie möglich gewahrt bleiben. Als unmittelbare Folgekosten im Sinne der Vorschrift zählen dabei nur solche Kosten, die dadurch veranlasst werden, dass beispielsweise im Falle des Widerrufs ein Mitarbeiter vom Außendienst des Versorgers vorbeikommen muss, um den intelligenten Zähler gegen einen analogen Zähler auszutauschen oder um die Sendefunktion zu deaktivieren.

Nicht zu den unmittelbaren Folgekosten im vorgenannten Sinne zählen hingegen die Kosten, die dadurch entstehen, dass der Zähler nun jährlich manuell abgelesen werden muss. Es ist also nicht zulässig, den Kunden mit der Ankündigung zur Erteilung der Einwilligung zu bewegen, dass im Falle der Verweigerung jedes Jahr zusätzliche Kosten auf ihn zukämen. Eine unter diesen Umständen erteile Einwilligung wäre nach hiesiger Auffassung unwirksam, weil sie gerade nicht freiwillig erfolgt.

Auf Seiten der Versorgungsunternehmen ist zudem zu berücksichtigen, dass durch die Umstellung auf funkbasierte Auslesung und den damit verfolgten unterschiedlichen Zwecken auch unterschiedliche Speicher- bzw. Löschfristen systemseitig umgesetzt werden müssen. Während die zum Zwecke der Jahresabrechnung erfassten Verbrauchsstände gespeichert werden dürfen, solange dies zur Abrechnung und aus haushaltsrechtlichen Gründen erforderlich ist, gelten für die unterjährig erfolgenden Erfassungen der Verbrauchsstände zum Zwecke des Netzmanagements und zur Verbesserung der Trinkwasserhygiene erheblich kürzere Aufbewahrungsfristen.

8.5 Online-Fundsachensuche

Im Rahmen einer Eingabe wurden wir darauf aufmerksam gemacht, dass die für jedermann recherchierbare Online-Fundsachensuche einer Kommune zu bestimmten Fundsachen zusätzlich personenbezogene Daten wie Name und Vorname sowie Ausweisnummer anzeige.

Eine Recherche auf der uns angegebenen Internetseite zeigte auf, dass für Fundsachen wie Ausweise, Dokumente oder Plastikkarten zwar die Suchanfrage durch Eingabe eines Geburtsdatums eingegrenzt werden konnte, eine Eingabe desselben aber

nicht zwingend erforderlich war. Wurde das Feld Geburtsdatum nicht befüllt, so wurden sämtliche im vergangenen Monat aufgefundenen Dokumente wie Ausweiskarte, Studierendenausweise, Krankenkassenkarten, Personalausweis u.a. mit Name und Vorname des Ausweisinhabers sowie - soweit vorhanden - der Ausweisnummer angezeigt.

Mangels einer entsprechenden Rechtsgrundlage für die Veröffentlichung der personenbezogenen Daten haben wir mit der in Rede stehenden Kommune umgehend Kontakt aufgenommen und diese aufgefordert, die Möglichkeit zur uneingeschränkten Suche, die zur Auflistung einer Vielzahl von personenbezogenen Daten in der Ergebnisliste führte, unverzüglich zu unterbinden. Die verantwortliche Kommune hat noch am gleichen Tag die Fundsachen Onlinerecherche vorläufig abgeschaltet.

Nunmehr werden im Suchbereich „Ausweise, Dokumente oder Plastikkarten" personenbezogene Daten wie Name, Vorname und Ausweisnummer nicht mehr ausgewiesen.

8.6 Erteilung einer falschen Meldeauskunft an einen Gläubiger

Ein Petent hatte sich an unsere Dienststelle gewandt und vorgetragen, dass einem Studierendenwerk durch eine saarländische Meldebehörde seine aktuelle Wohnanschrift sowie eine angeblich vorherige Wohnanschrift mitgeteilt worden sei. Weiterhin trug der Petent vor, weder unter der durch die Meldebehörde bescheinigten vorherigen Wohnadresse noch überhaupt in der betreffenden Gemeinde jemals gewohnt zu haben. Das Studierendenwerk hatte im Rahmen einer Bürgschaft gegen die unter der vorherigen Wohnanschrift gemeldete Person eine Forderung offen, welche sie nun bei dem Petenten beitreiben wollte.

Um den Vortrag des Petenten aufzuklären, haben wir daher die Meldebehörde gebeten, zu der seitens des Petenten vorgetragenen Fehlauskunft Stellung zu nehmen. Hierbei stellte sich heraus, dass dem vom Petenten vorgetragenen Sachverhalt offensichtlich eine Personenverwechselung wegen Namensgleichheit zu Grunde lag.

Die Meldebehörde legte in ihrer Stellungnahme dar, dass aufgrund des Auskunftsersuchens des Studierendenwerks die Sachbearbeitung des Meldeamtes eine Abfrage im Einwohnermeldeamtsprogramm der Gemeinde gestartet hatte. Die Suchabfrage erfolgte jedoch lediglich unter der Verwendung von Vorname und Familienname und war darüber hinaus nicht weiter eingegrenzt worden. In den dann angezeigten Suchergebnissen waren offensichtlich mehrere Personendatensätze angezeigt worden. Hierbei wurde leider übersehen, dass es sich um Datensätze zwar gleichnamiger aber verschiedener Personen handelte. Hierzu ist anzumerken, dass es nicht unüblich ist, dass zu ein und derselben Person mehrere Personendatensätze existieren können (z.B. bei mehreren Wohnanschriften). Die Meldebehörde räumte ein, dass in der Folge daher dem Studierendenwerk eine falsche Auskunft erteilt wurde.

Die Datensätze zur Person des Petenten wurden im Nachgang durch die Meldebehörde geprüft und waren im System korrekt gespeichert. Eine Vermischung mit Daten einer anderen Person bestand nicht. Die unrichtige Auskunftserteilung erfolgte mithin nicht systembedingt.

Auf unsere Anregung hin wurde mit der betroffenen Sachbearbeiterin der konkrete Sachverhalt nochmals erörtert und auf eine Sensibilisierung datenschutzrechtlicher Belange hingewirkt.

Außerdem teilte die Gemeinde mit, dass sie sich bei dem Petenten für das Versehen und die ihm hierdurch entstandenen Unannehmlichkeiten schriftlich entschuldigen werde.

9 Soziales

9.1 Fördermaßnahmen beim Übergang von Schule in den Beruf

Bundesweit wurden im Berichtszeitraum sogenannte Jugendberufsagenturen eingerichtet, die Jugendliche auf ihrem Weg von der Schule in den Beruf unterstützen sollen.

9.1.1 Jugendberufsagenturen

Für die Beratung und Integration junger Menschen in der Übergangsphase von der Schule in eine Ausbildung sind nach den Regelungen des Sozialgesetzbuches (SGB) die Agenturen für Arbeit (SGB III), die Jobcenter (SGB II) sowie die Träger der Jugendhilfe (SGB VIII) zuständig. Um eine umfassende Betreuung und Beratung von Jugendlichen zu erreichen, die nach Schulabgang noch keine Ausbildungsstelle gefunden haben und Unterstützung bei der Vermittlung in eine Ausbildung benötigen, arbeiten diese Träger in den Jugendberufsagenturen zusammen und tauschen im Rahmen von Fallkonferenzen personenbezogene Daten über Jugendliche aus.

Die bei den Trägern vorhandenen Daten sind Sozialdaten, da es sich um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten natürlichen Person (des Schulabgängers) handelt, die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach dem SGB erhoben, verarbeitet oder genutzt werden (§ 67 Abs. 1 SGB X). Für einen Datenaustausch zwischen diesen verschiedenen Sozialleistungsträgern kann § 69 Abs. 1 Nr. 1 SGB X eine rechtliche Grundlage bieten, wenn die Übermittlung für die Erfüllung einer gesetzlichen Aufgabe nach dem SGB unabdingbar und für einen aktuell und konkret feststehenden Zweck erforderlich ist. Eine spezialgesetzliche Regelung zur Datenübermittlung zwischen den Trägern der Grundsicherung für Arbeitssuchende und der Bundesagentur für Arbeit ist in § 50 Abs. 1 SGB II enthalten. Liegen die Voraussetzungen dieser Vorschriften nicht vor, kann eine Datenübermittlung zwischen diesen Leistungsträgern nur auf Grundlage einer vorherigen schriftlichen Einwilligungserklärung erfolgen.

Grundsätzlich muss die Person, deren Sozialdaten verarbeitet und genutzt werden sollen, diese Einwilligung in die Datenübermittlung höchstpersönlich erteilen. Die Volljährigkeit des Jugendlichen ist für die Wirksamkeit einer Einwilligung dabei nicht erforderlich, denn Kinder haben grundsätzlich wie Erwachsene das Recht, über die Preisgabe oder Verarbeitung ihrer personenbezogenen Daten selbst zu entscheiden. Das Datenschutzrecht kennt daher keine verbindlichen Altersgrenzen für die Wirksamkeit solcher Einwilligungserklärungen. Entscheidend ist allein die Einsichtsfähigkeit der Minderjährigen. Maßgeblich ist daher nur, ob die Betroffenen in der Lage sind, die Konsequenzen der Verwendung ihrer Daten zu überblicken. Diese Einsichtsfähigkeit liegt vor, wenn der Minderjährige nach seinem individuellen Reifegrad in der Lage ist, die Bedeutung und Tragweite der ebenfalls individuell zu betrachtenden

Datenverarbeitung zu beurteilen. Dies gilt auch für die Erteilung von Einwilligungen für das Tätigwerden der Jugendberufsagenturen. Fehlt es indes an der Einwilligungsfähigkeit des Jugendlichen, ist eine Einwilligung des gesetzlichen Vertreters in die Datenübermittlung einzuholen.

9.1.2 Kooperation von Schulen mit der Jugendberufsagentur

Auch im Saarland gibt es solche Kooperationen von Sozialleistungsträgern in Jugendberufsagenturen. Ein Landkreis wandte sich mit der Bitte um datenschutzrechtliche Beratung an unsere Dienststelle, da im Rahmen eines Modellversuchs eine Zusammenarbeit zwischen einer Jugendberufsagentur und den Schulen des Landkreises beabsichtigt war. Ziel des Projekts ist, dass kein Schüler die Schule ohne Abschluss, ohne weiteren Schulbesuch oder ohne Ausbildungs- oder Arbeitsstelle verlassen soll. Um dieses Ziel zu erreichen, sollte schon in den Vorabgangsklassen mit der Unterstützung im Hinblick auf einen erfolgreichen Schulabschluss und Übergang in den späteren Arbeitsmarkt begonnen werden, indem an der Schule sogenannte Förderkonferenzen mit Lehrern und Vertretern der Jugendberufsagenturen durchgeführt werden. Die Teilnehmer sollen sich im Rahmen individueller Unterstützungs- und Förderkonferenzen bezüglich einzelner Schüler austauschen können, um den betroffenen Schülern schon frühestmöglich Unterstützungsangebote machen und auf einen erfolgreichen Übergang von der Schule in den Beruf hinwirken zu können. Damit dies gelingt, ist jedoch eine Datenübermittlung von der Schule an die Vertreter der Jugendberufsagentur erforderlich. Bei den zu übermittelnden Daten handelt es sich neben den Personalien der betroffenen Schüler u.a. auch um die schulischen Leistungen des letzten Schulhalbjahres und um Angaben zum voraussichtlichen Schulabschluss. Ergibt sich in der Förderkonferenz ein Unterstützungsbedarf, soll von den Vertretern der Jugendberufsagentur aktiv auf die jeweiligen Schüler zugegangen und ihnen Beratung und speziell auf sie zugeschnittene Fördermaßnahmen angeboten werden.

Darüber hinaus war vorgesehen, diejenigen Schüler, die nach Schulabgang keine Anschlusstätigkeit oder -ausbildung beginnen, durch einen automatisierten Abgleich mit den Daten neu aufgenommener Schüler an weiterführenden Schulen und Einrichtungen zu identifizieren, damit diesen Jugendlichen eine weitere Beratung angeboten werden kann.

Bezüglich des in diesem Projekt beabsichtigten Datenaustauschs war zunächst festzustellen, dass keine gesetzliche Grundlage für eine Datenübermittlung zwischen der Schule und der Jugendberufsagentur existierte. Da Schulen keine Leistungsträger i.S.d. § 35 SGB I oder ihnen gleichgestellte Stellen nach § 69 Abs. 2 SGB X sind, kann ein Datenaustausch zwischen den Schulen und der Jugendberufsagentur nicht auf der Grundlage sozialrechtlicher Vorschriften erfolgen. Auch § 20b Abs. 2 Gesetz zur Ordnung des Schulwesens im Saarland (Schulordnungsgesetz - SchoG) i.V.m. der auf der Grundlage des § 20b Abs. 5 SchoG erlassenen Rechtsverordnung enthält keine gesetzliche Grundlage für eine Datenübermittlung von Schulen an die genannten Sozialleistungsträger.

Um das Vorhaben datenschutzkonform umsetzen zu können, musste also auf die Einwilligungslösung zurückgegriffen werden. § 20b Abs. 2 S. 1 SchoG in der bisher geltenden Fassung sah vor, dass eine Datenübermittlung von der Schule an andere öffentliche Stellen nur mit Einwilligung der Erziehungsberechtigten oder der volljährigen Schüler zulässig ist.

Die beteiligten Institutionen sahen diese Einwilligungsregelung als ein Hindernis an, da sie befürchteten, dass manche an dem Projekt interessierten minderjährigen Schüler wegen fehlender Einwilligungserklärungen ihrer Eltern nicht in den Genuss von Fördermaßnahmen kommen könnten. Derartige Fälle kämen häufig vor, wenn Eltern kein Interesse am beruflichen Werdegang ihrer Kinder zeigten oder die Unterzeichnung der Einwilligung schlicht vergessen würden.

Insbesondere mit Blick auf die erfolgreiche Durchführung derartiger Projekte war auch der Gesetzgeber der Auffassung, dass die Zulässigkeit einer Übermittlung von Schülerdaten durch die Schulen nicht generell von der Einwilligung der Erziehungsberechtigten abhängig gemacht werden sollte, da aus dem Recht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts folge, dass auch Minderjährige über die eigenen Daten verfügen könnten.

Daher wurde seitens der Regierungsfraktionen ein Gesetzentwurf in den Landtag eingebracht, der u.a. eine Änderung des § 20b SchoG dahingehend vorsah, dass für Datenübermittlungen die Einwilligung der betroffenen Schüler maßgeblich ist und die Erziehungsberechtigten über die Einholung der Einwilligung zu informieren sind. In dem Gesetzentwurf war ausgeführt, dass grundsätzlich anzunehmen sei, dass minderjährige Schüler in einem gewissen Alter die im schulischen Umfeld notwendige Einsichtsfähigkeit besitzen. Damit die Erziehungsberechtigten jedoch gegebenenfalls darlegen können, dass ihrem Kind im Einzelfall die Tragweite seiner Erklärung nicht bewusst ist, sei es notwendig, diese über die Einholung der Einwilligung zu informieren und sie darauf hinzuweisen, welche personenbezogenen Daten von der Einwilligung erfasst werden und welchem Zweck die Datenverarbeitung dient.

Unserer Dienststelle wurde im Rahmen des parlamentarischen Gesetzgebungsverfahrens Gelegenheit zur Stellungnahme gegeben. Grundsätzliche Bedenken gegen die Änderung haben wir nicht erhoben, da es im Sinne des Rechts auf informationelle Selbstbestimmung ist, hinsichtlich der Wirksamkeit einer Einwilligung maßgeblich auf die Einsichtsfähigkeit des Erklärenden abzustellen.

Wir haben aber darauf hingewiesen, dass bei Aufhebung der Altersgrenze für die Wirksamkeit von Einwilligungen im schulischen Bereich nunmehr die Lehrkräfte in jedem Einzelfall prüfen müssten, ob die erforderliche Einsichtsfähigkeit des Minderjährigen tatsächlich vorliege. Keinesfalls dürfe – wie aus einer Formulierung in der Gesetzesbegründung gefolgert werden könne – allgemein davon ausgegangen werden, dass Schülerinnen und Schüler in einem gewissen Alter die im schulischen Umfeld notwendige Einsichtsfähigkeit besitzen, zumal ein solches Alter nicht näher konkretisiert wurde. Da jedenfalls bei jüngeren Schülerinnen und Schülern von einer solchen Einsichtsfähigkeit nicht ausgegangen werden kann, wurde empfohlen, im Gesetz ein Mindestalter für die Möglichkeit der Erteilung von Einwilligungen aufzunehmen. Zudem haben wir empfohlen, im Gesetz zur Verdeutlichung ausdrücklich klar-

zustellen, dass selbst bei Erreichen dieses Mindestalters vor Einholung der Einwilligung die notwendige Einzelfallabwägung bezüglich der Einsichtsfähigkeit des Minderjährigen durch die Lehrkräfte vorzunehmen ist.

Der letztlich in unveränderter Fassung verabschiedete Gesetzentwurf ist am 19. Februar 2016 in Kraft getreten und kann mithin nunmehr als Grundlage für die Erteilung von Einwilligungen in Datenübermittlungen in dem oben geschilderten Projekt herangezogen werden. Er enthält insoweit kein Mindestalter und stellt auf die Einsichtsfähigkeit der Schüler bei Einwilligungen ab. Der Text der zu verwendenden Einwilligungserklärungen wurde seitens der Projektteilnehmer ebenfalls mit dem Unabhängigen Datenschutzzentrum abgestimmt.

Hinsichtlich des in dem Projekt weiter geplanten Verfahrens zum Datenabgleich wurden von unserer Seite zunächst erhebliche datenschutzrechtliche Bedenken erhoben, da keine rechtliche Grundlage für einen derartigen Abgleich mit den Daten sämtlicher an allen Schulen des Landes für das Folgeschuljahr angemeldeten Schüler existierte. Seitens des Ministeriums für Bildung und Kultur wurde jedoch ein technisches Verfahren entwickelt, das gewährleistet, dass nur die personenbezogenen Daten der Projektteilnehmer an die Projektstelle zurückgemeldet werden und die Daten aller anderen Schüler anonym bleiben.

Damit konnte dieser Modellversuch datenschutzkonform durchgeführt werden.

9.2 Unerlaubte Datenflüsse bei einem Gesundheitsamt

Immer wieder werden Datenübermittlungen von Gesundheitsämtern an Jobcenter bei unserer Dienststelle angezeigt. Die Betroffenen fühlen sich dadurch regelmäßig in ihrem Recht auf informationelle Selbstbestimmung verletzt und verlangen eine rechtliche Einschätzung bzw. ein Tätigwerden durch die Aufsichtsbehörde.

So teilte unter anderem ein Petent mit, dass durch ein saarländisches Gesundheitsamt ein Gutachten über seine Person angefertigt worden sei. In dem Gutachten wurde eine spezifische Krankheit diagnostiziert und auch explizit dort aufgeführt. Diese Informationen wurden durch den amtsärztlichen Dienst des Gesundheitsamts an das für den Betroffenen zuständige Jobcenter weitergeleitet. Nur durch einen Zufall erfuhr der Petent von dieser Datenübermittlung, da die Sachbearbeiterin des Jobcenters im Rahmen einer persönlichen Vorsprache bereits Kenntnis über die konkrete Beeinträchtigung des Betroffenen hatte.

Der Petent vermutete hier einen datenschutzrechtlichen Verstoß und bat unsere Dienststelle um entsprechendes Tätigwerden.

Das betroffene Gesundheitsamt wurde zu dem Sachverhalt zur Stellungnahme aufgefordert. Dieses teilte mit, dass die Gutachten, die vom Jobcenter in solchen Fällen angefordert werden, den zuständigen Sachbearbeitern als Grundlage für die Auswahl eines leidensgerechten Arbeitsplatzes für die Betroffenen übermittelt würden. Um es den Sachbearbeitern überhaupt zu ermöglichen, einen dem Gesundheitszustand des Betroffenen entsprechenden Arbeitsplatz zu finden, wäre die Übermittlung der vermittlungs- und beratungsrelevanten Gesundheitsstörungen unerlässlich. Aus Sicht

des Gesundheitsamtes sei vorliegend keine exakte Diagnose übermittelt worden, sondern lediglich eine Umschreibung der Erkrankung, was zur Aufgabenerfüllung des Jobcenters erforderlich gewesen sei.

Auch unsere Dienststelle sieht diese Vorgehensweise des Gesundheitsamtes als datenschutzkonform an, da die vermittlungs- und beratungsrelevanten Gesundheitsstörungen an das Jobcenter übermittelt werden und diese Informationen für die Aufgabenerfüllung des Jobcenters zwingend erforderlich sind. Jedoch bedingt durch den Umstand, dass die im Gutachten beschriebene Krankheit auch als Diagnose nach der ICD-10-Klassifikation genannt wurde, war davon auszugehen, dass keine Umschreibung, sondern eine exakte Diagnose übermittelt wurde. Das Gesundheitsamt wurde infolgedessen aufgefordert, künftig darauf zu achten, dass die Nennung von Diagnosen in den Gutachten vermieden wird.

9.3 Kopie eines Personalausweises bei Beantragung der Grundsicherung

Ein Petent beantragte bei dem zuständigen Amt für soziale Sicherung Leistungen zur Grundsicherung. Hierfür sollte er eine Reihe von Unterlagen vorlegen. Dabei wurde unter anderem verlangt, dass eine Kopie des amtlichen Personalausweises eingereicht werden sollte. Zweck der Anforderung einer Kopie des Personalausweises war es insbesondere, bei künftigen Vorsprachen die Identität des Vorsprechenden mit dem Hilfesuchenden anhand des Lichtbilds abgleichen zu können. Hierfür wurde die Kopie des Personalausweises in der Akte des Amtes hinterlegt.

Nach § 60 Abs. 1 S. 1 Nr. 1 und 3 Erstes Buch Sozialgesetzbuch (SGB I) hat derjenige, der Sozialleistungen beantragt, alle Tatsachen anzugeben, die für die Leistung erheblich sind, Beweismittel zu bezeichnen und auf Verlangen vorzulegen oder ihrer Vorlage zuzustimmen.

Zur Überprüfung der Identität ist es allerdings nicht notwendig, dass der Personalausweis als Kopie in der Akte des Hilfesuchenden hinterlegt wird. Dies gilt insbesondere auch für die Speicherung der Kopie in der elektronischen Akte. Es ist ausreichend, wenn in der Akte vermerkt wird, dass der Personalausweis vorgelegen hat, denn nur die zur Identifikation erforderlichen Daten dürfen erhoben werden.

Auch für den Fall, dass überprüft werden soll, ob der Vorsprechende mit dem Hilfesuchenden identisch ist, kann seitens des Amtes von dem Vorsprechenden verlangt werden, dass dieser sich durch die Vorlage des Personalausweises legitimiert. So kann auch die Übereinstimmung des Hilfesuchenden mit dem Vorsprechenden überprüft werden, wenn etwa der Sachbearbeiter vertreten wird oder Zweifel an der Personengleichheit bestehen.

Dies teilten wir dem zuständigen Amt für soziale Sicherung mit, woraufhin die Praxis entsprechend umgestellt wurde und keine Kopien von Personalausweisdokumenten mehr verlangt wurden.

9.4 Grundsicherung – Mietbescheinigung überflüssig

Grundsicherung und Sozialhilfe werden als Sozialleistungen nach den Vorschriften des Sozialgesetzbuches gewährt. Zuständig für die Gewährung entsprechender Leistungen sind die Sozialämter der Landkreise.

Im Berichtszeitraum meldete sich eine Petentin bei der Aufsichtsbehörde und gab an, dass sie von dem zuständigen Grundsicherungsträger aufgefordert worden sei, eine von ihrem Vermieter unterschriebene Mietbescheinigung vorzulegen. Sie teilte mit, dass es ihr unangenehm sei, ihrem Vermieter offenbaren zu müssen, dass sie Grundsicherungsleistungen beziehe. Da sie bereits den Mietvertrag und die Nebenkostenabrechnungen vorgelegt hatte, bestand aus ihrer Sicht keine Veranlassung, über diese Unterlagen hinausgehende Informationen vorzulegen.

Der Petentin wurde von unserer Dienststelle mitgeteilt, dass die Vorlage einer Mietbescheinigung in ihrem Falle gerade nicht erforderlich ist, da sich die für die Bemessung der Grundsicherung relevanten Informationen, nämlich Mietzins und Nebenkosten, bereits aus den vorgelegten Unterlagen ergaben. In der Mietbescheinigung sind außerdem keine weiteren Angaben enthalten, die für die Bearbeitung des Grundsicherungsantrages erforderlich sind. Insoweit war das Vorgehen des Landkreises als datenschutzrechtlich unzulässig zu werten.

Dem Grunde nach besteht auch keine Erforderlichkeit, eine Kopie des Mietvertrages zur Akte zu nehmen. Vielmehr ist es zur Aufgabenerfüllung des Grundsicherungsträgers bereits ausreichend, wenn durch die Vorlage der Unterlagen die Höhe der monatlichen Miete und der Nebenkosten nachgewiesen und durch den zuständigen Sachbearbeiter ein Vermerk hierüber gefertigt wird.

Die Petentin setzte sich auf eigenen Wunsch, gestützt auf die Ausführungen der Dienststelle, mit der behördlichen Datenschutzbeauftragten des Landkreises in Verbindung und konnte nach kurzer Zeit erreichen, dass der Landkreis von der Vorlage der Mietbescheinigung absah. Dadurch war nunmehr auch gewährleistet, dass der Vermieter nicht erfuhr, dass die Petentin Empfängerin von Sozialleistungen ist.

9.5 Information der Kindesmutter über Verurteilung des Kindesvaters wegen Besitz kinderpornografischer Dateien

Im Berichtszeitraum wurde das Unabhängige Datenschutzzentrum um rechtliche Bewertung gebeten, inwiefern ein Jugendamt im Rahmen einer Gefährdungseinschätzung nach § 8a Achtes Buch Sozialgesetzbuch (SGB VIII) die Kindesmutter über eine Verurteilung des Kindesvaters wegen des Besitzes kinderpornografischer Dateien informieren darf.

§ 8a Abs. 1 S. 1 SGB VIII

Werden dem Jugendamt gewichtige Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder Jugendlichen bekannt, so hat es das Gefährdungsrisiko im Zusammenwirken mehrerer Fachkräfte einzuschätzen. Soweit der wirksame Schutz dieses

Kindes oder dieses Jugendlichen nicht in Frage gestellt wird, hat das Jugendamt die Erziehungsberechtigten sowie das Kind oder den Jugendlichen in die Gefährdungseinschätzung einzubeziehen und, sofern dies nach fachlicher Einschätzung erforderlich ist, sich dabei einen unmittelbaren Eindruck von dem Kind und von seiner persönlichen Umgebung zu verschaffen. Hält das Jugendamt zur Abwendung der Gefährdung die Gewährung von Hilfen für geeignet und notwendig, so hat es diese den Erziehungsberechtigten anzubieten.

Das Jugendamt wurde gemäß der Anordnung über Mitteilungen in Strafsachen (MiStra) darüber informiert, dass der Familienvater wegen des Besitzes kinderpornografischer Dateien rechtskräftig verurteilt worden war. Der Kindesvater lebte in einer Hausgemeinschaft mit der Kindesmutter und dem gemeinsamen minderjährigen Sohn. Im Rahmen der Gefährdungseinschätzung wurde sowohl der Betroffene selbst als auch die Kindesmutter angeschrieben und beide wurden zu einem persönlichen Gespräch in das Jugendamt gebeten. In diesem Gespräch mit dem Kindesvater stellte sich heraus, dass die Kindesmutter keine Kenntnis von der Verurteilung ihres Ehemannes hatte und auch die Post des Jugendamtes durch den Ehemann abgefangen wurde. Gleichzeitig hatte der Kindesvater dem zuständigen Jugendamtsmitarbeiter untersagt, mit der Kindesmutter Kontakt aufzunehmen und diese über die Verurteilung in Kenntnis zu setzen. Insoweit stellte sich bei dem Jugendamt die Frage, ob es dennoch die Kindesmutter über die Verurteilung informieren dürfe.

Nach Nr. 35 MiStra erfolgt eine Mitteilung in Strafverfahren nur dann, wenn die übermittelnde Stelle davon ausgeht, dass eine erhebliche Gefährdung von Minderjährigen vorliegt und für das Jugendamt eine Kenntnis dieser Tatsachen zur Abwehr dieser Gefahr erforderlich ist. Aus Sicht der Staatsanwaltschaft als übermittelnde Stelle lagen in diesem Fall solche Tatsachen vor, so dass das zuständige Jugendamt über die Verurteilung informiert wurde. Das Jugendamt musste wiederum nach Kenntnis dieser Tatsachen nach § 8a Abs. 1 S. 1 SGB VIII eine Gefährdungseinschätzung vornehmen. Die Mitteilung des konkreten Sachverhalts, in diesem Fall die Verurteilung des Kindesvaters, durch das Jugendamt an die Kindesmutter konnte sich jedoch nicht allein auf § 8a SGB VIII stützen, da diese Norm nicht die Weitergabe personenbezogener Daten, hier die Verurteilung des Kindesvaters, rechtfertigen konnte. Die Datenweitergabe konnte sich vorliegend auch nicht aus einer Einwilligung des Betroffenen ergeben, da der Kindesvater einer Datenweitergabe an die Kindesmutter ausdrücklich widersprochen hatte. Folglich konnte eine solche Datenübermittlung lediglich aufgrund einer anderen gesetzlichen Erlaubnisnorm erfolgen.

Eine Offenbarungsbefugnis des Jugendamtes konnte sich im vorliegenden Fall aus § 65 Abs. 1 Nr. 5 Achtes Buch Sozialgesetzbuch (SGB VIII) in Verbindung mit § 34 Strafgesetzbuch (StGB) ergeben.

§ 65 Abs. 1 Nr. 5 SGB VIII

Sozialdaten, die dem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind, dürfen von diesem nur weitergegeben werden …

unter den Voraussetzungen, unter denen eine der in § 203 Absatz 1 oder 3 des Strafgesetzbuchs genannten Personen dazu befugt wäre.

§ 34 StGB

Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden.

Ein Fall des rechtfertigenden Notstands nach § 34 StGB liegt vor, wenn eine konkrete Gefahr einer wesentlichen Beeinträchtigung des Kindeswohls gegenwärtig ist. Das ist anzunehmen, wenn die natürliche Weiterentwicklung der Sachlage jederzeit in einen Schaden für das Kind umschlagen kann. Des Weiteren muss die Datenweitergabe eine geeignete Maßnahme sein und es darf kein milderes Mittel geben. Somit musste das Jugendamt beurteilen, ob es die Einbeziehung der Kindesmutter unter Mitteilung des konkreten Sachverhalts als geeignete Maßnahme und mildestes Mittel ansieht. Alternativ könnte das Jugendamt zur Gefährdungseinschätzung auch das Familiengericht nach § 8a Abs. 2 S. 1 2. Alt. SGB VIII einschalten, wobei dann die Datenweitergabe nach § 65 Abs. 1 Nr. 2 oder Nr. 5 SGB VIII möglich wäre. Diese Einschätzung wurde dem Jugendamt mitgeteilt.

10 Gesundheit

10.1 Videoüberwachung im Maßregelvollzug

Im Berichtszeitraum wandte sich die Personalvertretung der Saarländischen Klinik für Forensische Psychiatrie, der Maßregelvollzugseinrichtung des Saarlandes, mit der Bitte um Prüfung und Beratung in Bezug auf die in der Klinik installierte Videoüberwachung an unsere Dienststelle. Die Personalvertretung wies darauf hin, dass die Klinik derzeit mit neuer Videotechnik ausgestattet werde, eine Unterrichtung bislang jedoch weder über die konkrete technische Ausgestaltung noch über den Umfang der Videoüberwachung erfolgt sei.

Zur Vorbereitung einer datenschutzrechtlichen Bewertung der Videoüberwachungsmaßnahmen haben wir uns gemeinsam mit der Klinikleitung, der Personalvertretung sowie Vertretern des Ministeriums der Justiz, als Träger der Klinik, im Rahmen eines Vor-Ort-Termins einen Überblick über die Maßnahme verschafft. Neben der Bewertung der aktuellen Situation sollte dieser Termin auch dazu dienen, eine datenschutzkonform ausgestaltete Videoüberwachung in den neu zu errichtenden Gebäudeteilen vorzubereiten.

Die Situation vor Ort stellte sich dergestalt dar, dass die Außenumzäunung der Klinik vollständig videoüberwacht wurde. Darüber hinaus erfolgte eine Überwachung des zum Freigang genutzten Hofbereichs, der Stationsflure sowie innerhalb der besonders gesicherten Station auch der Besucherbereiche und einiger Patientenzimmer. Als Grund für die Maßnahmen wurden mit Blick auf die teilweise hohe Gefährlichkeit der Patienten die Gewährleistung der Sicherheit in der Einrichtung sowie die Sicherung der Patienten angegeben. Außerdem sollten Fluchtversuche und ein unbefugtes Eindringen von außen unterbunden werden. Von der Überwachung betroffen waren neben den Patienten auch die Beschäftigten der Klinik sowie teilweise auch Besucher.

Während bislang lediglich ein Live-Monitoring ohne Aufzeichnung der Aufnahmen stattfand, sollte mithilfe der neu angeschafften Videotechnik teilweise auch eine Speicherung der Aufnahmen erfolgen.

Zum Zeitpunkt des Vor-Ort-Termins konnte weder ein Übersichtsplan, aus dem sich die genaue Anbringung und Ausrichtung der Kameras ergab, noch eine Verfahrensbeschreibung mit der Festlegung von Löschfristen sowie Regelungen über Zugriffsbefugnisse auf gespeicherte Daten vorgelegt werden. Ebenso wenig gab es im Innenbereich der Klinik Hinweisschilder betreffend die Videoüberwachung.

Eine Videoüberwachung, insbesondere die damit verbundene Speicherung der Aufnahmen, stellt einen intensiven Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) dar, da die Betroffenen - gerade auch die Patienten, die sich in den überwachten Bereichen aufgrund hoheitlicher Maßnahmen zwangsweise aufhalten müssen - in

der Regel keine Möglichkeit haben, sich der Überwachung zu entziehen. Daher bedarf die Einschränkung dieses Grundrechts nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) einer gesetzlichen Regelung, die den Anlass, den Zweck und die Grenzen des Eingriffs bereichsspezifisch, präzise und normenklar festlegt (BVerfG, Beschluss vom 23. Februar 2007 – 1 BvR 2368/06).

Das aus dem Jahre 1989 stammende und letztmals im Jahre 2007 geänderte Maßregelvollzugsgesetz (MRVG) enthält allerdings keine ausdrückliche Regelung hinsichtlich des Einsatzes von Videokameras. Es ist aber geplant, das Maßregelvollzugsgesetz zeitnah zu überarbeiten und dabei auch die erforderliche bereichsspezifische Grundlage für eine Videoüberwachung zu schaffen.

Da die Klinik in nachvollziehbarer Weise dargelegt hatte, dass die Sicherheit der Einrichtung aufgrund des hierfür notwendigen erheblichen Personalbedarfs nicht allein durch Beschäftigte gewährleistet werden könne und daher ergänzende Videoüberwachungsmaßnahmen unerlässlich seien, wurde in Zusammenarbeit mit den Verantwortlichen der Einrichtung ein Konzept entwickelt, das für eine kurz zu bemessende Übergangszeit bis zu dem geplanten Erlass eines neuen Maßregelvollzugsgesetzes mit bereichsspezifischen Regelungen eine Videoüberwachung in der Klinik zulässt.

Hierbei war insbesondere zu berücksichtigen, dass die in ihrer privaten Lebensgestaltung ohnehin stark eingeschränkten, untergebrachten Personen durch die Videoüberwachung nicht zusätzlich in unverhältnismäßiger Weise in ihrem Grundrecht auf informationelle Selbstbestimmung beeinträchtigt werden.

Dementsprechend erfolgt im Innenbereich der Klinik nunmehr nur ein sog. Kamera-Monitoring–Verfahren, d.h. eine Speicherung von Aufnahmen ist dort generell unzulässig. Grundsätzlich darf in Räumen, die dem privaten Rückzug dienen, keine Überwachung erfolgen. Allenfalls in begründeten Einzelfällen ist in Kriseninterventions-, Wohn- und Schlafräumen eine Überwachung zur Abwehr einer erheblichen Selbst- oder Fremdgefährdung oder bei einer Fixierung der untergebrachten Person nach vorheriger schriftlicher Anordnung durch eine leitende Ärztin bzw. einen leitenden Arzt zulässig. Eine Speicherung von Aufnahmen darf nur zur Sicherung des Außenbereiches und nur für einen Zeitraum von 24 Stunden erfolgen.

Darüber hinaus wurde darauf hingewirkt, dass nicht wie bisher nur im Außenbereich Hinweise auf die Videoüberwachungsmaßnahme erfolgen, sondern auch im Inneren der Klinik vor Betreten des überwachten Bereichs in geeigneter und verständlicher Form auf die Maßnahme hingewiesen wird.

Daneben sind nunmehr eindeutige technische und organisatorische Maßnahmen, insbesondere bezüglich der Zugriffsbefugnisse auf die Aufnahmen, festgelegt worden. Schließlich wurde mit der Personalvertretung eine Dienstvereinbarung geschlossen, in der u.a. eindeutig klargestellt wurde, dass die Überwachung nicht der Verhaltens- und Leistungskontrolle der Beschäftigten dienen darf, so dass auch deren Interessen Rechnung getragen wird.

Die anstehende und dringend erforderliche Novellierung des Maßregelvollzugsgesetzes, die neben der Schaffung einer spezialgesetzlichen Grundlage für die Videoüberwachung auch weitergehende datenschutzrechtliche Vorschriften enthalten muss, wird von unserer Dienststelle begleitet.

10.2 Weitergabe von Meldedaten zur Krebsvorsorge

Im Berichtszeitraum wandten sich mehrere Petenten aufgrund der vermeintlich unzulässigen Übermittlung von Adressdaten durch Meldebehörden an das Datenschutzzentrum.

Die Beschwerdeführer trugen diesbezüglich vor, dass ihnen unbekannte Stellen Terminvorschläge im Rahmen eines Mammographie-Screening-Programms kommuniziert hätten und dies ihres Erachtens als Werbemaßnahme anzusehen sei. Da den Anschreiben entnommen werden konnte, dass die kommunalen Meldebehörden die Adressdaten zur Verfügung gestellt hatten, die Beschwerdeführer jedoch gegenüber der jeweiligen Meldebehörde der Weitergabe von Daten gemäß § 50 Abs. 5 Bundesmeldegesetz (BMG) widersprochen hatten, sei von einer datenschutzrechtlichen Unzulässigkeit dieses Anschreibens auszugehen.

Absender des verfahrensgegenständlichen Anschreibens war die Zentrale Stelle des Mammographie-Screening-Programms, welche beim Ministerium für Soziales, Gesundheit, Frauen und Familie angesiedelt ist und die die Einladung der Teilnahmeberechtigten und das Monitoring der Teilnahme im Zusammenhang mit dem bundesweiten Mammographie-Screening-Programm wahrnimmt (§ 17 Abs. 4 in Verbindung mit Abs. 5 Nr. 1 Saarländisches Krebsregistergesetz (SKRG)).

Nach § 17 Abs. 5 Nr. 2 und § 18 SKRG bezieht die Zentrale Stelle die für das Einladungswesen erforderlichen personenbezogenen Daten von den jeweiligen Einwohnermeldeämtern. Damit korrespondiert § 14 Abs. 1 Saarländische Meldedatenübermittlungsverordnung, welcher den Meldebehörden die Übermittlung festgelegter Daten von teilnahmeberechtigten Frauen an die Zentrale Stelle regelmäßig zum Ersten eines Monats vorgibt. Dies sind im Einzelnen Familienname (jetziger und früherer Name), Vorname, Doktorgrad, Geburtstag und -ort sowie die aktuelle Anschrift.

Der eingelegte Widerspruch gemäß § 50 Abs.5 BMG gegen die Übermittlung von Meldedaten umfasst jedoch nicht die gesetzlich vorgegebene Datenübermittlung zum Mammographie-Screening-Programm. Das BMG sieht hier lediglich eine Widerspruchsmöglichkeit gegen die Weitergabe von Daten an u.a. Parteien, Adressbuchverlage, Presse und Rundfunk oder bei Alters- oder Ehejubiläen vor. Trotz des bei der Meldebehörde eingelegten Widerspruchs war somit die Datenübermittlung an die Zentrale Stelle gesetzlich legitimiert und datenschutzrechtlich nicht zu beanstanden.

10.3 Biografie-Fragebögen in einem Pflegeheim

Eine anonyme Eingabe richtete sich gegen den Betreiber eines Pflegeheims, da dieser neu aufgenommenen Bewohnern beziehungsweise deren Betreuern oder Angehörigen einen Biografie-Fragebogen vorlegte, ohne ausreichend auf Zweck und Verarbeitungszusammenhang hinzuweisen. Mithilfe dieses Bogens wurden sehr weitreichend biografische Daten und, im Hinblick auf Verwandtschaftsverhältnisse, teilweise auch Daten Dritter erhoben.

Laut Stellungnahme des Pflegeheimbetreibers sei die biografische Befragung erheblich für die Konzeption der individuellen Pflege und Betreuung. Es sollten wichtige Aspekte der Biografie und der Lebensgeschichte der Bewohner herausgearbeitet werden, da die Begebenheiten aus der Biografie Aufschluss auf das gegenwärtige Erleben und Verhalten der Bewohner geben könnten.

Das Ausfüllen des Bogens sei jedoch ausdrücklich nicht für die Begründung oder Ausführung des Heimvertrags erforderlich und somit freiwillig. Genutzt werde in diesem Zusammenhang ein standardisierter Bogen, welcher in der Pflegedokumentationsmappe des jeweiligen Bewohners abgelegt werde. Lediglich die verantwortlichen Pflegefachkräfte hätten Zugriff auf die Angaben. Die zugriffsberechtigten Mitarbeiter würden schließlich auf das Datengeheimnis verpflichtet.

Dem Betreiber wurde mitgeteilt, dass der Biografie-Fragebogen mit einer Einwilligungserklärung verbunden sein muss, die anhand der Vorgaben des § 4a Bundesdatenschutzgesetz (BDSG) zu konzipieren ist. Dementsprechend war über den Verarbeitungszusammenhang aufzuklären (Informiertheit) und deutlich darauf hinzuweisen, dass die Angaben freiwillig gemacht werden können und nicht zur Begründung oder Durchführung des Heimvertrages benötigt werden. Der Betreiber des Pflegeheims legte uns daraufhin ein entsprechendes Muster vor, das den datenschutzrechtlichen Vorgaben entsprach.

10.4 Datenübermittlung an krankenhausfremde Personen und Einrichtungen

Im Berichtszeitraum beschwerte sich eine Petentin bei der Aufsichtsbehörde darüber, dass sie im Rahmen einer Untersuchung in einem Krankenhaus ohne weitere Information und ohne ihre vorherige Einwilligung zu einer nicht im Krankenhaus beschäftigten Person geführt wurde. Von dieser Person wurde die Petentin untersucht und hinsichtlich ihres Krankheitsbildes beraten.

Aufgrund datenschutzrechtlicher Bedenken gegen dieses Vorgehen wurde das betroffene Krankenhaus zur Stellungnahme aufgefordert.

Dieses teilte mit, die fragliche Person sei tatsächlich Angestellte einer Fremdfirma, welche im Bereich der Medizintechnik tätig sei und das Krankenhaus diesbezüglich bereits seit einigen Jahren unterstütze. Im Kern gehe es darum, dass sie im Rahmen der Anfertigung von medizinischen Diagnosen eine fachliche Beratung für die behandelnden Ärzte anbiete. Die Entscheidung darüber, welche medizinische Maßnahme bei einem bestimmten Krankheitsbild angewendet werden solle (sog. Indikation), treffe aber weiterhin der behandelnde Arzt. Für den Fall, dass eine bestimmte Indikation als sinnvollste Maßnahme empfohlen werde, werde auf die Firma, bei der die Kooperationspartnerin angestellt ist, verwiesen.

Die Klinik gab zu verstehen, dass sie es in der Vergangenheit versäumt habe, die Patienten über den Status der Kooperationspartnerin ausführlich zu informieren und sicherte Abhilfe zu.

Aus datenschutzrechtlicher Sicht war zu kritisieren, dass Patienten ohne vorherige Information und Einwilligung an eine Person weitergeleitet wurden, die nicht Mitarbeiter des betreffenden Krankenhauses war. Davon ausgehend, dass die Daten zur weiteren Behandlung an die Fremdfirma übermittelt wurden, wurde das Krankenhaus aufgefordert, eine Einwilligungserklärung samt Informationsblatt für die Patienten zu diesem Vorgang zu erstellen, das den betroffenen Patienten vor der Übergabe an die Fremdfirma ausgehändigt wird, um die Datenübermittlung über eine informierte Einwilligung der Patienten im Sinne des § 4a Bundesdatenschutzgesetz (BDSG) legitimieren zu können. Alternativ müsste auf die Einbindung der Fremdfirma verzichtet werden.

10.5 Schülerpraktika in Arztpraxen

Die Kassenärztliche Vereinigung Saarland in ihrer Funktion als Interessenvertretung der niedergelassenen Ärzte hat das Datenschutzzentrum um datenschutzrechtliche Bewertung des folgenden Sachverhaltes gebeten:

Niedergelassene Ärztinnen und Ärzte bieten in ihren Praxen sogenannte Schülerpraktika an, damit sich Schüler zum Zwecke der späteren Berufswahl einen ersten Einblick in den beruflichen Alltag eines Arztes oder einer medizinischen Fachangestellten verschaffen können. Mit dem Einblick in den Alltag einer Arztpraxis sind für die Schüler natürlich auch Offenbarungen verbunden, die der ärztlichen Schweigepflicht aus § 203 Strafgesetzbuch (StGB) unterliegen. Es stellt sich daher die Frage, unter welchen Voraussetzungen ein solches Schülerpraktikum in einer Arztpraxis überhaupt datenschutzkonform absolviert werden kann.

Maßgebend für die Beurteilung ist die Verpflichtung der Ärzte zur Wahrung der ärztlichen Schweigepflicht. Gemäß § 203 StGB sind die dort genannten Berufsgruppen sowie ihre berufsmäßig tätigen Gehilfen und die Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind, zur Verschwiegenheit verpflichtet. Da aber Praktikanten weder berufsmäßig tätig sind, noch sich in der Vorbereitung auf den Beruf befinden, sind sie nicht als Gehilfen in diesem Sinne anzusehen. Eine Offenbarung von Patientengeheimnissen gegenüber Praktikanten stellt somit eine Verletzung der ärztlichen Schweigepflicht dar.

Eine Befugnis zur Offenbarung von Patientengeheimnissen kann sich in diesen Fällen nur dann ergeben, wenn der Arzt im Vorfeld durch die betroffenen Patienten von der ärztlichen Schweigepflicht entbunden wird.

Unabdingbare Voraussetzung ist deshalb, dass jeder Patient in die Kenntnisnahme seiner personenbezogenen Daten durch einen Schülerpraktikanten, sei es im Rahmen der Einsichtnahme in Patientenakten oder durch die Teilnahme am Arztgespräch, ausdrücklich eingewilligt hat. Eine solche Einwilligung führt zur strafrechtlichen und datenschutzrechtlichen Zulässigkeit der Einbeziehung eines Praktikanten.

Diese Entscheidung muss der Patient freiwillig treffen können, ohne dass ihm das Gefühl vermittelt wird, der Arzt erwarte das Einverständnis.

Für die Teilnahme des Praktikanten beim Arztgespräch bedeutet dies, dass der Arzt den Patienten ohne Beisein des Praktikanten befragt, ob er mit dessen Teilnahme an dem Gespräch einverstanden ist. Des Weiteren muss der Patient auch darauf hingewiesen werden, dass er auch während des laufenden Arztgespräches dieses Einverständnis jederzeit widerrufen kann. Keinesfalls reicht es aus, wenn der Arzt den Patienten - möglicherweise auch noch in Anwesenheit des Praktikanten - mit den Worten empfängt: „Heute haben wir einen Praktikanten in der Praxis. Er wird an unserem Gespräch teilnehmen."

Im Ergebnis halten wir die Durchführung von Schülerpraktika in Arztpraxen unter den genannten Voraussetzungen für zulässig.

Darüber hinaus plant der Gesetzgeber derzeit eine Novellierung der Vorschrift des § 203 StGB. Es bleibt abzuwarten, ob der Gesetzgeber für diese Problematik eine gesetzliche Regelung treffen wird.

11 Schule und Bildung

11.1 Zusammenarbeit in der AG Medienkompetenz

Die AG Medienkompetenz ist ein Zusammenschluss saarländischer Akteure im Bereich Medienkompetenz. Neben dem Unabhängigen Datenschutzzentrum Saarland sind folgende Institutionen ständig in der AG Medienkompetenz organisiert: Die Landemedienanstalt Saarland, das Ministerium für Bildung und Kultur, das Landesinstitut für Präventives Handel, das Landesinstitut für Pädagogik und Medien, der Jugendserver-Saar, das Landespolizeipräsidium und die Europäische EDV-Akademie des Rechts. Die AG tauscht sich seit 2008 landesweit über neueste Entwicklungen im Medienbereich aus und klärt Eltern, Schüler sowie Lehr- und pädagogische Fachkräfte über Chancen, Möglichkeiten und Risiken auf, die neue Medien heute für Heranwachsende bieten.

Auch in diesem Berichtszeitraum konnten die Mitglieder der AG Medienkompetenz im Saarland aufgrund der Bündelung des Fachwissens der Mitglieder interessante Veranstaltungen und Hilfen zur Steigerung der Medienkompetenz anbieten.

Unter anderem wurden Flyer entwickelt, die Lehrkräfte, Eltern und Grundschulkinder für datenschutzrechtliche Problematiken im Umgang mit sozialen Netzwerken und Internetdiensten sensibilisieren sollen. Diese Flyer sind unserem Internetangebot zu entnehmen.

Am 28. September 2015 fand der 2. Saarländische Medientag der AG Medienkompetenz im Bildungszentrum der Arbeitskammer des Saarlandes in Kirkel statt. Die Veranstaltung richtete sich vor allem an Lehrkräfte, pädagogische Fachkräfte, Sozialpädagoginnen und Sozialpädagogen sowie an Erzieherinnen und Erzieher und wurde unter das Motto „Digitale Bildung" gestellt. Schon sehr früh zeichnete sich ein großes Interesse an der Veranstaltung ab, so dass die maximale Teilnehmeranzahl schnell erreicht wurde.

Im Eröffnungsvortrag von Herrn Richard Heinen (learning lab, Universität Duisburg-Essen), ging es um die medienpädagogische Nutzung und die Rolle von Smartphones oder Tablets in Bildungseinrichtungen. Im weiteren Verlauf wurden parallel stattfindende Workshops angeboten, die praxisnahe Einblicke rund um das Themenfeld „digitale Medien im medienpädagogischen Einsatz" vermittelten. Neben Dozenten der AG Medienkompetenz konnten kompetente Referentinnen und Referenten der Universität Kaiserslautern, von medien+bildung.com und von Planet Schule des SWR gewonnen werden. Begleitet wurde die Veranstaltung durch Infostände der Mitglieder der AG Medienkompetenz, der Gesellschaft für Medienpädagogik und Kommunikationskultur e.V. (GMK) und Planet Schule (SWR).

Die Teilnehmer des 2. Saarländischen Medientages haben der Veranstaltung durchweg eine positive Resonanz bescheinigt und freuen sich auf die nächste Veranstaltung dieser Art, die turnusgemäß am 19. Oktober 2017 wieder in Kirkel, diesmal unter

der neuen Bezeichnung „3. Saarländischer Medienkompetenztag“ stattfinden wird. Das Motto wird dann lauten: „Souverän in der digitalen Welt.“

11.2 Generelle Schweigepflichtentbindung an Grundschulen

Ein besorgter Vater wandte sich an unsere Dienststelle, da die Grundschule, an der sein Kind eingeschult werden sollte, im Einschulungsverfahren eine generelle Schweigepflichtentbindungserklärung hinsichtlich aller behandelnden Ärzte und Krankheiten, die im schulischen Umfeld von Relevanz sein könnten forderte. Dies schien dem Vater zu pauschal, da er nicht wissen könne, welche Erkrankungen noch auf sein Kind zukommen werden und welche Einsichtsrechte er der Schule diesbezüglich einräumen könne.

Mit der Bitte um Stellungnahme zu diesem Sachverhalt konfrontiert rechtfertigte die Schule die eingesetzte Schweigepflichtentbindungserklärung mit der Tatsache, dass es in der Vergangenheit Schwierigkeiten gegeben hätte, mit bestimmten Institutionen in Kontakt zu treten und die Eltern sich sehr lange Zeit ließen, eine für den Einzelfall konkrete Schweigepflichtentbindungserklärung vorzulegen. Deshalb entschied man sich, im Zuge des Einschulungsverfahrens ein Blankoformular herauszugeben.

Bei einer Schweigepflichtentbindungserklärung handelt es sich datenschutzrechtlich um eine Einwilligung der Betroffenen in die Datenverarbeitung von besonders sensiblen Daten, die dem Schutz des § 203 Strafgesetzbuch (StGB) unterliegen und diesen Schutzbereich verlassen sollen. Das Datenschutzrecht stellt an eine Einwilligung spezifische Anforderungen (§ 4 SDSG):

- Der Betroffene muss über Sinn und Zweck der Datenverarbeitung informiert werden.
- Der Betroffene muss wissen, an wen seine Daten übermittelt werden können und wann die Daten gelöscht werden.
- Die Einwilligung muss freiwillig erfolgen und darf nicht aus einer Drucksituation für den Betroffenen hervorgehen.
- Die Einwilligung kann jederzeit auch in der Zukunft ohne rechtliche Nachteile widerrufen werden.

Nach einem Urteil des OLG Karlsruhe vom 01. Oktober 1998 - 12 U 314/97 - müssen folgende Gesichtspunkte für eine Schweigepflichtentbindungserklärung beachtet werden:

- Der Einwilligende muss eine im Wesentlichen zutreffende Vorstellung davon haben, worin er einwilligt.
- Er muss die Bedeutung und Tragweite seiner Entscheidung überblicken.
- Er muss wissen, aus welchem Anlass und mit welcher Zielsetzung er welche Personen von ihrer Schweigepflicht entbindet (und so in die Preisgabe seiner Daten einwilligt).
- Er muss darüber hinaus über die Art und den Umfang der Einschaltung Dritter unterrichtet werden.

Der Betroffene muss sich im Moment der Einwilligung der Tragweite seiner Entscheidung bewusst sein.

Leider wurden diese Kriterien in den von der Grundschule eingesetzten Einwilligungserklärungen nicht erfüllt. Die Eltern konnten weder erfassen, welche Ärzte zukünftig von ihrer Schweigepflicht entbunden werden sollten, noch für welche Krankheitsbilder Daten an die Schule übermittelt werden dürfen.

Es ist unstrittig, dass es für eine Schule unentbehrlich ist, bestimmte Krankheitsbilder bei Schülern zu erfahren, um entsprechende Vorsorgemaßnahmen oder Erstversorgungen durchführen zu können. Zu wissen, ob ein Kind beispielsweise an Epilepsie oder Diabetes leidet und welche Maßnahmen im Ernstfall zu treffen sind, liegt nicht nur im Interesse der Schule sondern auch im Interesse der Eltern, die in solchen Fällen proaktiv diese Informationen an die Schule weitergeben werden.

Deshalb jedoch von allen Schülern einer Schule eine pauschale Schweigepflichtentbindungserklärung zu verlangen und diese Informationen Personen anzuvertrauen, die nicht über ein medizinisches Fachwissen verfügen ist unverhältnismäßig und folglich unzulässig.

Vom Einsatz der Schweigepflichtentbindungserklärung wurde daher in dieser pauschalen Form abgeraten. Die Einholung einer Schweigepflichtentbindungserklärung darf nur im konkreten Einzelfall erfolgen, soweit diese zum Zwecke der schulischen Betreuung eines Kindes erforderlich ist.

Es wäre daher empfehlenswert, wenn das Ministerium für Bildung und Kultur diverse Muster für die Schulen zur Verfügung stellen könnte, um Rechtssicherheit in den Schulen für Sachverhalte wie diesen herzustellen. Eine Zusammenarbeit mit unserer Dienststelle wäre diesbezüglich wünschenswert.

11.3 Schulworkshops durch das Unabhängige Datenschutzzentrum Saarland

Seit dem Schuljahr 2013/2014 bietet das Unabhängige Datenschutzzentrum Saarland mit großem Erfolg an weiterführenden Schulen Schülerworkshops zum Umgang mit persönlichen Daten im Internet an. Bereits im letzten Tätigkeitsbericht haben wir unter Kapitel 15.2 ausführlich zu diesem Thema berichtet. Mittlerweile wurden im Saarland bereits über 7000 Schülerinnen und Schüler in den Workshops im Zusammenhang mit der Nutzung von Social-Media-Angeboten wie WhatsApp, Snapchat, Instagram, Facebook, Twitter oder Wikis zu mehr Selbstverantwortung und digitaler Rücksichtnahme angeleitet. Ziel der Workshops ist es, die Fähigkeiten von Kindern und Jugendlichen zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer umzugehen. Dabei geht es nicht darum, sie von Social-Media-Angeboten fernzuhalten, sondern sie für Gefahren und Risiken der digitalen Welt zu sensibilisieren.

Die Workshops für die 6. Klassenstufe umfassen vier Unterrichtsstunden und werden von externen Referentinnen und Referenten durchgeführt, die durch das Unabhängige Datenschutzzentrum geschult werden. Für die Workshops an weiterführenden Schulen liegen die Themenschwerpunkte bei:

- Bedeutung und Verlust von Privatsphäre
- Online-Ethik
- Cybermobbing
- Smartphone Nutzung
- die Welt von Google, Facebook & Co.
- Fragen des Selbst-Datenschutzes.

Kinder und Jugendliche nutzen die Möglichkeiten digitaler Medien, sei es per PC, Tablet oder Smartphone immer früher. Die digitale Medienkompetenz stellt somit nach dem Lesen, Schreiben und Rechnen die vierte Kulturtechnik dar, die zunehmend an Bedeutung gewinnt. Vor diesem Hintergrund wurde von Eltern und Lehrern angeregt, bereits in der 4. Klassenstufe der Grundschulen eine Informationsveranstaltung für Schülerinnen und Schüler zum richtigen Umgang mit digitalen Medien anzubieten. Dieser Anregung sind wir gerne gefolgt.

Die Workshops in den Grundschulen sind auf die Dauer von zwei Unterrichtsstunden angelegt. In den Grundschulworkshops werden unter anderem folgende Fragen mit den Kindern thematisiert:

- Welche Daten darf ich von mir preisgeben?
- Welche Fotos und Filme darf ich ins Netz stellen?
- Was ist beim Umgang mit meinem Smartphone und mit Apps zu beachten?

Thematische Schwerpunkte können in beiden Workshopalternativen mit den Referenten im Vorfeld abgestimmt werden.

Um einen Workshop beantragen zu können, stellen wir auf unserer Internetseite ein entsprechendes Formular zur Verfügung. Nach Eingang des Antrages stellen wir den Kontakt zu einem unserer Referenten her, mit dem organisatorische und inhaltliche Einzelheiten besprochen werden können.

Das Angebot ist für Grundschulen ebenso kostenlos wie für die weiterführenden Schulen.

12 Beschäftigtendatenschutz

12.1 Elektronische Personalakte

Bereits Ende 2014 hatte die Staatskanzlei zu einem länderübergreifenden Workshop zwecks Erfahrungsaustausch über die Einführung der elektronischen Personalakte eingeladen, da zukünftig auch im Saarland in der öffentlichen Verwaltung die bisher in Papierform geführten Personalakten in digitaler Form vorgehalten werden sollen.

Als Folge dieser Veranstaltung wurde im Mai 2015 auf Landesebene eine ressortübergreifende Arbeitsgruppe eingerichtet, die sich mit den rechtlichen, technischen und organisatorischen Fragestellungen, die sich bei der Einführung einer elektronischen Personalakte ergeben, befassen sollte. Auch das Unabhängige Datenschutzzentrum war Teil dieser Arbeitsgruppe.

Insbesondere aus rechtlicher Sicht haben der Einführung der elektronischen Personalakte in der beabsichtigten Form zunächst grundsätzliche datenschutzrechtliche Bedenken entgegengestanden.

Gemäß § 50 Beamtenstatusgesetz (BeamtStG) ist für jeden Beamten eine Personalakte zu führen. Sie hat alle Daten zu beinhalten, die mit dem Dienstverhältnis in einem unmittelbaren Zusammenhang stehen. Die Personalakte umfasst somit auch sehr sensible und damit besonders schützenswerte Daten, die beispielsweise Auskunft über die Religions- und Gewerkschaftszugehörigkeit oder auch den Gesundheitszustand geben können.

Grundsätzlich hat der Landesgesetzgeber die digitale Personalaktenführung zum Zwecke der Personalverwaltung und -bewirtschaftung als Alternative zur Papierakte durch die Einführung der Regelung des § 102 Abs.1 S. 1 Saarländisches Beamtengesetz (SBG) bereits vor Jahren legitimiert.

Datenschutzrechtlich bedenklich ist es jedoch, wenn – wie beabsichtigt - die automatisiert verarbeiteten Personalaktendaten den Bereich der zuständigen Personalverwaltung verlassen und auf einem zentralen Server beim saarländischen IT-Dienstleistungszentrum geführt werden sollen. Ebenso problematisch ist die Tatsache, dass eine Möglichkeit geschaffen werden sollte, die das Einscannen der Personalakten durch externe Drittanbieter ermöglicht. In beiden Fällen erweitert sich somit der Kreis derjenigen, die Kenntnis vom Inhalt der Personalakten erhalten können.

Das Saarländische Beamtengesetz als einschlägige Spezialnorm enthält keine Legitimationsnorm, die eine Übermittlung und Verarbeitung von Personalaktendaten in den oben geschilderten Konstellationen abdeckt.

Ein Rückgriff auf die allgemeinen Regelungen des Saarländischen Datenschutzgesetzes (SDSG) schied in diesem Zusammenhang aus, da die beamtenrechtlichen Regelungen zum Personalaktenrecht ein umfassendes und abschließendes Regelungssystem zum Umgang mit Personalakten darstellen, das den allgemeinen datenschutzrechtlichen Regelungen vorgeht.

Es blieb daher nur die Schaffung einer Rechtsgrundlage für die Erhebung und Verwendung von Personalaktendaten im Auftrag sowie weiterer ergänzender Regelungen. In Zusammenarbeit mit dem Ministerium für Inneres und Sport und der Staatskanzlei konnte der Entwurf einer entsprechenden, an § 111a Bundesbeamtengesetz (BBG) angelehnten Rechtsgrundlage in das Saarländische Beamtengesetz erarbeitet werden, der den datenschutzrechtlichen Rahmen für die Einführung der elektronischen Personalakte bildet. Es wurde zugesagt, dass der Entwurf den erforderlichen Gesetzgebungsprozess noch in der aktuellen Legislaturperiode durchlaufen soll.

Neben der hier dargestellten datenschutzrechtlichen Problematik wirft die Einführung der elektronischen Personalakte aber auch Fragen technisch-organisatorischer Art auf. Bei der praktischen Umsetzung wird insbesondere auf die Umsetzung von Maßnahmen zur Gewährleistung der Vertraulichkeit und Integrität personenbezogener Personalaktendaten geachtet werden müssen. So wurde von unserer Seite bereits angemerkt, dass es für Systemadministratoren durch technische Gestaltungsmöglichkeiten ausgeschlossen werden müsse, dass Manipulationen an der eigenen Personalakte durchgeführt werden können. Davon unabhängig wurde gefordert, dass bei der Einführung einer neuen Netzstruktur und eines neuen Rechenzentrums im Saarland eine Transportverschlüsselung gewählt werden muss, die den aktuellen technischen und organisatorischen Standards entspricht und gewährleistet, dass die Personalaktendaten vor unbefugten externen und internen Zugriffen geschützt werden.

12.2 Interkommunale Zusammenarbeit im Bereich der Personalbewirtschaftung

Die im vorhergehenden Bericht geplante Novellierung des Saarländischen Beamtengesetzes kann bei Einführung auch als legitimierende Grundlage für einen weiteren Fall dienen, den wir datenschutzrechtlich zu bewerten hatten.

Im Amtsblatt des Saarlandes wurde eine öffentlich-rechtliche Vereinbarung zwischen zwei Kommunen veröffentlicht, die im Rahmen der interkommunalen Zusammenarbeit sowohl die Durchführung der Bezüge- und Entgeltabrechnung als auch die Aufgabe der Familienkasse (Kindergeld) auf eine gemeinsame Stelle zum Gegenstand hatte. Ziel dieser Vereinbarung war es, durch die Bündelung der Aufgaben bei einer Kommune Synergieeffekte zu erzielen.

Da auch in diesem Fall Personalaktendaten von einem Dienstherrn an eine andere Behörde übertragen werden sollten, sind für die in der Kommune tätigen Beamten, wie bereits erwähnt, die Vorgaben des Saarländischen Beamtengesetzes zur Personalaktenverarbeitung einschlägig.

Da die beamtenrechtlichen Vorschriften als Spezialnorm auch gegenüber den Regelungen aus dem Gesetz zur kommunalen Gemeinschaftsarbeit (KGG) vorgehen, kann § 17 KGG, der den beteiligten Stellen die Befugnis einräumt, einzelne Aufgaben in die eigene Zuständigkeit zu übernehmen bzw. solche Aufgaben für andere Beteiligte durchzuführen, nicht als Rechtsgrundlage für die Übermittlung von Personalakten-

daten an eine andere Kommune herangezogen werden. Die Regelung im KGG beinhaltet mithin lediglich eine organisationsrechtliche Befugnis, enthält aber keine Befugnis zum Umgang mit personenbezogenen Daten.

In der Stellungnahme der Kommunen zu dieser Problematik wurde uns mitgeteilt, dass man derzeit die Datenübermittlung auf die Einwilligung der betroffenen Beamten stütze. Entsprechende Erklärungen wurden uns vorgelegt. Aufgrund dieser Einwilligungserklärungen haben wir ungeachtet der derzeit noch fehlenden hinreichenden gesetzlichen Ermächtigung im Saarländischen Beamtengesetz keine datenschutzrechtlichen Bedenken gegen die geschilderte Zusammenarbeit erhoben.

Die im Entwurf des Gesetzes zur Neuregelung und Änderung dienstrechtlicher Vorschriften enthaltenen Anpassungen legitimieren die Übermittlung der Personalaktendaten von Beamten auch in Fällen der interkommunalen Zusammenarbeit, soweit die dort normierten Voraussetzungen erfüllt werden.

Bezüglich der datenschutzrechtlichen Problematik bei der Übertragung der Kindergeldzahlung auf die andere Behörde wurde davon ausgegangen, dass die in der Vereinbarung getroffene Regelung zur Übertragung der Aufgabe der Familienkasse obsolet ist. Das Gesetz zur Beendigung der Sonderzuständigkeit der Familienkassen des öffentlichen Dienstes im Bereich des Bundes ist mittlerweile verabschiedet und die beiden beteiligten Kommunen haben bereits ihr Interesse zur Übertragung der Kindergeldbearbeitung auf die Familienkasse der Bundesagentur für Arbeit bekundet.

12.3 Einsichtsrechte einer Wirtschaftsprüfungsgesellschaft in die Personalaktendaten

Landesbetriebe sind als rechtlich unselbstständiger Teil der Landesverwaltung nach der Verwaltungsvorschrift zu § 26 Landeshaushaltsordnung (VV zur LHO) dazu verpflichtet, einen Jahresabschluss nach den Vorschriften des dritten Buches des Handelsgesetzbuch (HGB) aufzustellen.

Die so erforderliche Jahresabschlussprüfung erfolgt in diesen Fällen durch externe Wirtschaftsprüfungsgesellschaften, als Stellen außerhalb des öffentlichen Dienstes. Die Wirtschaftsprüfungsgesellschaften legen dabei jährlich Prüfungsgegenstände fest, die schwerpunktmäßig untersucht werden sollen.

In einem von uns datenschutzrechtlich zu beurteilenden Fall legte die Wirtschaftsprüfungsgesellschaft den Prüfungsschwerpunkt auf den Bereich Personalaufwand und wollte Einsicht in die Personalakten der bei einem Landesbetrieb Beschäftigten in der Zentralen Besoldungs- und Versorgungsstelle des Saarlandes (ZBS) nehmen.

Für die ZBS als eine öffentliche Stelle des Landes gelten die Vorschriften des SDSG. Eine Übermittlung von personenbezogenen Daten ist nach § 4 Abs. 1 SDSG nur dann zulässig, wenn das SDSG oder eine andere Rechtsvorschrift sie erlaubt oder die oder der Betroffene eingewilligt hat.

Sollen also dem externen Wirtschaftsprüfungsunternehmen Einsichtsrechte eingeräumt werden oder an dieses Daten übermittelt werden, darf dies nur dann erfolgen,

wenn die Datenübermittlung durch eine Rechtsnorm oder die Einwilligung der Betroffenen legitimiert ist.

Die Einwilligung der Betroffenen einzuholen kommt in einem solchen Fall schon alleine aus praktischen Gründen nicht in Betracht, da nicht gewährleistet werden kann, dass jeder Beschäftigte seine Einwilligung erteilt.

Eine Rechtsgrundlage, auf die die Übermittlung von Personalaktendaten an externe Wirtschaftsprüfungsgesellschaften gestützt werden konnte, existierte nicht. Eine diesbezügliche Umfrage unter den anderen Landesdatenschutzbeauftragten ergab, dass es auch bundesweit keine Ermächtigungsgrundlage für eine solche Datenübermittlung gibt.

Sollte die Notwendigkeit der Einsichtnahme in die Personal- und Gehaltsdaten im Rahmen einer Prüfung durch externe Wirtschaftsprüfungsgesellschaften von Seiten des Gesetzgebers bejaht werden, müsste dies mithin spezialgesetzlich und normenklar geregelt werden. Dabei wird aber zunächst zu prüfen sein, ob eine Wirtschaftsprüfungsgesellschaft nicht auch mit anonymisierten oder pseudonymisierten Personal- und Gehaltsdaten den gewünschten Prüfungserfolg erzielen kann.

Das Ergebnis dieser Überprüfung wurde den beteiligten Stellen mitgeteilt. Es wurde als Folge daraufhin auf die Einsichtnahme in die Personalakten im Rahmen der Jahresabschlussprüfung verzichtet.

12.4 Der Abwesenheitsassistent und die Einsicht in die E-Mail-Konten

Immer wieder kommt es in der saarländischen Landesverwaltung zu Unstimmigkeiten zwischen Personalräten und der jeweiligen Dienststellenleitung wegen der Nutzung von E-Mail und Internet am Arbeitsplatz. Eigentlich ist die private Nutzung eines dienstlichen E-Mail-Accounts in der saarländischen Landesverwaltung aufgrund der Regelung in der Gemeinsamen Geschäftsordnung der obersten Landesbehörden (GGO) und den Ausführungen in Anlage 2 der GGO zur Regelung der Nutzung elektronischer Kommunikationssysteme verboten. Gleichwohl ist festzustellen, dass in vielen Dienststellen auch eine private Nutzung durch die Bediensteten stattfindet. Soweit diese Praxis über einen längeren Zeitraum durch den Dienstherrn nicht sanktioniert wird, geht die Rechtsprechung in solchen Fällen von einer Duldung aus. Dies hat zur Folge, dass der Dienstherr an bestimmte rechtliche Vorgaben gebunden ist, wie zum Beispiel das Fernmeldegeheimnis, das eine Einsichtnahme in private E-Mails der Beschäftigten beschränkt. Demgegenüber steht natürlich das Interesse des Arbeitgebers, im Falle einer Abwesenheit auf die dienstlichen E-Mails, die auf dem betroffenen E-Mail-Account eingehen, zuzugreifen, um den weiteren Betrieb sicherzustellen.

Da dieses Problem in allen Bundesländern immanent ist, haben die Datenschutzbeauftragten im Januar 2016 die ursprünglich für die öffentliche Verwaltung im Jahr 2007 veröffentlichte "Orientierungshilfe der Datenschutzaufsichtsbehörden zur da-

tenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz" gemeinsam novelliert und auch um die Privatwirtschaft betreffende Regelungen erweitert. Demnach gibt es drei Fallkonstellationen, aus denen unterschiedliche rechtliche Konsequenzen erwachsen:

- Die Nutzung der Dienste ist auch für private Zwecke erlaubt.
- Die Nutzung der Dienste ist lediglich für dienstliche Zwecke erlaubt.
- Die Nutzung der Dienste ist zwar lediglich für dienstliche Zwecke erlaubt, eine private Nutzung wurde jedoch durch die Dienststellenleitung über einen längeren Zeitraum hinweg erkannt und geduldet.

Welche Möglichkeiten ein Dienstherr zur Einsicht in die E-Mail-Konten hat, hängt entscheidend von der jeweiligen Fallkonstellation ab. Auch für den Fall einer länger andauernden Krankheit oder des unerwarteten Ablebens eines Beschäftigten bietet die Orientierungshilfe datenschutzrechtliche Lösungsansätze, die in der Praxis einen Rechtstreit verhindern können. Die rechtlichen Konsequenzen und die entsprechenden Lösungsmöglichkeiten können der in Auszügen im Anhang befindlichen Orientierungshilfe entnommen werden. Die vollständige Orientierungshilfe, die darüber hinaus auch eine Musterbetriebsvereinbarung zur privaten Nutzung von E-Mail und Internetdiensten am Arbeitsplatz beinhaltet, ist unserem Internetangebot zu entnehmen.

Die verantwortlichen Dienststellen im Saarland und die Privatwirtschaft sollten sich genau überlegen, welche Fallkonstellation in ihrem Zuständigkeitsbereich gewollt ist und diese strikt umsetzen, um mögliche Nachteile und rechtliche Konsequenzen schon im Vorfeld abwenden zu können.

Im Sommer letzten Jahres erreichte uns diesbezüglich die Anfrage eines Personalrates, da eine Hausverfügung in der betreffenden Dienststelle die Aktivierung eines Abwesenheitsassistenten und die Einsichtnahme in den dienstlichen E-Mail-Account der abwesenden Bediensteten regeln sollte.

Gegen die Einrichtung eines Abwesenheitsassistenten durch den Administrator, ohne Einsicht in die E-Mail-Konten zu nehmen, bestanden, soweit der Beschäftigte dies nicht selbst vornehmen konnte, von Seiten des Personalrates keine Bedenken.

Da jedoch die private Nutzung der E-Mail-Konten über einen längeren Zeitraum durch die Dienststellenleitung laut Aussage des Personalrates geduldet wurde und auch nicht ausgeschlossen werden kann, dass ein rein dienstlich genutzter Account private E-Mails erhalten kann, erhob der Personalrat datenschutzrechtliche Bedenken gegen die Einsichtnahme in die E-Mail-Konten der Beschäftigten durch die Dienststellenleitung und bat um Beratung durch das Unabhängige Datenschutzzentrum.

Wir wiesen darauf hin, dass eine Aktivierung des Abwesenheitsassistenten durch den Administrator auch ohne die Möglichkeit der Einsichtnahme in die E-Mail-Konten des betreffenden Beschäftigten und Zurücksetzen des eigentlichen Passwortes erfolgen kann.

Unter Beachtung der Orientierungshilfe konnte in diesem Fall schnell eine datenschutzkonforme Lösungsmöglichkeit gefunden werden, mit der sowohl der Personalrat als auch die Dienststellenleitung eine rechtssichere Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz erzielen konnten.

In einem anderen Fall wollte sich die Dienststellenleitung den erforderlichen Zugang zu den E-Mail-Konten sichern, indem jeder Beschäftigte der Dienststelle sein persönliches Passwort bei der Sachgebietsleitung hinterlegen sollte. Da in dieser Dienststelle bereits über Jahre hinweg die private Nutzung der E-Mail-Konten bekannt war und die betreffenden Beschäftigten bei entsprechenden Verstößen keinerlei Konsequenzen zu befürchten hatten, konnte man von einer Duldung durch den Dienstherrn ausgehen. Die Einsichtnahme in die E-Mail-Konten der Beschäftigten im Falle ihrer Abwesenheit ist damit eingeschränkt und in der Regel nicht ohne die Erlaubnis des Beschäftigten zulässig.

Auch hier verwiesen wir auf das Einrichten einer Abwesenheitsnotiz ohne ein vorheriges Zurücksetzen des Benutzerpasswortes sowie ohne einen Zugriff auf den Postfachinhalt durch einen IT-Administrator.

Darüber hinaus erscheint es als sinnvoll, sog. Funktions-E-Mail-Adressen einzurichten, die das Zusenden wichtiger Unterlagen und den gesicherten Abruf durch die jeweilige Dienststelle garantieren. Diese Funktionsadressen sind nicht nur für eine Person zugänglich, sondern für die komplette Funktionseinheit, in der sich der jeweilige Beschäftigte befindet. Ein Beispiel für eine solche Adresse könnte lauten: sozialamt@kommune.de.

Das Hinterlegen der persönlichen Passwörter für einen Zugriff durch die Dienststellenleitung verstößt indes gegen die in § 11 Saarländisches Datenschutzgesetz (SDSG) geforderten technisch-organisatorischen Maßnahmen, um Daten vor einem unbefugten Zugriff zu schützen.

Ein persönliches Passwort, im privaten sowie im dienstlichen Bereich, sollte sorgsam benutzt werden. Darüber hinaus sollte es niemandem zur Kenntnis oder gar Nutzung zur Verfügung gestellt und regelmäßig gewechselt werden. Es sollte nicht mit dem privat genutzten Passwort übereinstimmen und aufgrund seiner Konzeption dementsprechend sicher sein.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt dazu auf seiner Homepage unter www.bsi.bund.de regelmäßig Empfehlungen zur Mindestlänge und Zusammensetzung eines Passwortes heraus.

Die Gefahr, die in einer Veröffentlichung der Passwörter liegt - und sei es nur gegenüber der Sachgebietsleitung-, besteht darin, dass sich ein Dritter über das Passwort Zugang zum PC des betroffenen Nutzers verschaffen, dort Daten löschen oder ändern kann oder beispielsweise im Namen des eigentlichen Benutzers diskreditierende E-Mails schreiben kann.

Letztendlich wurde von der Abgabe der persönlichen Passwörter abgesehen und es wurden andere innerorganisatorische Maßnahmen gemäß unseren Empfehlungen, angepasst an die Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, ergriffen.

Auch dieser Fall zeigte, dass eine konsequente Umsetzung der Orientierungshilfe und der Ausführungen der Anlage 2 der GGO bereits im Vorfeld dazu geführt hätte, dass sich alle im rechtssicheren Bereich bewegen und nicht Gefahr laufen, auch unbewusst gegen Vorschriften zu verstoßen.

12.5 Zutrittskontrollsysteme

Der Personalrat einer saarländischen Behörde bat uns um eine datenschutzrechtliche Beurteilung des folgenden Sachverhaltes:

Nachdem erste Verdachtsmomente hinsichtlich eines Zeitkartenbetruges durch einen Auszubildenden in der Behörde vorlagen, veranlasste die Behördenleitung einen Abgleich des Zeiterfassungssystems mit den Daten der Zutrittskontrolle zum Dienstgebäude. Dabei stellte sich heraus, dass der Auszubildende mehrfach das Gebäude frühzeitig verlassen hatte, ohne die Zeiterfassung zu betätigen. Erst abends betrat er das Gebäude durch einen Nebeneingang wieder, um sein Gehen aus der Behörde an der Zeituhr zu dokumentieren.

Eines der Probleme hierbei war, dass der Personalrat weder bei der Überwachungsmaßnahme noch bei der Installation des Zutrittskontrollsystems involviert wurde und damit die notwendige Zweckbindung der Daten dafür fehlte. Gemäß § 84 S. 1 Nr. 2 Saarländisches Personalvertretungsgesetz ist der Personalrat bei der Einführung, Anwendung, wesentlichen Änderung oder wesentlichen Erweiterung von technischen Einrichtungen zu beteiligen, die geeignet sind, das Verhalten oder die Leistung der Angehörigen der Dienststelle zu überwachen, sobald durch den Einsatz die Leistungs- und Verhaltenskontrolle von Beschäftigten möglich ist.

Sinn des Zutrittskontrollsystems war laut Dienststellenleitung, nur Befugten Zutritt zum Behördengebäude zu ermöglichen. Das Zeiterfassungssystem wurde seinem Sinn entsprechend zur Dokumentation des Arbeitsbeginns und –endes, sowie eventuellen Unterbrechungen der Arbeitszeit installiert.

Unsere Dienststelle bewertet den Einsatz von Zutrittskontrollsystemen je nach ihrer Zweckausrichtung und hat die betroffene Dienststelle auf das Ergebnis der Prüfung hingewiesen.

Wurde das Zutrittskontrollsystem installiert, um die im Gebäude befindlichen Daten vor unbefugtem Zugriff zu schützen, ist die Maßnahme in diesem Fall als technisch-organisatorische Maßnahme im Sinne des § 11 Saarländisches Datenschutzgesetz (SDSG) zu werten. Dies hat zur Folge, dass die Auswertungen auch nur zu diesem Zweck erfolgen dürfen und ein Zugriff auf die Daten durch die spezielle Regelung des § 31 Abs. 5 SDSG nicht zur Leistungs- und Verhaltenskontrolle der Beschäftigten genutzt werden darf. Die oben genannte Auswertung der Zutrittsdaten wäre somit rechtswidrig.

Soweit der Zweck der Maßnahme lediglich in der Verhinderung des unbefugten Zutritts zu sehen ist, sind ähnlich wie bei der Benutzung eines herkömmlichen Schlüssels keine damit verbundenen Datenerhebungen erforderlich. Da automatisierte Systeme, mit denen personenbezogene Daten erhoben und verarbeitet werden, unter

Beachtung des Grundsatzes der Datensparsamkeit gemäß § 4 Abs. 4 SDSG auszugestalten sind, dürfen lediglich die zur Zweckerfüllung erforderlichen Daten erhoben werden. Im Ergebnis kann nicht abschließend dokumentiert werden, ob nur eine Person das Gebäude verlassen oder betreten hat oder mehrere gleichzeitig. Die Sicherung des befugten Gebäudezutritts wäre somit auch mit milderen Mitteln und ohne eine Dokumentation der Zutrittszeiten und des jeweiligen Benutzers zu erreichen. Da der angestrebte Zweck durch die Maßnahme nicht eindeutig verfolgt werden kann und der Eingriff in die Persönlichkeitsrechte der Beschäftigten somit unverhältnismäßig ist, führt dies zum Ergebnis, dass bereits die Datenerhebung unzulässig war. Dieses Ergebnis wurde sowohl dem Personalrat als auch der verantwortlichen Stelle mitgeteilt.

12.6 Videoüberwachung von Lehrkräften in einer Grundschule

Im Berichtszeitraum erhielten wir den anonymen Hinweis, dass eine im Außenbereich einer Grundschule angebrachte Videoüberwachungsanlage auch zur Leistungs- und Verhaltenskontrolle der Lehrkräfte genutzt werde. So wurde behauptet, dass der Rektor der Schule, dem vom Schulträger Zugriffsrechte auf die Aufnahmen eingeräumt worden seien, anhand der Videodokumentation Lehrkräfte kontaktiert hätte, um ihnen Fehlverhalten im Rahmen der Pausenaufsicht vorzuwerfen. So hätten die mit der Pausenaufsicht beauftragten Lehrkräfte die Aufsicht mitunter erst nach zeitlicher Verzögerung wahrgenommen, was aber der Tatsache geschuldet sei, dass gerade in Grundschulen die Lehrkräfte öfter mit ihren Schülern in den Klassenraum zurück gehen müssten, weil dort beispielsweise das Pausenbrot vergessen wurde.

Da wir auch bei der Installation der Kameraüberwachung nicht beteiligt wurden und der Schulträger seiner Verpflichtung zur Anhörung unserer Dienststelle im Vorfeld der Installation gemäß § 7 Abs. 2 Saarländisches Datenschutzgesetz (SDSG) nicht nachgekommen ist, wurde der Schulträger als verantwortliche Stelle im Sinne des Datenschutzgesetzes angeschrieben und um Stellungnahme zum Sachverhalt gebeten.

Gerade in Schulen steht einer Videoüberwachung der Erziehungs- und Bildungsauftrag der jeweiligen Schule entgegen. Dabei verträgt sich eine Videoüberwachung grundsätzlich nicht mit dem Auftrag der Schule, die Entwicklung der Schülerinnen und Schüler zu selbstbestimmten und mündigen Persönlichkeiten zu fördern. Der mit der Videoüberwachung einhergehende ständige Überwachungsdruck, der auf die Schüler in den Aufenthaltsbereichen ausgeübt wird, ist nicht mit der freien Entwicklung und Persönlichkeitsbildung der Schüler in Einklang zu bringen. Eine Videoüberwachung im Außenbereich eines Schulgeländes kann deshalb nur dann zulässig sein, wenn sie auf Zeiten außerhalb des Schulbetriebes begrenzt wird und die weiteren Voraussetzungen des § 34 SDSG erfüllt sind.

§ 34 SDSG fordert für die Videoüberwachung durch öffentliche Stellen unter anderem, dass es konkrete Anhaltspunkte geben muss, die eine Videoüberwachung als ultima ratio, in diesem Falle zum Schutz des Eigentumes, legitimieren können. Dies

konnte uns durch den Schulträger plausibel dargestellt werden, da es in der Vergangenheit, anhand von Strafanzeigen belegbar, zu Beschädigungen und Verschmutzungen durch Jugendliche außerhalb der Öffnungszeiten auf dem Schulgelände der Schule gekommen war. Auch vermehrte Kontrollfahrten durch die Polizei konnten die Beschädigungen und Verschmutzungen des Schulhofgeländes nicht verhindern.

Im vorliegenden Fall wurde jedoch keine zeitliche Befristung der Videoüberwachung auf die relevanten Zeiten außerhalb des Schulbetriebs eingestellt. Vielmehr waren die Kameras rund um die Uhr im Einsatz. Auch die Zugriffsrechte des Rektors waren nicht erforderlich, da der Schulträger als verantwortliche Stelle für die Videoüberwachungsmaßnahme über eventuelle Beschädigungen und Verschmutzungen an seinem Eigentum selbst Einsicht in die betreffenden Aufnahmen nehmen kann.

Als erste Maßnahmen wurden von Seiten des Schulträgers die Zugriffsrechte des Rektors gelöscht und die Kameraeinstellungen derart modifiziert, dass lediglich Aufnahmen außerhalb des Schulbetriebes möglich waren. Anschließend wurde die erforderliche Verfahrensbeschreibung nach § 9 SDSG angefertigt und die Überwachungsmaßnahme in Abstimmung mit unserer Dienststelle den Vorgaben des § 34 SDSG entsprechend in Betrieb genommen.

Obwohl damit der Betrieb der Videoanlage datenschutzkonform ausgestaltet wurde, stellte sich weiterhin die Frage, wie die Kontrolle der Lehrkräfte durch den Rektor zu bewerten war.

Die Nutzung der Daten der Videoüberwachungsanlage zur Leistungs- und Verhaltenskontrolle der Lehrkräfte stellt datenschutzrechtlich eine Zweckänderung dar. Die Daten der Überwachungsanlage sollten nämlich dem Zweck dienen, Vandalismus am und um das Schulgelände herum aufzuklären. Sie wurden durch den Rektor der Schule jedoch dazu genutzt, die Lehrkräfte in ihrem Verhalten zu kontrollieren. Eine Zweckänderung der Daten kann nur dann legitimiert werden, wenn die Voraussetzungen des § 13 Abs. 2 SDSG erfüllt sind. Da die dort geforderten Voraussetzungen im konkreten Einzelfall nicht vorlagen, war die Zweckänderung nicht zulässig und die Nutzung der Daten durch den Rektor rechtswidrig.

Der Fall wurde an unsere Bußgeldstelle zur Prüfung eines Ordnungswidrigkeitenverfahrens weitergleitet.

12.7 Videoüberwachung von Mitarbeitern in einer Bäckerei

Uns erreichte eine Eingabe von drei Mitarbeiterinnen einer Bäckereifiliale, die sich in ihrem Recht auf informationelle Selbstbestimmung verletzt sahen, weil ihr Arbeitgeber heimlich eine Videokamera installierte, ohne die Mitarbeiter darüber in Kenntnis zu setzen.

Mit diesen Vorwürfen durch unsere Dienststelle konfrontiert, bezog der Arbeitgeber Stellung und legte die datenschutzrechtliche Zulässigkeit der Maßnahme dar.

Die Videoüberwachung im Rahmen eines Beschäftigungsverhältnisses richtet sich in der Regel nach § 32 Bundesdatenschutzgesetz (BDSG). Wegen der besonders hohen

Eingriffsintensität in die Rechte der betroffenen Beschäftigten ist die Rechtfertigungsschwelle hoch anzusetzen. Eine nur präventive Videoüberwachung ohne konkreten Anlass genügt den Anforderungen des § 32 BDSG grundsätzlich nicht. So besagt § 32 Abs. 1 S. 2 BDSG, dass zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden dürfen, 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.

Der 2. Senat des Bundesarbeitsgerichts hat mit Urteil vom 21. Juni 2012 - 2 AZR 153/11 - in einem ähnlich gelagerten Fall folgende Ausführungen gemacht:

Die heimliche Videoüberwachung eines Arbeitnehmers ist zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit das einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist. Der Verdacht muss in Bezug auf eine konkrete strafbare Handlung oder andere schwere Verfehlungen zu Lasten des Arbeitgebers gegen einen zumindest räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern bestehen.

Der Arbeitgeber legte unserer Dienststelle Beweise vor, anhand derer man den konkreten Verdacht auf Diebstähle durch Mitarbeiter belegen konnte. Um die betroffenen Mitarbeiter des Diebstahls überführen zu können, wurde in vorheriger Absprache mit dem zuständigen Betriebsrat, räumlich und zeitlich begrenzt, eine heimliche Videoüberwachung in dieser Filiale durchgeführt. Von der Videoüberwachung waren ausschließlich Mitarbeiter und keine Kunden betroffen. Die konkreten Verdachtsmomente wurden im Vorfeld der Maßnahme dokumentiert, anschließend nach vergleichbaren Mitteln zur Aufklärung des Sachverhaltes gesucht und die Videoüberwachung als letzte Option zur Aufklärung der Verdachtsmomente ausgewählt. Die Maßnahme wurde im Vorfeld gemäß § 32 Abs. 3 BDSG dem zuständigen Betriebsrat erläutert und von diesem genehmigt. Nach erfolgter Auswertung der Videoaufzeichnung konnten bestimmte Mitarbeiter des Diebstahls überführt werden.

Soweit – wie vorliegend - die rechtlichen Rahmenbedingungen im Vorfeld eingehalten werden, die Vorgehensweise also ausreichend dokumentiert und die zu treffenden Maßnahmen unter Beachtung des Verhältnismäßigkeitsprinzips mit der zuständigen Interessenvertretung abgestimmt werden, kann auch eine derartige heimliche Videoüberwachung im Einzelfall zulässig sein. Hier zeigt sich, dass der häufig pauschal geäußerte Vorwurf „Datenschutz sei Täterschutz" nicht zutrifft. Datenschutzregelungen vereiteln keine effektiven Maßnahmen, sondern der Gesetzgeber möchte mit ihnen einen klaren Rahmen für verhältnismäßige Eingriffe in das informationelle Selbstbestimmungsrecht geben.

12.8 Umsetzung des Mindestlohngesetzes

Seit Einführung des Mindestlohngesetzes im Januar 2015 sind Arbeitgeber dazu verpflichtet nachzuweisen, dass sowohl ihre Beschäftigten als auch die Beschäftigten ihrer Subunternehmer den gesetzlichen Mindestlohn erhalten. Um diesen Nachweis führen zu können, verlangen viele Unternehmen von ihren Subunternehmen die Berechtigung, Aufzeichnungen über geleistete Arbeitsstunden und gezahlte Entgelte zu erhalten sowie zur Durchsetzung des Anspruchs Einblicke in diesbezügliche Unterlagen, insbesondere in die Gehaltsmitteilungen der Beschäftigten des jeweiligen Subunternehmers, zu nehmen.

In diesem Kontext wurde unsere Dienststelle vom Landesverband für Verkehrsgewerbe im Saarland e.V. kontaktiert, da einige dem Landesverband angehörige Busunternehmen einen solchen Nachweis erbringen und damit einhergehend eine entsprechende Erklärung unterschreiben sollten, die die umfangreichen Einsichtsrechte durch den jeweiligen Auftraggeber sicherstellen sollte. Wir wurden gebeten, die datenschutzrechtliche Zulässigkeit der Erklärung zu prüfen.

Bedauerlicherweise hat das Mindestlohngesetz keine Ausführungen zum Umfang der Kontrollrechte implementiert. Üblicherweise sind den Entgeltabrechnungen auch Daten wie die Religionszugehörigkeit, die Steuerklasse, eine vorliegende Schwerbehinderung oder der jeweilige Familienstand zu entnehmen, die für die Einhaltung des Mindestlohngesetzes nicht prüfungsrelevant sind. Mit der beschriebenen Vorgehensweise werden durch den Auftragnehmer somit Daten übermittelt, die für die Entscheidung, ob die Anforderungen des Mindestlohngesetzes eingehalten werden, nicht erforderlich sind.

Gemäß § 32 Bundesdatenschutzgesetz (BDSG) und § 31 Saarländisches Datenschutzgesetz (SDSG) dürfen Daten im Beschäftigungsverhältnis unter anderem jedoch nur insoweit durch den Arbeitgeber verarbeitet und damit auch an Dritte übermittelt werden, soweit sie für die Durchführung des Beschäftigungsverhältnisses erforderlich sind.

Hier kommt es zu einem Konflikt in der Auslegung der Regelungen zur Umsetzung des Mindestlohngesetzes und den jeweiligen Regelungen zum Beschäftigtendatenschutz in den zuständigen Datenschutzgesetzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat diesbezüglich die Entschließung „Mindestlohngesetz und Datenschutz“ vom 18./19. März 2015 (vgl. Kapitel 25.6) verabschiedet, die den Gesetzgeber zu einer Klarstellung dieser Problematik aufruft und datenschutzgerechte Möglichkeiten zur Umsetzung der Anforderungen aus dem Mindestlohngesetz aufzeigt. Bis dahin halten wir beispielsweise stichprobenartige Kontrollen von Gehaltsunterlagen, in denen nicht prüfungsrelevante Daten geschwärzt werden, für datenschutzrechtlich unbedenklich.

Diese Auffassung wurde dem Landesverband für Verkehrsgewerbe im Saarland e.V. in dieser Form mitgeteilt.

13 Brand- und Katastrophenschutz

13.1 Einsatz einer Software zur Feuerwehrverwaltung

Die Verwaltung der Feuerwehr stellt für die Gemeinden und Landkreise im Saarland eine große Herausforderung dar. Gerätschaften müssen in regelmäßigen Abständen gewartet und überprüft werden. Aber nicht nur die technische Ausstattung steht auf dem Prüfstand, auch die Feuerwehrangehörigen der Kommunen müssen regelmäßig beispielsweise ihre Atemschutztauglichkeit unter Beweis stellen und ein ärztliches Attest dazu vorlegen. Zur Dokumentation des Ausbildungsstandes der Feuerwehr muss unter anderem erfasst werden, welche Feuerwehrangehörige eine Sonderausbildung absolviert haben, wie viele Führungskräfte die entsprechenden Lehrgänge an der saarländischen Feuerwehrschule erfolgreich abgeschlossen haben oder inwiefern diese mit der digitalen Funktechnik vertraut sind.

Da es zur Lösung dieser Problematik oft selbst entwickelte Programme in den Kommunen gab, ist der Landkreis Sankt Wendel mit dem Ziel an uns herangetreten, eine datenschutzgerechte Vereinheitlichung der Feuerwehrverwaltungssoftware im Kreis zu initiieren. Allen Kommunen des Landkreises sollte die Software zur Verfügung gestellt werden, damit eine Erleichterung für die Zusammenarbeit von Gemeinden, Landkreis und vor allem für die jeweiligen Löschbezirke erreicht werden kann.

Geplant war, dass der Landkreis die erforderliche Software zentral für die Kommunen zur Verfügung stellt und auf einem externen Server mandantenbezogen hinterlegt werden können. Da die Gemeinden hier datenschutzrechtlich die verantwortlichen Stellen für die personenbezogenen Daten ihrer Feuerwehrangehörigen sind, mussten Auftragsdatenverarbeitungsverträge gemäß § 5 Saarländisches Datenschutzgesetz (SDSG) abgeschlossen werden, um das Projekt datenschutzgerecht gestalten zu können. So mussten die Gemeinden mit dem Landkreis jeweils einen Auftragsdatenverarbeitungsvertrag abschließen, damit der Landkreis der Kommune die erforderliche Software anbieten konnte. Der Landkreis musste sowohl mit dem Softwareanbieter, der das Programm entwickelt hat als auch mit dem Bereitsteller der Server, auf dem die Daten gespeichert werden, jeweils einen Unterauftragsdatenverarbeitungsvertrag abschließen.

Gemeinsam mit der Landkreisverwaltung und der Stadt Sankt Wendel wurden Musterverträge und Zugriffsberechtigungskonzepte entwickelt, die für alle Kommunen anwendbar sind. Ebenso wurde eine Musterverfahrensbeschreibung gemäß den Vorgaben des § 9 SDSG entwickelt, die uns vor dem erstmaligen Einsatz in der Kommune gemäß § 7 Abs. 2 SDSG im Anhörungsverfahren vorzulegen ist.

Durch die frühzeitige Einbindung unserer Dienststelle in den Entwicklungsprozess konnte eine datenschutzgerechte Lösung zur Feuerwehrverwaltung gefunden werden, die auch in anderen Landkreisen umgesetzt werden soll.

13.2 Zusatzalarmierung per App und E-Mail

Bereits seit einigen Jahren erfolgt die Alarmierung der Einsatzkräfte von Feuerwehr und Rettungsdienst, aber auch von anderen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) im Saarland mittels sog. Digitaler Meldeempfänger (DME). Es handelt sich hierbei um handliche digitale Funkempfänger, die von den Einsatzkräften (am Körper) getragen werden und über die die Kräfte im Einsatzfall text- bzw. nachrichtenbasiert alarmiert und vorab mit Zusatzinformationen (max. 240 Zeichen) zum Einsatz und der Einsatzörtlichkeit versorgt werden können.

Diese Alarmtexte werden bei der Übertragung verschlüsselt, um die Vertraulichkeit etwaig enthaltener sensibler Informationen bspw. zu Einsatzopfer oder Einsatzort zu gewährleisten. Hierzu müssen die DME bestimmte technische Anforderungen im Hinblick auf Verschlüsselungsverfahren, Schlüssellänge und -tausch erfüllen. Um den Kreis möglicher Empfänger kontrollieren zu können ist zudem nur eine Adressierung / Alarmierung vorher freigeschalteter DME möglich. Jeder DME muss zudem eine BOS-Zulassung besitzen, also die Konformität zur technischen Richtlinie der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) – Geräte für die digitale Funkalarmierung nachweisen.

Der für die Alarmierung zuständige Zweckverband für Rettungsdienst und Feuerwehralarmierung Saar (ZRF)[18] ist im Berichtszeitraum an unsere Dienststelle mit einer Anfrage zur datenschutzrechtlichen Beurteilung der Nutzung zusätzlicher Feuerwehralarmierungssysteme herangetreten. Alle Kommunen haben die für die Alarmierung der Feuerwehr erforderlichen örtlichen Alarmierungseinrichtungen vorzuhalten. Einige davon äußerten die Absicht, ergänzend zum bestehenden System Alarmierungsmöglichkeiten per App oder E-Mail einzurichten, um eine höhere Erreichbarkeit der verfügbaren Einsatzkräfte zu erzielen.

Sofern - zusätzlich zu der im Saarland bestehenden Alarmierungsmöglichkeit mittels DME - von einzelnen Kommunen dennoch der Bedarf zur Einführung von Zusatzalarmierungssystemen gesehen wird, haben wir im Rahmen unserer Beratung darauf hingewiesen, dass unbedingt der Grundsatz der Datensparsamkeit gem. § 4 Abs. 4 Saarländisches Datenschutzgesetz (SDSG) zu beachten ist, wonach technische Einrichtungen so wenig personenbezogene Daten wie möglich verarbeiten sollten. Soweit eine Zusatzalarmierung ohne Personenbezug stattfinden sollte und lediglich Stichworte wie „Hilfeleistungseinsatz" oder „Brand" ohne Ortsangabe übermittelt werden, bestehen gegen einen Einsatz einer App oder einer E-Mail keine datenschutzrechtlichen Bedenken. Sollten bei der Nutzung des Zusatzalarmierungssystems auch personenbezogene Daten übermittelt werden, die möglicherweise auch Gesundheitsdaten zum Gegenstand haben, ist im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen, ob die damit einhergehenden Eingriffe in die Persönlichkeitsrechte der Betroffenen diese Art der Zusatzalarmierung rechtfertigen.

Sollte nach dieser Abwägung die Entscheidung zu Gunsten einer Zusatzalarmierung ausfallen, wäre durch technisch-organisatorische Maßnahmen gemäß § 11 Abs. 2

[18] § 3 Abs. 2 Gesetz zur Änderung des Gesetzes über die Errichtung und den Betrieb der Integrierten Leitstelle des Saarlandes (ILSG).

SDSG im Rahmen der Zusatzalarmierung sicherzustellen, dass insbesondere auch die Vertraulichkeit und Zweckbindung gewahrt werden müssen. Sollte sich also beispielsweise eine Kommune dazu entscheiden, ein zusätzliches Alarmierungssystem für Feuerwehrangehörige zu etablieren, muss sie dabei sicherstellen, dass Unbefugte keine Kenntnis von personenbezogenen Inhalten der Alarmierung erhalten, was insbesondere bei der Nutzung privater Kommunikationsdienste relevant ist. Es müssen zudem Vorkehrungen getroffen werden, mit denen der Kreis der Empfänger kontrolliert werden kann und die gewährleisten, dass die übertragenen personenbezogenen Daten nur für Zwecke der Alarmierung verwendet und nicht beispielsweise in sozialen Netzwerken weiterverbreitet werden. Zudem muss die Kommune zunächst eine Vorabkontrolle gemäß § 11 Abs. 1 SDSG sowie eine Verfahrensbeschreibung nach § 9 SDSG erstellen. Sollte die Software eines Drittanbieters verwendet werden, muss zudem mit diesem ein Auftragsdatenverarbeitungsvertrag gemäß § 5 SDSG abgeschlossen und unserer Dienststelle vorgelegt werden. Schließlich ist vor dem erstmaligen Einsatz eines solchen Systems das Unabhängige Datenschutzzentrum gemäß § 7 Abs. 2 SDSG zu hören.

Da bei der Entscheidung über den Einsatz von zusätzlichen Alarmierungssystemen ein Einvernehmen mit dem Ministerium für Inneres und Sport herzustellen ist, wurde dem Ministerium unsere datenschutzrechtliche Bewertung mitgeteilt. Auch das Ministerium hält weitere Alarmierungssysteme grundsätzlich für entbehrlich, da die Erreichbarkeit durch die Ausstattung der Wehren mit Meldeempfängern, Sirenenalarmierung und dem digitalen BOS-Funknetz ausreichend ist, um den Brand- und Katastrophenschutz im Saarland sicherzustellen. Die Freigabe weiterer Alarmierungseinrichtungen ist durch das Ministerium für Inneres und Sport bis dato nicht erfolgt.

14 Ausländerwesen

14.1 Videoüberwachung in Aufnahmeeinrichtungen für Flüchtlinge

Stark ansteigende Flüchtlingszahlen in Deutschland im Jahr 2015 stellten auch die saarländische Landesregierung vor große Herausforderungen. Dabei ergaben sich unter anderem bei der Gewährleistung der Sicherheit in den Flüchtlingsunterkünften auch datenschutzrechtliche Fragestellungen.

14.1.1 Videoüberwachung in der Landesaufnahmestelle für Flüchtlinge

Seitens des Ministeriums für Inneres und Sport wurden erste Überlegungen angestellt, ob eine Videoüberwachungsmaßnahme in der Landesaufnahmestelle für Flüchtlinge ein geeignetes Mittel zum Schutz der Menschen in dieser Einrichtung darstellen kann.

Geplant war zunächst, die beiden durch die Landesaufnahmestelle führenden öffentlichen Straßen mithilfe von Kameras zu überwachen. Grund hierfür war zum einen, dass die Bewohner und die in der Aufnahmestelle tätigen Beschäftigten und Helfer, die diese Straßen als Fußgänger nutzen, durch zu schnell fahrende Fahrzeuge erheblich gefährdet würden. Zum anderen sollten mit Hilfe der Kameras auch die Kennzeichen von Fahrzeugen erfasst werden, um hierdurch mögliche Schleuser zu identifizieren, die häufig nachts Flüchtlinge in der Einrichtung absetzen würden. Um die Voraussetzungen für eine Videoüberwachung in diesem Bereich zu schaffen, wurden zunächst die kommunalen Straßen an das Saarland übertragen, die dann entwidmet und wie Privatstraßen behandelt werden sollten. Eine Zufahrtsbeschränkung für den Bereich war jedoch nicht beabsichtigt.

Im Rahmen einer gemeinsamen Begehung der Landesaufnahmestelle wurden seitens der Verantwortlichen weitere Bereiche aufgezeigt, in denen zur Gewährleistung der Sicherheit der Flüchtlinge sowie der Beschäftigten und Helfer eine zum Teil großflächige Videoüberwachung in der Landesaufnahmestelle stattfinden sollte.

Seitens unserer Dienststelle wurde zunächst darauf hingewiesen, dass eine Videoüberwachung vorliegend allenfalls unter den Voraussetzungen des § 34 Saarländisches Datenschutzgesetz (SDSG) zulässig sein kann.

§ 34 Videoüberwachung

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

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

2. zur Aufgabenerfüllung der verantwortlichen Stelle

erforderlich ist. Für die Gefährdung der in Nummer 1 genannten Rechtsgüter müssen konkrete Anhaltspunkte bestehen. Die Videoüberwachung nach Nummer 2 ist nur zulässig, wenn Anhaltspunkte für eine konkrete Gefährdung von Gesundheit, Leib oder Leben, Eigentum oder sonstigen hochrangigen Rechtsgütern vorliegen. Es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

In dem Vor-Ort-Termin wurde des Weiteren klargestellt, dass einer flächendeckenden Videoüberwachung im Bereich der Landesaufnahmestelle in jedem Falle schützenswerte Persönlichkeitsrechte der Bewohner der Aufnahmestelle sowie der dort Beschäftigten entgegenstehen, da sie sich einer solchen Überwachung nicht entziehen könnten.

Eine Videoüberwachung der durch die Landesaufnahmestelle führenden Straßen in dem zunächst beabsichtigten Umfang wurde gleichfalls als nicht zulässig angesehen. Ungeachtet der geplanten Entwidmung der Straßen würde es sich weiterhin um öffentlich zugängliche Bereiche handeln, die nach wie vor in zulässiger Weise von einer Vielzahl von Menschen genutzt werden können. Auch hier stünden einer Videoüberwachung überwiegende schutzwürdige Interessen der Betroffenen entgegen. Dem unkontrollierten Fahrzeugverkehr könnte jedoch durch eine Zufahrtsbeschränkung durch eine Schrankenanlage und gegebenenfalls durch zusätzliche Zufahrtskontrollen in ausreichendem Maße begegnet werden.

Auch in Bereichen, in denen sich besonders schutzbedürftige Personen wie Kinder oder stillende Mütter aufhalten oder in denen Personen privaten Angelegenheiten wie Telefonieren oder Essensaufnahme nachgehen, steht der Schutz der Privatsphäre der betroffenen Personen einer Videoüberwachung entgegen.

Videografisch überwachbar wären nach hiesiger Auffassung lediglich die unmittelbaren Eingangsbereiche zu den Verwaltungsgebäuden sowie technische Einrichtungen wie Heizanlagen und zugehörige Öltanks, bei denen bei unsachgemäßer Behandlung eine mögliche Brand- oder Explosionsgefahr besteht.

Mit Blick darauf, dass eine Videoüberwachung nur in einem begrenzten Umfang als rechtlich zulässig anzusehen ist, wurde auf die Umsetzung der beabsichtigten Maßnahmen verzichtet und beschlossen, zur Steigerung der Sicherheit den Personaleinsatz eines Sicherheitsdienstes zu erhöhen.

14.1.2 Videoüberwachung in der Aufnahmestelle für minderjährige unbegleitete Flüchtlinge

Zum Schutz vor Angriffen auf eine Unterkunft für minderjährige unbegleitete Flüchtlinge und zur Vermeidung von Vorkommnissen zwischen den Jugendlichen untereinander plante das für die Unterbringung der Jugendlichen zuständige Landesamt die Einrichtung einer Videoüberwachung.

Da es sich bei der Installation einer Videoüberwachungsmaßnahme um ein automatisiertes Verfahren im Sinne des § 3 Abs. 6 SDSG handelt, bedarf dieses hinsichtlich

der in der Verfahrensbeschreibung festzulegenden Angaben gemäß § 7 Abs. 2 SDSG zunächst einer schriftlichen Freigabe. Im Rahmen der gemäß § 7 Abs. 2 S. 5 SDSG vor dieser Entscheidung durchzuführenden Anhörung der Landesbeauftragten für Datenschutz wurde uns die Verfahrensbeschreibung für die Maßnahme vorgelegt.

Zur Begründung der geplanten Videoüberwachungsmaßnahme trug die verantwortliche Stelle vor, dass die Sicherheit auf dem Gelände nicht allein durch den Einsatz des vorhandenen Sicherheitspersonals gewährleistet werden könne. Daher war vorgesehen, in erster Linie die Zugangsbereiche zu der Unterkunft zu überwachen, um unzulässige Zutritte durch Unbefugte und damit auch Angriffe auf die Einrichtung zu verhindern. Darüber hinaus war geplant, auch im Innenhof des Geländes, der den Jugendlichen als Aufenthaltsbereich dient, Videokameras zu installieren, um Vorkommnisse unter den Jugendlichen zu dokumentieren.

Angesichts einer seitens der verantwortlichen Stelle dargelegten allgemeinen Gefährdungslage durch gehäufte Angriffe auf Unterkünfte für minderjährige unbegleitete Flüchtlinge haben wir unter der Voraussetzung, dass die Vorschläge in einem von dem Landespolizeipräsidium erarbeiteten Sicherheitskonzept beachtet werden, eine Videoüberwachung der Zugangsbereiche zum Schutz von Leben und körperlicher Unversehrtheit der in der Aufnahmestelle untergebrachten Minderjährigen sowie der dort Beschäftigten im Wege eines Live-Monitorings auf Grundlage des § 34 SDSG als zulässig angesehen. Nur mit Hilfe eines Live-Monitorings besteht die Möglichkeit, den Zutritt Unbefugter oder mögliche Übergriffe frühzeitig zu erkennen und zu verhindern sowie ein unmittelbares Eingreifen der vorhandenen Sicherheitskräfte zu gewährleisten.

Hinsichtlich der Überwachung des Innenhofs der Einrichtung haben wir dagegen ausdrücklich darauf hingewiesen, dass es sich hierbei um einen Aufenthaltsbereich für die Jugendlichen handelt und dementsprechend eine ständige Überwachung dieses Bereichs einen besonders intensiven Eingriff in das Recht der Jugendlichen auf Schutz ihrer Privatsphäre darstellt. Auch das zuständige Landesamt selbst wies darauf hin, dass die Jugendlichen sich frei bewegen können und ihnen nicht das Gefühl vermittelt werden solle, dass sie einer kompletten Überwachung unterliegen. Da seitens der verantwortlichen Stelle auch keine hinreichenden Anhaltspunkte dafür dargelegt worden sind, dass die beabsichtigte Überwachung im Innenbereich erforderlich im Sinne des § 34 Abs. 1 S. 1 SDSG ist, standen die schützenswerten Interessen der betroffenen Jugendlichen einer Videoüberwachung in diesem Bereich entgegen. Unsere Rechtsauffassung haben wir sodann dem Landesamt mitgeteilt.

14.2 Registrierung von Asylsuchenden mittels Fingerabdruck

Aufgrund der hohen Flüchtlingszahlen im Jahr 2015 entstand in der Landesaufnahmestelle für Flüchtlinge ein erheblicher Bearbeitungsrückstand. Hinzu kam, dass sich ein nicht geringfügiger Teil der Asylsuchenden aus unterschiedlichen Beweggründen mehrfach unter verschiedenen Identitäten registrieren ließ. Um dem damit verbundenen Missbrauch entgegenzuwirken, wurde seitens des zuständigen Ministeriums für Inneres und Sport beabsichtigt, ein System zur biometrischen Registrierung und

Erkennung von Fingerabdrücken einzusetzen, das eine eindeutige Identifizierung der Asylsuchenden ermöglicht.

Gemäß § 7 Abs. 2 SDSG wurde das Unabhängige Datenschutzzentrum vor Einführung dieses Verfahrens beteiligt.

Die Nutzung eines solchen biometrischen Identifikationsverfahrens stellt einen gravierenden Eingriff in das Recht auf informelle Selbstbestimmung dar und erfordert mithin eine gesetzliche Grundlage. Diese findet sich in § 16 Abs. 1 S. 1 und 2 Asylgesetz (AsylG). Nach der bis zum 04. Februar 2016 gültigen Fassung der Vorschrift ist die Identität eines Ausländers, der um Asyl nachsucht, durch erkennungsdienstliche Maßnahmen zu sichern, es sei denn, dass er noch nicht das 14. Lebensjahr vollendet hat. Aufgenommen werden dürfen nur Lichtbilder und Abdrucke aller zehn Finger. Zuständig für die Maßnahme ist u.a. auch die Aufnahmeeinrichtung, bei der der Ausländer sich meldet.

Bei dem gewählten Verfahren werden die Abdrücke aller Finger gescannt, hieraus ein biometrisches Template generiert, dieses in einer Datenbank abgelegt und mit dem dort hinterlegten Bestand verglichen. Da die Abnahme der Fingerabdrücke zu dem Zweck erfolgt, zu klären, ob der betreffende Asylbewerber bereits im Saarland einen Asylantrag gestellt hat, erfolgt der Datenabgleich nur innerhalb desselben Verfahrens. Automatisierte Schnittstellen zu anderen bei der Landesaufnahmestelle geführten (Fach)Verfahren oder zu anderen Stellen existieren daher nicht. Gleichwohl wird die dem Asylsuchenden im Asylverfahren zugeordnete Identifikationsnummer mitgespeichert, sodass über diese Identifikationsnummer eine manuelle Zusammenführung mit den Antrags- und Personendaten aus dem Asylverfahren möglich ist. Im Trefferfall, also wenn bei der Abnahme der Fingerabdrücke durch die Anwendung festgestellt wird, dass bereits ein entsprechendes Template existiert, kann über die zum bereits existierenden Template hinterlegte Identifikationsnummer der entsprechende Vorgang im Fachverfahren herangezogen werden.

Entsprechend der gesetzlichen Vorgaben erfolgt die Abnahme der Fingerabdrücke nur bei Asylsuchenden, die das 14. Lebensjahr vollendet haben.

Nachdem von unserer Dienststelle erbetene ergänzende Angaben zu den in der Verfahrensbeschreibung beschriebenen technischen und organisatorischen Maßnahmen geprüft wurden, standen der Freigabe dieses Verfahrens keine datenschutzrechtlichen Bedenken entgegen.

14.3 Integration von Flüchtlingen über Sportangebote

Der Landessportverband für das Saarland (LSVS) initiierte in Kooperation mit dem Landkreis Saarlouis und dem Ministerium für Inneres und Sport (MfIS) ein Projekt zur Integration von Flüchtlingen durch gezielte Sportangebote.

Hierzu hatte das Innenministerium einen entsprechenden Fragebogen in den Sprachen Englisch, Französisch, Arabisch und Deutsch vorbereitet, der in der Landesaufnahmestelle ausgelegt werden sollte. Interessierte Flüchtlinge sollten dann die Möglichkeit haben, ihre Lieblingssportarten dort einzutragen. Anschließend sollten die

Fragebögen in der Landesaufnahmestelle gesammelt und dem LSVS gebündelt zur Verfügung gestellt werden.

Im Nachgang sollte es dem LSVS möglich sein, über eine Abfrage beim Landesverwaltungsamt des Saarlandes (LaVA) die Adresse des jeweiligen Flüchtlings, auch wenn er mittlerweile einer Kommune im Saarland zugewiesen worden ist, zu erheben. Über eine Einwilligungserklärung, welche im Fragebogen implementiert war, sollte es dem LSVS datenschutzrechtlich ermöglicht werden, die Fragebögen den Kommunen bzw. den in Frage kommenden Vereinen zur Verfügung zu stellen, die sich dann wiederum mit dem Flüchtling in Kontakt setzen könnten.

Die datenschutzrechtliche Verantwortung sollte beim LSVS liegen.

Auf Nachfrage des MfIS bei der Aufsichtsbehörde wurden datenschutzrechtliche Bedenken angemeldet. Insbesondere bestanden Zweifel daran, ob die Einwilligung eines Flüchtlings in der Landesaufnahmestelle tatsächlich informiert abgegeben werden kann. Ebenso würde die Abfrage der Kontaktdaten des jeweiligen Flüchtlings bei dem LaVA dem Direkterhebungsgrundsatz zuwiderlaufen.

Daher wurde vorgeschlagen, die Fragebögen direkt bei den Kommunen zu hinterlegen. Durch die kommunalen Mitarbeiter könnten die Fragebögen an die Flüchtlinge verteilt werden. Die Flüchtlinge könnten dann wiederum ihre Kontaktdaten und ihre bevorzugten Sportarten in die Fragebögen eintragen.

Die Fragebögen wurden sodann in enger Abstimmung mit dem MfIS ausformuliert. Auf den Schreiben wurde explizit der Zweck der Datenverarbeitung erläutert. Dies beinhaltete auch Ausführungen darüber, dass sich infrage kommende Sportvereine mit den Flüchtlingen in Verbindung setzen dürfen, gegebenenfalls unter Mitwirkung der Kommune.

Durch dieses Vorgehen verschob sich die datenschutzrechtliche Verantwortung der Datenverarbeitung auf die jeweils beteiligten Kommunen.

14.4 Flüchtlingsatlas – Veröffentlichung personenbezogener Daten im Internet

Aufgrund einer entsprechenden Pressemeldung wurde bekannt, dass „unter Hintanstellung datenschutzrechtlicher Bedenken“ der saarländische Flüchtlingsatlas durch das Ministerium für Soziales, Gesundheit, Frauen und Familie im Internet veröffentlicht wurde.

Neben allgemeinem Zahlenmaterial in Bezug auf die Verteilung der Flüchtlinge auf saarländische Kommunen, ihre Herkunftsländer und ihren Anerkennungsstatus enthielt der veröffentlichte Bericht auch personenbezogene Daten von ehrenamtlichen Helfern.

Die Veröffentlichung personenbezogener Daten im Internet durch eine öffentliche Stelle stellt eine Datenverarbeitung im Sinne des § 3 Abs. 2 SDSG dar. Eine Verarbeitung personenbezogener Daten ist gemäß § 4 Abs. 1 SDSG jedoch nur zulässig, wenn eine gesetzliche Vorschrift dies erlaubt oder die Betroffenen eingewilligt haben.

Da vorliegend kein gesetzlicher Übermittlungstatbestand für diese Art der Veröffentlichung im Internet gegeben war, wäre eine Veröffentlichung nur bei Vorliegen einer schriftlichen Einwilligung der Betroffenen zulässig gewesen. Nachdem das zuständige Ministerium von uns auf diese Rechtslage hingewiesen wurde, sind die Informationen kurzfristig von der Internetseite entfernt worden.

Der Flüchtlingsatlas wurde überarbeitet und ohne die personenbezogenen Daten der ehrenamtlichen Helfer erneut veröffentlicht. Er gibt nunmehr in datenschutzgerechter Form Aufschluss über die integrationsrelevanten Rahmenbedingungen im Saarland.

15 Videoüberwachung

15.1 Videoüberwachung an einem Mehrfamilienhaus

Im Berichtszeitraum erhielt die Aufsichtsbehörde eine Mitteilung einer saarländischen Polizeiinspektion, in der diese eine Videoüberwachungsmaßnahme an einem Mehrfamilienhaus anzeigte. Konkret ging es dabei um mehrere Kameras, die hinter einer Schaufensterscheibe im Erdgeschoss angebracht waren. Aufgrund der Ausrichtung der Kameras war davon auszugehen, dass mithilfe der Kameras der ganze Straßenzug überwacht wurde. Daneben befand sich eine weitere Kamera im unmittelbaren Hauseingangsbereich und überwachte somit sämtliche Anwohner beim Betreten und Verlassen des Anwesens.

Von der Polizeiinspektion wurde eine Privatperson als für die Videoüberwachung verantwortliche Stelle genannt, die bereits in der Vergangenheit durch eine am gleichen Anwesen betriebene Videoüberwachung bei der Aufsichtsbehörde in Erscheinung getreten ist. Zu dieser Zeit weigerte sich die Person, die Mieter und Hausmeister in besagtem Anwesen war, zunächst, die Videoüberwachung einzustellen und demontierte die Kameras erst, nachdem von der Aufsichtsbehörde die Einstellung der Videoüberwachung nach § 38 Abs. 5 Bundesdatenschutzgesetz (BDSG) förmlich angeordnet wurde.

Nachdem der Mieter nunmehr von der Aufsichtsbehörde zur Stellungnahme aufgefordert wurde, gab er an, mit der verfahrensgegenständlichen Videoüberwachungsmaßnahme nichts zu tun zu haben. Aufgrund der beschriebenen Vorgeschichte erschien diese Aussage nur bedingt nachvollziehbar, weshalb erneut zur Stellungnahme aufgefordert wurde. Hierauf meldete sich dieser telefonisch bei der Aufsichtsbehörde und verzettelte sich dabei gegenüber der vorherigen schriftlichen Stellungnahme in diversen Widersprüchen. Obwohl er für die Videoüberwachung nicht verantwortlich sei, sei diese doch zum Schutz von Leib und Leben der Hausbewohner unbedingt erforderlich, da ein ehemaliger Mieter ihm gegenüber tätlich übergriffig geworden sei. Daneben gab er im weiteren Telefonverlauf an, die Kameras im Beisein einer dritten Person in der ehemaligen Ladenfläche angebracht zu haben. Trotz dieser mündlichen Einlassungen lehnte er in der schriftlichen Stellungnahme jegliche Verantwortung für den Betrieb der Videoüberwachung ab.

Im Rahmen eines bei der Polizeiinspektion angestrengten Amtshilfeersuchens wurde mitgeteilt, dass der vermeintliche Anlagenbetreiber telefonisch mit dem Betrieb der Videoüberwachung konfrontiert wurde. In diesem Zusammenhang wurde zu Protokoll gegeben, die Kameras seien aufgrund des aggressiven Verhaltens eines ehemaligen Mieters aufgestellt worden. Ein entsprechendes Verfahren, bei dem er Geschädigter sei, wäre dort anhängig. Die dies belegenden Videoaufzeichnungen, welche mit den verfahrensgegenständlichen Kameras angefertigt wurden, habe er der Polizei zur Verfügung gestellt. Die Polizeiinspektion hat der Datenschutzaufsichtsbehörde entsprechende Ausdrucke der Videoaufzeichnungen übersandt, aus denen der Erfassungsbereich der Kameras entnommen werden konnte. Es stellte sich heraus,

dass neben dem Hauseingangsbereich der gesamte Straßenzug in beide Richtungen bis zu den auf der anderen Straßenseite gelegenen Anwesen überwacht wurde.

Trotz der nunmehr feststehenden Verantwortlichkeit für den Betrieb der Videoüberwachung beharrte die Person auf ihrer Angabe und teilte darüber hinaus mit, nicht im Besitz der Schlüssel zu der Räumlichkeit, in der sich die Kameras befinden, zu sein.

Die Einlassungen des Mieters mussten aufgrund der bisherigen Erkenntnisse als unzutreffend eingestuft werden.

Da die Videoüberwachung keineswegs datenschutzrechtlichen Anforderungen genügte, wurde die Einstellung der Videoüberwachung angeordnet. Da der Mieter trotz der rechtskräftigen Anordnung weiterhin bzw. erneut datenschutzwidrig eine Überwachung betrieb, war somit auch künftig mit weiteren Rechtsverletzungen zu rechnen. Daher wurde zudem die Demontage der Kameras angeordnet.

Dieser Bescheid wurde rechtskräftig. Da die Befolgung der Anordnung der Aufsichtsbehörde nicht rechtzeitig angezeigt wurde, wurde ein Zwangsvollstreckungsverfahren in die Wege geleitet, welches bis zum Ende des Berichtszeitraums noch nicht abgeschlossen war. Auch wurden für das Verfahren Gebühren in dreistelliger Höhe erhoben.

15.2 Videoüberwachung durch einen Hauseigentümer und gerichtlicher Vergleich

Anlässlich einer Vielzahl von Beschwerden wurde ein bereits im Jahre 2012 abgeschlossenes Verwaltungsverfahren wieder aufgegriffen und durch Vergleich vor dem Verwaltungsgericht des Saarlandes im Berichtszeitraum des vorliegenden Tätigkeitsberichts zu einem Abschluss gebracht.

Das Datenschutzzentrum wurde auf den Einsatz von Videokameras an der Fassade eines an einem zentralen Platz einer Gemeinde gelegenen Hauses aufmerksam gemacht. Besagtes Gebäude wurde von dem Eigentümer bewohnt und gewerblich genutzt. Im Rahmen eines Vororttermins wurden den damaligen Mitarbeitern des Datenschutzzentrums als Anlass für die Überwachung Sachbeschädigungen an der Hausfassade in der Vergangenheit und die zukünftige Abschreckung von potentiellen Tätern kommuniziert.

Nach dem damaligen Votum der Aufsichtsbehörde wurde die Überwachung der Hausfassade und die damit verbundene Erfassung eines Toleranzbereichs des Gehwegs nach § 6b Bundesdatenschutzgesetz (BDSG) unter der Voraussetzung als zulässig erachtet, dass die Videoüberwachung auf den Zeitraum außerhalb der Öffnungszeiten eines im Gebäude befindlichen Gewerkschaftsbüros beschränkt, ein Schild, das auf den Umstand der Videoüberwachung und die dafür verantwortliche Stelle hinweist, angebracht und die Speicherdauer auf das notwendige Maß beschränkt wird. Nachdem der Hauseigentümer die Umsetzung der Maßnahmen telefonisch bestätigte, wurde das Verwaltungsverfahren abgeschlossen.

Aufgrund einer erneuten Eingabe wurde der Sachverhalt wieder aufgegriffen. Eine kursorische Bewertung des vorliegenden Akteninhalts hatte zum Ergebnis, dass an

dem damaligen Votum hinsichtlich der Zulässigkeit der Videoüberwachung nicht weiter festgehalten werden konnte.

Nach erneuter Stellungnahme des Eigentümers zu dem Anlass und der konkreten Ausgestaltung und aufgrund einer unangekündigten Inaugenscheinnahme der Örtlichkeit ergaben sich erhebliche Zweifel an der Zulässigkeit der Fortführung der Überwachungsmaßnahme.

In diesem Zusammenhang konnte weder eine objektiv nachvollziehbare Schadensdokumentation vorgelegt werden, noch konnten - trotz entgegenstehender Mitteilung des Eigentümers - Schilder aufgefunden werden, mit denen auf den Umstand der Videoüberwachung hingewiesen wurde. Darüber hinaus ergab sich im Verfahren, dass die Überwachung ohne Beachtung der Öffnungszeiten des im Gebäude befindlichen Gewerkschaftsbüros permanent betrieben wurde. Zudem lagen grundsätzlich der gesamte Gehweg und Teile der Straße vor der Fassade im Aufnahmebereich der Kamera und wurden lediglich durch softwareseitige Maßnahmen (Privacy-Filter) unkenntlich gemacht. Der Hauseigentümer übersandte schließlich noch Einwilligungserklärungen der Mieter hinsichtlich der verfahrensgegenständlichen Videoüberwachung.

Dem Betreiber der Überwachung wurde mitgeteilt, dass Einwilligungserklärungen der Mieter den Kameraeinsatz nicht legitimieren, da der überwachte Bereich, mithin auch der Gehweg vor der Hausfassade, nicht ausschließlich durch die Mieter, sondern auch von dritten Personen genutzt wird. Weiterhin könne die Videoüberwachung nur aufgrund einer konkreten und objektiv nachvollziehbaren Gefährdungslage, die beispielsweise anhand einer detaillierten Schadensdokumentation dargelegt wird, zulässig betrieben werden. Eine solche Gefährdungslage wurde jedoch gerade nicht belegt. Zudem standen der Fortführung der permanenten und lückenlosen Videoüberwachung schutzwürdige Interessen der Betroffenen entgegen. Zu nennen waren in diesem Zusammenhang Besucher und Mitarbeiter des im Gebäude gelegenen Gewerkschaftsbüros und Passanten im Allgemeinen, die sich der Videoüberwachung nicht oder nur bedingt entziehen konnten.

Bezüglich des Ausblendens der Straße und von Teilen des Gehwegs im Aufnahmebereich durch Einsatz von Privacy-Filtern war festzuhalten, dass es mangels objektiver und revisionssicherer Kontrollmöglichkeit[19] nicht überprüft werden konnte, inwiefern dieses Ausblenden im täglichen Betrieb tatsächlich eingesetzt und nicht bloß im Falle der Intervention des Datenschutzzentrums diesem gegenüber erklärt wurde. Aufgrund des Einsatzes von Dome-Kameras, deren Ausrichtung regelmäßig nicht erkennbar ist, blieb für die Betroffenen im Übrigen die räumliche Reichweite der Überwachung zudem intransparent.

Schließlich war im Hinblick auf die beabsichtigte Abschreckungswirkung die Videoüberwachungsmaßnahme dahingehend kritisch zu hinterfragen, als auf diese, wie

[19] § 38 Abs. 4 BDSG bestimmt den Umfang der aufsichtsbehördlichen Kontrollbefugnisse und räumt umfangreiche Betretens- und Kontrollrechte ein, jedoch sind Privathäuser und -wohnungen davon nicht erfasst. Eine dortige Kontrolle ist damit ausschließlich im Einvernehmen mit dem Eigentümer oder Mieter möglich, so dass unangekündigte und tiefgehende Vorort-Prüfungen in diesem Zusammenhang somit ausgeschlossen sind.

festgestellt, nicht dergestalt erkennbar hingewiesen wurde, dass potentielle Störer gegebenenfalls von einer Schadenshandlung absehen.

Da der Hauseigentümer auf der Fortführung der Überwachungsmaßnahme in der bisherigen Form bestand, wurde nach erfolgter Anhörung die Einstellung der Videoüberwachung nach § 38 Abs. 5 S. 2 BDSG durch Bescheid verfügt. Gegen den Bescheid des Datenschutzzentrums wurde beim Verwaltungsgericht des Saarlandes Klage eingelegt.

§ 38 Abs. 5 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 Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden.

Die Klage wurde damit begründet, dass ein die Videoüberwachung rechtfertigendes berechtigtes Interesse im Sinne des § 6b Abs. 1 Nr. 3 BDSG gegeben sei, da eine konkrete Gefährdungslage belegt werden könne. Diesbezüglich wurden Rechnungen über geleistete Reparaturen und Fotos über vermeintliche Sachbeschädigungen vorgelegt. Dass bisher Täter mithilfe der seit Jahren im Einsatz befindlichen Überwachung hätten identifiziert werden können, wurde nicht dargetan. Außerdem würde die Videoüberwachung auch im Interesse der gewerblichen Mieter erfolgen, da es in der Vergangenheit zu einem Trickbetrug in einem Einzelhandelsgeschäft im besagten Gebäude gekommen sei. Zudem könne aufgrund der zentralen Lage in der Nähe eines Festplatzes auch von einer abstrakten Gefährdungslage[20] ausgegangen werden. Schutzwürdige Interessen Betroffener würden der Videoüberwachung auch nicht entgegenstehen, da diese den überwachten Bereich zügig durchschreiten; im Übrigen könnten Passanten durch Vermeiden des Gehwegs vor der Hausfassade der Überwachung aus dem Wege gehen.

Da eine abstrakte Gefährdungslage abgestellt auf die geografische Lage des Hauses in diesem Zusammenhang nicht angenommen werden konnte, hätten nachgewiesene Schädigungshandlungen zu Lasten des Hauseigentümers allenfalls für eine konkrete Gefährdungslage sprechen können. Jedoch wurde eine solche auch nicht im verwaltungsgerichtlichen Verfahren durch konkrete Benennung stattgefundener Schadensereignisse, das heißt welche Art von Schäden zu welchem Zeitpunkt an welchem Ort eingetreten ist, dargelegt. Insbesondere ließen die vorgelegten Rechnun-

[20] Eine abstrakte Gefährdungslage wäre beispielsweise typischerweise bei Geschäften, die wertvolle Ware verkaufen (Juweliere etc.) oder die im Hinblick auf Vermögens- und Eigentumsdelikte potentiell besonders gefährdet sind (Tankstellen oder Spielhallen etc.), zu bejahen. Auch könnte aufgrund der geografischen Lage eines Wohnhauses eine abstrakte Gefährdungslage zumindest zeitweise angenommen werden, wenn beispielsweise in der Nachbarschaft wiederholt Schadenereignisse eingetreten sind und auch in Zukunft glaubhaft drohen.

gen über Reparaturen eben keine räumliche und zeitliche Zuordnung zu einem spezifischen Schadensereignis im überwachten Bereich zu. Auch dass bisher keine Strafanzeigen gestützt auf Aufnahmen der Videoüberwachung gestellt wurden oder vermeintliche Täter identifiziert werden konnten, war erstaunlich. Der klagende Eigentümer erklärte den Widerspruch zwischen der von ihm so dargestellten erheblichen Summe an Schadenshandlungen zu seinen Lasten und jeglichem Fehlen von Strafanzeigen damit, dass Strafanzeigen wegen zu erwartender Aussichtslosigkeit nicht gestellt wurden.

Soweit darüber hinaus versucht wurde, die Videoüberwachung mit einem Trickbetrug in dem Einzelhandelsgeschäft zu rechtfertigen, konnte auch dieser Vorfall die Maßnahme nicht legitimieren, denn der Schutz fremder Interessen stellt nicht per se ein berechtigtes Interesse des Überwachenden im Sinne der Vorschrift dar.

Auch erfüllte die Videoüberwachung nicht das Merkmal der Erforderlichkeit im Sinne des § 6b Abs. 1 BDSG. Diese ist nur dann zu bejahen, wenn das festgelegte Ziel mit der Überwachung tatsächlich erreicht werden kann und es dafür kein anderes, gleich wirksames, aber mit Blick auf die informationelle Selbstbestimmung des betroffenen Personenkreises weniger einschneidendes Mittel gibt. Da nach Aussage des Klägers gerade auch eine abschreckende Wirkung von den Kameras ausgehen sollte, war eine Geeignetheit der Videoüberwachung zur präventiven Abwehr von Störern und Straftätern gerade dadurch nicht gegeben, dass der Umstand der Überwachung aufgrund fehlender deutlich angebrachter Hinweisschilder im Sinne des § 6b Abs. 2 BDSG nicht zu erkennen war. Auch die Tatsache, dass laut Vorbringen des Eigentümers Schadenshandlungen seit Einsatz der Videoüberwachung eingetreten seien, jedoch trotzdem kein Täter mithilfe der Videoüberwachung identifiziert werden konnte, sprach zudem gerade nicht für deren Erforderlichkeit. Schließlich sei ergänzt, dass selbst wenn der Trickbetrug zu Lasten des gewerblichen Mieters als berechtigtes Interesse anzuerkennen wäre, als milderes Mittel die eigenverantwortliche Überwachung durch den Mieter in den Räumen der Einzelhandelsgeschäfts vorzuziehen wäre.

Das Verwaltungsgericht des Saarlandes hat abschließend im Rahmen der anberaumten mündlichen Verhandlung von einer Entscheidung durch Urteil abgesehen und einen Vergleich folgenden Inhalts vorgeschlagen:

- Die Videoüberwachung sollte im Hinblick auf die fehlende aufsichtsbehördliche Prüfungskompetenz von Privatwohnungen durch einen im Saarland ansässigen Auftragsdatenverarbeiter im Sinne des § 11 BDSG wahrgenommen werden. Ein entsprechender Auftragsdatenverarbeitungsvertrag nach § 11 Abs. 2 S. 2 BDSG sollte dem Datenschutzzentrum bis zu einem Stichtag vorgelegt werden. Sollte besagter Auftragsdatenverarbeitungsvertrag nicht abgeschlossen werden, ist die Videoüberwachung durch den Eigentümer einzustellen und dies dem Datenschutzzentrum mitzuteilen.
- Die Videoüberwachung sollte räumlich und im Hinblick auf die Öffnungszeiten des im Gebäude befindlichen Gewerkschaftsbüros zeitlich eng begrenzt werden.
- Hinweisschilder nach DIN 33450 sollten deutlich erkennbar angebracht werden.

- Nach einem festgelegten Zeitraum sollte eine Evaluation der Videoüberwachung im Hinblick auf die Notwendigkeit ihrer Fortführung erfolgen.

Der Vergleich wurde in der vom Gericht vorgeschlagenen Form abgeschlossen, jedoch mit dem Ergebnis, dass seitens des Klägers im Nachgang die Einstellung der streitgegenständlichen Videoüberwachung mitgeteilt wurde.

15.3 Schießen unter Aufsicht neu definiert

Im Berichtszeitraum meldete sich ein Petent bei der Aufsichtsbehörde und zeigte an, dass ihm bei seinem letzten Aufenthalt in einem Schützenhaus aufgefallen sei, dass dort fast der gesamte Innen- und Außenbereich von Kameras überwacht werde. Neben den einzelnen Schießanlagen würden die öffentlich zugänglichen Bereiche der Straße und des Gehweges sowie die Parkplätze vor dem Anwesen überwacht. Zudem befinde sich im Anwesen selbst eine Gaststätte, zu der auch ein Biergarten gehöre, der ebenfalls von einer der vielen Kameras erfasst werde.

Beim Einsatz von Videoüberwachungsmaßnahmen ist zu berücksichtigten, dass jede Videoüberwachung intensiv in das Grundrecht der betroffenen Personen, selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten zu bestimmen, eingreift. Daher bedarf es einer Rechtsgrundlage, um den Einsatz der Videoüberwachung und den damit verbundenen Grundrechtseingriff zu legitimieren.

Grundsätzlich geregelt ist die Videoüberwachung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen in § 6b Bundesdatenschutzgesetz (BDSG). Danach dürfen private Stellen öffentlich zugängliche Räume dann mit Videokameras überwachen, wenn dies zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Die Schilderungen des Petenten ließen Zweifel an der datenschutzrechtlichen Zulässigkeit der Überwachungsmaßnahme aufkommen. Daher wurde der für die Videoüberwachung verantwortliche Schützenverein zur Stellungnahme aufgefordert.

In der schriftlichen Stellungnahme des Vereins wurden im Wesentlichen die Angaben des Petenten bestätigt. So wurden in der Schießstätte selbst elf Kameras betrieben, die neben den Durchgangsbereichen vor allem die einzelnen Schießstände überwachten. Auch die Überwachung der Außenbereiche stellte sich wie vom Petenten beschrieben dar. Hierbei war eine der Kameras auf eine Behindertenrampe, die vor dem Eingangsbereich lag, sowie auf die davorgelegenen Parkplätze ausgerichtet.

Da die Videoüberwachung rund um die Uhr im Einsatz war, waren neben Passanten und Waldbesuchern im Außenbereich auch Vereinsmitglieder und sog. Gastschützen von der Videoüberwachungsmaßnahme betroffen.

Von Vereinsseite wurde argumentiert, dass die Videoüberwachung zur Wahrnehmung des Hausrechts sowie zur Wahrnehmung berechtigter Interessen erforderlich sei. So hätten in der Vergangenheit Schützen mit nicht zugelassenen Kalibern auf

Kugelfänge geschossen und dabei einen nicht unerheblichen Schaden verursacht. Dies sei insbesondere deshalb möglich gewesen, da bestimmte Personen einen Schlüssel zur Schießanlage haben und damit ohne Aufsicht die Anlage außerhalb der öffentlichen Zugangszeiten nutzen können.[21]

Daneben diene die Videoüberwachung vor allem der Diebstahlsicherung, die deshalb wichtig sei, weil auf der Anlage Waffen und Munition gelagert würden. Aus der sich hieraus ergebenden besonderen Sorgfaltspflicht ergebe sich die Erforderlichkeit der Überwachung der Schießstätte in vorliegendem Umfang. Schadensmeldungen an die Polizei wurden durch den Verein keine gestellt, sodass auch ein objektiv nachvollziehbarer Beleg hinsichtlich einer besonderen Gefährdungslage nicht erbracht werden konnte. Vielmehr berief man sich auf Einbrüche in umliegenden Schützenhäuser und argumentierte hieraus die Erforderlichkeit eines umfassenden Überwachungsszenarios.

Darüber hinaus wurden weitere Überwachungszwecke aufgeführt, die aber nicht objektiv nachvollziehbar belegt werden konnten und demnach unberücksichtigt bleiben mussten. Unter anderem seien auf der Anlage trotz des strikten Rauchverbots Zigarettenstummel gefunden worden. Sportschützen würden außerdem bewusst auf Leuchtkörper in den Hallen feuern. Außerdem würde mit Druckflaschen hantiert, was wegen der Explosionsgefahr ausdrücklich untersagt sei. Die Videoüberwachung könne in diesen Fällen entsprechende Erkenntnisse liefern.

Da eine abschließende Klärung hinsichtlich der datenschutzrechtlichen Zulässigkeit im Schriftverkehr nicht erreicht werden konnte, wurde die Anlage durch Mitarbeiter der Aufsichtsbehörde in einem Vor-Ort-Termin im Beisein mehrerer Vereinsmitglieder in Augenschein genommen. Im Verlauf des Termins konnte unter anderem festgestellt werden, dass einige Kameras unbemerkt ausgefallen waren, was in eklatantem Widerspruch zu der von Vereinsseite kommunizierten essentiellen Bedeutung der Videoüberwachung stand und Fragen an deren tatsächlichen Erforderlichkeit aufwarf. Dies wurde dem Verein auch dementsprechend kommuniziert.

Auch konnte für die Überwachung des Biergartens kein berechtigtes Interesse dargelegt werden. Ungeachtet dessen führt die datenschutzrechtliche Wertung bei der Überwachung gastronomisch genutzter Bereiche, in dem sich Besucher typischerweise über einen längeren Zeitraum aufhalten, regelmäßig zu dem Ergebnis, dass schutzwürdige Interessen der Betroffenen dem zulässigen Betrieb einer Videoüberwachung entgegen stehen. Auch die Überwachung der Parkplätze und der Behindertenrampe konnten mangels eines berechtigten Interesses nicht weiter datenschutzkonform betrieben werden. Rechtspositionen Dritter (z.B. Beschädigungen an Kraftfahrzeugen) spielen in diesem Zusammenhang nämlich regelmäßig keine Rolle.

Bei der Beurteilung, ob die Überwachung des Eingangsbereichs zwecks Einbruchsschutzes aufrecht erhalten bleiben kann, wurde dem Verein zugutegehalten, dass aufgrund der Lage der Schießstätte inmitten des Waldes zumindest außerhalb der Öffnungszeiten eine soziale Kontrolle (wie dies beispielsweise im Wohngebiet durch Nachbarn der Fall sein kann) nahezu ausgeschlossen und eine Gefährdungslage nicht

[21] So sieht § 11 Abs. 3 Allgemeine Waffengesetz-Verordnung (AWaffV) vor, dass eine zur Aufsichtsführung befähigte Person schießen darf, ohne selbst beaufsichtigt zu werden, wenn sichergestellt ist, dass sie sich allein auf dem Schießstand befindet.

per se von der Hand zu weisen ist. Auch wurde berücksichtigt, dass es sich bei dem Eingangsbereich um einen Bereich handelte, in dem Betroffene nur kurz beim Durchschreiten erfasst werden und damit lediglich ein marginaler Grundrechtseingriff vorliegt. Insoweit konnte die Überwachung dieses Bereichs vor dem Hintergrund des Einbruchsschutzes außerhalb der Öffnungszeiten zulässig betrieben werden.

Unzulässig war hingegen die Videoüberwachung des Innenbereichs der Schießstätte. So konnte die Argumentation, die Schießstände müssten aufgrund einer entsprechenden Gefahrgeneigtheit überwacht werden, nicht überzeugen. Insbesondere konnte von Seiten des Vereins nicht nachgewiesen werden, dass über die gesetzlich bestehenden Verkehrssicherungspflichten im Zusammenhang mit dem Betrieb einer Schießstätte hinaus weitere Sicherungsmaßnahmen in Form von Überwachungskameras erforderlich gewesen wären.

So ist nach § 11 Abs. 1 AWaffV das Schießen in der Schießstätte durch die verantwortlichen Aufsichtspersonen ständig zu beaufsichtigen. Daneben sind im Hinblick auf die Aufbewahrung von Waffen und/oder Munition besondere Sicherheitsbehältnisse vorgeschrieben (§§ 13 ff. AWaffV). Somit bedarf es einer unterstützenden Überwachung durch Videotechnik auch aus Sicht des Gesetzgebers augenscheinlich nicht.

Da durch den Verein auch keine Schadensereignisse nachgewiesen werden konnten, die auf das Vorhandensein einer besonderen Gefahrensituation hingewiesen hätten, war die Videoüberwachung als unzulässig zu werten.

Zu berücksichtigen war in diesem Zusammenhang auch, dass die von der Videoüberwachung betroffenen Schützen über den gesamten Aufenthalt in der Schießstätte gefilmt wurden. Damit verbunden ist ein – im Vergleich zu dem Eingangsbereich – wesentlich schwerwiegenderer Eingriff in das Persönlichkeitsrecht, dem die Betroffenen ausgesetzt waren.

Dass die Videoüberwachung auch nicht das richtige Mittel für die vom Verein kommunizierten Zwecke war, machte der Umstand deutlich, dass seit Inbetriebnahme der Kameras vor einigen Jahren kein einziger Schaden aufgedeckt bzw. verhindert werden konnte. Zudem fiel auf, dass in bestimmten Räumen bereits Kameras installiert worden waren, die sich im Zeitpunkt der Vor-Ort-Kontrolle noch im Rohbau befanden. Dies vermittelte den Eindruck einer reinen anlasslosen Gefahrenvorsorge, ohne dass sich die Vereinsvertreter über datenschutzrechtliche Gesichtspunkte irgendwelche Gedanken gemacht haben.

Da der Verein die Videoüberwachung ungeachtet der datenschutzrechtlichen Bewertung durch die Aufsichtsbehörde weiterhin betrieb, wurde die teilweise Einstellung der Videoüberwachung nach § 38 Abs. 5 BDSG angeordnet. Dieser Anordnung leistete der Verein dann zwar folge, musste jedoch darüber hinaus noch die Gebühr, welche sich im dreistelligen Bereich bewegte, aus dem Vereinsvermögen entrichten.

15.4 Datenschutzrechtliche Bewertung von Kameras in einer Apotheke

Im 25. Tätigkeitsbericht wurde unter Kapitel 19.8 die datenschutzrechtliche Bewertung einer Videoüberwachungsmaßnahme in einer Apotheke und die in diesem Zusammenhang zur Herstellung eines datenschutzkonformen Zustands ergriffenen aufsichtsbehördlichen Maßnahmen dargestellt.

Zusammenfassend konnte nach Auffassung des Datenschutzzentrums die Videoüberwachung im Verkaufsraum (Offizin) und des im nur für Mitarbeiter zugänglichen Teil der Apotheke befindlichen Betäubungsmittelschranks nicht im Sinne des § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) auf eine wirksame Einwilligung der Betroffenen oder eine gesetzliche Grundlage gestützt werden.

§ 4 Abs. 1 BDSG

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

Da sich der Apotheker dem Ergebnis der aufsichtsbehördlichen Bewertung der von ihm betriebenen Videoüberwachung nicht anschließen konnte, wurde die Einstellung der Videoüberwachung des Betäubungsmittelschranks und der Offizin auf Grundlage von § 38 Abs. 5 BDSG durch Bescheid angeordnet. Gegen diesen Bescheid wurde Klage beim Verwaltungsgericht des Saarlandes erhoben.

Mit Urteil vom 29. Januar 2016 - 1 K 1122/14 - wurde der Bescheid des Datenschutzzentrums durch das Verwaltungsgericht insoweit aufgehoben, als die Videoüberwachung des Betäubungsmittelschranks gestützt auf Einwilligungserklärungen der Mitarbeiter zulässig erfolgen könne.

Hinsichtlich der Videoüberwachung in der Offizin teilte das Gericht jedoch die Auffassung des Datenschutzzentrums, dass ein berechtigtes Interesse, mithin eine konkrete Gefährdungslage, seitens des Apothekenbetreibers nicht ausreichend dargelegt worden ist. In welchem Umfang Medikamente oder sonstige Handelswaren abhandengekommen sind, ob eventuelle Fehlbestände überhaupt auf Diebstähle zurückzuführen waren und ob diese gerade im Verkaufsraum stattgefunden haben, wurde durch den Apotheker auch im Verfahren nicht objektiv überprüfbar konkretisiert.

Aufgrund der klägerseitig unzureichenden Substantiierung des Sachvortrages kam das Gericht ebenfalls zu dem Ergebnis, dass die Überwachungsmaßnahme in der Offizin nicht als erforderlich zur Wahrnehmung des Hausrechts im Sinne des § 6b Abs. 1 Nr. 2 BDSG bezeichnet werden konnte. Eine Abwägung der schutzwürdigen Interessen Betroffener mit den Interessen des Überwachenden war somit nicht mehr erheblich.

Die zur Legitimation der Überwachung des Betäubungsmittelschranks erst im Verfahren vorgelegten Einwilligungserklärungen würden nach Auffassung des Gerichts grundsätzlich auf der freien Entscheidung der betroffenen Arbeitnehmer beruhen. Dass ein abhängiges Beschäftigungsverhältnis gegeben war, dem ein Weisungsrecht

des Arbeitgebers immanent ist, stehe - auch im Hinblick auf die Rechtsprechung des Bundesarbeitsgerichts[22] - der Möglichkeit der Annahme einer unbeeinflussten Disposition des Arbeitnehmers über das eigene Recht auf informationelle Selbstbestimmung grundsätzlich nicht entgegen. Sofern der Arbeitnehmer im Hinblick auf § 4a Abs. 1 BDSG über den Zweck des Umgangs ausreichend informiert wird, könne dieser eine Einwilligung somit freiwillig und wirksam erklären und diese eben auch nachträglich mit Wirkung für die Zukunft widerrufen. Das Verwaltungsgericht betonte in diesem Zusammenhang ausdrücklich, dass der datenschutzrechtlichen Kommentarliteratur, soweit dort das Merkmal der Freiwilligkeit im Zusammenhang mit Einwilligungserklärungen im Beschäftigungsverhältnis aufgrund eines anzunehmenden Machtungleichgewichts apodiktisch verneint wird[23], nicht zuzustimmen sei.

Im Übrigen sei die Videoüberwachung des Betäubungsmittelschranks für sich genommen auch derart punktuell, dass kein unverhältnismäßiger Eingriff in das Persönlichkeitsrecht der Mitarbeiter mit ihr einhergehe.

Den Erwägungen des Verwaltungsgerichts war dahingehend zuzustimmen, dass eine Einwilligung des Arbeitnehmers in einen Datenumgang im Beschäftigungsverhältnis nicht per se unwirksam ist, jedoch war die grundsätzliche Annahme einer voraussetzungslosen Wirksamkeit jeglicher Einwilligungserklärung wenig überzeugend. Auch die Bezugnahme des Verwaltungsgerichts auf die Urteile des Bundesarbeitsgerichts war vor dem Hintergrund nicht nageliegend, als die Umstände der Einholung einer Einwilligungserklärung im Beschäftigungsverhältnis für die arbeitsgerichtlich zu entscheidende Frage nicht von Bedeutung war.

Daher wurde seitens der Aufsichtsbehörde im März 2016 ein Antrag auf Zulassung der Berufung nach § 124 Abs. 2 Verwaltungsgerichtsordnung (VwGO) gestellt.

Begründet wurde dies im Einzelnen damit, dass für die Klärung der Frage nach dem Merkmal der Freiwilligkeit der Einwilligung die Umstände des Einzelfalls entscheidungserheblich waren und seitens des Gerichts außer Acht gelassen wurden. Weiterhin waren für den zu entscheidenden Sachverhalt, trotz gegenläufiger Annahme des Gerichts, die an einen Erklärungstext anzulegenden formalen Anforderungen des § 4a Abs. 1 S. 2 BDSG nicht umgesetzt.

Offensichtlich gegen die Annahme einer Abgabe der vorliegenden Einwilligungserklärungen ohne jeglichen Zwang sprachen eben der Zweck der Videoüberwachung und die ursprünglich damit verbundene Eingriffstiefe.

- Da der Apothekenbetreiber letztlich die Arbeitnehmer für den unbelegten Warenschwund verantwortlich machte und diese somit seitens ihres Arbeitgebers einer präventiven und repressiven Verhaltenskontrolle ausgesetzt wurden, hatten die Mitarbeiter die Wahl entweder in ihre eigene Überwachung einzuwilligen oder sich durch eine Verweigerung oder einen späteren

[22] Urteile des Bundesarbeitsgerichts vom 11. Dezember 2014 - 8 AZR 1010/13 - und 19. Februar 2015 - 8 AZR 1011/13 - zur Zulässigkeit des Widerrufs einer Einwilligungserklärung des Arbeitnehmers in seine Veröffentlichung in einem Werbefilm des Arbeitgebers nach Beendigung des Beschäftigungsverhältnisses.

[23] Beispielsweise Simitis, in: Simitis, Bundesdatenschutzgesetz 8. Auflage, § 4a Rn. 62.

Widerruf der Einwilligung zwangsläufig dem Vorwurf der Täterschaft auszusetzen.

- Im Hinblick auf die datenschutzrechtliche Zulässigkeit der Videoüberwachung - als Verfahren der automatisierten Datenverarbeitung - wäre aufgrund der Verweigerung der Einwilligung oder deren nachträglichen Widerruf durch einen einzigen Arbeitnehmer die Überwachung des Betäubungsmittelschranks datenschutzrechtlich unzulässig geworden. Insoweit konnte auch in diesem Zusammenhang nicht davon ausgegangen werden, dass es tatsächlich in der Absicht des Arbeitgebers lag, den Arbeitnehmern eine freie Wahl zu überlassen.

  Auch das Verwaltungsgericht hatte diesbezüglich in seiner Entscheidung ausdrücklich ausgeführt, dass es die Einwilligung von Arbeitnehmern als datenschutzrechtliche Legitimationsgrundlage für eine Überwachungsmaßnahme für eher ungeeignet hielt.

- Der vorliegende Text der Erklärungen ließ keinen Zweifel daran, dass mithilfe der Einwilligungen die Videoüberwachung in der gesamten Apotheke legitimiert werden sollte. Insoweit beabsichtigte der Apothekenbetreiber mithilfe der Einwilligungserklärung ursprünglich eine wesentlich weiträumigere und damit eingriffsintensivere Überwachung zu legitimieren, der sich die Mitarbeiter nicht ohne Weiteres hätten entziehen können.

  Der Ansicht des Gerichts, dass mit der Videoüberwachung des Betäubungsmittelschranks aufgrund der räumlichen Begrenztheit der Überwachung lediglich ein geringer Eingriff in das Persönlichkeitsrecht der Arbeitnehmer verbunden ist, konnte daher nicht zugestimmt werden.

- Weiterhin blieb zweifelhaft, ob letztlich alle betroffenen Arbeitnehmer eine Erklärung abgegeben hatten. Die Tatsache, dass die im Verwaltungsverfahren vorgelegte tabellarische Unterschriftenliste und die im Verwaltungsgerichtsverfahren nachgereichten Einzelerklärungen eine unterschiedliche Anzahl an erklärenden Personen umfasste, kann zwar auch auf Personalfluktuationen zurückgeführt werden, jedoch wurde im Gerichtsverfahren nicht geklärt, inwiefern gewährleistet werden kann, dass alle Betroffenen eingewilligt haben.

Neben der in Zweifel zu ziehenden Freiwilligkeit entsprach der konkrete Erklärungsgehalt der vorliegenden Einwilligungen auch nicht den formalen Vorgaben des § 4a Abs. 1 S. 2 BDSG.

Da weder der intendierte Zweck, mithin die Verhaltenskontrolle der Mitarbeiter, noch die konkrete Ausgestaltung der Überwachungsmaßnahme (Löschfristen, zugriffsberechtigte Personen, Umstände der Auswertung etc.) in der textlich knappen Erklärung benannt oder gar erläutert wurden, konnte nicht von einer hinreichenden inhaltlichen Bestimmtheit ausgegangen werden. Die Befürchtung einer zweckändernden Nutzung der Aufnahmen, beispielsweise für eine unzulässige Leistungskontrolle, war daher nicht von der Hand zu weisen. Zudem war aufgrund der Sachlage auch ein Hinweis auf die Folgen der Verweigerung der Einwilligung im Sinne der Vorschrift in der Erklärung unabdingbar.

Zum Ende des Berichtszeitraums hat das Oberverwaltungsgericht noch nicht über den Antrag auf Zulassung der Berufung entschieden.

15.5 Videoüberwachung in einem Saunaclub

Ein Mitarbeiter eines Saunaclubs wandte sich mit einer Eingabe an unsere Dienststelle und wies auf eine seiner Auffassung nach unzulässige Videoüberwachungsmaßnahme im Küchenbereich der Lokalität hin. Im Rahmen einer unangekündigten Vor-Ort-Kontrolle durch Mitarbeiter unserer Dienststelle stellte sich heraus, dass tatsächlich der gesamte Küchenbereich und somit auch die dort arbeitenden Mitarbeiter permanent videoüberwacht wurden. Darüber hinaus zeigte sich, dass es dort nicht bei einer Videoüberwachungsmaßnahme geblieben ist. Das gesamte Anwesen, angefangen von den Parkplätzen, die gesamte Außenanlage über den Eingangsbereich, Buffet- und Barbereich, Durchgangs- und Ruhebereiche, sogar die Umkleiden wurden mit insgesamt 28 Kameras videografiert. Die Live-Bilder sämtlicher im Einsatz befindlicher Kameras liefen im Büro des Betriebsleiters auf. Darüber hinaus fand eine Speicherung der Aufnahmen statt.

Als erste Maßnahme wurde auf unsere Veranlassung hin die Kamera in der Küche, mit der eine permanente Mitarbeiterüberwachung erfolgte, sowie die Kameras in den Umkleidebereichen aufgrund des besonders tiefen Eingriffs in die Intimsphäre der Betroffenen deaktiviert. Dem Betreiber wurde sodann die Gelegenheit zur schriftlichen Stellungnahme eingeräumt, aufgrund welcher Gegebenheiten die anderen Kameras rechtmäßig betrieben sein sollten.

Im Rahmen der Stellungnahme wurde vorgetragen, die Videoüberwachung innerhalb des Gebäudes diene dem Zweck, Vandalismusschäden entgegenzuwirken, das Verhalten der Besucher dahingehend zu beeinflussen, sich rechtskonform zu verhalten, Missstände bei den Mitarbeitern in der Küche aufzudecken und im Falle eines Einbruchs eine Täteridentifizierung zu ermöglichen. Außerhalb des Gebäudes soll mithilfe der Videoüberwachung Belästigungen der Mitarbeiterinnen und auch Beschädigungen an Fahrzeugen der Kunden begegnet werden können. Ergänzend wurde mitgeteilt, dass in einigen Bereichen des Betriebes die Überwachung bereits eingeschränkt bzw. ganz eingestellt worden sei.

In Rahmen der datenschutzrechtlichen Bewertung wurde hinsichtlich der noch aktivierten Kameras festgestellt, dass sich die Videoüberwachungsmaßnahme mit Ausnahme der Rezeption, in allen für Kunden zugänglichen Aufenthaltsbereichen des Clubs als unzulässig darstellt.

Soweit die mit Videokameras überwachten Bereiche nicht allein von Mitarbeitern, sondern auch von den Besuchern des Clubs betreten werden können, handelt es sich – unabhängig davon, dass ein Zutritt erst nach Zahlung eines Eintrittsgeldes erfolgen darf – um öffentlich zugängliche Räume im Sinne des § 6b Bundesdatenschutzgesetz (BDSG). Nach § 6b Abs. 1 dürfen nicht-öffentliche Stellen öffentlich zugängliche Räume nur dann mit optisch-elektronischen Einrichtungen beobachten, wenn dies

- zur Wahrnehmung des Hausrechts (Nr. 2) oder

- zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (Nr. 3)

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

Hinsichtlich der öffentlich zugänglichen Aufenthaltsbereiche in dem Club konnte der Betreiber bereits kein berechtigtes Interesse an einer Videoüberwachung darlegen, da es keine nachvollziehbaren Belege dafür gab, dass es zu den von ihm behaupteten Schadenshandlungen gekommen ist bzw. solche zu erwarten waren.

Entscheidender Gesichtspunkt für die Unzulässigkeit der Überwachung in diesem Bereich war indes, dass der Videoüberwachung schutzwürdige Interessen der von der Maßnahme betroffenen Personen entgegenstanden. Gerade in einem solchen Club, in dem aufgrund des konkreten Betriebszwecks der Aufenthalt mit einer besonderen Sensibilität verbunden ist, greift eine Videoüberwachung besonders tief in das Persönlichkeitsrecht der Betroffenen ein, so dass deren Interessen an einem unbeobachteten Aufenthalt in dem Club gegenüber den Überwachungsinteressen des Betreibers überwiegen.

Soweit die Videoüberwachung auch Mitarbeiterbereiche erfasste, verbunden mit dem Zweck, Straftaten durch Mitarbeiter aufzudecken, war diese Maßnahme an der Regelung des § 32 BDSG zu messen. Nach Abs. 1 S. 2 dieser Vorschrift dürfen zur Aufdeckung von Straftaten 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 zu deren Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten am Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Eine nur präventive dauerhafte Videoüberwachung ohne konkreten Grund genügt diesen Anforderungen grundsätzlich nicht. Zu verlangen ist, dass sich das Interesse des Arbeitgebers an einer Videoüberwachung wegen des Vorliegens konkreter Anhaltspunkte für Straftaten als überwiegend erweist. Davon konnte vorliegend bereits deshalb nicht ausgegangen werden, weil auch hier eine konkrete Gefährdungslage nicht ansatzweise belegt worden ist. Die Überwachung des nur für Arbeitnehmer zugänglichen Bereichs der Bar und der Rezeption am Eingang war daher gleichfalls als datenschutzrechtlich unzulässig anzusehen. Auch, weil die Arbeitnehmer dort einem permanenten Überwachungsdruck ausgeliefert waren.

Lediglich in Bezug auf die nachgewiesenen Schäden an der Gebäudefassade und an der Eingangstür sowie der mithilfe der Videoüberwachung dokumentierten und den Strafverfolgungsbehörden zur Kenntnis gebrachten Schadenshandlung im Eingangsbereich an der Rezeption konnte der Betreiber ein berechtigtes Interesse an einer Videoüberwachung belegen.

Da der Betreiber sich der aufsichtsbehördlichen Rechtsauffassung nicht anschließen konnte, wurde ihm unter Androhung und aufschiebend bedingter Festsetzung von Zwangsgeldern für den Fall der Zuwiderhandlung aufgegeben, die noch in Betrieb befindliche Videoüberwachung im Innenbereich während der Öffnungszeiten einzustellen, die zur Sicherung der Fassade des Gebäudes installierte Videoüberwachung

einzustellen, soweit die Erfassung einen Toleranzbereich von einem Meter zur Hausfassade überschreitet und die Kamera im Empfangsbereich so auszurichten, dass keine Mitarbeiter permanent überwacht werden. Daneben wurde angeordnet, dass die im Zusammenhang mit dem Betrieb einer datenschutzkonformen Videoüberwachung notwendigen technisch organisatorischen Maßnahmen umzusetzen sind und auf den Umstand der Videoüberwachung so hinzuweisen ist, dass vor Betreten des überwachten Bereichs eine Kenntnisnahme möglich ist.

Erst nachdem bereits erste Zwangsgelder fällig gestellt worden waren, teilte der Betreiber mit, dass alle Anordnungsgegenstände umgesetzt worden sind und legte die angeforderten Nachweise vor.

15.6 Zusammenarbeit mit dem Landesverwaltungsamt im Bereich Glücksspielwesen

Das Landesverwaltungsamt (LaVA), als dem Ministerium für Inneres und Sport nachgeordnete Landesaufsichtsbehörde im Bereich des Glückspielwesens, hat das Unabhängige Datenschutzzentrum im Berichtszeitraum auf Videoüberwachungsmaßnahmen in Spielhallen und Gastronomiebetrieben mit Spielautomaten aufmerksam gemacht. Quasi als Beifang zu im Rahmen der gesetzlichen Aufgabenzuweisung erfolgenden Vorortkontrollen stießen die Mitarbeiter des LaVA auf datenschutzrechtlich fragwürdige Videoüberwachungsmaßnahmen. Fehlende Hinweisschilder, weiträumige Überwachungen von Straßen und Gehwegen sowie ein exzessiver Kameraeinsatz auf engstem Raum waren dabei für eine Unterrichtung des Datenschutzzentrums ausschlaggebend.

Im Wege eines gemeinsamen Besprechungstermins zwischen Glücksspiel- und Datenschutzaufsichtsbehörde wurden die Feststellungen des LaVA, die Grundlagen einer datenschutzrechtlich zulässigen Videoüberwachung im Zusammenhang mit dem Betrieb von Spielhallen und dem Aufstellen von Spielautomaten in Gastronomiebetrieben erörtert. Dem Datenschutzzentrum wurde im Anschluss an das Treffen die von den Mitarbeitern des LaVA kontrollierten Stellen und die dabei getroffenen Feststellungen zur Kenntnis gebracht. Anhand der vorgelegten Informationen war bereits abzusehen, dass aller Voraussicht nach keine der noch zu prüfenden Stellen eine datenschutzkonforme Videoüberwachung betreibt. Regelmäßig wurden Innenräume inklusive gastronomisch genutzter Bereiche sowie Gehwege und Straßen vor den Betriebsstätten großflächig videoüberwacht.

Nach Einleitung von Verwaltungsverfahren wurden die vom LaVA benannten Stellen unter Zuhilfenahme eines standardisierten Fragenkatalogs zur Stellungnahme aufgefordert. Mehrheitlich erfolgte weder eine Reaktion auf den übersandten Fragenkatalog noch auf das nachfolgende Erinnerungsschreiben, so dass die angeschriebenen Stellen zur Vorbereitung von Auskunftsbescheiden nach § 38 Abs. 3 Bundesdatenschutzgesetz (BDSG) gemäß § 28 Saarländisches Verwaltungsverfahrensgesetz (SVwVfG) angehört wurden. Erst danach erfolgte in allen Fällen zumindest in Teilen eine Stellungnahme. Allen abgegebenen Stellungnahmen war zu entnehmen, dass

datenschutzrechtliche Erwägungen bei der Implementierung der Videoüberwachungsmaßnahmen nahezu keine Rolle gespielt haben und den Inhabern und Geschäftsführern die Rechtslage gänzlich unbekannt war. Darüber hinaus wurden die Videokameras in einigen Betriebsstätten reflexartig demontiert, ohne dass dies zu diesem Zeitpunkt gefordert worden wäre.

Im Hinblick darauf, dass für einige der zu prüfenden Stellen spezifische Unfallverhütungsvorschriften Anwendung fanden, war mitunter sogar von einer Verpflichtung zur Videoüberwachung auszugehen. Nach § 2 in Verbindung mit § 6 Unfallverhütungsvorschrift für Spielhallen, Spielcasinos und Automatensäle von Spielbanken (DGUV Vorschrift 20)[24] ist u.a. für Spielhallen mit mehr als drei Geldspielgeräten eine optische Raumüberwachungsanlage verpflichtend zu betreiben.

§ 6 Abs. 1 DGUV Vorschrift 20

Jede Spielhalle, jedes Spielcasino und jeder Automatensaal von Spielbanken muss mit einer optischen Raumüberwachungsanlage ausgerüstet sein. Auf die optische Raumüberwachungsanlage ist im Eingangsbereich deutlich erkennbar und dauerhaft hinzuweisen.

Der für Videoüberwachungsmaßnahmen in öffentlich zugänglichen Bereichen grundsätzlich heranzuziehende § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG) wird hierbei nach § 1 Abs. 3 S. 1 BDSG von der Unfallverhütungsvorschrift der Berufsgenossenschaft verdrängt.

§ 1 Abs. 3 S. 1 BDSG

Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.

Da in den berufsgenossenschaftlichen Vorschriften eben nicht vorgegeben wird, wie diese Videoüberwachung im Einzelnen rechtskonform auszugestalten ist, ist es notwendig, diese Regelung verfassungskonform zu interpretieren. Im Übrigen bleiben formalrechtliche Regelungen des BDSG in diesem Zusammenhang vollumfänglich anwendbar.

Soweit lediglich von einem Gastronomiebetrieb mit Geldspielautomaten auszugehen war oder bei einer Spielhalle aufgrund der Anzahl der aufgestellten Spielautomaten die DGUV Vorschrift 20 keine Anwendung fand, war für die datenschutzrechtliche Bewertung der Videoüberwachung ausschließlich § 6b BDSG maßgebend.

§ 6b Abs. 1 BDSG

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

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

[24] Auf Grundlage des § 15 Siebtes Buch Sozialgesetzbuch (SGB VII) können die Berufsgenossenschaften als Träger der gesetzlichen Unfallversicherung Unfallverhütungsvorschriften als autonomes Recht erlassen.

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

Im Hinblick auf eine eingeholte Stellungnahme der örtlich zuständigen Polizeiinspektion konnte von einer Gefährdungslage für alle in räumlicher Nähe zueinander liegenden Stellen ausgegangen werden. Die in der Vergangenheit in einzelnen Betrieben stattgefundenen und polizeilich dokumentierten Delikte, wie Diebstähle, Raubüberfälle und Körperverletzungen, sprachen für eine abstrakte Gefährdungslage. Auch für die Betriebe, die bisher noch nicht polizeilich in Erscheinung getreten sind, wäre insoweit eine hinreichende Viktimisierungsgefahr zu bejahen.

Vor diesem Hintergrund machte es somit keinen Unterscheid, ob die Videoüberwachung nach § 6 DGUV Vorschrift 20 gesetzlich vorgeschrieben oder fakultativ auf Grundlage einer gegebenen abstrakten Gefährdungslage nach § 6b BDSG zulässig betrieben werden kann.

Jedoch waren schutzwürdige Interessen der von der Videoüberwachung betroffenen Kunden, Mitarbeiter und auch unbeteiligten Passanten miteinzubeziehen. Die durchweg anzutreffende Überwachung gastronomisch genutzter Bereiche, von festen Arbeitsplätzen oder des öffentlichen Verkehrsraums im Umfeld der Betriebe konnte angesichts dessen weder im Rahmen des § 6 DGUV Vorschrift 20 noch des § 6b Abs. 1 BDSG als datenschutzrechtlich zulässig erachtet werden. Unter Beachtung des in § 3a BDSG normierten Datensparsamkeitsgebots wäre in diesem Zusammenhang allenfalls eine Videoüberwachung der Automaten und von Durchgangsbereichen denkbar.

Zudem konnte den Stellungnahmen entnommen werden, dass weder formalrechtliche Vorgaben umgesetzt oder revisionssichere Maßnahmen zur Datensicherheit ergriffen wurden:

- In keinem Fall konnte das gesetzlich vorgeschriebene Verfahrensverzeichnis nach § 4e in Verbindung mit § 4g Abs. 2 oder 2a BDSG vorgelegt werden.
- Auch Schilder im Sinne des § 6b Abs. 2 BDSG beziehungsweise § 6 Abs. 1 S. 2DGUV Vorschrift 20, die vor Betreten des überwachten Bereichs auf den Umstand der Videoüberwachung hinweisen, waren nicht oder nicht deutlich erkennbar angebracht.
- Obwohl teilweise auch dritte Unternehmen mit der Ausführung oder Wartung der Videoüberwachungsmaßnahmen beauftragt waren, waren Verträge über eine Auftragsdatenverarbeitung im Sinne des § 11 Abs. 2 BDSG nicht vorhanden.
- Schriftliche Festlegungen von technischen und organisatorischen Maßnahmen im Sinne des § 9 BDSG und der Anlage dazu gab es in keinem einzigen Fall.
- Die Speicherung von Aufnahmen für mehrere Wochen war die Regel.
- In einzelnen Betrieben wäre vor dem Hintergrund der großen Anzahl angebrachter Videokameras notwendigerweise eine Vorabkontrolle nach § 4d Abs. 5 S. 1 BDSG durch betriebliche Beauftragte für den Datenschutz im Sinne § 4 Abs. 1 S. 6 BDSG vorzunehmen gewesen.

Aufgrund der Vielgestaltigkeit der Verstöße gegen datenschutzrechtliche Vorgaben und der teilweise mangelnden Kooperationsbereitschaft der Betriebsinhaber wird die Aufarbeitung der einzelnen Fälle über den Berichtszeitraum hinaus andauern.

15.7 Webcams

Der Einsatz von Webcams dient dazu, dem Beobachter einen Eindruck der aktuellen Gegebenheiten vor Ort zu vermitteln, sei es die Wetterlage oder etwa der aktuelle Besucherstrom in Städten. Soweit lediglich Landschaftsaufnahmen gefertigt werden, auf denen einzelne Personen aufgrund der räumlichen Distanz oder der Ausrichtung nicht zu erkennen sind, ist der Einsatz von Webcams datenschutzrechtlich unbedenklich.

Neuerdings installieren zunehmend Privatleute neben Videoüberwachungskameras auch Webcams an ihren Anwesen, zum Teil auch mitten in Wohngebieten. Die Anlagenbetreiber lassen dabei häufig datenschutzrechtliche Gesichtspunkte außer Acht. Die Bilder werden auf Internetseiten zum Abruf zur Verfügung gestellt. Dort können oftmals in Echtzeit das anliegende Wohngebiet mitsamt Nachbargrundstücken sowie Gehwegen und Straßen beobachtet werden. Dies führt dazu, dass die Nachbarn bei allen Bewegungen im Freien beobachtet werden und jeder dies über einen Internetabruf nachvollziehen kann.

Beim Einsatz von Webcams werden regelmäßig öffentlich zugängliche Bereiche überwacht, so dass sich die datenschutzrechtliche Zulässigkeit nach § 6b Bundesdatenschutzgesetz (BDSG) richtet.

§ 6b Abs. 1 BDSG

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

1. *(...),*
2. *zur Wahrnehmung des Hausrechts oder*
3. *zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke*

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

Die Überwachung von Nachbargrundstücken, also von Bereichen, die nicht öffentlich zugänglich sind, da sie nach dem erkennbaren Willen des Verfügungsberechtigten nicht von jedem betreten werden dürfen, richtet sich demgegenüber nach § 28 Abs. 1 Nr. 2 BDSG, wobei in diesen Fällen die gleichen Bewertungsmaßstäbe an die Zulässigkeit des Webcam-Einsatzes zu richten sind wie bei der Beobachtung öffentlich zugänglicher Bereiche.

Da die Überwachung in der Regel über die eigene Grundstücksgrenze hinausgeht, kann die Beobachtung nicht zur Wahrnehmung des Hausrechts erfolgen.

Häufig teilen die Anlagenbetreiber mit, der Einsatz der Webcam diene der Wetterdokumentation. Hierfür ist die Beobachtung des Wohnumfelds nicht erforderlich, da es in diesen Fällen ausreichend ist, die Kamera in Richtung des Himmels auszurichten

und so eine Erhebung personenbezogener Daten nahezu ausgeschlossen werden kann.

Demgegenüber bestehen in der Regel auch erhebliche Anhaltspunkte dafür, dass die schutzwürdigen Interessen der betroffenen Nachbarn, Passanten, Verkehrsteilnehmer etc. überwiegen. Die Überwachung der Betroffenen bei der Verrichtung ihrer Alltagstätigkeiten, z.B. wenn sich die Nachbarn auf der Terrasse gerade sonnen, in Verbindung mit der Möglichkeit, diese Beobachtung weltweit über das Internet abrufen zu können, stellt einen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht einer Vielzahl von Betroffenen dar. Dass die Aufnahmen oftmals in Echtzeit dargestellt werden, vertieft den Eingriff.

Die Anlagenbetreiber vertreten häufig die Ansicht, dass auf den dargestellten Aufnahmen keine Personen zu erkennen sind und das BDSG schon deshalb nicht anwendbar sei. Allerdings wird verkannt, dass es im Falle der Videoüberwachung nicht zwingend darauf ankommt, dass individuelle Körpermerkmale und Gesichter zu erkennen sind. Vielmehr kann ein Personenbezug bereits dann vorliegen, wenn sich durch das Beobachten von Bewegungsabfolgen Rückschlussmöglichkeiten auf einzelne Personen ergeben oder Sachumstände wie Kfz-Kennzeichen oder Gärten erfasst werden, die Rückschlüsse auf individuelle Verhältnisse ermöglichen. Dies wirkt umso schwerer, als durch das Veröffentlichen der Bilder im Internet der Empfängerkreis um ein Vielfaches größer ist und mit entsprechendem Hintergrundwissen ein Personenbezug bereits anhand weniger Anhaltspunkte hergestellt werden kann. Dies gilt gerade im nachbarschaftlichen Kontext. Auf eine tatsächlich erfolgreiche Identifizierung im Einzelfall kommt es in diesem Zusammenhang nicht an (vgl. VG Schwerin, Beschluss vom 18. Juni 2015 – 6 B 1637/15 SN).

Im Ergebnis lässt sich feststellen, dass bei dem Einsatz einer Webcam regelmäßig dann datenschutzrechtliche Bedenken bestehen, wenn ein Personenbezug Betroffener nicht ausgeschlossen werden kann. Dies kann nicht nur in Wohngebieten besonders problematisch sein, sondern kann auch bei Landschaftsaufnahmen zu unzulässigen Persönlichkeitseingriffen führen, wenn die Kamera etwa so eingestellt ist, dass Spaziergänger etc. ohne weiteres erkennbar sind.

Da der Betrieb von Webcams weder nach § 6b BDSG noch nach § 28 BDSG zulässig erfolgen kann, ist darauf zu achten, dass regelmäßig keine personenbezogenen bzw. –beziehbaren Daten unbeteiligter Dritter im Internet zum Abruf zur Verfügung gestellt werden.

Unproblematisch kann eine Webcam also beispielsweise zum Zwecke der Wetterdokumentation eingesetzt werden, wenn das Objektiv auch tatsächlich nach oben in Richtung Himmel ausgerichtet ist. Auch klassische Landschaftsaufnahmen, auf denen Personen nicht erkennbar sind, da die Kameras in größerer Entfernung zum beobachteten Umfeld angebracht sind, können in der Regel ohne Weiteres betrieben werden.

Alternativ ist beim Einsatz von Webcams darauf zu achten, dass eine entsprechend niedrige Auflösung gewählt wird, bei der sichergestellt ist, dass auch mit vorhandenem Zusatzwissen keine Personen identifiziert werden können. Hier muss jedoch berücksichtigt werden, dass Betroffenen gegebenenfalls ein zivilrechtlicher Abwehr-

und Beseitigungsanspruch zusteht, wenn diese aufgrund der örtlichen Gegebenheiten objektiv nachvollziehbar eine Überwachung befürchten müssen.

15.8 Drohnen

15.8.1 Genehmigungsverfahren bei der Luftfahrtbehörde

Im 25. Tätigkeitsberichtsbericht wurde im Kapitel 19.5.1 dargestellt, welche luftverkehrs- und datenschutzrechtlichen Vorgaben von Drohnenbetreibern zu beachten sind und wie der Prozess der Beantragung einer Aufstiegsgenehmigung bei der saarländischen Luftfahrtbehörde, welche im Rahmen des Genehmigungsverfahrens auch die Gefährdung datenschutzrechtlicher Vorschriften durch den Drohneneinsatz zu bewerten hat[25], konzipiert ist.

In diesem Zusammenhang wurde kritisch angemerkt, dass sich im Hinblick auf die Ausgestaltung des Antragsvordrucks der in § 20 Abs. 4 S. 1 Luftverkehrs-Ordnung (LuftVO) gesetzlich zugewiesene Prüfungsauftrag in der Selbstverpflichtung des Antragsstellers erschöpfte datenschutzrechtliche Bestimmungen nicht zu verletzen.

§ 20 Abs. 4 S. 1 LuftVO

Die Erlaubnis wird erteilt, wenn die Nutzung nicht zu einer Gefahr für die Sicherheit des Luftverkehrs oder die öffentliche Sicherheit oder Ordnung führen kann und insbesondere durch den Aufstieg von unbemannten Luftfahrtsystemen die Vorschriften über den Datenschutz nicht verletzt werden.

Weiterhin wurde zum damaligen Zeitpunkt seitens der Luftfahrtbehörde der Vorschlag des Datenschutzzentrums zur Erstellung einer gemeinsamen Informationsbroschüre, welche den Antragstellern die Voraussetzungen und Pflichten im Zusammenhang mit einem datenschutzkonformen Drohneneinsatz erläutern könne, nicht aufgegriffen.

Ein im Berichtszeitraum unter Hinweis auf den 25. Tätigkeitsbericht und den hinsichtlich des Einsatzes von Drohnen durch Privatpersonen ergangenen Beschluss des Düsseldorfer Kreises vom 15./16. September 2015[26] an die saarländische Luftfahrtbehörde herangetragenes erneutes Gesprächsangebot wurde erfreulicherweise angenommen.

Im Rahmen des Gesprächstermins wurde sodann erläutert, in welcher Tiefe eine datenschutzrechtliche Prüfung der Angaben im Antrag auf Erteilung einer Aufstiegsgenehmigung durch die Luftfahrtbehörde erfolgt. Wenig überraschend war in diesem

---

[25] Für die im damaligen Bericht dargestellten, für Drohnenbetreiber maßgeblichen luftverkehrsrechtlichen Regelungen sind verschiedene Änderungen zu beachten; die Luftverkehrs-Ordnung (LuftVO) wurde am 29. Oktober 2015 mit Wirkung zum 6. November 2015 novelliert. Die im Rahmen der beantragten Aufstiegsgenehmigung notwendige Prüfung der Einhaltung datenschutzrechtlicher Vorgaben ist mittlerweile in § 20 Abs. 4 S. 1 LuftVO normiert.

[26] Siehe Kapitel 26.1.

Zusammenhang die Klarstellung, dass dort eine grundsätzlich fachfremde datenschutzrechtliche Prüfung nicht möglich ist und man auf sich auf die Erklärung des Antragstellers im Antragsvordruck verlasse, dass durch die beantragte Nutzung des Luftraums mit unbemannten Luftfahrtsystemen datenschutzrechtliche Bestimmungen nicht verletzt werden.

Dementsprechend wurden mögliche Optionen diskutiert, inwiefern datenschutzrechtlichen Gesichtspunkten bei der Antragsbearbeitung ein größeres Gewicht verschafft werden kann.

Da eine Ergänzung des zwischen den Luftfahrtbehörden des Bundes und der Länder konsolidierten Antragsvordrucks um explizite datenschutzrechtliche Fragestellungen außer Frage stand, kam lediglich das Hinzufügen eines Informationsblatts zum Antrag in Betracht, dem der Antragsteller die datenschutzrechtlichen Vorgaben entnehmen kann. Aufgrund der konstruktiven Zusammenarbeit mit der Luftfahrtbehörde konnte besagtes Informationsblatt sehr zeitnah abgestimmt und dem Antrag beigefügt werden.[27]

Im Nachgang zur Anpassung des Antragsvordrucks trat im Zusammenhang mit den nach § 4d Abs. 1 BDSG zahlreich abgegebenen Meldungen deutlich zu Tage, dass den gewerblichen Drohnennutzern die datenschutzrechtlichen Gegebenheiten grundsätzlich nicht oder jedenfalls kaum bekannt waren. So konnten die Drohnennutzer durch vorbeugende Beratung hinsichtlich der Obliegenheiten eines datenschutzkonformen Geräteeinsatzes sensibilisiert werden.

15.8.2 Drohneneinsatz im Auftrag einer öffentlichen Stelle

Seitens einer Landesbehörde wurde geplant, den Auftrag für einen im Zusammenhang mit einer Sanierungsmaßnahme stehenden Drohneneinsatz an ein Unternehmen zu vergeben, welches seinen Sitz nicht im Zuständigkeitsbereich der saarländischen Aufsichtsbehörde hatte.

Die Landesbehörde bat dahingehend um Auskunft, inwiefern - neben den Vorgaben aus dem Auftragsdatenverarbeitungsverhältnis aus § 5 Abs. 3 Saarländisches Datenschutzgesetz (SDSG) - davon ausgegangen werden kann, dass im Rahmen des Drohneneinsatzes durch das zu beauftragende Unternehmen datenschutzrechtliche Vorgaben beachtet werden.

Aufgrund der nicht gegebenen örtlichen Zuständigkeit hiesiger Dienststelle, konnte somit auch nicht überprüft werden, ob eine Meldung nach § 4d Abs. 1 Bundesdatenschutzgesetz (BDSG) zum bei der Aufsichtsbehörde geführten Register nach § 38 Abs. 2 BDSG abgegeben wurde.

[27] Der Antrag mit dem datenschutzrechtlichen Informationsblatt kann auf der Webseite des Ministeriums für Wirtschaft, Arbeit, Energie und Verkehr unter http://www.saarland.de/109178.htm abgerufen werden.

§ 4d Abs. 1 BDSG

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 der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

§ 38 Abs. 2 BDSG

Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1. Das Register kann von jedem eingesehen werden. Das Einsichtsrecht erstreckt sich nicht auf die Angaben nach § 4e S. 1 Nr. 9 sowie auf die Angabe der zugriffsberechtigten Personen.

Der Landesbehörde wurde daher empfohlen sich von dem zu beauftragenden Unternehmen bestätigen zu lassen, dass an die örtlich zuständige Datenschutzaufsichtsbehörde die gesetzlich vorgeschriebene Meldung nach § 4d Abs. 1 BDSG zum Verfahrensregister abgegeben wurde oder ein Beauftragter für den Datenschutz nach § 4f BDSG bestellt wurde, wodurch die Meldepflicht entfallen wäre. Entsprechende Unterlagen sollten vor Auftragserteilung eingesehen werden.

Wie sich sodann herausstellte, waren dem zu beauftragenden Unternehmen die datenschutzrechtlichen Obliegenheiten und insbesondere die Meldepflicht nach § 4d Abs. 1 BDSG nicht bekannt. Ob der Auftrag an das Unternehmen vergeben wurde, ist nicht bekannt.

15.9 Wildkameras

Im 25. Tätigkeitsbericht wurde unter Kapitel 19.11 dargestellt, welche datenschutzrechtlichen Vorgaben beim Einsatz sogenannter Tierbeobachtungskameras einzuhalten sind.

In der Folgezeit entstand zwischen Teilen der saarländischen Jägerschaft und der Landesdatenschutzbeauftragten eine Diskussion darüber, ob der Einsatz von Wildkameras in saarländischen Wäldern zur Beobachtung von Kirrungen meldepflichtig sei.

Zu diesem Thema hatte das Datenschutzzentrum ein „Merkblatt zum datenschutzkonformen Einsatz von Tierbeobachtungskameras in saarländischen Wäldern" entworfen und veröffentlicht.[28] Darin wird darauf hingewiesen, dass der Betrieb von Wildkameras der Aufsichtsbehörde vor Inbetriebnahme anzuzeigen ist. Die unterlassene Meldung ist nach § 43 Abs. 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) bußgeldbewehrt.

Mit Urteil vom 18. Mai 2016 - 1 K 63/15 - hat das Verwaltungsgericht des Saarlandes bestätigt, dass der Betrieb von Wildbeobachtungskameras grundsätzlich melde-

[28] Vgl. https://datenschutz.saarland.de/themen/videoueberwachung/wildkameras/

pflichtig und damit der Aufsichtsbehörde vor Inbetriebnahme anzuzeigen ist. Geklagt hatten drei Jäger, die festgestellt wissen wollten, dass insbesondere im Bereich von Kirrungen eine entsprechende Meldepflicht nicht bestehe.

Das Verwaltungsgericht schloss sich der Rechtsauffassung der Aufsichtsbehörde an, wonach sich eine Meldepflicht der Kamerabetreiber aus § 4d Abs. 1 BDSG ergibt. Hierfür war entscheidend, dass es sich bei der Beobachtung von Kirrungen mittels entsprechender Tierbeobachtungskameras um eine Tätigkeit handelt, die dem Anwendungsbereich des Bundesdatenschutzgesetzes unterfällt. Das Vorliegen einer privat-familiären Tätigkeit, wie sie von den Klägern vorgetragen wurde und was zum Ausschluss der Anwendbarkeit des BDSG geführt hätte, verneinten die Richter.

Darüber hinaus bestätigte das Gericht, dass eine Erhebung, Verarbeitung oder Nutzung der mittels einer Tierbeobachtungskamera gewonnenen Bilddaten als eine automatisierte Verarbeitung zu qualifizieren ist.

Da die Wildkameras nicht nur den mit einem Betretungsverbot nach § 23 Abs. 3 S. 1 Saarländisches Jagdgesetz belegten Bereich der Kirrung, sondern auch den angrenzenden Waldbereich erfassten, und darüber hinaus auch die Kirrung an sich faktisch uneingeschränkt betretbar ist, handelt es sich bei dem erfassten Bereich unstrittig um einen öffentlich zugänglichen Raum im Sinne des § 6b BDSG. Bauliche Abgrenzungen (z.B. Mauer, Zaun) oder Verbotsschilder könnten hingegen zur Nicht-Öffentlichkeit des Bereichs führen, in dem dadurch der entgegenstehende Wille des Verfügungsberechtigten zum Ausdruck gebracht wird.

Wegen grundsätzlicher Bedeutung der Rechtssache wurde die Berufung zugelassen, welche die Kläger auch eingelegt haben. Das Berufungsverfahren ist noch anhängig.

15.10 Videoüberwachungsverbesserungsgesetz

Der zurückliegende Berichtszeitraum konnte im Hinblick auf den Dauerbrenner Videoüberwachung doppeldeutiger nicht ausfallen: Während sich eine stetig wachsende Zahl von Bürgern beschwerdeführend an die Datenschutzaufsichtsbehörde wendet, wird die Videoüberwachung gleichzeitig im gesellschaftlichen Diskurs zunehmend zur vermeintlichen Erhöhung der öffentlichen Sicherheit befürwortet.[29]

Vor allem als Reaktion auf den Amoklauf in München und den Terroranschlag in Ansbach im Jahr 2016 avisierte das Bundesinnenministerium die Ergänzung des § 6b Bundesdatenschutzgesetz (BDSG), als zentrale Vorschrift zur Videoüberwachung durch nicht-öffentliche Stellen, durch das *Gesetz zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen Anlagen und im öffentlichen Personennahverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz)*.

[29] Umfrage von YouGov im Auftrag der Deutschen Presseagentur, abrufbar unter: https://yougov.de/news/2016/12/28/mehrheit-der-burger-spricht-sich-nach-dem-anschlag/

Artikel 1 Videoüberwachungsverbesserungsgesetz

Dem Absatz 1 wird folgender Satz 2 angefügt:

„Bei der Videoüberwachung von

1. *öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder*
2. *Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs,*

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse."

Die Zielsetzung des Gesetzentwurfs, [30] mithin die Ausweitung der von Privaten betriebenen Videoüberwachung zur Wahrnehmung von eigentlich staatlichen Stellen obliegenden Aufgaben der öffentlichen Sicherheit, stößt auf Seiten des Datenschützer zwangsläufig auf erhebliche Bedenken.[31]

Gesetzeslage im Berichtszeitraum

Hinsichtlich der Darstellung im Gesetzentwurf, dass bei der Abwägungsentscheidung zur Zulässigkeit der Videoüberwachung der Sicherheit und dem Schutz der Bevölkerung ein größeres Gewicht beizumessen sei, ist festzustellen, dass die seit dem Jahr 2001 geltende Gesetzeslage vollkommen ausreichend ist, um eine Videoüberwachung von räumlich begrenzten Gefährdungsschwerpunkten zum Schutz der Bürger zu ermöglichen.

Sofern für einen öffentlich zugänglichen Raum im Einzelfall aufgrund von Ereignissen in der Vergangenheit oder einer objektiv bewertbaren Eintrittswahrscheinlichkeit für die Zukunft eine Gefährdungslage, eben auch im Hinblick auf eine drohende Beeinträchtigung von Kunden, Besuchern oder Nutzern der überwachenden Stellen, anzunehmen ist, wird eine Abwägungsentscheidung zwischen den berechtigten Interessen des Betreibers einer Videoüberwachung und möglichen gegenläufigen schutzwürdigen Interessen von betroffenen Personen zugunsten der Überwachung ausfallen.

Eine Ergänzung der bisher gegebenen Gesetzeslage ist daher nicht geboten.

Zweck der Novelle

Im Hinblick auf den Zweck der Gesetzesnovelle

Ziel des Gesetzesentwurfes ist es, die Sicherheit bei öffentlich zugänglichen großflächigen Anlagen (z. B. Einkaufszentren) sowie bei Fahrzeugen und öffentlich zugäng-

[30] Zum Redaktionsschluss des Tätigkeitsberichts befand sich das Gesetz noch im Entwurfsstadium.

[31] Vgl. dazu auch die Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Kapitel 25.21.

lichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs, der in Privatrechtsform betrieben wird, zu erhöhen und Anschläge wie in Ansbach und München im Sommer 2016 zu ***verhindern****. […]*

Der Einsatz optisch-elektronischer Sicherheitstechnologie in öffentlich zugänglichen groß-flächigen Anlagen und im öffentlichen Schienen-, Schiffs- und Busverkehr kann ***präventiv*** *dazu beitragen, die Sicherheit der Bevölkerung zu erhöhen, indem potentielle Täter etwa bei der Erkundung von Örtlichkeiten im Vorfeld oder unmittelbar vor einer Tatbegehung erkannt und diese vereitelt werden kann.*

ist zweifelhaft, ob dieser durch eine extensiv betriebene Videoüberwachung erreicht werden kann.

Offensichtlich wurde bei der Konzeption des Entwurfs auf nach rationalen Maßstäben handelnde Täter abgestellt, jedoch muss bei Gewaltverbrechen im Allgemeinen und terroristisch motivierten Taten im Besonderen davon ausgegangen werden, dass Überwachungskameras zumeist keinerlei abschreckende Wirkung entfalten. Während Gewaltverbrechen zumeist spontan aus einem Affekt heraus und mitunter aufgrund einer alkohol- oder rauschmittelinduzierten Enthemmung begangen werden, sucht ein Terrorist, der seinen eigenen Tod bei Verübung eines propagandistischen Anschlags intendiert oder zumindest in Kauf nimmt, gerade die Öffentlichkeit.[32] [33] Der vom Gesetzgeber beabsichtigte präventive Effekt einer Ausweitung der Überwachung kann damit nicht ansatzweise angenommen werden.

Verfassungsmäßigkeit der Novelle

Da nach dem Gesetzentwurf der Schwerpunkt in der Abwägung einseitig hin zu dem Kriterium Gefahrenvorsorge verschoben wird und somit verfassungsmäßig garantierte Betroffenenrechte in den Hintergrund treten, ist fraglich, inwiefern der Verhältnismäßigkeitsgrundsatz des gesetzlich legitimierten permanenten und flächendeckenden Eingriffs in das informationelle Selbstbestimmungsrecht gewahrt bleibt. [34]

Auch ist kritisch anzumerken, dass in diesem Zusammenhang über die gesetzliche Legitimation einer extensiven Videoüberwachung durch Private, mittelbar staatliche Überwachungsbefugnisse - als Mittel der staatlichen Kernaufgabe der Gefahrenvorsorge - erheblich ausgedehnt werden, ohne dass in präventiver noch in repressiver Hinsicht mit einem Zuwachs an Sicherheit zu rechnen ist.

---

[32] „Ein Terrorist will entdeckt werden", in Saarbrücker Zeitung vom 24. Dezember 2016, abrufbar unter: http://www.saarbruecker-zeitung.de/saarland/saarbruecken/saarbruecken/saarbruecken/Kameras-und-Photoapparate-Terroristen-Verbrechensfaelle-Video-Ueberwachung-Ueberwachungskameras-Saarbruecken;art446398,6338083;

[33] http://www.stern.de/politik/deutschland/anis-amri--berlin-attentaeter-posierte-nach-tat-vor-ueberwachungskamera-7267434.html

[34] Stellungnahme des Deutschen Richterbundes Nr. 20/16, abrufbar unter: http://www.drb.de/fileadmin/docs/Stellungnahmen/2016/DRB_161110_Stn_Nr_20_Videoüberwachungsverbesserungsgesetz.pdf

Datenschutzgrundverordnung löst mitgliedstaatliche Datenschutzgesetze ab Mai 2018 ab

Durch die ab dem 25. Mai 2018 unmittelbar in allen Mitgliedstaaten anzuwendende Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DS-GVO) wird das BDSG in der dann geltenden Fassung (und somit auch mit den Ergänzungen durch das Videoüberwachungsverbesserungsgesetz) außer Kraft gesetzt.[35]

Obwohl sich abzeichnet, dass gerade die von Privaten betriebenen Videoüberwachungsmaßnahmen abschließend in Art. 6 Abs. 1 lit. f DS-GVO geregelt werden sollen und diesbezüglich kein darüberhinausgehender normativer Gestaltungsspielraum durch den nationalen Gesetzgeber angenommen werden kann, sieht der Entwurf des Nachfolgegesetzes zum BDSG (BDSG-neu) eine im Hinblick auf den novellierten § 6b BDSG gleichlautende Vorschrift zur Videoüberwachung[36] vor.

Artikel 6 Abs. 1 lit. f

Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Folgerichtig dürfte zu erwarten sein, dass der EuGH sich mit der Frage nach der Kollision der Regelung des BDSG-neu mit der DS-GVO beschäftigen wird.

Fazit

Bereits im Hinblick auf die pauschale Grundannahme des Gesetzentwurfs, dass erhebliche Teile des öffentlichen Raums (großflächige Anlagen wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätze) per se als Terrorziele gefährdet seien, wird erkennbar, dass durch das angenommene permanente Bedrohungsszenario letztlich die einzelfallbezogene, unter objektiven Gesichtspunkten anzustellende Abwägung zwischen Überwachungsinteresse und schutzwürdigen Interessen Betroffener zukünftig nicht nur in den Hintergrund treten, sondern geradezu entbehrlich werden soll.

---

[35] Das BDSG, das maßgeblich durch die Umsetzung der seit dem Jahr 1995 gegebenen Datenschutzrichtlinie (RL 95/46 EG) geprägt war, wird ab dem 25. Mai 2018 von der gemäß Artikel 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) unmittelbar in den Mitgliedstaaten der EU geltenden EU-DS-GVO abgelöst. EU-Recht hat entsprechend der Rechtsprechung des EuGH Vorrang vor nationalem Recht.

[36] Artikel 1 Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU: § 4 Abs. 1 Satz 2 BDSG-neu, Referentenentwurf auf der Webseite des BMI abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/entwurf-datenschutz-grundverordnung.pdf?__blob=publicationFile

Somit wird in der praktischen Anwendung des vorliegenden Gesetzestextes quasi das Ergebnis einer nur noch der Form halber stattfindenden Abwägungsentscheidung vorweggenommen, welches durch den Imperativ der abstrakten Gefahrenvorsorge vorgegeben ist.

In Konsequenz dazu dürfte die flächendeckende Videoüberwachung somit zur Regel, überwachungsfreie Räume zur Ausnahme werden.

15.11 Prävention durch Öffentlichkeitsarbeit

Da ein Schwerpunkt der aufsichtsbehördlichen Tätigkeit gerade auch in der Vorbeugung von Verstößen mittels Öffentlichkeitsarbeit und punktueller Aufklärung liegt, wurde im Berichtszeitraum Kontakt zu Wirtschaftsverbänden, Kammern und sonstigen Stellen aufgenommen mit dem Ziel, durch Vortragsveranstaltungen und Fragestunden sowie durch Zurverfügungstellung von Informationsmaterialien auf datenschutzrechtliche Gegebenheiten im Zusammenhang mit Videoüberwachungsmaßnahmen aufmerksam zu machen und für diese zu sensibilisieren.

- Im September 2015 wurden im Rahmen einer gemeinsam mit der Industrie- und Handelskammer des Saarlandes und der saarländischen Handwerkskammer konzipierten Veranstaltung durch Mitarbeiter des Datenschutzzentrums die im Zusammenhang mit dem Einsatz von Videokameras zu beachtenden datenschutzrechtlichen Regelungen dargestellt und anhand aktueller Praxisfälle beispielhaft erläutert.

  Im Anschluss an den in den Räumen der Handwerkskammer stattgefundenen Vortrag bestand für die Zuhörer die Möglichkeit, Fragen zu stellen.

- Aufgrund der großen Anzahl an Eingaben betreffend Videoüberwachungsmaßnahmen in Gastronomiebetrieben war besonders erfreulich, den Landesverband des Gastgewerbes im Saarland (DEHOGA Saarland) für eine Zusammenarbeit gewinnen zu können.

  Im Zuge dessen referierte die Landesdatenschutzbeauftragte im Rahmen des DEHOGA Marktplatzes 2016 über die datenschutzrechtliche Zulässigkeit von Videoüberwachungsmaßnahmen in Hotellerie und Gastronomie.

  Es ist beabsichtigt, die Zusammenarbeit fortzuführen und über Veröffentlichungen in der verbandseigenen Mitgliederzeitschrift über Entwicklungen im Bereich des Datenschutzes zu informieren.

- Den saarländischen Schwimmbadbetreibern wurde der im August 2015 beschlossene Zusatz „Videoüberwachung in Schwimmbädern“[37] zur Orientierungshilfe des Düsseldorfer Kreises „Videoüberwachung durch nicht-öffentliche Stellen“ im Januar 2016 übersandt, mit der Empfehlung, eingesetzte

[37] Vgl. Kapitel 26.3 sowie die Webseite des Datenschutzzentrums unter: https://datenschutz.saarland.de/themen/videoueberwachung/videoueberwachung-durch-nichtoeffentliche-stellen/

Videoüberwachungsmaßnahmen hinsichtlich ihrer Vereinbarkeit mit datenschutzrechtlichen Gegebenheiten zu überprüfen.

- Da zum Ende des Berichtszeitraums das Thema Videoüberwachung in Spielcasinos und in Gastronomiebetrieben mit Spielautomaten akut geworden ist[38], wird eine zeitnahe Kontaktaufnahme mit dem Automaten-Verband-Saar e.V., als Wirtschaftsverband der Aufstellunternehmen im Saarland, erfolgen.

  Gerade in diesem aufgrund der Grenznähe zu Frankreich[39] häufig anzutreffenden Wirtschaftsbereich, in dem Videoüberwachungsmaßnahmen die Regel sind, wurden im Rahmen der bisherigen Prüfungstätigkeit häufig Missstände und Unkenntnis bezüglich datenschutzrechtlicher Obliegenheiten angetroffen.

[38] Siehe dazu auch den Bericht unter Kapitel 15.6.

[39] Aufgrund des Glückspielverbots in Frankreich sind in unmittelbarer Nähe zur französischen Grenze Glückspielanbieter besonders häufig anzutreffen

16 Versicherungswirtschaft

16.1 Anbindung der privaten Krankenversicherungen an das Hinweis- und Informationssystem der Versicherungswirtschaft

Das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) ist eine vom Gesamtverband der deutschen Versicherungswirtschaft e.V. (GDV) geführte Auskunftei, mittels derer Fälle des Versicherungsbetrugs und –missbrauchs verhindert werden sollen. Hierzu melden Versicherungsunternehmen Personen (wie etwa Versicherungsnehmer) und Objekte (wie zum Beispiel KFZ oder Gebäude) an das HIS. Eine solche Meldung erfolgt aber nur unter der Voraussetzung, dass spezifische Auffälligkeiten zutage treten. Eine solche Auffälligkeit kann unter anderem in einer besonderen Schadenshäufigkeit[40] oder bei besonderen Risiken[41] bestehen.

Bislang wurde das HIS von den privaten Krankenversicherungen nicht genutzt. Über den Verband der privaten Krankenversicherungen e.V. (PKV) planen nunmehr die privaten Krankenversicherungsunternehmen entweder eine Beteiligung am HIS oder den Aufbau einer eigenen vergleichbaren PKV-Auskunftei. Unabhängig von dieser, von dem PKV zu klärenden Frage gibt es auch in dieser Versicherungssparte erheblichen Abstimmungsbedarf zwischen der PKV und den Aufsichtsbehörden zu datenschutzrechtlichen Fragestellungen.[42] Den größten Abstimmungsbedarf bezüglich der PKV-Auskunftei gibt es dabei über die Frage, unter welchen Voraussetzungen ein Verdachtsfall angenommen werden kann sowie damit zusammenhängend, welche und wie viele Verdachtstatbestände erfüllt sein müssen, um einen Verdachtsfall zu begründen. Dieser Abstimmungsprozess wird über den Berichtszeitraum hinaus andauern.

16.2 Dashcam-Aufnahmen bei der Schadenregulierung

Die datenschutzrechtliche Zulässigkeit des Einsatzes sog. Dashcams und die Verwendung der hiermit erzeugten Aufnahmen bildete über den Berichtszeitraum hinaus eine äußerst umstrittene Fragestellung ab. Bei diesen Geräten handelt es sich um

---

40 Eine atypische Schadenshäufigkeit wird zum Beispiel in der Rechtsschutzversicherung dann angenommen, wenn innerhalb von 12 Monaten vier oder mehr Versicherungsfälle eingetreten sind.

41 Besondere Risiken werden beispielsweise in der Lebensversicherung angenommen, wenn risikoerhebliche Vorerkrankungen bestehen oder ein gefährlicher Beruf ausgeübt wird. Dabei dürfen jedoch nicht der konkrete Beruf oder Gesundheitsdaten an das HIS übermittelt werden.

42 Die Abstimmung zwischen den Aufsichtsbehörden erfolgt in der AG Versicherungswirtschaft des Düsseldorfers Kreis, an der auch unsere Behörde beteiligt ist.

Kameras, die im Regelfall im Bereich der Frontscheibe eines Kraftfahrzeuges angebracht sind und das Verkehrsgeschehen dauerhaft aufzeichnen. Im Falle eines Unfalls sollen die Aufzeichnungen dann zu Beweisführungszwecken eingesetzt werden.

Aus datenschutzrechtlicher Sicht ist beim Einsatz solcher Geräte allerdings zu berücksichtigen, dass auch von solchen Personen Daten erhoben und gespeichert werden, die für den eigentlichen Datenumgang überhaupt keinen Anlass geben. Die Gerichte hatten sich daher mit der Frage zu befassen, ob der damit verbundene Eingriff in das Persönlichkeitsrecht sämtlicher Verkehrsteilnehmer, sei es nun Passanten oder auch andere Kraftfahrzeugführer, durch das Beweisführungsinteresse des Kamerabetreibers im Falle eines Verkehrsunfalls gerechtfertigt werden könne.

Der Einsatz von Dashcams ist nach § 6b Bundesdatenschutzgesetz (BDSG) zu beurteilen. Nach Absatz 1 ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Die Verwaltungsgerichte kamen überwiegend zu der Feststellung, die Voraussetzungen des § 6b BDSG seien nicht erfüllt und der Einsatz von Dashcams demnach datenschutzrechtlich unzulässig. Zwar wird der Einsatzzweck, nämlich die Erhebung möglicher Beweismittel bei einem Verkehrsunfall oder einem anderen verkehrsrechtlichen Sachverhalt, als berechtigtes Interesse im Sinne der Vorschrift anerkannt, zu dem auch der Einsatz der Dashcam erforderlich sein kann. Allerdings überwiegen in der Regel die schutzwürdigen Interessen der anderen Verkehrsteilnehmer, mithin das Recht auf informationelle Selbstbestimmung, die Interessen des Anlagenbetreibers an der Beschaffung von Beweismitteln. Das Verwaltungsgericht Ansbach stellte in seiner Entscheidung fest, dass *„eine solche großflächige Beobachtung von öffentlichen Straßen (…) schon deshalb einen schwerwiegenden Eingriff in die Persönlichkeitsrechte der Betroffenen dar[stellt], weil durch die permanente Aufzeichnung mit der On-Board-Kamera einen Vielzahl von Personen in kurzer Zeit in ihrem allgemeinen Persönlichkeitsrecht beeinträchtigt wird."*[43]

Dieser Umstand wirkt regelmäßig umso schwerer, als nicht auf die Videoüberwachung im Sinne des § 6b Abs. 2 BDSG, beispielsweise durch Hinweisschilder, aufmerksam gemacht wird und es sich damit um eine wesentlich eingriffsintensivere heimliche Überwachung handelt, bei der die Betroffenen nicht erkennen können, dass sie überhaupt überwacht werden.

Im Berichtszeitraum meldete sich ein Petent bei der Aufsichtsbehörde, der mitteilte, in einen Verkehrsunfall verwickelt gewesen zu sein. Ohne sein Wissen habe der Unfallgegner mithilfe einer Dashcam das Unfallgeschehen aufgezeichnet und das entsprechende Bildmaterial der Versicherung des Petenten zur Verfügung gestellt. Wie aus dem der Aufsichtsbehörde zur Verfügung gestellten Schriftverkehr zu entnehmen war, bildeten die Videoaufzeichnungen für die Versicherung die Entscheidungsgrundlage für die Schadenregulierung.

[43] VG Ansbach vom 12. August 2014 – AN 4 K 13.01634, Rn. 59 – juris.

Nachdem der Petent seine Versicherung gebeten hatte, ihm Einsicht in die Versicherungsakte inklusive der Aufzeichnungen zu gewähren, wurde ihm von Seiten der Versicherung mitgeteilt, dass dies nur mit der Erlaubnis des Unfallgegners möglich sei. Aufgrund dessen forderte der Petent die Versicherung auf, das Video zu löschen, was diese jedoch ablehnte.

Die Versicherer haben grundsätzlich die Möglichkeit, im Rahmen der Schadenregulierung solche Informationen zu sammeln, die für die Entscheidungsfindung erforderlich sind.

Vorliegend hatte die Versicherung jedoch eine Dashcam-Aufnahme gespeichert und genutzt, die ursprünglich durch einen Dritten in unzulässiger Weise angefertigt worden war. Demnach war auch die Speicherung durch den Versicherer selbst unzulässig. Nach § 35 Abs. 2 S. 2 Nr. 1 BDSG sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig war. Der Versicherer wurde daher aufgefordert, dieser Löschpflicht nachzukommen und dafür Sorge zu tragen, dass etwaige in der Zukunft übermittelte Dashcam-Aufnahmen nicht mehr genutzt werden. Dies wurde entsprechend zugesagt.

Die Zivil- und Strafgerichte vertreten zunehmend die Auffassung, dass kein generelles Beweisverwertungsverbot für Dashcam-Aufzeichnungen besteht.[44] An der datenschutzrechtlichen Bewertung ändert dies nichts.[45]

16.3 Signpads in der Versicherungswirtschaft

Im laufenden Berichtszeitraum wurden die Datenschutzaufsichtsbehörden von des Bundes und der Länder durch eine Fachzeitschrift mit der Fragestellung befasst, inwiefern der Einsatz von Signpads beim Abschluss von Versicherungsverträgen unter Beachtung datenschutzrechtlicher Vorgaben zulässig erfolgen könne.

Beim Abschluss derartiger Verträge ist zu berücksichtigen, dass sie – gerade im Bereich der Krankenversicherungen – den Umgang mit besonders schützenswerten Gesundheitsdaten bedingen können, deren Verarbeitung nur mit einer Einwilligung der betroffenen Personen zulässig ist. Dabei müssen Erklärungen, die eine Einwilligung zur Verarbeitung personenbezogener Daten beinhalten, die Vorgaben des § 4a Abs. 1 S. 3 Bundesdatenschutzgesetz (BDSG) beachten, wonach Einwilligungen grundsätzlich schriftlich gemäß § 126 Bürgerliches Gesetzbuch (BGB) erteilt werden müssen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

Da das Display nicht dazu geeignet ist, Schriftzeichen dauerhaft festzuhalten, genügen Unterschriften, die mittels Touch-Eingabe auf einem Tablet-Computer gezeichnet werden, nicht dem Schriftformerfordernis im Sinne der vorgenannten Vorschrift. Dass die Unterschrift digital einfacher zu verwalten ist oder beide Parteien auf die

---

[44] OLG Stuttgart vom 4. Mai 2016 – 4 Ss 543/15; AG Nienburg vom 20. Januar 2015 – 4 Ds 155/14, 4 Ds 520 Js 39473/14 (155/14); LG Landshut vom 1. Dezember 2015 – 12 S 2603/15.

[45] Siehe Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 25./26. Februar 2014) – Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams).

zivilrechtliche Schriftform einvernehmlich verzichten, rechtfertigt darüber hinaus kein Abweichen von dem grundsätzlichen Schriftformerfordernis.

Die Möglichkeit, datenschutzrechtliche Einwilligungen mittels Unterschriftenpads abzugeben, besteht daher nicht. Verstöße gegen das Schriftformerfordernis können daher Aufsichts- und Ordnungswidrigkeitenverfahren zur Folge haben. Die Wirksamkeit der Versicherungsverträge bleibt davon unberührt.

Aber auch in den Fällen, in denen der Einsatz zulässig ist, sind Vorkehrungsmaßnahmen zu treffen, um einen Datenmissbrauch, insbesondere im Hinblick auf die elektronische Unterschrift bei Versicherungsverträgen, zu verhindern. So muss gewährleistet sein, dass die elektronische Unterschrift mitsamt ihrer biometrischen Daten nicht von unbefugten Dritten genutzt werden kann, um Verträge in fremdem Namen zu schließen. Die Unterschrift ist daher untrennbar in das Vertragsdokument zu integrieren, um ein Extrahieren unmöglich zu machen.

17 Auskunfteien und Inkassounternehmen

17.1 Fallstricke bei der Tätigkeit von Auskunfteien

Immer wieder melden sich Betroffene bei unserer Dienststelle, die sich im Umgang mit ihren personenbezogenen Daten durch Auskunfteien in ihren Persönlichkeitsrechten verletzt sehen.

Oftmals erlangen die betroffenen Personen erst dann von der Speicherung negativer Bonitätsmerkmale über ihre Person Kenntnis, wenn ihnen von Seiten eines potentiellen Vertragspartners mitgeteilt wird, dass ihre Bonitätsprüfung zu einem negativen Ergebnis geführt hat.

Dies kann für die Betroffenen schwerwiegende Folgen haben: der Abschluss eines Mobilfunkvertrages oder der Abschluss eines Wohnraummietvertrages werden damit nahezu unmöglich sein.

Aus diesem Grund empfiehlt es sich, regelmäßig von seinem Auskunftsrecht nach § 34 Bundesdatenschutzgesetz (BDSG) Gebrauch zu machen. Auf Anforderung sind von der Auskunftei alle Daten, die zur Person des Betroffenen gespeichert sind, sowie deren Herkunft und die Empfänger mitzuteilen. Die Auskunft ist je Kalenderjahr einmal unentgeltlich zu erteilen.[46] Stellt der Betroffene fest, dass die über ihn gespeicherten Daten unrichtig sind, hat er nach § 35 Abs. 1 S. 1 BDSG einen Anspruch auf Berichtigung.

Dabei müssen sich die Auskunfteien ebenso an datenschutzrechtlichen Vorgaben orientieren wie die Stellen, die bonitätsrelevante Daten an die Auskunfteien übermitteln. Die einschlägige Rechtsvorschrift für die Übermittlung von Daten an Auskunfteien ist § 28a BDSG.

In der aufsichtsbehördlichen Praxis zeigt sich hier immer wieder, dass die gesetzlichen Voraussetzungen für die Datenübermittlung (teilweise) nicht vorgelegen haben und die Daten überhaupt nicht hätten übermittelt werden dürfen. Insbesondere dann, wenn sich die datenübermittelnde Stelle auf § 28a Abs. 1 Nr. 4 BDSG beruft, kann sich ein Blick ins Gesetz lohnen.

§ 28a Abs. 1 Nr. 4 BDSG

Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,

[46] § 34 Abs. 8 S. 2 BDSG.

b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,

c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und

d) der Betroffene die Forderung nicht bestritten hat

Besonders kritisch wird es dann, wenn ein Unternehmen sowohl als Inkassobüro als auch als Auskunftei tätig ist. In diesem Zusammenhang zeigten sich im Laufe des Berichtszeitraums einige Problemstellungen, die beispielhaft erläutert werden.

17.1.1 Einmeldung trotz Bestreitens der Forderung

In einem Fall legte uns ein Petent den zwischen ihm und der Auskunftei geführten Schriftverkehr vor. Darin kam zum Vorschein, dass der Petent eine Forderung nach der ersten Mahnung beglichen hatte, jedoch nicht bereit war, die Kosten des mit dem Forderungseinzug beauftragten Inkassobüros zu tragen. Die Kosten und Auslagen wurden mehrmals angemahnt, bis schließlich ein Mahnbescheid gegen den Petenten beauftragt wurde. Gegen diesen Bescheid legte der Petent Widerspruch ein, woraufhin das Inkassobüro den Auftrag zurückzog und an die Auskunftei das Merkmal „abgeschlossenes kaufmännisches Mahnverfahren" einmeldete. Das einmeldende Inkassobüro teilte mit, dass die Einmeldung nachvollziehbar sei, da es mehrere Monate gedauert habe, bis überhaupt die erste Rechnung beglichen worden sei und man zudem auf den eigenen Kosten sitzen blieb. Ungeachtet dessen war festzustellen, dass die Einmeldevoraussetzungen nicht vorlagen. Hier kam überhaupt nur § 28a Abs. 1 S. 1 Nr. 4 BDSG als Übermittlungsvoraussetzung in Betracht. Danach ist die Einmeldung jedoch nur zulässig, wenn der Schuldner die Forderung nicht bestritten hat. Vorliegend hat der Petent durch Einlegen eines Rechtsbehelfs (hier durch Widerspruch gegen den Mahnbescheid) zum Ausdruck gebracht, dass er die Forderung nicht akzeptiert. Die übermittelnde Stelle wurde insoweit aufgefordert, die Einmeldung bei der Auskunftei nach § 35 Abs. 1 und 2 BDSG zu widerrufen und berichtigen zu lassen. Dieser Aufforderung wurde Folge geleistet.

17.1.2 Berechnung der Speicherfristen

Im Rahmen einer Selbstauskunft nach § 34 BDSG erhielt ein Petent die Mitteilung, dass über seine Person keine bonitätsrelevanten Negativmerkmale vorlagen und wurde folglich in die bestmögliche Bonitätsklasse eingestuft. In gleichem Zusammenhang wurde ihm dann aber mündlich mitgeteilt, dass noch eine Angelegenheit aus dem Jahr 1999 aktenkundig sei. Wie sich im weiteren Verlauf des Verwaltungsverfahrens zeigen sollte, kam es bei dem Petenten versehentlich zu einer Datensatzdoppelanlage; es existierten also zu dem Petenten zwei Datensätze. Die dem Petenten mitgeteilte Auskunft enthielt den fraglichen Vorgang nicht.

Aus diesem Grund sah sich der Petent veranlasst, eine Forderungsaufstellung anzufordern. Die Angelegenheit erledigte er dann im unmittelbaren Anschluss durch Zahlung, woraufhin er von der Auskunftei eine entsprechende Bestätigung erhielt.

Aufgrund der widersprüchlichen Sachlage forderte der Petent nachträglich erneut eine Selbstauskunft an. Diese enthielt nunmehr Angaben über Zahlungsstörungen mit der Folge, dass die Bonität des Petenten nicht mehr erstklassig war.

Die Zahlungsstörung ging auf eine titulierte Forderung aus dem Jahr 1999 zurück, die unstreitig durch den Petenten zu zahlen gewesen war. Die Mitteilung über die Forderung erhielt die Auskunftei erst im Jahr 2008.

Diese vertrat die Auffassung, dass auch gerade erst bezahlte Inkassovor-gänge bonitätsrelevant seien, da sie etwas über das Zahlungsverhalten des Schuldners aus der Vergangenheit aussagen. Somit blieben abgeschlossene Inkassofälle regelmäßig in den Auskunfteibeständen gespeichert, bis die Frist des § 35 Abs. 2 Nr. 4 BDSG abgelaufen sei.

§ 35 Abs. 2 S. 2 Nr. 4 BDSG

Personenbezogene Daten sind zu löschen, wenn sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, dass der erstmaligen Speicherung folgt, ergibt, dass eine länger währende Speicherung nicht erforderlich ist.

Die erstmalige Speicherung lag im Kalenderjahr 2008. Bei einem unerledigten Sachverhalt hätte eine Überprüfung durch die Auskunftei damit spätestens zum Ende des Jahres 2012 erfolgen müssen. Zu diesem Zeitpunkt hatte der Petent die Forderung nicht beglichen, weshalb eine stattgefundene Prüfung aller Voraussicht nach eine längerwährende Speicherung ergeben und damit eine neue vierjährige Prüfungsfrist – somit zum Ende des Jahres 2016 – ausgelöst hätte.

Aufgrund des Umstandes, dass der Petent die Forderung zwischenzeitlich beglichen hatte, verkürzte sich die ursprüngliche vierjährige Prüffrist auf drei Jahre, was im Ergebnis zu einer Prüffrist zum 31. Dezember 2015 geführt hätte. Die von der Auskunftei vertretene Auffassung, dass der Umstand der Erledigung Anknüpfungspunkt für die Berechnung der Prüffrist sei und zu einer Prüfung zum Ende 2018 geführt hätte, konnte hingegen nicht gefolgt werden.

Im Rahmen der zum 31. Dezember 2015 vorzunehmenden Prüfung wäre festzustellen gewesen, ob ein Erfordernis der längerwährenden Speicherung des Negativmerkmals über das Ende der Prüffrist hinaus besteht. Abzustellen ist dabei auf die Bonität im Prüfungszeitpunkt. Der alleinige Umstand, dass ein langjähriges Inkassoverfahren gerade erst abgeschlossen worden ist, stellt für sich genommen kein aussagekräftiges Bonitätsmerkmal zu Lasten des Betroffenen dar. Insbesondere war aufgrund der vorgelegten Unterlagen davon auszugehen, dass zu dem gespeicherten Inkassovorgang kein weiteres Negativmerkmal hinzugetreten ist, welches die Zahlungsunwilligkeit des Petenten untermauern würde.

Zu Gunsten des Petenten war außerdem zu berücksichtigen, dass die Doppelanlage nicht vom Schuldner zu vertreten war und das langjährige Inkassoverfahren nur

durch das Tätigwerden des Petenten im Rahmen der angeforderten Selbstauskunft zum Abschluss gebracht werden konnte. Der Petent hatte hierdurch gerade seine Zahlungswilligkeit zum Ausdruck gebracht.

Für eine Speicherung des Negativmerkmals über das Datum der verkürzten Prüffrist hinaus bestand somit keine Erforderlichkeit. Das Datum war somit zu löschen, was durch die Auskunftei auch entsprechend umgesetzt wurde.

17.1.3 Mängel bei der Umsetzung der Hinweispflicht

Die Übermittlungsvoraussetzungen nach § 28a Abs. 1 S. 1 Nr. 4 BDSG sehen unter Buchstabe c vor, dass die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung zu unterrichten hat.

Im Rahmen einer weiteren Eingabe erhielten wir von einem Mahnschreiben eines Inkassounternehmens Kenntnis, welches lediglich einen pauschalen Verweis enthielt, dass Negativdaten nach den Vorgaben des § 28a BDSG an eine bestimmte Auskunftei übermittelt werden können. Dem Unternehmen wurde mitgeteilt, dass ein in der Mahnung enthaltener Hinweis nur im Einklang mit den Vorgaben des § 28a Abs. 1 S. 1 Nr. 4 BDSG steht, wenn nicht verschleiert wird, dass durch Bestreiten einer Forderung die Einmeldung von Schuldnerdaten verhindert werden kann. Der enthaltene Verweis genügte dieser Anforderung insoweit keineswegs.

Darüber hinaus ist der Betroffene über den beabsichtigten Zeitpunkt der Übermittlung zu informieren, um klarzustellen, bis zu welchem konkreten Datum die Möglichkeit besteht, durch entsprechendes Tätigwerden die Einmeldung abwenden zu können. Auch hierzu enthielt das Anschreiben keinen Hinweis.

Aufgrund der Tatsache, dass das Mahnschreiben nicht den gesetzlichen Anforderungen entsprach, entfielen die Übermittlungsvoraussetzungen, weshalb das Negativmerkmal zu löschen war. Das Inkassobüro wurde darüber hinaus aufgefordert, den Hinweis entsprechend anzupassen.

18 Werbung

18.1 Fallgestaltungen im Zusammenhang mit Marketingmaßnahmen

Fehler im Zusammenhang mit der Nutzung und Verarbeitung personenbezogener Daten für Zwecke des Direktmarketings sind nicht nur typischerweise bei kleinen Unternehmen anzutreffen. Die Prüfpraxis lässt offen zu Tage treten, dass auch mittlere und vergleichsweise große Unternehmen oftmals mit personenbezogenen Daten für Werbezwecke umgehen, ohne die datenschutz- und wettbewerbsrechtlichen Gegebenheiten in der gebotenen Art und Weise zu beachten.

Anlass für an das Datenschutzzentrum gerichtete Beschwerden sind zuvorderst die konkreten Werbebotschaften, die die Adressaten regelmäßig per E-Mail, postalisch oder auf sonstigem Wege erreichen. Dabei ist zumeist weniger entscheidend wie die Werbebotschaft als solche inhaltlich ausgestaltet ist, sondern dass für die Empfänger - abgesehen von dem Direktmarketing gegenüber Bestandskunden - regelmäßig unklar bleibt, woher und auf welche Art und Weise die werbenden Unternehmen die Adress- und Kontaktdaten der Betroffenen bezogen haben.

Regelmäßig kommt es vor, dass an die werbenden Stellen gerichtete Auskunftsersuchen nach § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) nicht beachtet oder lediglich unvollständig beantwortet werden.

§ 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.*

Dieses gesetzlich normierte Auskunftsrecht ist von zentraler Bedeutung für Betroffene, was sich auch daran ablesen lässt, dass ein Verstoß dagegen nach § 43 Abs. 1 Nr. 8a BDSG einen Bußgeldtatbestand darstellt.

Das Vorgesagte gilt gleichsam für bereits von Kunden eingelegte Werbewidersprüche nach § 28 Abs. 4 S. 1 BDSG, welche von werbenden Unternehmen nicht beachtet wurden.

§ 28 Abs. 4 S. 1 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.

18.1.1 Einwilligung oder Listendaten

Im Berichtszeitraum war ein Werbeschreiben, welches trotz eingelegten Werbewiderspruchs von einem Handelsunternehmen postalisch an eine Petentin gesandt wurde, Anlass dafür, die zugrundeliegenden Prozesse der Erhebung, Verarbeitung und Nutzung personenbezogener Daten für Werbezwecke genauer unter die Lupe zu nehmen.

Dabei traten vor allem organisatorische Mängel im Zusammenhang mit der Verwaltung von Werbewidersprüchen zu Tage. So wurden eingelegte Werbewidersprüche, die in den einzelnen Betriebsstätten eingingen, nicht zeitnah an die Unternehmenszentrale, die das Marketing zentral koordinierte, weitergeleitet. Aber auch der vor Werbemaßnahmen durchzuführende manuelle Abgleich mit der tabellarisch geführten Werbewiderspruchsdatei gestaltete sich aufgrund einer Vielzahl von Doubletten und mitarbeiterbezogener Fehler schwierig.

Insoweit stellte das Unternehmen in Aussicht, die Marketingprozesse zu automatisieren und eine Organisationsanweisung zu erstellen, um eine rasche Bearbeitung von Kundenanliegen im Zusammenhang mit Marketingmaßnahmen zu gewährleisten.

Auch hinsichtlich der datenschutzrechtlichen Grundlage für den Umgang mit Kundendaten für Werbezwecke war erkennbar, dass die gesetzlichen Gegebenheiten unzureichend beachtet wurden.

Die ausschließlich für eine postalische Werbeansprache genutzten Kundendaten wurden im Zusammenhang mit abgeschlossenen Kaufverträgen datenschutzrechtlich zulässig erhoben. Aus unbekanntem Grund wurde lediglich beim Verkauf spezifischer Produkte eine Einwilligungserklärung von Kunden im Sinne des § 28 Abs. 3 S. 1 BDSG in Verbindung mit § 4a BDSG eingeholt. Im Übrigen wurde zur Legitimation von Werbemaßnahmen nicht auf die Einwilligung, sondern auf Listendaten im Sinne des § 28 Abs. 3 S. 2 Nr. 1 BDSG abgestellt.

§ 28 Abs. 3 S. 1 und 2 BDSG

Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. 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,*

2. *für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder*

3. *für Zwecke der Werbung für Spenden, die nach § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.*

Diese Vorgehensweise brachte jedoch folgendes Problem mit sich: Sofern die Daten eines Kunden aufgrund eines früheren Einkaufs im Kundenmanagementsystem gespeichert wurden, konnten diese auch ohne Einwilligung des Betroffenen auf Grundlage des § 28 Abs. 3 S. 2 BDSG - bis zur Erteilung eines Werbewiderspruchs nach § 28 Abs. 4 S. 1 BDSG - für eine postalische Werbeansprache genutzt werden.

Wurde dem Kunden jedoch bei einem nachfolgenden Einkauf eines spezifischen Produkts eine Einwilligung in die postalische Werbeansprache vorgelegt und diese nicht erteilt, wurde zwangsläufig konkludent somit jegliche weitere Werbeansprache des Bestandskunden datenschutzrechtlich unzulässig.

Infolgedessen war die Sinnhaftigkeit an dem Festhalten an unterschiedlichen Legitimationsgrundlagen für die Nutzung von Kundendaten für Werbezwecke kritisch zu hinterfragen. Das Unternehmen ging schließlich dazu über, keine Einwilligungserklärungen mehr einzuholen.

18.1.2 Lettershop-Verfahren

In einem weiteren Verfahren wandte sich ein Petent an die Aufsichtsbehörde, da er postalisch ein Werbeschreiben von einem Zeitungsverlag erhielt, mit dem er zu keinem Zeitpunkt in Geschäftsbeziehung stand. Ein diesbezügliches Auskunftsersuchen nach § 34 Abs. 1 BDSG blieb ohne Ergebnis.

Auf Nachfrage der Aufsichtsbehörde stellte sich heraus, dass das Auskunftsersuchen aufgrund eines personellen Engpasses nicht fristgemäß beantwortet wurde. Im Übrigen war der Verlag nicht die datenschutzrechtlich verantwortliche Stelle für die Werbeansprache im Sinne des § 3 Abs. 7 BDSG, da in dessen Bestand keine personenbezogenen Daten des Petenten gespeichert waren und besagtes Schreiben nicht von diesem versandt wurde.

Laut Stellungnahme des Verlags „mietete" dieser im sogenannten Lettershop-Verfahren den Adressenbestand eines schweizerischen Unternehmens (Adresseigner) an.

Dazu wurden von dem Verlag lediglich Blanko-Werbeschreiben zur Verfügung gestellt, welche von dem schweizerischen Adresseigner mit Name und Anschrift der Werbeadressaten bedruckt und versendet wurden. Eine Übermittlung von personenbezogenen Daten vom Adresseigner an den saarländischen Verlag fand somit nicht statt.

Diese Konstruktion ist datenschutzrechtlich grundsätzlich nicht zu beanstanden, jedoch durchaus als kritisch zu bewerten, da verantwortliche Stellen, für die die Vorgaben des BDSG zu beachten sind, vollkommen legitim von im Ausland aggregierten Adressdatenbeständen profitieren. Herkunft und sonstige Umstände des Zustandekommens dieser Adressdatenbestände im Ausland können dabei regelmäßig nicht

nachvollzogen werden, so dass dieses Geschäftsmodell des Lettershop-Verfahrens insoweit auch unlautere Methoden der Generierung von Datensätzen für Werbezwecke begünstigt.

Daher wird in der Beratungspraxis hiesiger Dienststelle das Lettershop-Verfahren auch nur unter der Voraussetzung gutgeheißen, wenn gewährleistet ist, dass die Adressdaten beim Dateneigner nachweisbar datenschutzkonform generiert wurden und dies von dem Auftraggeber überprüft wird.

18.2 Werbeanrufe durch ein Unternehmen (B2B)

Dass zum aufsichtsbehördlichen Aufgabenspektrum nicht bloß der Schutz personenbezogener Daten von Privatpersonen zählt sondern auch wettbewerbsrechtliche Erwägungen auch für datenschutzrechtliche Bewertungen relevant sind, wird an folgendem Fall deutlich.

Ein Freiberufler wandte sich beschwerdeführend an das Datenschutzzentrum und thematisierte die telefonische Kontaktaufnahme durch ein saarländisches Unternehmen. Der Zweck des Anrufs war in diesem Zusammenhang als werbliche Ansprache des Betroffenen zu qualifizieren.

Das betreffende Unternehmen teilte nach Aufforderung zur Stellungnahme mit, dass der Zweck der telefonischen Ansprache von Freiberuflern und anderen gewerblichen Adressaten darin bestand, diesen eine Abnahmemöglichkeit für im Zusammenhang mit der Tätigkeit anfallende Nebenprodukte zu offerieren. Die für die Ansprache der Betroffenen genutzten Daten würden aus allgemein zugänglichen Quellen erhoben; eine Geschäftsbeziehung mit den Werbeadressaten bestand somit vor dem Anruf nicht.

Zielsetzung des Bundesdatenschutzgesetzes (BDSG) ist zwar ausdrücklich der Schutz des Rechts auf informationelle Selbstbestimmung natürlicher Personen, jedoch können Angaben zu einem Freiberufler oder sonstigem Gewerbetreibenden mit personenbezogenen Daten im Sinne des § 3 Abs. 1 BDSG deckungsgleich sein.[47]

Legitimationsgrundlage für den in einem werblichen Kontext und ohne Einwilligung der Betroffenen stattfindenden initialen Telefonanruf könnte § 28 Abs. 3 S. 2 Nr. 1 BDSG sein.

§ 28 Abs. 3 S. 2 Nr. 1 BDSG

Die Verarbeitung oder Nutzung personenbezogener Daten ist 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

[47] Siehe dazu beispielsweise das Urteil des Verwaltungsgerichts Wiesbaden vom 7. Dezember 2007 - 6 E 928/07 - und das Urteil des Europäischen Gerichtshofs vom 9. November 2010 - C-92/09 und C-93/09.

Verarbeitung oder Nutzung erforderlich ist 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.

Die Telefonnummer der Freiberufler fällt somit ausdrücklich nicht unter die Listendaten im Sinne der Vorschrift, jedoch könnte nach § 28 Abs. 3 S. 3 in Verbindung mit § 28 Abs. 3 S. 2 Nr. 1 BDSG eine Möglichkeit gegeben sein, weitere Daten zu den Listendaten hinzuzuspeichern mit dem Ziel, diese für Werbezwecke zu nutzen.

Den „Anwendungshinweisen der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke" lässt sich unter Ziffer 3.10 diesbezüglich Folgendes entnehmen:[48]

Bei Werbung mit einem Telefonanruf gegenüber einem sonstigen Marktteilnehmer (B2B)[49] kommt es für die wettbewerbsrechtliche Zulässigkeit nach § 7 Abs. 2 Nr. 2 UWG[50] darauf an, dass von dessen zumindest mutmaßlicher Einwilligung ausgegangen werden kann. Im B2B-Bereich stehen deshalb bei einem Hinzuspeichern und Nutzen von Telefonnummern für Werbeanrufe nach § 28 Abs. 3 S. 3 BDSG i. V. m. § 28 Abs. 3 S. 2 Nr. 1 BDSG (Eigenwerbung bei Bestandskunden oder Eigenwerbung bei Firmenkontakten aus allgemein zugänglichen Verzeichnissen) datenschutzrechtlich nicht von vorne herein die schutzwürdigen Interessen der telefonisch anzusprechenden Gewerbetreibenden nach § 28 Abs. 3 S. 6 BDSG entgegen.

§ 7 Abs. 2 Nr. 2 UWG

Eine unzumutbare Belästigung ist stets anzunehmen bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung oder gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung.

Entscheidend für die Möglichkeit der Hinzuspeicherung der Telefonnummer des Freiberuflers zu den Listendaten im Sinne des § 28 Abs. 3 BDSG und für die Zulässigkeit der Nutzung der Telefonnummer für Werbezwecke ist die Frage, ob eine mutmaßliche Einwilligung des Betroffenen im Sinne des § 7 Abs. 2 Nr. 2 UWG gegeben ist. Somit hängt letztlich die datenschutzrechtliche Zulässigkeit der telefonischen Werbeansprache eines Freiberuflers von der wettbewerbsrechtlichen Frage nach der mutmaßlichen Einwilligung des Betroffenen ab.

Dies war anhand der Umstände vor dem Anruf sowie der Art und des Inhalts der Werbung festzustellen. Maßgeblich war, ob der Anrufer bei verständiger Würdigung der Umstände annehmen durfte, der Anzurufende erwarte einen solchen Anruf oder

---

48 Die Anwendungshinweise wurden in der Ad-hoc-Arbeitsgruppe „Werbung und Adresshandel" von den beteiligten Datenschutzaufsichtsbehörden erstellt und sind abrufbar unter:
https://datenschutz.saarland.de/fileadmin/themen/Anwendungshinweise_Werbung.pdf

49 Business-to-business steht für Geschäftsbeziehungen zwischen Unternehmen. Im Unterschied dazu steht Business-to-consumer (B2C) für Geschäftsbeziehungen zwischen Unternehmen und Verbrauchern.

50 Gesetz gegen den unlauteren Wettbewerb.

werde ihm jedenfalls aufgeschlossen gegenüberstehen. Abzustellen war für diese Betrachtung ausdrücklich nicht auf die subjektive Sichtweise des Angerufenen, sondern auf eine objektive Bewertung der Erwartungshaltung des Werbeadressaten.

Folgende Kriterien waren zur Bewertung der Fragestellung heranzuziehen und in einer Gesamtbetrachtung abzuwägen:

- Art und Inhalt der konkreten Werbeansprache

  Eine allgemeine Sachbezogenheit des Angebotenen zu dem Geschäftsbetrieb reicht nicht aus, um ein sachliches Interesse des Adressaten am Anruf anzunehmen; erheblich war, inwiefern eine Nähe des Angebotenen zum spezifischen Bedarf des Werbeadressaten bejaht werden konnte.[51]

  Auch wenn das anrufende Unternehmen seinen Geschäftszweck sehr spezifisch auf die angerufenen Freiberufler fokussiert hatte, stand die angebotene Leistung gerade in keinem unmittelbaren Zusammenhang mit der originären Geschäftstätigkeit der von den Anrufen betroffenen Freiberufler. Mithin wurde lediglich eine Abnahmemöglichkeit für in unerheblichem Umfang anfallende Nebenprodukte angeboten. Eine derartige Veräußerung von Nebenprodukten stellt für die Angerufenen ein Nebengeschäft dar.

  Da insoweit weder das Kerngeschäft des Freiberuflers unmittelbar von der Offerte des Anrufers tangiert war noch eine Dringlichkeit der Angelegenheit aus Sicht des Angerufenen gerade für eine telefonische Kontaktaufnahme sprach, war eine andere, weniger belästigende Art der Kontaktaufnahme, beispielsweise postalisch, naheliegender.

  Zwar kann eine mutmaßliche Einwilligung auch dann angenommen werden kann, wenn der Werbeanruf gegenüber der postalischen Werbung zwar keine Vorzüge aufweist, aber den Interessen des Angerufenen gleichsam dient, so dass die mit dem Anruf verbundene Belästigung hinnehmbar wäre[52]. Jedoch spielt in diesem Zusammenhang das Interesse des Anrufers keine Rolle. Dass aus der Perspektive des anrufenden Unternehmens eine initiale telefonische Kontaktaufnahme geeigneter erscheint, um organisatorische Abläufe oder sonstige Fragen im Zusammenhang mit der Offerte zu klären, beziehungsweise im zustande gekommenen Gespräch die Vorteilhaftigkeit des eigenen Angebots im Vergleich zu anderen Anbietern zu erörtern, war hierbei unbeachtlich.

- Wirtschaftliche Bedeutung des Angebots[53]

  Gegen das Vorliegen einer mutmaßlichen Einwilligung spricht grundsätzlich, wenn ein Angebot objektiv wirtschaftlich nachteilig ist. Im Umkehrschluss kann jedoch nicht gefolgert werden, dass ein für den Adressaten vorteilhaftes Angebot, welches telefonisch unterbreitet wird, von dem Adressaten nicht trotzdem als belästigend wahrgenommen wird.

---

51 BGH vom 5. Februar 2004 - I ZR 87/02.
52 BGH vom 20. September 2007 - I ZR 88/05 - und 11. März 2010 - I ZR 27/08.
53 BGH vom 16. November 2006 - I ZR 191/03.

Dass die Dienstleistung des anrufenden Unternehmens letztlich für den angerufenen Freiberufler durchaus einträglich war, legitimierte somit für sich genommen den Werbeanruf nicht.

- Nachahmungsgefahr durch Mitbewerber[54]

  Da das anrufende Unternehmen bundesweit mit einer Vielzahl an Mitbewerbern konkurrierte und die Geschäftstätigkeit gerade auf eine spezifische Gruppe von Freiberuflern ausgerichtet war, war somit auch die Gefahr einer empfindlichen Störung des Geschäftsbetriebs der Werbeadressaten anzunehmen.

- Branchenüblichkeit[55]

  Für die Annahme eines Interesses des Angerufenen am konkreten Werbeanruf hätte ausdrücklich sprechen können, dass sich hinsichtlich der telefonischen Werbeansprache eine diesbezügliche Verkehrssitte (§ 157 Bürgerliches Gesetzbuch (BGB)) herausgebildet hat.

  § 157 BGB

  Verträge sind so auszulegen, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern.

  Ein dahingehend belastbarer Sachvortrag, der für die Annahme einer solchen Branchenüblichkeit gesprochen hätte, wurde im Verfahren trotz konkreter Nachfrage nicht vorgebracht. Im Sinne der Urteile des Bundesgerichtshofs (BGH) vom 11. März 2010 - I ZR 27/08 - und 20. September 2007 - I ZR 88/05 -, war vielmehr davon auszugehen, dass eine verbreitete oder sich verbreitende Praxis der telefonischen Kundenakquise im Übrigen nicht für eine Branchenüblichkeit spricht und nicht im Sinne des Adressaten der Werbeansprache sein dürfte.

In der Summe konnte somit nicht von einem sachlichen Interesse des Angerufenen an der telefonischen Werbeansprache und dem Vorliegen einer mutmaßlichen Einwilligung im Sinne des § 7 Abs. 2 Nr. 2 UWG ausgegangen werden. Eine nicht zu bejahende mutmaßliche Einwilligung im wettbewerbsrechtlichen Sinne führte mithin in Konsequenz zur datenschutzrechtlichen Unzulässigkeit der Erhebung und Nutzung der personenbezogenen Daten der Freiberufler für eine telefonische Werbeansprache. Von dieser Bewertung unberührt blieb die Zulässigkeit einer schriftlichen Werbeansprache.

Da sich das Unternehmen dieser Rechtsauffassung nicht anschließen konnte, wurde eine Anordnung nach § 38 Abs. 5 BDSG erlassen und die Einstellung der Anrufpraxis verfügt.

---

[54] BGH vom 20. September 2007 - I ZR 88/05.

[55] BGH vom 25. Januar 2001 - I ZR 53/99: Laut der Entscheidung war die dem Sachverhalt zugrundeliegende telefonische Werbeansprache durch Werkstätten für Blindenwaren seit Jahrzehnten branchenüblich und nicht zu beanstanden.

18.3 Werbeanrufe durch ein Unternehmen (B2C)

Ein Petent erhielt im vermeintlichen Zusammenhang mit einer Meinungsumfrage Anrufe einer ihm unbekannten Stelle. Der Beschwerdeführer konnte die für die Anrufe genutzte Telefonnummer einem saarländischen Versicherungsunternehmen zuordnen und richtete ein Auskunftsersuchen nach § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) an das Unternehmen um die Herkunft seiner Telefonnummer zu erfahren. Da keine Reaktion auf das Auskunftsersuchen erfolgte, wandte sich der Petent an das Datenschutzzentrum.

Nach Aufforderung zur Stellungnahme durch die Aufsichtsbehörde teilte das Versicherungsunternehmen mit, dass die Telefonnummer des Petenten von einem österreichischen Adresshändler erhoben und von dort zur Verfügung gestellt wurde. Nach Ansicht des Unternehmens handele es sich bei dem Anruf nicht um eine Werbeansprache, sondern vor allem um eine Meinungsumfrage. Das Gespräch werde zur Auswertung der Umfrage und als Nachweis für die im Rahmen des Gesprächs mündlich erteilte Einwilligung zur erneuten telefonischen Kontaktaufnahme mit dem Ziel der werblichen Ansprache aufgezeichnet. Im Übrigen sei das Auskunftsersuchen des Petenten postalisch beantwortet worden und wohl auf dem Postweg verloren gegangen.

Im Zuge eines Gesprächstermins in den Räumen des Versicherers wurde der Sachverhalt weitergehend erörtert und dargestellt, dass es sich bei den Anrufen eindeutig um Werbemaßnahmen handelte. Im Hinblick auf den vorliegenden Gesprächsleitfaden war nicht in Abrede zu stellen, dass die initiale Meinungsumfrage nur dem Zweck diente, eine Einwilligung in eine weitergehende telefonische Werbeansprache zu generieren (Opt-In-Abfrage).[56]

Die Geschäftsleitung des Versicherungsunternehmens konnte sich der dahingehenden Einordnung des Anrufs als Werbemaßnahme durchaus anschließen, vertrat jedoch weiterhin die Auffassung, dass die Telefonnummern, die unter anderem von österreichischen und schweizerischen Adresshändlern bezogen wurden, letztlich für Werbeanrufe zulässig genutzt werden könnten, da von dem Adresshändler ohnehin die Anrufe legitimierende Einwilligungserklärungen bereits zur Verfügung gestellt worden seien.

Diese Aussage war vor dem Hintergrund erstaunlich, als von dem Versicherungsunternehmen im Rahmen der als Meinungsumfrage vorgegebenen Werbeanrufe erneut Werbeeinwilligungen eingeholt wurden. Die Geschäftsleitung erklärte hierzu eine erneute Einholung der Einwilligung sei schlichtweg zweckmäßig.

Eine stichprobenartige Überprüfung der dem Versicherungsunternehmen von Adresshändlern zur Verfügung gestellten Werbeeinwilligungen der Betroffenen offenbarte, dass diese in keiner Weise die für eine Wirksamkeit der Erklärung notwendigen Voraussetzungen erfüllten.

---

[56] Siehe dazu auch Urteil des Verwaltungsgerichts Berlin vom 7. Mai 2014 - VG 1 K 253.12 - und Urteil des Landgerichts Düsseldorf vom 20. Dezember 2013 - 33 O 95/13 U.

Die Einwilligungen in die telefonische Werbeansprache seien in diesem Zusammenhang im Rahmen der Teilnahme an einem Online-Gewinnspiel eines indonesischen Webseitenbetreibers generiert worden. Vorgelegt wurden diesbezüglich Datensätze (sog. Leads), denen sich vermeintlich entnehmen lassen sollte, welche Daten die Betroffenen unter welcher IP-Adresse zu welchem Zeitpunkt im Rahmen des Online-Gewinnspiels preisgegeben haben. Unabhängig davon, dass sich die Angaben in den Datensätzen nicht verifizieren ließen, stellten sie auch für sich genommen keinen geeigneten und belastbaren Nachweis für die zu fordernde ausdrückliche Einwilligung der Betroffenen dar.[57]

Eine weitere Nutzung der vorliegenden Datensätze für Werbeanrufe war damit datenschutzrechtlich und auch im Hinblick auf § 7 Abs. 2 S. 2 Gesetz gegen den unlauteren Wettbewerb (UWG) wettbewerbsrechtlich ausgeschlossen.

§ 7 Abs. 2 Nr. 2 UWG

Eine unzumutbare Belästigung ist stets anzunehmen bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung oder gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung.

Nachdem dem Versicherungsunternehmen die aufsichtsbehördliche Bewertung des Sachverhalts kommuniziert wurde, teilte dieses mit, dass die telefonische Werbeansprache eingestellt worden sei und die dementsprechenden Datensätze gelöscht worden seien. Daher bedurfte es insoweit keiner weitergehenden aufsichtsbehördlichen Maßnahmen gegenüber dem Versicherer. Dies wurde dem Petenten mitgeteilt.

Da die unzulässigen Werbeanrufe des Versicherungsunternehmens aber auch einen Bußgeldtatbestand im Sinne des § 20 Abs. 1 Nr. 1 UWG darstellten und die Bundesnetzagentur nach § 20 Abs. 3 in Verbindung mit § 7 UWG zuständige Bußgeldbehörde zur Ahndung von Maßnahmen unerlaubter Telefonwerbung ist, wurde der Petent darauf aufmerksam gemacht, dass er eine diesbezügliche Beschwerde an die Bundesnetzagentur richten kann.[58]

Abschließend bat das Versicherungsunternehmen das Datenschutzzentrum um Auskunft, unter welchen Voraussetzungen der Versicherer personenbezogene Daten von Adresshändlern für telefonische Werbemaßnahmen beziehen und nutzen kann. Hintergrund war, dass dem Versicherer von einem in Deutschland ansässigen Adresshändler Leads für eine telefonische Werbeansprache angeboten wurden.

Dieser Adresshändler habe über ein Online-Gewinnspiel Einwilligungen generiert, die Anrufe unmittelbar durch diesen ermöglichten (Grund-Opt-In). Im Rahmen dieser Anrufe könne der Adresshändler sodann auftragsbezogen telefonisch nachfragen, ob der Angerufene seinerseits mit einem Werbeanruf des Aufgebers einverstanden wäre. Diese telefonisch erteilte Einwilligung in den Werbeanruf durch den Auftraggeber würde sodann mit Zustimmung des Angerufenen aufgenommen (Voicefile).

---

[57] Siehe dazu auch das Urteil des Bundesgerichtshofs vom 10. Februar 2011- I ZR 164/09.

[58] Siehe dazu auch die Webseite der Bundesnetzagentur unter: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Verbraucher/UnerlaubteTelefonwerbung/unerlaubtetelefonwerbung-node.html

Dem Versicherer wurde diesbezüglich mitgeteilt, dass er als die für die werbliche Nutzung dieser Daten verantwortliche Stelle überprüfen müsse, auf welche Art und Weise und in welchem Zusammenhang der Adresshändler die Einwilligung in die telefonische Werbeansprache datenschutzrechtlich (sowie wettbewerbsrechtlich) zulässig generiert. Die diesbezüglich durchgeführten Prüfschritte und die Erwägungen, die aus Sicht des werbenden Unternehmens zur Zulässigkeit der Nutzung der Leads führen, seien zu dokumentieren.

Eine alleinige Versicherung des Adresshändlers, dass die zur Verfügung gestellten Datensätze für eine telefonische Werbeansprache genutzt werden können, entlässt das werbende Unternehmen nicht aus der Verantwortung.

Dementsprechend wird ein seriöser Adresshändler, der unter Beachtung der rechtlichen Gegebenheiten operiert, bereitwillig darlegen, in welchem Zusammenhang ein zu veräußernder Datenbestand generiert wurde und diesbezügliche Einwilligungserklärungen rechtlich wirksam sind.

Bei näherer Betrachtung der Umstände der Generierung des Grund-Opt-Ins war bereits ersichtlich, dass diese Einwilligungserklärung rechtlich nicht als wirksam bezeichnet werden konnte. Die Leadgenerierung über das Online-Gewinnspiel erfolgte nicht unmittelbar über den Adresshändler, sondern über eine dritte Stelle. Der Adresshändler wurde lediglich mit über 20 anderen Stellen als „Sponsor" des Gewinnspiels benannt, an die die Leads für telefonische Ansprachen übermittelt wurden (Leadgenerierung durch Co-Registrierung).

Im Hinblick auf die Entscheidung des Bundesgerichthofs vom 25. Oktober 2012 - I ZR 169/10 - (Einwilligung in Werbeanrufe II) ist eine Einwilligung nur wirksam, wenn sie in Kenntnis der Sachlage und für den konkreten Fall erklärt wird. Dahingehend muss sich der Erklärende darüber im Klaren sein, welchen Unternehmen die Möglichkeit eingeräumt wird, sich mit Werbeanrufen an ihn zu wenden.

Eine zu fordernde Transparenz der Erklärung ist dann fraglich, wenn die Liste der Sponsoren nicht mehr übersichtlich ist. Bei über zwanzig Sponsoren war nach Ansicht des Datenschutzzentrums keine Transparenz der Erklärung mehr gegeben und das Grund-Opt-In als unwirksam anzusehen.

Das Unternehmen sah schließlich davon ab, die betreffenden Leads anzukaufen.

19 Wohnungswirtschaft

19.1 Fragerecht des Vermieters

Im laufenden Berichtszeitraum zeigte sich, dass der Datenumgang durch Vermieter bzw. Makler bei etlichen Wohnungssuchenden zu Unverständnis und Verdruss führt.

Gleich zu Beginn eines potentiellen Mietvertragsverhältnisses wollen viele Vermieter bereits ein Maximum an Informationen über den Mietinteressenten in Erfahrung bringen. Bevor überhaupt ein Besichtigungstermin zustande kommt, sollen vielfach Angaben zum Familienstand, zum Einkommen und zu weiteren Lebenssachverhalten gemacht werden. Kommt es dann zum Besichtigungstermin, wird seitens der Vermieterpartei häufig eine Kopie des Personalausweises, eine Verdienstbescheinigung sowie die Vorlage einer Schufa-Auskunft o.ä. gefordert.

Aufgrund der Drucksituation auf den angespannten Wohnungsmärkten insbesondere in den Städten zögern viele Mietinteressenten nicht, die geforderten Unterlagen vorzulegen, um überhaupt eine Chance bei der Wohnungsvergabe zu haben.

Dass Mietinteressenten aufgefordert werden, bereits zum Besichtigungstermin eine Schufa-Auskunft mitzubringen, begegnet datenschutzrechtlichen Bedenken. Zwar benötigt der künftige Vermieter Informationen zu den wirtschaftlichen Verhältnissen, um die Zahlungsfähigkeit des Mietinteressenten zu beurteilen, jedoch ist es keineswegs erforderlich, dass dem Vermieter von allen Mietinteressenten Schufa-Auskünfte vorliegen, sondern nur von demjenigen, mit dem er den Mietvertrag auch tatsächlich schließen möchte.

Nicht zulässig ist es auch, sich von Auskunfteien den Mietinteressenten zur Verfügung gestellte Selbstauskünfte vorlegen zu lassen, da diese nur für die Antragsteller selbst bestimmt sind und auch mehr Angaben über deren wirtschaftliche Verhältnisse enthalten, als es bei reinen Bonitätsauskünften der Fall ist. Aber auch das Verlangen des künftigen Vermieters, eine Einwilligungserklärung für die Einholung einer Bonitätsauskunft abzugeben, ist nicht zulässig, da davon auszugehen ist, dass die Einwilligung – bedingt durch die auf dem Wohnungsmarkt vorherrschende Drucksituation – nicht freiwillig im Sinne des § 4a Abs. 1 Bundesdatenschutzgesetz (BDSG) abgegeben wird.

Aus diesem Grund ist die Einholung einer Bonitätsauskunft über einen Mietinteressenten erst dann zulässig, wenn der Abschluss des Mietvertrages nur noch vom positiven Ergebnis der Bonitätsprüfung abhängig ist.

Das Beschriebene zeigt, dass sich die Vermieter bzw. Makler bei der Wohnungsvermittlung häufig zielgerichtet oder in Unkenntnis der rechtlichen Gegebenheiten jenseits datenschutzrechtlicher Grenzen bewegen. Um dem überhaupt Einhalt gebieten zu können und auch datenschutzbewussten Mietinteressenten Chancengleichheit zu gewährleisten, haben die Datenschutzaufsichtsbehörden des Bundes und der Länder

bereits vor geraumer Zeit eine Orientierungshilfe erstellt, die die wichtigsten Vorgaben zum Fragerecht des Vermieters und zur Einholung von Selbstauskünften bei Mietinteressenten prägnant zusammenfasst.[59]

Darin wird das Mietvertragsanbahnungsverhältnis in drei Stufen aufgeteilt. So sind für die Vereinbarung eines Besichtigungstermins Angaben zur Identifikation und gegebenenfalls zum Wohnberechtigungsschein und zu Haustieren zulässig, wohingegen Angaben zur wirtschaftlichen Situation in diesem frühen Stadium noch nicht erforderlich sind. Auch die Anfertigung einer Personalausweiskopie ist grundsätzlich unzulässig. Vielmehr ist es ausreichend, wenn sich der Vermieter den Ausweis vorlegen lässt und so die Identität feststellt.

19.2 Verkauf von Wohneigentum

Im Vergleich zur Wohnraumvermietung sind für einen Makler beim Verkauf von Wohnimmobilien weitere Vorgaben zu beachten.

Nach § 2 Abs. 1 Nr. 10 Geldwäschegesetz (GwG) werden Immobilienmakler zur Mitarbeit bei der Bekämpfung von Steuerhinterziehung verpflichtet. Dabei müssen Sie die Identität ihrer Kunden prüfen und dokumentieren (gilt nur bei Veräußerungs- und nicht bei Mietgeschäften). Diese Pflicht ergibt sich aus § 3 Abs. 1 Nr. 1 GwG. Daneben schreibt § 4 Abs. 1 GwG vor, dass die Identitätsprüfung vor Begründung der Geschäftsbeziehung oder Durchführung der Transaktion stattzufinden hat. Bei den zur Identitätsfeststellung erforderlichen Daten handelt es sich um Name, Geburtsort und -datum, Staatsangehörigkeit sowie die Wohnanschrift. Nach § 8 Abs. 1 GwG darf der Makler auch den Ausweis des Kunden kopieren.

Insoweit kommt es darauf an, zu welchem Zeitpunkt der konkrete Maklervertrag zustande kommt. Nach überwiegender Meinung löst allein die Übersendung des Exposés die Identifizierungspflicht noch nicht aus. Es müssen daneben weitere Umstände hinzutreten, die den Maklervertrag begründen, wie beispielsweise die Durchführung eines Besichtigungstermins und ein eindeutiges Signal eines Kaufinteressenten, ein Objekt erwerben zu wollen. Eine Identifizierungspflicht sämtlicher Kaufinteressenten würde zudem dem Datensparsamkeitsgebot zuwiderlaufen.

19.3 Anmeldung beim Grundversorger durch Vermieter rechtens?

Im Berichtszeitraum schilderte ein Petent, dass er nach Unterzeichnung des Mietvertrages und noch vor dem Einzugstermin in seinem neuen Briefkasten einen vorgefertigten Antrag des regionalen Energiegrundversorgers, welcher bereits mit seinen personenbezogenen Daten ausgefüllt war, vorfand. Auf Nachfrage wurde ihm von diesem mitgeteilt, dass die Daten von dem Vermieter stammten. Eine Einwilligung in

[59] Vgl. https://datenschutz.saarland.de/themen/wohnungswirtschaft/

diese Datenübermittlung hatte der Petent laut eigener Aussage nicht erteilt. Er vermutete einen Datenschutzverstoß und bat die Aufsichtsbehörde um rechtliche Einschätzung.

Dem Beschwerdeführer wurde mitgeteilt, dass die Übermittlung von Daten durch den Vermieter an den Energiegrundversorger unter bestimmten Voraussetzungen zulässig sein kann, im vorliegenden Fall allerdings datenschutzrechtlich unzulässig erfolgte.

Nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist eine Datenübermittlung nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Da eine Einwilligung nicht erteilt wurde und eine bereichsspezifische Übermittlungsgrundlage nicht ersichtlich war, kam als Ermächtigungsgrundlage allein § 28 BDSG in Betracht.

So war zu prüfen, ob die Datenübermittlung zur Wahrung berechtigter Interessen eines Dritten, nämlich des Grundversorgers, erforderlich war und kein Grund zu der Annahme bestand, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hatte, § 28 Abs. 2 Nr. 2 lit. a BDSG.

Die Versorgung aller Haushaltskunden wird in Deutschland durch die Grund- und Ersatzversorgung gewährleistet. Bei der Wahl ihres Energielieferanten sind die Verbraucher frei und nicht an den Energiegrundversorger gebunden. Häufig beziehen viele Haushalte dennoch ihren Strom von dem jeweiligen Grundversorger. In der Regel wird hierzu ein schriftlicher Grundversorgungsvertrag geschlossen, in dem die Einzelheiten der Belieferung festgehalten werden. Die Strom- bzw. Gasgrundversorgungsverordnung bilden den Rechtsrahmen der Grundversorgung.

Ein Grundversorgungsvertrag kommt allerdings auch durch konkludentes Handeln zustande, d.h. wenn der Verbraucher nach dem Einzug beispielsweise durch das erstmalige Einschalten des Lichts Energie verbraucht (vgl. Urteil des Bundesgerichtshof vom 2. Juli 2014 – VIII ZR 316/13).

Nach § 2 Abs. 2 der Stromgrundversorgungsverordnung besteht sodann eine unverzügliche Mitteilungspflicht des Verbrauchers an den Grundversorger.

Der Petent hatte mitgeteilt, dass die mit seinen Daten ausgefüllten Antragsunterlagen bereits im Briefkasten lagen, noch bevor er die Wohnung erstmals nach der Schlüsselübergabe betreten hatte. Infolgedessen war davon auszugehen, dass der Vermieter die Mieterdaten proaktiv an den Grundversorger übermittelt hatte, um gegebenenfalls zu verhindern, dass sein Mieter der Mitteilungspflicht nicht nachkommen würde. Jedenfalls war im Zeitpunkt der Datenübermittlung noch kein (konkludenter) Vertrag zwischen Mieter und Versorgungsunternehmen zustande gekommen, so dass die Übermittlung auch nicht zur Wahrnehmung eines berechtigten Interesses des Versorgers erforderlich war und demnach datenschutzrechtlich unzulässig erfolgte.

Etwas anderes wäre dann anzunehmen gewesen, wenn der Mieter den Stromverbrauch nach seinem Einzug entgegen seiner Mitteilungspflicht nicht beim Grundversorger angezeigt hätte. In diesem Fall wäre der Mieter durch die fortwährende Stromentnahme zum Vertragspartner des Grundversorgers geworden. Dieser hat ein

besonders schützenswertes Interesse an der Kenntnisnahme der Identität seines Vertragspartners, um mit diesem die mit dem Abschluss des Grundversorgungsvertrages verbundenen Entscheidungen sachgerecht treffen zu können (vgl. Urteil des Oberlandesgerichts Nürnberg vom 23. Mai 2014 – 2 U 2401/12). Die Übermittlung von Vor- und Nachname des Mieters auf Anfrage des Grundversorgers durch den Vermieter ist danach zulässig, da auch keine schützenswerten Interessen des Betroffenen, der seinen in seiner Mietereigenschaft begründeten Pflichten nicht nachgekommen ist, der Datenübermittlung entgegenstehen.

19.4 Zulässigkeit von Klimasensoren in Mietwohnungen

Ein Unternehmen trat im Berichtszeitraum mit der Frage an das Unabhängige Datenschutzzentrum heran, unter welchen datenschutzrechtlichen Bedingungen von dem Unternehmen angebotene Klimasensoren in Mietwohnungen im Saarland auf Wunsch der Vermieter dauerhaft angebracht werden können.

Im Hinblick auf das heikle Thema Schimmel in der Mietsache und die in diesem Zusammenhang in großer Zahl vorkommenden gerichtlichen Auseinandersetzungen zwischen Mietern und Vermietern würde das anfragende Unternehmen ein Sensorsystem anbieten, welches in „gefährdeten" Räumen einer Mietwohnung die relative Luftfeuchtigkeit, die Temperatur, den Luftdruck sowie den CO- und CO_2-Gehalt permanent erfasst. Die ermittelten Daten würden sodann von dem einzelnen Sensor an das Unternehmen übermittelt und dort für einen beliebigen Zeitraum gespeichert.

Nach dem vorgelegten Konzept sollte bei der Feststellung eines den Schimmel begünstigenden Raumklimas der Mieter über eine automatisch durch das System erzeugte Meldung informiert werden, damit dieser Gegenmaßnahmen ergreifen kann. Gleichzeitig erhielte auch der Vermieter eine Meldung über die Grenzwertüberschreitung. Beide Parteien sollten zudem gleichermaßen auf die gespeicherten Daten zugreifen können.

Im Rahmen des Einsatzes des Sensorsystems würde somit unstrittig mit personenbezogenen Daten von Mietern im Sinne des § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) umgegangen, da gerade eine Personenbeziehbarkeit der systemseitig im Wohnraum des jeweiligen Mieters erfassten und gespeicherten Werte intendiert wird.

§ 3 Abs. 1 BDSG

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Weiterhin war davon auszugehen, dass der jeweilige Vermieter für den Datenumgang verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG wäre und von dem Unternehmen, das seinen Sitz nicht im Zuständigkeitsbereich der saarländischen Aufsichtsbehörde hatte, lediglich die Infrastruktur zur Verfügung gestellt würde.

§ 3 Abs. 7 BDSG

Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Zwischen der verantwortliche Stelle und dem Bereitsteller der Infrastruktur wäre somit notwendigerweise ein Auftragsdatenverarbeitungsverhältnis im Sinne des § 11 BDSG anzunehmen.

§ 11 Abs. 1 S. 1 BDSG

Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich.

Grundlage für den Datenumgang könnte im Hinblick auf § 4 Abs. 1 BDSG allenfalls die Einwilligung des betroffenen Mieters sein. Grundsätzlich wäre eine Legitimation des Umgangs mit den genannten Mieterdaten durch den Vermieter auf Grundlage einer Einwilligung denkbar, jedoch könnte beispielsweise eine unmittelbar im Mietvertrag aufgeführte Klausel aus den folgenden Gründen keine Einwilligungserklärung im Sinne des § 4 in Verbindung mit § 4a Abs. 1 BDSG darstellen.

Entscheidendes Merkmal einer wirksamen Einwilligungserklärung ist, dass diese von dem Betroffenen ohne Zwang und somit freiwillig abgegeben wird (§ 4a Abs. 1 S. 1 BDSG). Dem betroffenen Mieter muss es, ohne Sanktionen des Vermieters befürchten zu müssen, anheimgestellt bleiben, ob er sich mit der diesbezüglichen Datenverarbeitung einverstanden erklärt oder eben nicht.

Eine Einwilligungserklärung als Bestandteil des Mietvertrags würde vor allem bei der Neubegründung eines Mietverhältnisses erheblichen datenschutzrechtlichen Bedenken begegnen, da aufgrund des anzunehmenden Verhandlungsungleichgewichts zwischen Vermieter und Mietinteressent der Eindruck erweckt wird, dass der Abschluss des Mietvertrages von der Einwilligung des Mieters in den Einsatz des Sensorsystems abhängig gemacht wird. Aus diesem Grund wäre beispielsweise bei Neubegründung eines Mietverhältnisses eine datenschutzkonforme Einwilligungserklärung losgelöst von der mietvertraglichen Vereinbarung einzuholen, da ansonsten nicht von einer freiwilligen und somit wirksamen Einwilligung des betroffenen Mieters ausgegangen werden kann.

Nach Darlegung der aufsichtsbehördlichen Bewertung des Sachverhalts, erfolgte keine weitere Rückmeldung des Unternehmens. Ob besagte Klimasensoren von saarländischen Vermietern tatsächlich eingesetzt werden, konnte bis dato nicht in Erfahrung gebracht werden.

19.5 Fernüberwachbare Funk-Rauchwarnmelder

Bis zum Stichtag 31. Dezember 2016 waren nach § 46 Abs. 4 Landesbauordnung Saarland (LBO) die Wohnungseigentümer verpflichtet, in den Schlafräumen und Flu-

ren von bestehenden Wohnungen Rauchmelder zu installieren. Für die Betriebsbereitschaft haftet der jeweilige Mieter, es sei denn der Eigentümer übernimmt die Verpflichtung selbst.

Im Berichtszeitraum meldeten sich bei der Aufsichtsbehörde mehrere Personen, die von ihren Vermietern angeschrieben wurden, da in den Wohnungen sogenannte fernüberwachbare Funk-Rauchwarnmelder eingebaut werden sollten. Die Petenten befürchteten, dass mithilfe der Melder auch sensible Daten erhoben werden, und baten die Aufsichtsbehörde um rechtliche Einschätzung. Einige wollten den Vermietern daher den Einbau der Geräte auch verwehren. Da die Kosten der Rauchwarnmelder und die Kosten für deren Wartung als Mietnebenkosten auf den Mieter umgelegt werden können, standen dem Einbau wohl aber auch wirtschaftliche Interessen von Seiten der Mieter entgegen.

Den Betroffenen wurde mitgeteilt, dass die Anbringung von Funk-Rauchwarnmeldern dann von datenschutzrechtlicher Relevanz ist, wenn per Funkabfrage nicht bloß die reine Funktionstüchtigkeit der Geräte abgefragt wird, sondern auch noch weitere Daten mithilfe der Geräte erhoben und gespeichert werden. Je nach eingesetztem Gerät werden Daten über räumliche Zustände bzw. Veränderungen im Umfeld des Rauchwarnmelders erhoben. Dies betrifft beispielsweise Angaben über den Verschmutzungsgrad der Rauchkammer, eine Demontageerkennung und die Umfeldüberwachung. Jedoch spricht auch dann aufgrund des geringen Detaillierungsgrades der Informationen einiges dafür, dass die Anbringung solcher Geräte datenschutzrechtlich zulässig erfolgen kann.

So hat das Bundesverfassungsgericht (BVerfG) entschieden, dass die Installation von Funk-Rauchwarnmeldern keine Verletzung allgemeiner Persönlichkeitsrechte bedeutet und vom Mieter zu dulden sei. Insbesondere sei die durch den Einsatz von Funk-Rauchwarnmeldern gewonnene Möglichkeit der Fernwartung mit Vorteilen für die Bewohner verbunden (BVerfG, Beschluss vom 8. Dezember 2015 – 1 BvR 2921/15). Auch der Bundesgerichtshof hat eine Duldungspflicht der Mieter bei der ähnlich gelagerten Fragestellung zur Zulässigkeit der Anbringung funkbasierter Ablesegeräte für Heizung und Wasser bejaht (Entscheidung vom 28. September 2011 – VIII ZR 326/10). In die gleiche Richtung tendiert auch das AG Dortmund, nach dessen Ausführungen funkbasierte Heizkostengeräte nicht zwangsläufig gegen datenschutzrechtliche Bestimmungen verstoßen (Urteil vom 26. November 2013 – 512 C 42/13).

Im Zweifel sollten sich Mieter mit ihrem Vermieter bzw. der Hausverwaltung in Verbindung setzen und dort erfragen, ob und welche Daten gegebenenfalls durch die Rauchwarnmelder erhoben und gespeichert werden. Wird lediglich die reine Funktionstüchtigkeit der Geräte per Funk abgefragt, spricht datenschutzrechtlich nichts gegen die Zulässigkeit der Anbringung eines solchen Geräts.

20 Wirtschaft

20.1 Bußgeldverfahren wegen unzulässigen Umgangs mit Kundendaten in Franchisesystemen

Sachverhalt

Bereits im letzten Tätigkeitsbericht[60] hatten wir über den Fall eines Franchisegebers mit Sitz im Saarland berichtet, der seinen Franchisenehmern die Nutzung einer webbasierten Anwendung verpflichtend vorgab, mit deren Hilfe nahezu die Gesamtheit ihrer administrativen Prozesse abgebildet wurde. Im Rahmen der vom Franchisegeber entwickelten und administrierten Anwendung waren die Franchisenehmer verpflichtet, zwangsläufig alle Kundendaten in diese Webanwendung einzugeben und dauerhaft zu pflegen. Die Verpflichtung zur Nutzung dieser Webanwendung wurde unter Verweis auf die lizenzvertragliche Weisungsbefugnis des Franchisegebers vorgeschrieben und von diesem auch zivilrechtlich durchgesetzt.

Zu dieser Webanwendung erhielt jeder Franchisenehmer einen eigenen Zugang. Hinsichtlich dieses Datenverarbeitungsprogramms hatten die Franchisenehmer mit Ausnahme der Funktionen, die das Web-Frontend zur Verfügung stellte, keinen Einfluss auf die technische oder organisatorische Ausgestaltung. Weder konnten die Franchisenehmer entscheiden, welche Arten von personenbezogenen Daten sie eingeben, wo die Daten der Endkunden gespeichert werden, wer zu welchem Zeitpunkt Zugriff auf diese hat, wohin diese übermittelt werden, noch wie lange die Daten aufbewahrt werden. Der Betrieb des Systems, der Zugriff auf die Daten sowie die technischen und organisatorischen Parameter wurden allein durch den Franchisegeber bereitgestellt und gesteuert.

Die auf Servern des Franchisegebers gespeicherten vollständigen Kundendatensätze wurden von diesem zur Erstellung nicht-personenbezogener betriebswirtschaftlicher Kennzahlen und zur Entgeltabrechnungskontrolle herangezogen. Im Übrigen wurden durch den Systemgeber keine zentralen Aufgaben für alle Stellen des Netzwerks wahrgenommen, die eine Weitergabe von Kundendaten erforderlich gemacht hätten.

Trotz anfänglichen Widerstands konnte schließlich eine datenschutzkonforme Ausgestaltung des Franchisesystems erreicht werden. Daneben war der Sachverhalt noch ordnungswidrigkeitenrechtlich zu bewerten.

Da der Umgang des Franchisegebers mit den personenbezogenen Daten der Endkunden der Franchisenehmer den Anfangsverdacht wegen Verstoßes gegen § 43 Abs. 1 Nr. 8 Bundesdatenschutzgesetz (BDSG) und Verstoßes gegen § 43 Abs. 2 Nr. 1 BDSG begründete, wurde ein entsprechendes Bußgeldverfahren eingeleitet.

---

[60] Vgl. 25. Tätigkeitsbericht, 2013/2014, Kapitel 20.2, S. 134-137.

Aus dem Verwaltungsverfahren ergaben sich tatsächliche Anhaltspunkte dafür, dass es sich wegen Art und Umfang der Datenverarbeitung und der Vielzahl der Franchisenehmer um eine erhebliche Datenmenge handeln musste, die in dem Datenbanksystem, das der Webanwendung des Franchisegebers zugrunde lag, hinterlegt war. Daher beantragten wir beim Ermittlungsrichter den Erlass einer Durchsuchungs- und Beschlagnahmeanordnung zur Sicherstellung der MySQL-Datenbank.

Die Auswertung der sichergestellten MySQL-Datenbank ergab, dass in der etwa zwei Gigabyte großen Datenbank Endkundendaten von insgesamt 143 Franchisenehmern aus Deutschland, Österreich, der Schweiz und Luxemburg enthalten waren. Die Datenbank enthielt Informationen / Stammdaten zu 144.849 Vertragsverhältnissen und knapp 380.000 Einzelpersonen. Darunter Angaben zu Namen, Geburtsdatum, Anschrift, Mobilfunknummern und E-Mail-Adressen, Konto- und Zahlungsdaten bis hin zu besonders sensiblen Gesundheitsdaten über die Betroffenen. Teilweise gingen die in der Datenbank enthaltenen Informationen zu Endkundenvertragsverhältnissen bis in das Jahr 2000 zurück. In 132.044 von 144.849 Fällen bezogen sich die gespeicherten Informationen auf Vertragsverhältnisse, die auf Grund von Kündigung, Widerruf oder Zeitablauf überhaupt nicht mehr existent waren.

Rechtliche Würdigung

Indem der Franchisegeber seine Franchisenehmer vertraglich dazu verpflichtete, über die Eingabeformulare des Erfassungs- und Verarbeitungsmoduls der Webanwendung Informationen über die eigenen Kunden einzugeben und die so eingegebenen Informationen in der MySQL-Datenbank auf dem Server des Franchisegebers hinterlegt wurden, lag eine Erhebung und Speicherung personenbezogener Daten durch den Franchisegeber vor.

Nach § 3 Abs. 3 BDSG ist das Erheben das Beschaffen von Daten über einen Betroffenen. Erheben setzt daher ein aktives und zielgerichtetes Handeln voraus, mit dem personenbezogene Daten in den eigenen Verantwortungsbereich der verantwortlichen Stelle gelangen. Die Anweisung an die Franchisenehmer, die vom Franchisegeber bereitgestellte Webanwendung zu nutzen, stellte ein solch aktives Handeln dar. In Ausübung der vertraglich eingeräumten Weisungsbefugnis verpflichtete der Franchisegeber die Franchisenehmer dazu, dass diese die Webanwendung nutzen sollten, um dort die eigenen Kundendaten einzupflegen. Franchisenehmer, die sich weigerten, wurden vom Franchisegeber zunächst abgemahnt und schließlich mit zivilprozessualen Mitteln auf die Nutzung der Webanwendung verpflichtet. Dieses Handeln des Franchisegebers war auch zielgerichtet, da es mit der Verpflichtung zur Eingabe der Kundendaten durch den Franchisenehmer gerade darauf abzielte, dass die so eingegebenen Daten in der vom Franchisegeber bereitgestellten MySQL-Datenbank gespeichert wurden und damit in seinen Herrschaftsbereich gelangten. Dort wurden die personenbezogenen Daten der Endkunden entsprechend § 3 Abs. 4 Nr. 1 BDSG aufbewahrt.

Eine Rechtsgrundlage für diese Datenverarbeitungsvorgänge war nicht erkennbar. Eine Einwilligung schied schon deshalb als Rechtfertigungsgrundlage aus, weil die Weitergabe der Daten an den Franchisegeber ohne Kenntnis der Betroffenen

geschah und damit auch gegen den Direkterhebungsgrundsatz verstieß. Auch gesetzliche Erlaubnistatbestände schieden vor dem Hintergrund von Art und Umfang der Datenverarbeitung durch den Franchisegeber offensichtlich aus.

Der Franchisegeber wurde auch nicht als Auftragsdatenverarbeiter für den jeweiligen Franchisenehmer tätig. Hierfür fehlte es bereits an einem Vertrag im Sinne des § 11 BDSG. Zudem ließen die Feststellungen im Verwaltungs- und Bußgeldverfahren den Schluss zu, dass das Verhältnis von Franchisegeber zu -nehmer derart ausgestaltet war, dass, anders als von § 11 BDSG verlangt, der Franchisegeber hier nicht weisungsgebunden agierte, sondern dass er sich selbst als vollumfänglich weisungsbefugt gegenüber dem Franchisenehmer betrachtete. Eine wirksame Auftragsdaten-verarbeitung konnte unter diesen Umständen nicht zustande kommen.

Aber auch aus anderen Gründen bestanden Vorbehalte gegen eine Auftragsdatenverarbeitung durch den Franchisegeber als Auftragnehmer. § 11 Abs. 2 Satz 1 BDSG verlangt, dass der Auftraggeber den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen hat. Eine entsprechende Auswahlentscheidung konnte der Franchisenehmer im hier zugrundeliegenden Fall aber nicht treffen. Er hatte die Vorgaben des Franchisegebers zur Nutzung der Webanwendung zu befolgen, wodurch dem Franchisenehmer die Auswahlentscheidung im Hinblick auf die Stelle, die er mit der Verarbeitung seiner Kundendaten betrauen wollte, gerade nicht möglich war. Eine „aufgedrängte" Auftragsdatenvereinbarung ist mit dem Grundgedanken des § 11 Abs. 2 Satz 1 BDSG und den daran anknüpfenden Haftungsfolgen (etwa § 7 BDSG) nicht vereinbar.

Ergebnis

In dem Ordnungswidrigkeitsverfahren erging ein Bußgeld in fünfstelliger Höhe gegen den Franchisegeber. Der Bußgeldbescheid ist bestandskräftig.

20.2 Crowd Sensing

Durch eine Veröffentlichung in einer Lokalzeitung wurden wir darauf aufmerksam gemacht, dass die Stadtwerke einer saarländischen Kommune im Zusammenhang mit einer bevorstehenden Großveranstaltung eine App mit sog. Crowd Sensing-Technologie veröffentlichte. Mit dieser Technologie können Menschenmassen und Bewegungsrichtungen erkannt werden. Nach Installation der App auf dem Endgerät war es den Stadtwerken möglich, die Besucherströme während der Veranstaltung zu erfassen, um dadurch die Einsatzkräfte im Notfall mit zusätzlichen Informationen versorgen zu können. Dies sollte anonym erfolgen.

Die zur Visualisierung der Besucherströme notwendige Crowd Sensing-Technik setzt dabei auf die GPS-Sensorik der Smartphones, auf denen die App installiert wurde. Mit Hilfe des GPS-Sensors werden die Position und die Geschwindigkeit, mit der sich eine Person bewegt, bestimmt. Der Kompass gibt die Richtung an. Hierfür sind zwei

Parameter entscheidend: die sog. Geozone und der Crowd Sensing-Zeitraum. Die Geozone beschreibt (an Hand von GPS-Koordinaten) einen geographischen Bereich innerhalb dessen eine Aufzeichnung der Positionen und Bewegungen des Mobilgerätes stattfindet. Der Crowd Sensing-Zeitraum bestimmt den Zeitpunkt einer Aufzeichnung. Das Crowd Sensing-Modul auf dem Gerät des Nutzers schaltet sich also dann „scharf", wenn der Nutzer sich während des vorher definierten Zeitraums in der vordefinierten Geozone befindet.

Ist dies der Fall, sind also die beiden Voraussetzungen (Nutzer innerhalb der Geozone, während des Aufnahmezeitraums) gleichzeitig erfüllt und die App damit „scharf" geschaltet, so erfasst das Crowd Sensing Modul jede Sekunde die GPS-Position des Mobilgerätes, die Genauigkeit der erfassten GPS-Position sowie die Bewegungsrichtung und -geschwindigkeit. Einmal pro Minute werden die so gesammelten Werte an einen Cloud-Server übertragen und dann in eine Karte des Areals in Form einer Heatmap[61] zur Visualisierung der Daten eingetragen und dargestellt. So lässt sich erkennen, wie dicht gedrängt an bestimmten Stellen die Menge ist und ob es darin Turbulenzen gibt, also Menschen, die sich auffallend abweichend von gewöhnlichen Bewegungsmustern verhalten.

Um die von der App an den Cloud-Server gelieferten Positions- und Bewegungsdaten voneinander unterscheiden und diese einem Besucher zuordnen zu können, ist die Verwendung eines Identifikators zwingend notwendig. Ohne diesen Identifikator wäre eine Erfassung des Besucheraufkommens nicht möglich. In unserem Fall wurde beim erstmaligen Start der App ein zufälliger, aber global eindeutiger Identifikator, eine sog. UUID (Universally Unique Identifier) generiert. Diese UUID blieb dauerhaft erhalten. Erst beim Löschen und nach einer Neuinstallation der App wurde eine neue UUID generiert. Diese UUID wurde jede Minute zusammen mit den Positions- und Bewegungsdaten der letzten 60 Sekunden an den Cloud-Server der Stadtwerke mitübertragen.

Voraussetzung für das Funktionieren der Crowd Sensing-Technologie war jedoch, dass der Nutzer beim erstmaligen Start der App dieser den Zugriff auf den GPS-Sensor gestattete. In dem entsprechenden Bestätigungsdialog wurde der Nutzer darauf hingewiesen, dass die App Zugriff auf den Standort benötige, um *„ortsbezogene Nachrichten während der Großveranstaltung empfangen zu können."*

Zunächst galt es zu prüfen, ob die an den Cloud-Server übertragenen Informationen als personenbezogene Daten zu werten waren. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen. Dies traf auf die hier übermittelten Daten unzweifelhaft zu. Zwar stellt die in der App generierte UUID für sich genommen noch kein personenbezogenes Datum dar. Allerdings war hierbei zu berücksichtigen, dass diese UUID auf dem Cloud-Server zusammen mit weiteren GPS-Informationen gespeichert wurde. Diese GPS-Informationen bildeten hier das für die Bestimmbarkeit erforderliche Zusatzwissen. In diesem Zusammenhang war zu berücksichtigen, dass die oben erwähnte Geozone so gewählt war, dass nicht nur das Veranstaltungsgelände erfasst war, sondern in einem Radius von mehreren Kilometern um das Veranstaltungsgelände herum eine GPS-Erfassung während des gesamten Veranstaltungszeitraums

[61] https://de.wikipedia.org/wiki/Heatmap.

erfolgte. Hierdurch war es nicht nur möglich zu erkennen, wie sich ein bestimmtes Gerät und damit der Eigentümer innerhalb des Veranstaltungsbereichs bewegte. Darüber hinaus war gerade bei Personen, die im Umkreis der Veranstaltung ihren Wohnsitz hatten, erkennbar, an welchem Ort diese Personen bspw. die Nacht verbrachten. Durch die Auswertung dieses Bewegungsprofils war es möglich zu bestimmen, wer Eigentümer des georteten Gerätes war.

Eine solche Erhebung und Verarbeitung personenbezogener Daten ist nur mit Einwilligung des Betroffenen zulässig. Eine den Anforderungen des Datenschutzrechts genügende Einwilligung in die Erhebung und Verarbeitung der Positions- und Bewegungsdaten in Verbindung mit der UUID war indes in der App nicht vorgesehen. Zwar musste der Nutzer beim erstmaligen Start der App dieser die Freigabe für den Zugriff auf den GPS-Sensor erteilen, jedoch genügten die hierbei erteilten Informationen nicht den Anforderungen an eine informierte Einwilligung. Insbesondere wurde weder über die genaue Aufzeichnungszone noch über den Aufzeichnungszeitraum informiert[62].

Die verantwortliche Stelle hat auf unsere Intervention hin die App wieder vom Markt genommen und alle bisher erhobenen personenbezogenen Daten gelöscht. Eine weitere Bewertung der Datenverarbeitung mittels der App, insbesondere im Hinblick auf technisch-organisatorische Fragen, war daher entbehrlich.

20.3 Ausgabeliste für den "Gelben Sack"

Die Mülltrennung verfolgt das Ziel, verwertbaren von nicht verwertbarem Müll zu trennen und den verwertbaren Müll zu recyceln. Aus diesem Grund wurde das „Duale System" eingeführt. Dadurch wird der Handel verpflichtet, Verpackungsmittel zurückzunehmen und einer Verwertung zuzuführen. Hierbei bedient er sich in aller Regel privater Entsorgungsunternehmen, die den Müll mit dem „Grünen Punkt" einsammeln und verwerten.

Zum Einsammeln des Mülls werden im Saarland sog. „Gelbe Säcke" verwendet. Diese sind bei den Ausgabestellen der Kommunen und in einer Vielzahl von Geschäften erhältlich. Die Ausgabe erfolgt kostenlos.

Bereits im unserem 24. Tätigkeitsbericht[63] wurde beanstandet, dass die Ausgabelisten für „Gelbe Säcke" bei verschiedenen Ausgabestellen nicht datenschutzkonform ausgestaltet sind. Von einzelnen Bürgern, aber auch von Gemeinden wurde uns zugetragen, dass weiterhin Listen ausliegen, in denen der Erhalt einer Rolle der „Gelben Säcke" mit Namen, Adresse und Unterschrift zu bestätigen ist.

Die damalige Vereinbarung mit der Entsorgungsfirma, nach der alleine eine Unterschrift als Empfangsbestätigung zwingend verlangt wird, hatte sich in der Praxis anscheinend nicht bei allen Ausgabestellen herumgesprochen. Unsere Nachfrage bei

---

62 Die Formulierung in der App war: „Eine Übertragung der Daten findet nur während kritischer Zeiten und nur räumlich begrenzt statt"

63 Vgl. 24. Tätigkeitsbericht, 2011/2012, Kapitel 10.1.2, S. 67f.

der Entsorgungsfirma erweckte den Eindruck, als habe man dort nicht mit dem nötigen Nachdruck auf die Verwendung neuer Ausgabelisten hingewiesen.

Es wurde zugesagt, dass man zukünftig Ausgabelisten auslegen werde, in denen deutlich auf die Freiwilligkeit der Adressangaben hingewiesen werde. Diese Vorgehensweise entspricht der erwähnten Vereinbarung.

21 Kreditwirtschaft

21.1 Kopieren, Scannen und Speichern von Personalausweisen

Seit Inkrafttreten des Personalausweisgesetzes im Jahre 2009 kam immer wieder die Frage auf, ob Personalausweise zur Identifikation eines Antragstellers, Kunden oder Besuchers kopiert oder eingescannt werden dürfen.[64]

Das Kopieren seines neuen Personalausweises durch eine Mitarbeiterin seiner „Hausbank" veranlasste in diesem Berichtszeitraum einen Petenten, sich an das Unabhängige Datenschutzzentrum zu wenden.

Der Petent beabsichtigte die Eröffnung eines Bankschließfachs. Nach einem Blick in die Kundendatei des Petenten bat die Mitarbeiterin des Kreditinstituts um den Personalausweis des Petenten und kopierte sowohl die Vorder- als auch die Rückseite des neuen Personalausweises. Auf die Rückfrage des Petenten, zu welchem Zweck eine Kopie des Ausweises angefertigt wurde, antwortete die Mitarbeiterin des Kreditinstituts, dass die Kopie eingescannt und weiterverarbeitet würde. Der Petent vertrat gegenüber der Mitarbeiterin aber die Meinung, dass auf dem Personalausweis Angaben enthalten seien, die nicht zur Identitätsfeststellung erforderlich sind. Die Mitarbeiterin entgegnete hierauf, dass dies nach dem Geldwäschegesetz in Ordnung sei.

In dem vorliegenden Fall handelte es sich um ein neues Ausweisdokument, welches grundsätzlich gemäß § 14 Personalausweisgesetz (PAuswG) in Verbindung mit § 20 PAuswG weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden durfte. Von dieser Vorschrift sind alle Formen des automatischen Abrufs (insbesondere das Scannen und Speichern) der im Ausweis enthaltenen Daten umfasst. Hiervon können auch digitale Kopiergeräte betroffen sein, da diese Dokumente erst einscannen, dann in einem Zwischenspeicher ablegen und zuletzt ausdrucken.

§ 14 PAuswG

Die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises darf ausschließlich erfolgen durch

1. *zur Identitätsfeststellung berechtigte Behörden nach Maßgabe der §§ 15 bis 17,*
2. *öffentliche Stellen und nichtöffentliche Stellen nach Maßgabe der §§ 18 bis 20.*

§ 20 Abs. 1 bis 3 PAuswG

(1) Der Inhaber kann den Ausweis bei öffentlichen und nichtöffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden.

(2) Außer zum elektronischen Identitätsnachweis darf der Ausweis durch öffentliche und nichtöffentliche Stellen weder zum automatisierten Abruf personenbezogener

[64] Vgl. 25. Tätigkeitsbericht, 2013/2014, Kapitel 12.3, S. 81-82.

Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden.

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

Auf der anderen Seite sind Kreditinstitute gemäß § 3 Abs. 1 Nr. 1 in Verbindung mit § 4 Abs. 1 Geldwäschegesetz (GwG) und § 154 Abgabenordnung (AO) zur Identifikations- und Legitimationsprüfung unter anderem verpflichtet, wenn beispielsweise ein Vertrag über die Überlassung eines Bankschließfachs abgeschlossen werden soll.

Die dann nach § 4 Abs. 3 Nr. 1 GwG von dem Kreditinstitut zur Feststellung der Identität des Vertragspartners zu erhebenden Angaben sind bei natürlichen Personen der Name, der Geburtsort, das Geburtsdatum, die Staatsangehörigkeit und die Anschrift.

Diese Angaben sind nach § 4 Abs. 4 Nr. 1 GwG einem im Sinne dieser Vorschrift gültigen amtlichen Ausweis zu entnehmen (dies sind insbesondere Personalausweise, Reisepässe oder entsprechende Ersatzdokumente) und nach § 8 Abs. 1 S. 1 GwG aufzuzeichnen. Nach § 8 Abs. 1 S. 2 GwG sind diese Angaben um die Ausweisnummer und die ausstellende Behörde zu ergänzen.

Die Anfertigung einer Kopie des gültigen Ausweises gilt dabei nach § 8 Abs. 1 S. 3 GwG als Aufzeichnung der darin enthaltenen Angaben.

Vor diesem Hintergrund hatte die Bundesanstalt für Finanzdienstleistungen (BaFin) mit ihrem Rundschreiben 7/2014 (GW) das Einscannen eines solchen Dokuments der Erstellung einer Kopie gleichgestellt.

In dem vorliegenden Beschwerdefall wurde der gesamte Personalausweis zunächst kopiert, so dass sich als Erstes die Frage der Zulässigkeit dieser Datenerhebung stellte. Sofern nur die im GwG bzw. in der AO geforderten Angaben kopiert werden, ist die Datenerhebung und –speicherung auf Grundlage einer gesetzlichen Erlaubnisnorm zulässig. Diese gilt jedoch nur für die nach GwG bzw. AO erforderlichen Angaben. Der Personalausweis enthält aber auch Angaben, die über die im GwG oder in der AO geforderten Angaben hinausgehen. Dazu gehören etwa die Angaben über Augenfarbe und Körpergröße sowie bei den neuen Personalausweisen auch die Zugangsnummer.

Die Zulässigkeit der Erhebung dieser Daten lässt sich weder aus der AO noch dem GwG oder § 28 Abs. 1 Nr. 1 oder 2 Bundesdatenschutzgesetz (BDSG) herleiten.

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

Für alle mitkopierten Angaben, die nicht für die Legitimationsprüfung erforderlich sind, fehlt es somit an einer gesetzlichen Grundlage für die Zulässigkeit der Datenerhebung.

Umgekehrt wäre ein Kopieren des Personalausweises auf Grundlage dieser gesetzlichen Regelung zulässig gewesen, wenn alle Angaben des Personalausweises von vorneherein geschwärzt worden wären, sofern sie nicht nach dem GwG oder der AO zur Identifikations- oder Legitimationsprüfung erforderlich sind.

Allerdings kann eine Datenerhebung auch ohne eine gesetzliche Regelung legitimiert sein, wenn der Betroffene eine wirksame Einwilligung nach § 4a Abs. 1 BDSG erteilt hat. Zwar hatte der Betroffene in dem vorliegenden Fall das Kopieren des Ausweises hingenommen, dies konnte jedoch nicht als wirksame Einwilligung im Sinne des Gesetzes angesehen werden, da weder eine konkludente oder erst recht keine stillschweigende oder mutmaßliche Einwilligung ausreichend ist, so dass keine Zulässigkeit der Erhebung der nach GwG nicht notwendigen Angaben gegeben war.[65]

§ 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 im vorliegenden Fall bereits das Kopieren des Personalausweises unzulässig war, gilt gleiches folglich auch für das spätere Einscannen und Speichern der Kopie in der Kundenakte; unabhängig von der Frage der Zulässigkeit des Scannens und Speicherns nach § 14 PAuswG in Verbindung mit § 20 PAuswG.[66]

Im vorliegenden Fall wurden nach einem Schriftwechsel zwischen dem Unabhängigen Datenschutzzentrum Saarland und dem Kreditinstitut die vorhandenen Papierkopien vernichtet und die eingescannten Dokumente aus den Kundendateien[67] gelöscht. Der Verpflichtung zur Aufzeichnung der nach dem GWG und der AO erforderlichen Angaben wird künftig durch Notieren nachgekommen.

---

[65] Gemäß einem BMI-Schreiben aus dem Jahr 2011 gibt es aus der Eigentümerstellung der Bundesrepublik Deutschland kein grundsätzliches Kopierverbot mehr.

[66] Siehe hierzu Entscheidung des VG Hannover vom 28. November 2013 - 10 A 5342/11. Nach dieser Entscheidung ist das Scannen und Speichern von Personalausweisen grundsätzlich unzulässig, da es einen schwerwiegenden Verstoß gegen datenschutzrechtliche Bestimmungen des Personalausweisgesetzes darstellt.

[67] Außerdem hätte im Falle der Zulässigkeit des Abspeicherns der gescannten Ausweiskopie sichergestellt werden müssen, dass nur die Mitarbeiter des Kreditinstituts Zugriff haben, die diesen auch tatsächlich benötigen und eine Löschung erfolgt, sobald keine Aufzeichnungspflicht mehr besteht.

21.2 Videoidentifizierung

Kreditgeschäfte mittels einer Videoidentifizierung abzuschließen, findet europaweit eine größer werdende Verbreitung. Dies gilt insbesondere auch für Kreditinstitute.

Mit dem Begriff „Videoidentifizierung“ ist die Identifizierung mittels Bild- und Tondaten gemeint, die zwischen dem Kunden und dem Kreditinstitut mittels einer speziellen Anwendung übertragen werden. Der Kunde braucht dazu nur ein Endgerät mit Kamera, die Software eines Internettelefondienstes und eine Anbindung an das Internet.

Der Ablauf stellt sich im Wesentlichen dann wie folgt dar: einen Ausweis in die Kamera halten, die Seriennummer vorlesen und zum Schluss eine Transaktionsnummer (TAN) online eingeben, die zuvor per E-Mail oder SMS an den Kunden gesendet wurde.

Bei diesem Verfahren sind die Beteiligten zwar nicht physisch am gleichen Ort anwesend, können sich aber im Rahmen der Videoübertragung visuell wahrnehmen und sprachlich verständigen. Die nach dem Geldwäschegesetz (GwG) bei bestimmten Bank- und Kreditgeschäften notwendige Identifikation erfolgt während der Videoübertragung mittels eines geeigneten Identifikationsdokuments (etwa Personalausweis oder Reisepass, die über optische Sicherheitsmerkmale wie zum Beispiel holographische Bilder verfügen müssen). Dabei werden vom Kunden sowie von der Vorder- und Rückseite des Ausweisdokuments Screenshots angefertigt. Der Kunde muss während der Videoübertragung die vollständige Seriennummer seines Ausweisdokuments mitteilen. Das Gespräch zwischen dem Mitarbeiter und dem Vertragspartner wird dabei akustisch aufgezeichnet.

Hintergrund dieser Vorgehensweise ist, dass die Bundesanstalt für Finanzdienstleistungen (BaFin) in dem Rundschreiben 1/2014 (GW), Ziffer III., vom 5. März 2014 mitgeteilt hat, dass dieses Verfahren keine erhöhte Sorgfaltspflichten auslöst, die in Fällen der Fernidentifizierung (bei denen die Vertragspartner nicht persönlich anwesend sind) nach § 6 Abs. 2 Nr. 2 Geldwäschegesetz (GwG) gefordert werden, sondern die allgemeinen Identifizierungspflichten nach § 3 Abs. 1 Nr. 1 in Verbindung mit § 4 Abs. 1, Abs. 3 Nr. 1 und Abs. 4 Nr. 1 GwG gelten.

Allerdings sind im Falle einer Videoidentifizierung auch datenschutzrechtliche Aspekte zu berücksichtigen.

Zunächst ist die Identifizierung des Kunden mittels Videoübertragung nur zulässig, wenn sich dieser zu Beginn der Videoübertragung mit den Aufzeichnungen einverstanden erklärt. Hier ist eine ausdrückliche und informierte Einwilligung des Kunden nach § 4a BDSG erforderlich.

§ 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 Ein-

willigung 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.

Auf den Screenshots dürfen nur diejenigen Daten erkennbar sein, die für die Identifizierung nach dem GwG auch tatsächlich erforderlich sind. Auch hier gilt, dass nur die Angaben erkennbar sein dürfen, die nach § 4 Abs. 3 Nr. 1 GwG von dem Kreditinstitut zur Feststellung der Identität des Vertragspartners zu erheben sind.[68] Bei natürlichen Personen sind dies der Name, der Geburtsort, das Geburtsdatum, die Staatsangehörigkeit und die Anschrift. Alle weiteren Angaben, die das Ausweisdokument enthält, wie etwa Körpergröße und Augenfarbe sowie im Falle eines neuen Personalausweises die Zugangsnummer, sind zu schwärzen.

Eine akustische Aufzeichnung des gesamten Gesprächs oder gar eine Videoaufzeichnung des gesamten Vorgangs der Videoidentifikation sind im Hinblick auf das in § 3a BDSG normierte Gebot der Datenvermeidung und Datensparsamkeit unzulässig.

So normiert § 3a BDSG einen wesentlichen Grundsatz des Datenschutzrechts mit dem Ziel, dass so wenige personenbezogene Daten wie möglich erhoben und verarbeitet werden sollen. Für die Aufzeichnungspflicht nach § 8 Abs. 1 S. 1 ff GwG ist eine Aufzeichnung des Gesprächs, sowohl als Tonmitschnitt wie auch als Videoaufzeichnung, nicht erforderlich. Durch die Anfertigung von Screenshots sind das Vorliegen eines Ausweisdokuments und alle nach § 4 Abs. 3 Nr. 1 GwG erforderlichen Angaben ausreichend dokumentiert.

Bei der Auswahl eines Internettelefondienstes ist darauf zu achten, dass anderen Nutzern oder Firmen keine umfassenden Rechte an den Inhalten der Kommunikation eingeräumt werden, da in dem Videoidentifikationsverfahren neben Bildern des Ausweises auch alle Identifikationsdaten übermittelt werden. Somit scheiden alle Diensteanbieter aus, die sich solche Rechte durch ihre Nutzungsbedingungen einräumen lassen.

21.3 Rechtmäßigkeit der Verarbeitung biometrischer Daten

Am 13. Januar 2016 ist die EU-Richtlinie über Zahlungsdienste (EU) 2015/2366 (Payment Services Directive II (PSD II)) in Kraft getreten. Ziel der Richtlinie ist zum einen die Erhöhung der Sicherheit von Zahlungsdiensten und zum anderen ein hohes Maß an Verbraucherschutz.

Daher fordert die PSD II auch eine verstärkte Kundenauthentifizierung. Diese ist gegeben, wenn zwei der folgenden drei Faktoren vorliegen: Wissen (z.B. ein statisches Passwort), Besitz (z.B. eine Smartcard) und Sein (z.B. ein Fingerabdruck). Bei dem Faktor „Sein" handelt es sich um sogenannte biometrische Daten.

Die EU-Mitgliedstaaten müssen die PSD II bis zum 13. Januar 2018 in nationales Recht umsetzen. Da die EU-Datenschutzgrundverordnung (DS-GVO) wenig später

[68] Dies ist in dem vorhergehenden Punkt ausführlich dargestellt.

am 25. Mai 2018 anzuwenden ist und spezielle Regelungen zu biometrischen Daten enthält, ist diese bei der Umsetzung der PSD II sinnvollerweise miteinzubeziehen.

Art. 4 Nr. 14 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck „biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

Daneben ist weiterhin zu berücksichtigen, dass biometrische Daten auch Gesundheitsdaten sein können. So ist etwa der individuelle Herzschlag („kardiologischer Fingerabdruck") nicht nur ein biometrisches Datum, sondern zugleich auch ein Gesundheitsdatum, da er Auskunft darüber gibt, ob der Kunde kardiologisch gesehen gesund oder krank ist.

Da es sich sowohl bei den biometrischen Daten als auch bei den Gesundheitsdaten um eine besondere Kategorie personenbezogener Daten handelt, ist deren Verarbeitung nach Art. 9 Abs. 1 DS-GVO grundsätzlich untersagt.

Gemäß Art. 94 Abs. 2 PSD II dürfen Zahlungsdienstleister die für das Erbringen ihrer Zahlungsdienste notwendigen personenbezogenen Daten nur mit der ausdrücklichen Zustimmung des Zahlungsdienstnutzers abrufen, verarbeiten und speichern. Eine entsprechende Regelung enthält auch der gerade noch im Berichtszeitraum veröffentlichte Referentenentwurf des Zahlungsdiensteumsetzungsgesetzes (ZDUG).[69]

Dies führte zu der Frage inwieweit die Verarbeitung biometrischer Daten gemäß der PSD II auch nach der DS-GVO rechtmäßig sein kann.

Art. 9 Abs. 2 lit. a DS-GVO lässt eine Verarbeitung zu, wenn der Betroffene ausdrücklich einwilligt. Eine solche Einwilligung führt aber wiederum nach Art. 7 Abs. 4 DS-GVO nur dann zu einer Zulässigkeit der Datenverarbeitung, wenn diese auch freiwillig erfolgt. Die Freiwilligkeit der Einwilligung ist wiederum gegeben, wenn der Kunde eine alternative Möglichkeit hat, um an den Zahlungsdiensten teilnehmen zu können, ohne in die Verarbeitung biometrischer Daten einwilligen zu müssen.

Zudem sind auch technische Vorkehrungen zu treffen, um sicherstellen zu können, dass die Daten nicht abhandenkommen. Dabei ist zu beachten, dass biometrische Daten nicht zwingend sicherer sind als die beiden anderen Faktoren „Wissen" und „Besitz". Ein Fingerabdruck ist zum Beispiel nicht geheim, sondern ist vielen anderen Personen zugänglich und kann gefälscht werden. Hierzu benötigt man nur einen Fingerabdruck auf einem physischen Gegenstand (z.B. einem Glas). Sodann kann mittels dieses Modells eine Kopie des Fingerabdrucks erstellt werden.[70]

Gleichzeitig ist zu beachten, dass zwar ein Passwort geändert werden kann, aber biometrische Daten unveränderbar sind, da z.B. ein Fingerabdruck individuell und ein Leben lang so erhalten bleibt. Ist ein biometrisches Datum „verloren", kann es also

---

[69] http://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Referentenentwuerfe/2016-12-21-Zahlungsdiensteumsetzungsgesetz.html

[70] Dies hat der Chaos Computer Club unter Beweis gestellt (siehe http://www.giga.de/fingerabdruck-faelschung-per-foto-moeglich/).

nicht mehr geändert werden und ist folglich zu einer sicheren Authentifizierung künftig nicht mehr geeignet. Daher ist bei dem Umgang mit entsprechenden Daten auf ein sehr sicheres Speicherverfahren zurückzugreifen.

22 Vereine

22.1 (Dorf-)Chroniken

Immer wieder erhalten wir Anfragen von heimatkundlichen Vereinen, die sich mit der Frage an uns gewandt hatten, welche personenbezogenen Daten unter welchen Voraussetzungen datenschutzrechtlich verwendet und bei der Erstellung von Dorfchroniken genannt werden dürfen.

Die Herkunft der gesammelten Daten ist dabei sehr unterschiedlich: Oftmals stellen die ortsansässigen Familien und Anwohner den Vereinen Informationsmaterial zur Verfügung oder diese erheben Daten von Grabsteinen, aus Todesanzeigen, Zeitungsartikeln, dem Personenstandsregister und aus öffentlichen Archiven. Die Beantwortung hinsichtlich der datenschutzrechtlichen Zulässigkeit muss daher differenziert ausfallen.

So gilt das Bundesdatenschutzgesetz (BDSG) nur für den Umgang mit personenbezogenen Daten natürlicher Personen. Bei Verstorbenen handelt es sich – im Gegensatz zu lebenden Menschen – nicht um natürliche Personen im rechtlichen Sinne, weshalb das BDSG schon deshalb keine Anwendung findet.

Trotzdem sind bei der Verwendung von Daten Verstorbener einige gesetzliche Regeln zu beachten. Ein besonderes Schutzbedürfnis kann sich aus der Art der Quelle, aus der die Daten erhoben werden, ergeben. Bei der Erhebung beispielsweise aus dem Personenstandsregister sind die Regelfristen des Personenstandsgesetzes zu beachten. Werden die Daten bei den Angehörigen selbst oder aus öffentlich zugänglichen Quellen wie Zeitungsanzeigen, Grabinschriften, Amtsblättern, kirchlichen Gemeindebriefen, Gefallenentafeln etc. erhoben, bestehen hingegen keine grundsätzlichen Bedenken aus datenschutzrechtlicher Sicht.

In diesem Zusammenhang gilt es allerdings, auf das sogenannte postmortale Persönlichkeitsrecht hinzuweisen. Dieses beschränkt sich zwar auf den Schutz der Menschenwürde sowie den Schutz des allgemeinen Lebensbildes gegen grob ehrverletzende Entstellungen, Erniedrigungen und Herabwürdigungen, jedoch nicht auf die reinen biografischen Daten. Dieses „Schutzbedürfnis schwindet in dem Maße, in dem die Erinnerung an den Verstorbenen verblasst und im Laufe der Zeit auch das Interesse an der Nichtverfälschung des Lebensbildes abnimmt“ (BVerfG, Beschluss vom 24. Februar 1971 - 1 BvR 435/68, „Mephisto“ = BVerfGE 30, 173).

So können bei der Veröffentlichung personenbezogener Daten beispielsweise im Zusammenhang mit den Kriegsgeschehnissen des Zweiten Weltkrieges mehrere Grundrechte aufeinander prallen. Dem Recht auf Meinungs- und Pressefreiheit kann das Persönlichkeitsrecht Betroffener, denen unter Umständen eine Veröffentlichung der damaligen Geschehnisse unangenehm sein könnte, entgegenstehen. Gegen die Verletzung des ideellen Anteils am postmortalen Persönlichkeitsrecht können nur

nahestehende Angehörige, in der Regel die Totensorgepflichtigen oder Wahrnehmungsberechtigte, die der Betroffene zu Lebzeiten dazu berufen hat (dies kann auch eine Institution sein), vorgehen.

Um möglichen Klagen von Betroffenen und deren Angehörigen im Vorfeld einer Veröffentlichung vorzubeugen, empfiehlt es sich, in Zweifelsfällen die schriftliche Einwilligung dieser Personen einzuholen.

22.2 Grabsteinfotos im Internet

Der Verein für Computergenealogie e.V. zur Ahnen- und Familienforschung veröffentlicht bundesweit Fotos von Grabsteinen auf seiner Internetseite, so auch Grabsteinfotos von einigen saarländischen Friedhöfen. Ein Ortsvorsteher einer saarländischen Gemeinde wandte sich an unsere Dienststelle, mit der Frage, ob die Veröffentlichung von Grabsteinfotos im Internet datenschutzrechtlich zulässig sei und ob es Möglichkeiten gäbe, diese zu unterbinden.

Mehrere Bürgerinnen und Bürger seines Ortes beschwerten sich bei ihm darüber, dass die Fotos Diebe animieren könnten, auf den Bildern ebenfalls zu sehende Gegenstände, wie etwa Statuen, zu entwenden.

In einer Prüfung des Sachverhaltes konnte festgestellt werden, dass die Internetveröffentlichung von Grabsteinfotos grundsätzlich keinen Verstoß gegen den Datenschutz darstellt. Diese Ansicht wird auch durch ein Urteil des Amtsgerichts Mettmann vom 16. Juni 2015 - 25 C 384/14 - bekräftigt, das entschied:

Die Veröffentlichung von Grabsteinfotografien mit dem Namen des Verstorbenen auf einem Internetportal ist – auch nach § 28 Abs. 1 Nr. 3 BDSG – datenschutzrechtlich zulässig und verletzt nicht das postmortale Persönlichkeitsrecht des Verstorbenen.

Ungeachtet dessen erwirkte der Ortsvorsteher mittels schriftlicher Eingabe beim Verein für Computergenealogie e.V., dass dieser alle Grabsteinfotos des betroffenen Friedhofs von der Internetseite entfernte.

23 Sonstiges

23.1 Gebühren für Amtshandlungen der Aufsichtsbehörde

Mit der Verordnung zur Änderung der Verordnung über den Erlass eines Allgemeinen Gebührenverzeichnisses vom 6. April 2016 (Amtsbl. S. 246) wurde im Allgemeinen Gebührenverzeichnis unter Ziffer 240 ein eigener Gebührentatbestand geschaffen, der es ermöglicht, für Amtshandlungen nach dem Bundesdatenschutzgesetz (BDSG) Verwaltungsgebühren zu erheben. Die Einführung eines eigenen Gebührentatbestandes war erforderlich gewesen, da der Rückgriff auf den Auffanggebührentatbestand nach Ziffer 1.1 des Allgemeinen Gebührenverzeichnisses nicht mehr möglich war.[71]

Das Gebührenverzeichnis sieht u.a. für datenschutzrechtliche Kontrollmaßnahmen einen Gebührenrahmen von 50 – 5.000 Euro vor, wenn diese mit einem besonderen Prüfungsaufwand einhergehen.

In der Vergangenheit zeigte sich sehr häufig, dass bei Kontrollen nach § 38 Abs. 1 BDSG Auskünfte und Unterlagen, die zur datenschutzrechtlichen Beurteilung notwendig sind, durch die verantwortliche Stellen oft nur unzureichend, widerwillig, nach mehrmaliger Mahnung oder überhaupt nicht zur Verfügung gestellt werden. Dies bindet personelle Ressourcen in erheblichem Umfang und verzögert eine zeitnahe Erledigung der Verfahren. Die Einführung der Gebührentatbestände kann daher nunmehr einen zügigeren Abschluss von aufsichtsrechtlichen Verfahren nach § 38 Abs. 1 BDSG unterstützen. In Fällen, in denen die verantwortlichen Stellen nachweislich kooperieren, um datenschutzkonforme Zustände herzustellen, kann auf die Festsetzung einer Gebühr aus Billigkeitsgründen ganz verzichtet werden.

Für Anordnungen zur Beseitigung festgestellter Datenschutzverstöße oder technischer oder organisatorischer Mängel nach § 38 Abs. 5 Satz 1 BDSG können ebenfalls 50 – 5.000 Euro festgesetzt werden.

Auch die Beratung betrieblicher Datenschutzbeauftragter oder anderer nicht-öffentlicher Stellen kann mit einer Gebühr zwischen 200 – 10.000 Euro veranschlagt werden, wenn es sich nicht bloß um einfache Auskünfte handelt. Durch die Gebührenfreiheit für einfache Auskünfte sollen die verantwortlichen Stellen auch weiterhin dazu ermuntert werden bei konkreten datenschutzrechtlichen Fragestellungen mit

[71] Zwar sind nach § 1 Saarländisches Gebührengesetz (SGebG) grundsätzlich für Amtshandlungen der Verwaltungsbehörden des Saarlandes, zu denen auch das Unabhängige Datenschutzzentrum zählt, Gebühren zu erheben, jedoch können Gebühren nur dann erhoben werden, wenn für das konkrete Verwaltungshandeln ein Gebührentatbestand existiert. Als Auffanggebührentatbestand sieht Ziffer 1.1 des Allgemeinen Gebührenverzeichnisses längstens bis zum Ablauf von drei Jahren nach Inkrafttreten der Rechtsvorschrift, auf der die Amtshandlung beruht (vorliegend § 38 BDSG, der 2009 neu geregelt wurde), eine Rahmengebühr von 2,55 – 10.225,00 Euro vor. Nach Ablauf der Drei-Jahresfrist des Auffanggebührentatbestandes war der Anwendungsbereich des Auffanggebührentatbestandes daher nicht mehr eröffnet.

der Aufsichtsbehörde Rücksprache zu halten und deren Expertise und Rechtsrat einzuholen.

Gleichwohl ist eine Gebührenerhebung für Beratungsleistungen trotz der gesetzlich vorgesehenen Beratungsaufgabe der Landesbeauftragten für Datenschutz dann angemessen, wenn diese Beratung im Sinne einer umfassenden Rechtsberatung und datenschutzrechtlichen Bewertung eigener Datenverarbeitungsprozesse in Anspruch genommen wird. Die sich aus einer solchen umfassenden Beratung ergebenden Vorteile für die Unternehmen sind wirtschaftlicher Art und verschaffen den entsprechenden Stellen erhebliche Wettbewerbsvorteile. Auf der einen Seite vermeiden die verantwortlichen Stellen durch die Einschaltung externer Dienstleister und Beratungsunternehmen entstehende Kosten. Gleichzeitig verringern sie das Risiko von gegen das Unternehmen geführten Verwaltungs- und Bußgeldverfahren wegen unzulässiger Datenverarbeitung und gerichtlicher Inanspruchnahme durch etwaig Betroffene. Dies alles rechtfertigt es, dass die hierbei entstehenden Personal- und Sachkosten nicht der Steuerzahler zu tragen hat, sondern dass diese Kostenpositionen auf die verantwortliche Stelle umgelegt werden.

Im Kalenderjahr 2016 wurden in sieben Verfahren Gebühren erhoben. Die Höhe der Gebühr bewegte sich dabei in allen Verfahren im dreistelligen Bereich. Es ist von einer steigenden Tendenz der gebührenrelevanten Verwaltungsverfahren auszugehen.

Informationsfreiheit

24 Informationsfreiheit

24.1 Eingabe gegen eine Regulierungsbehörde

Im Berichtszeitraum wandte sich ein Petent gestützt auf § 4 Saarländisches Informationsfreiheitsgesetz (SIFG) an die Informationsfreiheitsbeauftragte, da er sich durch einen nur teilweise gewährten Informationszugang durch die Regulierungskammer für das Saarland[72] in seinem Recht auf Informationsfreiheit beeinträchtigt wähnte.

Das SIFG gewährt jedem einen grundsätzlich voraussetzungslosen Anspruch auf Zugang zu amtlichen Informationen, die bei den Behörden des Landes, der Gemeinden und Gemeindeverbände vorhanden sind. Nach § 1 S. 1 SIFG finden die §§ 1 bis 9 und 11 Informationsfreiheitsgesetz (IFG) entsprechend Anwendung, so dass eine Reihe von Ausnahmetatbeständen zu berücksichtigen sind, die dem Informationsanspruch entgegenstehen können. Neben öffentlichen Belangen wie Sicherheitsinteressen (§ 3 IFG) werden auch solche Informationen geschützt, die privater (personenbezogene Daten, § 5 IFG) oder auch wirtschaftlicher (Betriebs- und Geschäftsgeheimnisse, § 6 IFG) Natur sind. Daneben ist auch der behördliche Entscheidungsprozess an sich geschützt, das heißt wenn durch die Bekanntgabe der begehrten Informationen zu erwarten ist, dass eine behördliche Entscheidung gefährdet werden könnte.

Der an die Regulierungskammer - als Behörde des Landes im Sinne des § 1 SIFG - gerichtete Antrag auf Informationszugang war auf sämtliche Entscheidungen gerichtet, welche die Behörde im Rahmen ihres gesetzlich zugewiesenen Auftrags getroffen hatte.[73] Die begehrten Unterlagen enthielten u.a. auch verschiedenste Angaben über natürliche und juristische Personen sowie über Betriebs- und Geschäftsbelange, weshalb die informationsverpflichtete Behörde zu dem Schluss kam, dass Anhaltspunkte für das Vorliegen geheimhaltungsbedürftiger Informationen bestanden und folglich ein sog. Drittbeteiligungsverfahren gemäß § 8 Abs. 1 IFG durchführte.

§ 8 Abs. 1 IFG

Die Behörde gibt einem Dritten, dessen Belange durch den Antrag auf Informationszugang berührt sind, schriftlich Gelegenheit zur Stellungnahme innerhalb eines Monats, sofern Anhaltspunkte dafür vorliegen, dass er ein schutzwürdiges Interesse am Ausschluss des Informationszugangs haben kann.

---

[72] Die Regulierungskammer für das Saarland ist gemäß § 1 Gesetz Nr. 1854 zur Einrichtung einer Regulierungskammer für das Saarland (RegKSG) für den Vollzug der Aufgaben nach § 54 Abs. 2 Energiewirtschaftsgesetz (EnWG) zuständig (siehe auch folgende Fußnote). Im Saarland unterliegen rund 40 Strom- und Gasnetzbetreiber (die weniger als 100.000 Kunden angeschlossen haben und deren Netz vollständig im Saarland liegt) der Regulierungsaufsicht des Landes. Diese Aufsicht wird durch die unabhängige Regulierungskammer entsprechend den europarechtlichen Vorgaben ausgeübt. Ziel der Aufsicht ist es, einen unverfälschten und wirksamen Wettbewerb zu gewährleisten.

[73] Gemäß § 54 Abs. 2 EnWG fallen unter diese Aufgaben unter anderem die Genehmigung von Entgelten für den Netzzugang, Überwachung der Vorschriften zur Entflechtung und zur Systemverantwortung der Betreiber von Energieversorgungsnetzen sowie die Überwachung der Vorschriften zum Netzanschluss und der technischen Vorschriften.

Den beiden beteiligten Netzbetreibern als Dritte im Sinne des § 2 Nr. 2 IFG wurde Gelegenheit zur Stellungnahme eingeräumt, inwiefern ihres Erachtens Ausschlussgründe für eine Auskunftserteilung gegeben sind. Für die Stellungnahme wurde schriftlich eine Frist von einem Monat gesetzt. Ein Netzbetreiber teilte daraufhin ohne weitergehende Begründung mit, dass es sich bei den Informationen um Betriebs- und Geschäftsgeheimnisse gemäß § 6 IFG handele, in deren Bekanntgabe nicht einwilligt werde.

§ 6 IFG

Der Anspruch auf Informationszugang besteht nicht, soweit der Schutz geistigen Eigentums entgegensteht. Zugang zu Betriebs- oder Geschäftsgeheimnissen darf nur gewährt werden, soweit der Betroffene eingewilligt hat.

Die weitere beteiligte Stelle äußerte sich nicht fristgemäß innerhalb eines Monats, so dass die Einwilligung als nicht erteilt angesehen werden musste.

Aufgrund der abgegebenen Stellungnahme sowie im Rahmen der eigenverantwortlichen Prüfung kam die Behörde zu dem Ergebnis, dass es sich vorliegend zumindest partiell um geheimhaltungsbedürftige Betriebs- und Geschäftsgeheimnisse handelte.[74] Die fehlende Einwilligung stand demnach dem vollumfänglichen Informationszugang entgegen, da Zugang zu Betriebs- und Geschäftsgeheimnissen nur gewährt werden darf, wenn der oder die Betroffene eingewilligt hat.[75]

Die Behörde teilte den beteiligten Stellen in der Folge gemäß § 8 Abs. 2 S. 1 IFG sowie dem Antragsteller mit, dass sie beabsichtige, dem Informationszugang teilweise im Sinne des § 7 Abs. 2 S. 1 IFG zu entsprechen, indem sie die entsprechend schützenswerten Informationen schwärze.

§ 7 Abs. 2 IFG

Besteht ein Anspruch auf Informationszugang zum Teil, ist dem Antrag in dem Umfang stattzugeben, in dem der Informationszugang ohne Preisgabe der geheimhaltungsbedürftigen Informationen oder ohne unverhältnismäßigen Verwaltungsaufwand möglich ist. Entsprechendes gilt, wenn sich der Antragsteller in den Fällen, in denen Belange Dritter berührt sind, mit einer Unkenntlichmachung der diesbezüglichen Informationen einverstanden erklärt.

---

[74] Der Geheimhaltungswille geht mit einem berechtigten wirtschaftlichen Interesse an der Geheimhaltung einher. Diese Prüfung obliegt der informationspflichtigen Stelle. Hier konnte die Regulierungskammer von Amts wegen prüfen, ob schützenswerte Betriebs- und Geschäftsgeheimnisse vorliegen (die Regulierungskammer kann eigenständig darüber entscheiden, ob ein Betriebs- und Geschäftsgeheimnis vorliegt, wenn sie über die entsprechenden Kenntnisse verfügt). Im vorliegenden Fall kam die Regulierungskammer nach eigener Prüfung zu dem Ergebnis, dass bestimmte Informationen als Betriebs- und Geschäftsgeheimnis anzusehen waren.

[75] Dabei hatte die Regulierungskammer jedoch eine Einschränkung vorgenommen, dass trotz der Berührung wettbewerbsrelevanter Bereiche eine Schwärzung nicht vorgenommen wird, wenn die Informationen durch Erreichen einer „Halbwertszeit" die Wettbewerbsrelevanz verloren haben. Dies ist der Fall, wenn die Information nicht aus den letzten fünf Jahren stammt und auch nicht in diesen Zeitraum hineinwirkt (Verwaltungsgericht Köln, Urteil vom 25. Februar 2016 – 13 K 5017/13).

Nachdem die Regulierungsbehörde die Entscheidung getroffen hatte, einen beschränkten Informationszugang zu gewähren, war die Entscheidung gemäß § 8 Abs. 2 IFG auch dem betroffenen Dritten bekannt zu geben.

§ 8 Abs. 2 IFG

Die Entscheidung nach § 7 Absatz 1 Satz 1 ergeht schriftlich und ist auch dem Dritten bekannt zu geben. Der Informationszugang darf erst erfolgen, wenn die Entscheidung dem Dritten gegenüber bestandskräftig ist oder die sofortige Vollziehung angeordnet worden ist und seit der Bekanntgabe der Anordnung an den Dritten zwei Wochen verstrichen sind. § 9 Absatz 4 gilt entsprechend.

Des Weiteren musste die Bestandskraft der Entscheidung über den Informationszugang dem Dritten gegenüber eingetreten sein, bevor der Informationszugang gewährt werden konnte. Die Bestandskraft des Verwaltungsaktes, mit dem der Informationszugang gewährte wurde, tritt ein, sobald der Dritte diesen nicht mehr mittels eines Rechtsbehelfs angreifen kann.[76]

Dem Antragssteller wiederum standen seinerseits die Rechtsbehelfe des Widerspruchs bzw. der Verpflichtungsklage gegen einen nur teilweise gewährten Anspruch auf Informationszugang zur Verfügung.[77] Wird die Entscheidung zeitgleich dem Dritten als auch dem Antragssteller zugestellt, laufen die Rechtsbehelfsfristen sowohl der Dritten als auch des Antragsstellers zeitgleich ab. Würde der Antragssteller nunmehr abwarten, bis er den teilweisen Informationszugang tatsächlich erhält und beurteilen kann, ob dieser seiner Ansicht nach ausreichend ist, stünden ihm unter Umständen keine Rechtsbehelfe gegen diese Bescheide mehr zur Verfügung. Dem Antragssteller wurde allerdings bekannt gegeben, welche Informationen geschwärzt wurden (z.B. Informationen beim Wettbewerb um ein Netz wie etwa Konzessionsvergabe-Verfahren). Somit konnte er beurteilen, ob er mit diesem teilweisen Informationszugang einverstanden ist oder nicht. Dass der tatsächliche Informationszugang erst nach dem Ablauf der Rechtsbehelfsfristen des Dritten erfolgt, liegt daran, dass der Gesetzgeber den Verfahrensrechten des Dritten Vorrang vor einem zeitigen Informationszugang des Antragstellers einräumt.

Daneben wandte sich der Petent unter Bezugnahme auf die Entscheidung des Oberverwaltungsgerichts Berlin-Brandenburg vom 19. März 2015 - 12 B 26.14 - gegen die Aufspaltung seines Informationsbegehrens in mehrere Einzelbescheide, da er annahm, dass damit auch mehrere Gebührenbescheide einhergehen.

Eine Aufgliederung des Informationsbegehrens in mehrere Einzelbescheide durch die informationspflichtige Stelle musste sich jedoch nicht zwingend gebührenrechtlich beim Antragssteller auswirken. Es konnte insofern auch nur ein Gebührenbescheid ergehen, der aber zu diesem Zeitpunkt noch nicht vorlag.[78]

---

[76] Nach entsprechender Anwendung des § 9 Abs. 4 S. 1 IFG in Form eines Anfechtungswiderspruchs bzw. einer Anfechtungsklage.

[77] § 9 Abs. 4 S. 1 IFG. „Gegen die ablehnende Entscheidung sind Widerspruch und Verpflichtungsklage zulässig".

[78] Der von dem Petenten angeführten Gerichtsentscheidung lag die Aufspaltung zweier Informationsbegehren in 66 einzelne Anträge und entsprechenden Bescheide zugrunde. Dies führte nach Ansicht des Gerichts zu einem Verstoß gegen das Verbot einer prohibitiven wirkenden Gebührenbemessung (§ 10 Abs. 2 IFG); ob dies aber auch bei Aufspaltung

Im Übrigen wurde von Seiten der informationsverpflichteten Behörde von der Beteiligung weiterer Dritter, deren Belange durch den Informationszugang ebenfalls berührt waren, abgesehen und Angaben zu diesen mit der Begründung geschwärzt, dass es sich hierbei um für den Antragsteller wertfreie Angaben handele, die dieser mit seinem Informationsantrag nicht habe erlangen wollen. Dieses Vorgehen stand jedoch nicht im Einklang mit § 7 Abs. 2 S. 2 IFG, da die Behörde für eine entsprechende Verfahrensbeschleunigung die Einwilligung des Antragstellers hätte einholen müssen. Dieses Vorgehen wurde von dem Petenten jedoch nicht beanstandet.

Im Ergebnis wurde dem Petent mitgeteilt, dass die Bestandskraft der Entscheidung über den Informationszugang dem Dritten gegenüber eingetreten sein musste, bevor ihm der tatsächliche Informationszugang gewährt werden konnte. Dies konnte somit faktisch dazu führen, dass ihm unter Umständen keine Rechtsbehelfe gegen diese Bescheide mehr zur Verfügung standen. Außerdem wurde ihm mitgeteilt, dass mehrere IFG-Bescheide nicht automatisch zu mehreren Gebührenbescheiden führen. Da der Petent sich nicht mehr an unsere Dienststelle gewandt hat, dürfte nur ein Gebührenbescheid ergangen sein.

24.2 Keine Geheimhaltungsbedürftigkeit eines Brandschutzbedarfsplans

Im Berichtszeitraum bat ein Landkreis die Dienststelle um Einschätzung darüber, ob ein Anspruch gestützt auf das Saarländische Informationsfreiheitsgesetz (SIFG) auf Herausgabe eines Brandschutzbedarfsplans einer saarländischen Kommune bestehe.

§ 1 S. 1 SIFG räumt dabei jedem einen grundsätzlich voraussetzungslosen Anspruch auf Zugang zu bei den Behörden der Gemeinden vorhandenen amtlichen Informationen ein.

In einem ersten Schritt musste ermittelt werden, welchen Charakter ein solcher Plan hat und welche Informationen er enthält.

Die Pflicht zur Aufstellung eines Brandschutzbedarfsplans ergibt sich aus § 3 Abs. 3 des Gesetzes über den Brandschutz, die Technische Hilfe und den Katastrophenschutz im Saarland (SBKG). Den Inhalt eines Brandschutzbedarfsplans gibt die Verwaltungsvorschrift zur Erstellung einer Bedarfs- und Entwicklungsplanung für den Brandschutz und die Technische Hilfe und zur Regelausstattung der Feuerwehren mit Fahrzeugen (Planungs- und AusstattungsVV) vor. Die Gemeinden sollen die Ausstattung und die Leistungsfähigkeit ihrer Feuerwehr festlegen und die danach erforderlichen Maßnahmen veranlassen. Die Gemeinde analysiert die in ihrem Gebiet vorhandenen Gefahrenpotentiale und die Fähigkeit der Feuerwehr, diesen zu begegnen.

---

eines Informationsbegehrens in zwei Anträge so zu sehen ist, erscheint hier fraglich, da in diesem Fall nicht zwingend von einer abschreckenden Wirkung ausgegangen werden konnte. Für die ausstehenden Gebührenbescheide, sollte es nach der Rechtslage daher darauf ankommen, ob ein IFG-Antrag bei einer informationspflichtigen Stelle vorlag oder ob ein Informationsbegehren im Rechtssinne mehrere IFG-Anträge umfasste.

Somit stand fest, dass es sich bei dem von der Gemeinde aufzustellenden Plan um eine amtliche Information handelt, die bei der Gemeinde als informationsverpflichteter Stelle auch vorhanden ist.

Allerdings können dem grundsätzlichen Informationsanspruch eine Reihe von Ausnahmetatbeständen entgegenstehen, die den Informationszugang ausschließen. Vorliegend mussten zwei Tatbestände geprüft werden:

a) *Gefährdung der öffentlichen Sicherheit im Sinne des § 3 Nr. 2 Informationsfreiheitsgesetz (IFG)*

So ist der Informationszugang zu verwehren, wenn das Bekanntwerden der Information die öffentliche Sicherheit gefährden kann, § 1 S. 1 SIFG in Verbindung mit § 3 Nr. 2 (IFG). Das schützenswerte Gut der öffentlichen Sicherheit entstammt dem Gefahrenabwehrrecht. Unter dem Begriff „öffentliche Sicherheit" wird die Unversehrtheit der Rechtsordnung und der grundlegenden Einrichtungen und Veranstaltungen des Staates sowie die Unversehrtheit von Gesundheit, Ehre, Freiheit, Eigentum und sonstigen Rechtsgütern der Bürger verstanden. Dabei genügt nicht irgendeine abstrakte Gefahr, sondern es ist eine konkrete Gefährdungslage darzulegen. Die Anforderungen an die Gefährdung hängen einzelfallbedingt vom konkreten Schutzbedarf ab. Sensible verwaltungsinterne Abläufe und Strukturen wie beispielsweise Ausstattungs- und Einsatzkonzepte der Polizeien des Bundes sind ausweislich der Gesetzesbegründung (vgl. BT-Drs. 15/4493 S. 10) vor dem Bekanntwerden zu schützen.

Im Rahmen des Brandschutzbedarfsplans sind in einer Beschreibung des Gemeindegebietes die charakteristischen Angaben der Gemeinde für eine Gefährdungsabschätzung und Gefahrenabwehrplanung aufzuführen. Dass im Falle der Informationsgewährung in absehbarer Zeit mit hinreichender Wahrscheinlichkeit ein Schaden für eines der Schutzgüter eintritt, also eine konkrete Gefahr besteht, war im Hinblick auf den Brandschutzbedarfsplan mehr als fraglich. Das Bundesverfassungsgericht hat mit Urteil vom 4. April 2006 (1 BvR 518/02) festgehalten, dass eine allgemeine Bedrohungslage für das Vorliegen einer konkreten Gefahr nicht ausreichend sei, sondern vielmehr weitere Tatsachen vorliegen müssen, aus denen sich eine solche ergibt. Die für die Feststellung einer konkreten Gefahr erforderliche Wahrscheinlichkeitsprognose muss sich auf Tatsachen beziehen. Vage Anhaltspunkte oder bloße Vermutungen ohne greifbaren, auf den Einzelfall bezogenen Anlass reichen hingegen nicht aus. Anhaltspunkte, aus denen sich das Vorliegen einer konkreten Gefahr ergibt, lagen in diesem Fall nicht vor.

Daher konnte der Informationszugang nicht im Hinblick auf diesen Ausnahmetatbestand abgelehnt werden.

b) Nachteilige Auswirkungen auf Belange der inneren und äußeren Sicherheit (§ 3 Nr. 1 lit. c IFG)

Daneben ist der Informationszugang zu verwehren, wenn das Bekanntwerden der Information nachteilige Auswirkungen auf Belange der inneren und äußeren Sicherheit haben kann.

Im Vergleich zu § 3 Nr. 2 IFG verzichtet die Vorschrift auf das Gefahrenerfordernis und spricht lediglich von nachteiligen Auswirkungen. So wurde beispielsweise die abstrakte Terrorgefahr bei Zugang zu Informationen über die Verkehrsinfrastruktur wegen der Bedeutung der fraglichen Bauwerke für die Infrastruktur der Bundesrepublik Deutschland für die Ablehnung des Informationsbegehrens als ausreichend angesehen, da nicht auszuschließen sei, dass Terroristen Anschläge auf Brücken und Tunnelwerke in Betracht zögen (vgl. Verwaltungsgericht Berlin, Urteil vom 10. Februar 2011 – 2 K 23/10 – juris Rn. 33 ff., 37).

Zumindest bezüglich bestimmter Teile der Brandschutzbedarfsplanung konnten nachteilige Auswirkungen im Sinne der oben genannten Vorschrift bei deren Bekanntwerden nicht gänzlich ausgeschlossen werden. So sind beispielsweise unter Ziffer 2.3.3 der Verwaltungsvorschrift Gefahrstoffe auszuweisen (atomare, biologische, chemische Stoffe). Hier könnte zumindest eine abstrakte Gefährdungslage bejaht werden. Diese Einschätzung wurde vom zuständigen Fachreferat im saarländischen Ministerium für Inneres und Sport geteilt.

Im Ergebnis ist festzuhalten, dass nicht hinsichtlich aller Informationen des Brandschutzbedarfsplans ohne weiteres ein Anspruch auf Zugang besteht. Lediglich nach intensiver Prüfung durch die Kommunen selbst kann die Schwärzung besonders sensibler Angaben zulässig sein. Der anfragende Landkreis benachrichtigte die seinem Zuständigkeitsbereich unterfallenden Kommunen bezüglich der Vorgehensweise bei entsprechenden Anfragen.

24.3 Formulierungshilfen bei Informationsfreiheitsanträgen

Über das Internetportal „Frag-den-Staat" haben Bürgerinnen und Bürger die Möglichkeit, Anträge nach dem Informationsfreiheitsgesetz an die öffentlichen Stellen des Bundes und der Länder zu richten. Die Anträge sind vorformuliert und sollen damit den Informationszugang erleichtern.[79] Das Portal wird von der Open Knowledge Foundation Deutschland e.V. betrieben.

Da der Informationsanspruch grundsätzlich voraussetzungslos jedem zusteht, können die Anträge auch anonym gestellt werden. Lediglich dann, wenn Rechte Dritter durch den Informationszugang berührt sind, kann es unter Umständen erforderlich sein, dass der Antragsteller sein Informationsinteresse begründet, um eine Abwägung zwischen dem Geheimhaltungsinteresse des Dritten und dem Interesse des Antragstellers an der Zugänglichmachung der Information zu ermöglichen. Auch dann, wenn mit dem Informationszugang eine Gebühr verbunden ist, können von dem Antragsteller Angaben über dessen Identität und Anschrift verlangt werden, um

[79] Vgl. https://fragdenstaat.de/anfrage-stellen/

den Gebührenbescheid zustellen zu können. In allen anderen Fällen sollte die Bearbeitung von Informationsfreiheitsanträgen auch dann möglich sein, wenn die Identität des Antragstellers nicht bekannt ist.

Die Besonderheit der Plattform besteht außerdem darin, dass die gestellten Informationszugangsanträge und die darauf ergangenen Antworten bzw. Informationen für jeden in anonymisierter Form, d.h. durch Unkenntlichmachung der Identität des Antragstellers und des Sachbearbeiters der informationsverpflichteten Behörde abrufbar sind. Dies trägt zu einer stärkeren Transparenz staatlichen Handelns bei, in dem es aufzeigt, welche Anträge wie bearbeitet wurden und vermeidet darüber hinaus Doppelanfragen.

24.4 Erstattung von Gebühren bei Informationsfreiheitsanträgen

Für Amtshandlungen nach dem Saarländischen Informationsfreiheitsgesetz (SIFG) können Gebühren und Auslagen erhoben werden. Nach Ziffer 455 des Allgemeinen Gebührenverzeichnisses (GebVerz) ist ein Gebührenrahmen von bis zu 500,- Euro vorgesehen. Gebührenfrei sind lediglich mündliche und einfache schriftliche Auskünfte.

Mit einem Informationsfreiheitsantrag sind insofern immer auch finanzielle Risiken verbunden. Auch zeigt die Verwaltungspraxis, dass etliche Antragsteller ihre Anträge zurückziehen, wenn die Behörden mitteilen, dass mit der begehrten Information eine Gebühr einhergeht. Zwar sollen die Kosten laut Gesetzgeber nicht abschreckend wirken, um einen effektiven Informationszugang nicht zu gefährden, jedoch sieht die Realität teilweise anders aus.

Um dem entgegenzuwirken, hat der Verein Wikimedia in Kooperation mit der Open Knowledge Foundation und deren Internetportal „Frag-den-Staat" eine Initiative gegründet, die es ermöglichen soll, den Antragstellern die Kosten für die von den Behörden erhobenen Gebühren zu erstatten.

Voraussetzungen für eine mögliche Kostenerstattung sind, dass die begehrten Informationen für Wikimedia-Initiativen relevant sind (und ggfs. in die Online-Enzyklopädie einfließen) und die Anträge über „Frag-den-Staat" gestellt wurden. Sollte der Antragsteller von der Behörde einen Gebührenbescheid erhalten, kann er bei Wikimedia einen formlosen Kostenerstattungsantrag stellen.[80]

Ob die Initiative auch dauerhaft Erfolg haben wird und die mit ihr verbundenen Ziele fördern bzw. erreichen kann, wird sich noch zeigen müssen.

[80] Vgl. https://www.heise.de/newsticker/meldung/Wikipedia-Kosten-fuer-Akteneinsicht-bei-Aemtern-werden-erstattet-3580779.html (Stand: 20. März 2017)

24.5 Kein Anrufungsrecht bei Verweigerung von Umweltinformationen

Im Berichtszeitraum wurden gehäuft Anfragen in Bezug auf den Zugang zu Informationen im Zusammenhang mit Windkraftanlagen an uns herangetragen. Hierbei handelte es sich um Umweltinformationen im Sinne des § 3 Abs. 2 Saarländisches Umweltinformationsgesetz (SUIG). Eine Vermittlung durch die Landesbeauftragte für Informationsfreiheit bei abgelehnten Anträgen ist in diesen Fällen allerdings nicht möglich.

Das SUIG sieht zwar einen Anspruch auf Zugang zu Umweltinformationen vor, nicht vorgesehen ist aber eine Möglichkeit, die Informationsfreiheitsbeauftragte anzurufen, wenn der Antragsteller sein Recht auf Informationszugang nach dem SUIG als verletzt ansieht.

Um das Informationszugangsrecht der Bürgerinnen und Bürger maßgeblich zu verbessern, wäre es wünschenswert, wenn sich die Zuständigkeit der Informationsfreiheitsbeauftragten auch auf Eingaben nach dem SUIG erstrecken würde. Trotz der häufig auftretenden inhaltlichen Nähe zu allgemeinen Behördeninformationen kann die Informationsfreiheitsbeauftragte dann nicht vermittelnd tätig werden, wenn ein Bürger beispielsweise Informationen zu einem Bauvorhaben, welches Auswirkungen auf die Umwelt hat, begehrt. Zwar kann der Antragsteller Widerspruch bzw. Klage gegen die ablehnende Entscheidung der informationsverpflichteten Stelle einlegen, jedoch ist damit immer ein Kostenrisiko verbunden, was einem effektiven Informationszugang entgegensteht. Daher wäre es begrüßenswert, wenn sich das Anrufungsrecht der Informationsfreiheitsbeauftragten auch auf das SUIG beziehen würde, um im Vorfeld eines möglicherweise kostspieligen Widerspruchs- und Klageverfahrens vermittelnd tätig werden zu können (Vorbilder sind hier beispielsweise Rheinland-Pfalz und Schleswig-Holstein).

24.6 Proaktive Veröffentlichungspflichten im Saarland

Mit der Schaffung von zwei Rechtsvorschriften im Laufe des Berichtszeitraums wurde der Weg hin zu mehr Transparenz in der öffentlichen Verwaltung im Saarland beschritten. Hierbei handelt es sich um die Sponsoring-Richtlinie und das sog. Vergütungstransparenzgesetz.

24.6.1 Sponsoring- Richtlinie

Am 1. Januar 2015 ist die Richtlinie über Sponsoring in der saarländischen Landesverwaltung (Amtsbl. vom 4. Dezember 2014, S. 1041) in Kraft getreten. Mit der Richtlinie geht insbesondere das Ziel einher, bei der Finanzierung öffentlicher Aufgaben eine größtmögliche Transparenz zu erreichen.

Hierbei werden die Behörden und Einrichtungen des Saarlandes verpflichtet, die Entgegennahme von Zuwendungen in Form von Sponsoringleistungen durch Dritte ab einer Wertgrenze von 500,- Euro netto durch einen schriftlichen Vertrag oder durch eine Dokumentation der Vereinbarung aktenkundig zu machen. Über diese Sponsoringmaßnahmen wird in jedem Ressort der Landesregierung eine interne Liste geführt. Dabei sind Angaben zu machen über den Sponsor, den Betrag oder den Wert und die Veranstaltung oder die Institution.

Daneben erstellt die Landesregierung zweijährlich einen Bericht, der jedes Sponsoring ab einem Wert von 3.000,- Euro netto aufführt (sog. Sponsoringbericht). Dieser ist bis Ende des auf den Berichtszeitraum folgenden Jahres im Internet zu veröffentlichen und nennt die jeweils geförderten Projekte, die verantwortliche Behörde sowie die entsprechenden Sponsoren samt Wert der Sponsoringleistung. Eine namentliche Nennung ist nur mit Zustimmung der betreffenden Person zulässig.

24.6.2 Vergütungstransparenzgesetz

Mit dem Gesetz Nr. 1895 zur Schaffung von Transparenz in öffentlichen Unternehmen im Saarland vom 15. Juni 2016 wurde ein neues Vergütungsoffenlegungsgesetz (VergütungsOG) geschaffen, welches öffentlich-rechtliche Unternehmen mit einer mehrheitlichen Beteiligung des Landes dazu verpflichtet, die gewährten Bezüge der Führungsebenen in kumulierter Form im Jahresbericht auszuweisen. Bei einer Beteiligung von mehr als 25 Prozent ist auf die Veröffentlichung hinzuwirken. Daneben soll die Beteiligung an einem privatrechtlichen Unternehmen künftig nur dann erfolgen, wenn die kumulierte Offenlegung der Bezüge gewährleistet ist. Die Vorgaben sind ab dem Geschäftsjahr 2017 zu beachten und umzusetzen.

Mit den Neuregelungen in der Landeshaushaltsordnung (LHO), im saarländischen Sparkassengesetz (SSpG), im Kommunalselbstverwaltungsgesetz (KSVG) und in der Eigenbetriebsverordnung (EigVO) wurden entsprechende Vorgaben für die jeweils infrage kommenden Betriebe und Anstalten geschaffen.

Anlagen

25 Konferenzen der unabhängigen Datenschutzbehörden des Bundes und der Länder

25.1 Entschließung: Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten

18./19. März 2015

Zunehmend sind Systeme zur Datenanalyse auch für Polizeibehörden am Markt verfügbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist daher frühzeitig – bevor diese Systeme in der Fläche beschafft werden – darauf hin, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen. Solche Verfahren können enorme Mengen von heterogenen – strukturierten wie unstrukturierten – Daten mit hoher Geschwindigkeit auswerten. Sogenannte selbst lernende Algorithmen sind in der Lage, die Kriterien für die Auswertung selbst zu entwickeln und an neue Erkenntnisse anzupassen. Damit sollen Zusammenhänge zwischen Straftaten erkannt werden und Vorhersagen über künftige Straftaten oder Gefahren bereits im Vorfeld getroffen werden ("Predictive Policing").

Dies kann zu einer weiteren Verschiebung der polizeilichen Eingriffsschwelle in das Vorfeld von Gefahren und Straftaten führen. Die Gefahr fehlerhafter Prognosen ist der Vorfeldanalyse stets immanent – mit erheblichen Auswirkungen auf die dabei in Verdacht geratenen Personen.

Besonders kritisch ist es, wenn Analysesysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozialen Netzwerken. Diese können zudem mit polizeilichen Speicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien bewertet werden – zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertealgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

Auch wenn die derzeit in der Praxis bei einzelnen Länderpolizeien eingesetzten Verfahren, mit denen relevante polizeiliche Daten ausschließlich ortsbezogen und nicht personenbezogen ausgewertet werden, nicht die beschriebenen Risiken hervorrufen, kann die Bewertung bei nur geringfügigen Änderungen eine ganz andere sein. Die ständig weiterentwickelten technischen Auswertemöglichkeiten bergen schon heute das Potential dafür, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten - in

einem Umfang und auf eine Art und Weise - verlieren könnten, die in der Vergangenheit nicht vorstellbar gewesen ist.

Die derzeitigen gesetzlichen Vorschriften in Bund und Ländern enthalten – mit Ausnahme der Regelungen zur Rasterfahndung – keine ausdrücklichen Vorgaben für den Einsatz weit gefasster Analysesysteme. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist angesichts der beschriebenen Gefahren darauf hin, dass der Einsatz solcher Systeme durch die Polizei nur in engen Grenzen als verfassungsrechtlich zulässig zu betrachten ist.

25.2 Entschließung: Datenschutz nach „Charlie Hebdo": Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

18./19. März 2015

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen. Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terror-Anschlägen vom 11. September 2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder – mit den Worten des Bundesverfassungsgerichts – „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens". Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

25.3 Entschließung: Datenschutzgrundverordnung darf keine Mogelpackung werden!

18./19. März 2015

Der Rat der Europäischen Innen- und Justizminister hat sich am 12. und 13. März 2015 erneut mit der Reform des Europäischen Datenschutzrechts befasst und dabei über drei weitere Kapitel der geplanten Datenschutz-Grundverordnung (DS-GVO) grundsätzlich geeinigt. Hierzu gehören u. a. die zentralen Vorschriften über die Datenschutzgrundsätze und die Zulässigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Länder warnen eindringlich vor einer Aushöhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundsätzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DS-GVO hebelt zentrale Datenschutzgrundsätze aus:

- Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Maß reduziert und einen Anreiz für datenschutzfreundliche Technologien darstellt.
- Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Zweckänderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten und die ausdrücklich gewünschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.
- Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (Opt-Out) eben nicht mit einer expliziten Willensbekundung (Opt-In) gleichzusetzen ist. Der Vorschlag des Rates, „ausdrücklich“ zu streichen und durch den minder klaren Begriff „eindeutig“ zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.

- Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist.

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

25.4 Entschließung: Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

18./19. März 2015

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz“) würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

- Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfügung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

- Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen" ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.
- Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z.B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

25.5 Entschließung: IT-Sicherheitsgesetz nicht ohne Datenschutz!

18./19. März 2015

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Der von der Bundesregierung eingebrachte Gesetzentwurf für ein IT-Sicherheitsgesetz (BT-Drs. 18/4096 v. 25. Februar 2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale für Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Melde- und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfällen sollen dabei wichtige Bausteine einer nationalen Strategie für mehr Informationssicherheit sein.

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevölkerung in die Gesetzgebung zur IT-Sicherheit zu stärken, muss ein beiden Seiten gerecht werdender Abwägungs- und Abstimmungsprozess deutlich zum Ausdruck kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards, als auch bei der Beurteilung von Einzelfällen.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Die damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventions- und -erkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Strafverfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des BSI für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Insofern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des o.g. Abwägungsprozesses zwischen Informationssicherheits- und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldeplicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resultiert. Dies setzt unabhängige und leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus.

Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren

eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermöglichen.

25.6 Entschließung: Mindestlohngesetz und Datenschutz

18./19. März 2015

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

Unter anderem haftet ein Unternehmen dafür, wenn ein Subunternehmer - und ggf. auch dessen Subunternehmer - den Beschäftigten nicht den Mindestlohn zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich - wie Industrie- und Handelskammern berichten - zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaften sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes, sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

25.7 Entschließung: Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

18./19. März 2015

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

25.8 Entschließung: Verschlüsselung ohne Einschränkungen ermöglichen

18./19. März 2015

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,

- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,
- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und
- kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014-2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist[81]. Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

25.9 Entschließung: Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken

9. Juni 2015

Mit der Vorlage des „Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" (BR-Drs. 249/15) beabsichtigt die Bundesregierung, eine Vorratsspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen.

Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt.

---

[81] Zitat: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."

Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde.

Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (z.B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt.

Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standort- und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe, hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecken zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtbegriffe (z.B. angemessenes Verhältnis oder ein besonderes Schwerwiegen einer Tat) verwendet werden und den Sicherheitsbehörden somit ein weiter Spielraum eröffnet wird.

Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotential sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen.

Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

25.10 Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung

14. August 2015

I. Vorbemerkung

Nachdem der Rat der Justiz- und Innenminister am 15. Juni 2015 seinen Standpunkt zur Datenschutz-Grundverordnung abgeschlossen hat, beraten Kommission, Parla-

ment und Rat seit Ende Juni im sogenannten Trilog über ihre verschiedenen Positionen zur Datenschutz-Grundverordnung mit dem Ziel einer Gesamteinigung und Verabschiedung des Rechtsaktes zum Jahresende 2015.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012 mehrfach öffentlich zur Datenschutzreform positioniert. Sie hat sowohl zum gesamten Paket am 11. Juni 2012 eine Stellungnahme abgegeben als auch in einer Reihe von Entschließungen und Stellungnahmen zu einzelnen Fragen der Datenschutzreform Position bezogen[82]. Die Konferenz hat von Anfang an das Ziel der Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union bereitzustellen“[83]. Dies gilt umso mehr, als die Kommission ausdrücklich das Grundrecht des Einzelnen auf Datenschutz in den Mittelpunkt gerückt hat, dem die Reform zugutekommen soll.

Deshalb ist es für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder von außerordentlicher Bedeutung, dass die Datenschutz-Grundverordnung im Vergleich zum geltenden Rechtsstand – der im Wesentlichen durch die Richtlinie 95/46/EG geprägt ist – einen verbesserten, mindestens aber gleichwertigen Grundrechtsschutz gewährleistet. Keinesfalls darf die Reform des Europäischen Datenschutzrechts dazu führen, hinter dem geltenden Datenschutzniveau zurückzubleiben. Die Konferenz betont, dass die sich aus Artikel 8 der Grundrechtecharta und Art. 16 Abs. 1 AEUV ergebenden Grundprinzipien des Datenschutzes daher nicht zur Disposition stehen dürfen. Nach wie vor fehlen spezifische Anforderungen an riskante Datenverarbeitungen, wie z.B. beim Profiling oder bei der Videoüberwachung.

Auch sollen Daten für Werbezwecke weiterhin ohne Einwilligung der Betroffenen verarbeitet werden können. Gerade in Zeiten von Big Data und globaler Datenverarbeitung sind die Autonomie des Einzelnen, Transparenz und Rechtmäßigkeit der Datenverarbeitung, die Zweckbindung oder die Verantwortlichkeit des Datenverarbeiters ebenso wichtige Elemente der Grundrechtsgewährleistung wie eine starke Datenschutzaufsicht und wirksame Sanktionen.

Bei den genannten und den im Folgenden angesprochenen Themen handelt es sich um die wichtigsten Punkte, denen sich nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die am Trilog teilnehmenden Parteien insbesondere widmen sollten.

Zur besseren Handhabbarkeit orientiert sich diese Stellungnahme an der Struktur der vorliegenden Entwürfe der Datenschutz-Grundverordnung.

---

[82] Entschließungen „Ein hohes Datenschutzniveau für ganz Europa“ vom 21./22. März 2012 sowie Stellungnahme vom 11. Juni 2012; „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ vom 8./9. November 2012; „Europa muss den Datenschutz stärken“ nebst Erläuterungen vom 13./14. März 2013; „Zur Struktur der Europäischen Datenschutzaufsicht“ vom 27./28. März 2014 sowie „Datenschutz-Grundverordnung darf keine Mogelpackung werden!“ vom 8./19. März 2015, jeweils abrufbar unter: http://www.bfdi.bund.de/DE/Infothek/Entschliessungen/DSBundLaender/Functions/DSK_table.html.

[83] Mitteilung der Kommission Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg., Ziff. 6.

II. Die Vorschläge im Einzelnen

1. Der Anwendungsbereich der Datenschutz-Grundverordnung

a. Keine Ausweitung der Haushaltsausnahme!

Der Rat hat die so genannte Haushaltsausnahme in Art. 2(2)(d) Datenschutz-Grundverordnung (DS-GVO) in der Weise erweitert, dass er die im Kommissionsvorschlag enthaltenen Worte „ausschließlich" und „ohne jede Gewinnerzielungsabsicht" gestrichen hat.

Der Vorschlag des Rates ist in einer Weise formuliert, dass ein maßgeblicher Teil der Verarbeitung personenbezogener Daten durch natürliche Personen auch dann aus dem Anwendungsbereich des Datenschutzrechts herausfiele, wenn in erheblicher Weise in das Datenschutzgrundrecht Dritter eingegriffen würde. Nach der Formulierung des Rates würde es bereits genügen, wenn die Verarbeitung zu persönlichen oder familiären Zwecken bei einer Gesamtbetrachtung lediglich einen völlig untergeordneten Zweck darstellte, um unter die Haushaltsausnahme zu fallen und damit nicht mehr dem Datenschutzrecht zu unterliegen.

Ein Nutzer eines sozialen Netzwerks oder der Betreiber einer privaten Homepage würde selbst dann nicht unter das Datenschutzrecht fallen, wenn er in großem Umfang personenbezogene Daten unbeschränkt im Internet veröffentlicht, solange er die Datenverarbeitung (auch) als eine solche zu persönlichen oder familiären Zwecken deklariert. Eine derartige Erweiterung wäre nicht akzeptabel. Ebenso wenig kann die Gewinnerzielungsabsicht ein Kriterium für die Anwendung des Datenschutzrechts sein, da die Eingriffstiefe einer Datenverarbeitung hiervon nicht abhängt. Eine zu weitgehende Ausdehnung der Haushaltsausnahme stünde im Widerspruch zum primärrechtlich garantierten Grundrecht auf Datenschutz und kann deshalb im Sekundärrecht nicht umgesetzt werden.

> Die Konferenz spricht sich gegen eine Erweiterung der Haushaltsausnahme in Art. 2(2)(d) DS-GVO und die damit verbundene Einschränkung des Anwendungsbereichs des Datenschutzrechts aus. Die Haushaltsausnahme sollte sich daher weiterhin an dem Wortlaut von Art. 2(2) der Richtlinie 95/46/EG orientieren und nur solche Verarbeitungsvorgänge aus dem Anwendungsbereich herausnehmen, die sich ausschließlich auf persönliche und familiäre Tätigkeiten beziehen.

b. Keine weitere Beschränkung des Anwendungsbereichs der DS-GVO zugunsten der JI-Richtlinie!

Die DS-GVO wird keine Anwendung finden, soweit die Richtlinie für den Bereich Polizei und Justiz (JI-RL) Anwendung finden wird. Somit bestimmt der Anwendungsbereich der JI-RL zugleich den Anwendungsbereich der DS-GVO. Vor diesem Hintergrund hat der Rat in den letzten Monaten verschiedene Entwürfe diskutiert, die teilweise zu einer deutlichen Ausdehnung des Anwendungsbereichs der JI-RL führen könnten.

Die Konferenz sieht keine überzeugenden Gründe dafür, von der ursprünglich vorgesehenen Trennung der Anwendungsbereiche von DS-GVO und der JI-RL wesent-

lich abzuweichen. Nach dem ursprünglichen Entwurf der KOM enthält die JI-RL Regelungen zum "Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung". Der Rat kritisiert, dass damit die präventive Gefahrenabwehr nicht erfasst ist, soweit sie der Prävention einer Straftat dient. Dies führe wiederum dazu, dass die Datenverarbeitung der Polizeien unterschiedlichen Rechtsakten unterliege. Um die gesamte Aufgabenerfüllung der Polizei unter einem Rechtsakt – der JI-RL – zusammenzufassen, soll der Anwendungsbereich der RL entsprechend erweitert werden. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltung unter die RL zu fassen.

Eine solche Ausweitung lehnt die Konferenz ab. Sofern überhaupt ein Kompromiss gefunden werden muss, der den Anwendungsbereich der JI-RL für die polizeiliche Datenverarbeitung erweitern soll, muss durch die Formulierung im Gesetzestext und in den Erwägungsgründen zumindest sichergestellt sein, dass davon nicht auch noch die Datenverarbeitung der Ordnungsverwaltung erfasst wird. Die Datenverarbeitung von anderen Behörden muss weiterhin von der DS-GVO geregelt werden, wie es auch der gegenwärtige Rechtsrahmen vorsieht.

> Die Konferenz spricht sich gegen die in der Ratsfassung hinzugefügte Beschränkung des Anwendungsbereichs der DS-GVO zugunsten der JI-Richtlinie in Art. 2(2)(e) DS-GVO aus. Die Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte von der DS-GVO geregelt werden.

2. Für eine klare Definition des Personenbezugs!

Die DS-GVO knüpft wie auch das geltende Recht weiterhin am Begriff des personenbezogenen Datums an. Dies ist die logische Konsequenz aus der grundrechtlichen und primärrechtlichen Gewährleistung in Art. 8 Abs. 1 EU-Grundrechtecharta und Art. 16 Abs. 1 AEUV, wonach jede Person das Recht auf Schutz der sie betreffenden Daten hat. Deshalb kommt der Definition des personenbezogenen Datums in Art. 4(1) DS-GVO eine außerordentlich hohe Bedeutung zu, denn sie entscheidet letztlich über die Anwendbarkeit des Datenschutzrechts.

Dabei muss klargestellt sein, dass eine natürliche Person auch dann als identifizierbar anzusehen ist, wenn sie innerhalb einer Gruppe von Personen von anderen Personen unterschieden und damit auch unterschiedlich behandelt werden kann. Deshalb muss die Identifizierbarkeit einer Person auch deren Herausgreifen einschließen, wie es dem Vorschlag des Parlaments in EG 23 zugrunde liegt.

Die Vorschläge von Kommission und Rat zu EG 24 führen zudem zu einer unnötig restriktiven Auslegung des Begriffs des personenbezogenen Datums, indem sie Kennnummern, Standortdaten, Online-Kennungen oder IP-Adressen nicht notwendigerweise als personenbezogene Daten ansehen. Für diese Daten gelten die gleichen Kriterien für die Bestimmung des Personenbezugs wie für jede andere Information. Deren gesonderte Erwähnung verleitet zu dem unzulässigen Schluss, dass hier andere Kriterien gelten würden. Dies widerspräche auch der Rechtsprechung des EuGH.

Die Konferenz unterstützt insoweit den Vorschlag des Parlaments zu EG 23, wonach klargestellt ist, dass die Möglichkeit des Herausgreifens einer natürlichen Person aus einer Gruppe ein Mittel zu deren Identifizierbarkeit ist.

Die Konferenz fordert, bei EG 24 dem Vorschlag des Parlaments zu folgen, der klarstellt, dass Kennnummern, Standortdaten, Online-Kennungen, IP-Adressen oder sonstige Elemente grundsätzlich als personenbezogene Daten zu betrachten sind.

3. Datensparsamkeit muss Gestaltungsziel bleiben!

Für eine möglichst grundrechtsschonende Datenverarbeitung ist es unabdingbar, dass sich Staat und Wirtschaft auf das zur Erreichung ihrer rechtlichen oder legitimen Zwecke notwendige Maß beschränken. Die allgegenwärtige Datenverarbeitung und der Einsatz von Big-Data-Technologien erzeugen eine unvorstellbare Menge an (auch personenbezogenen) Daten.

Dies führt zu einer für viele als diffus bedrohlich empfundenen Situation, da auf diese Weise Unternehmen oder Behörden potentiell in der Lage sind, über jeden Einzelnen Informationen aus sämtlichen Lebensbereichen zu erfassen und beliebig auszuwerten. Gerade deshalb ist das Prinzip von Datenvermeidung und Datensparsamkeit, das seit vielen Jahren im deutschen Datenschutzrecht verankert ist, wichtiger denn je. Auf diese Weise werden Anreize für eine datenschutzfreundliche Gestaltung von Verarbeitungs- und Geschäftsprozessen geschaffen.

Dies haben die Kommission und das Parlament erfreulicherweise auch erkannt, indem sie das Prinzip der Datensparsamkeit ausdrücklich als eines der Grundprinzipien des Datenschutzes in Art. 5(1)(c) DS-GVO verankert haben. Umso unverständlicher ist es, dass der Rat in seinem Entwurf das Prinzip der Datenvermeidung aus dem Text gestrichen hat – ein fatales Zeichen zugunsten einer noch weiter ausufernden Verarbeitung personenbezogener Daten.

Die Konferenz spricht sich für eine ausdrückliche Verankerung des Prinzips der Datensparsamkeit in Art. 5(1)(c) DS-GVO entsprechend der Formulierung der Kommission bzw. des Parlaments aus.

4. Keine Aufweichung der Zweckbindung!

Die Zweckbindung ist seit jeher eines der zentralen Prinzipien des Datenschutzrechts. Sie dient der Transparenz und Vorhersehbarkeit der Verarbeitung personenbezogener Daten und stärkt damit die Autonomie der Betroffenen. Angesichts der Unsichtbarkeit und des Umfangs der Datenverarbeitung muss sich der Betroffene darauf verlassen können, dass seine personenbezogenen Daten grundsätzlich nur zu den Zwecken weiterverarbeitet werden, zu denen sie erhoben worden sind. Art. 8 Abs. 2 der Europäischen Grundrechtecharta hat daher die Zweckbindung als tragendes Prinzip des Datenschutzes verankert.

Dementsprechend folgt der Kommissionsentwurf der DS-GVO grundsätzlich dem hergebrachten Ansatz der Richtlinie 95/46/EG, indem er in Art. 5(1)(b) zunächst festlegt, dass personenbezogene Daten nur für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen.

Die Konzeption der geltenden Richtlinie 95/46/EG ist dadurch geprägt, dass sie eine Verarbeitung personenbezogener Daten zu anderen Zwecken nur zulässt, wenn diese neuen Zwecke mit dem Ursprungszweck vereinbar sind. Weitere Zweckänderungen lässt die Richtlinie nicht zu. Auf dieser Basis ist es in der Regel gelungen, einen starken Schutz des Rechts auf informationelle Selbstbestimmung in einen angemessenen Ausgleich mit den öffentlichen Datenverarbeitungsinteressen des Staates und den legitimen Interessen der Unternehmen zu bringen.

Hiervon abweichend hat die Kommission in ihrem Vorschlag zu Art. 6(4) DS-GVO zusätzlich die Möglichkeit vorgesehen, dass personenbezogene Daten auch zu solchen Zwecken weiterverarbeitet werden dürfen, die mit dem ursprünglichen Verarbeitungszweck nicht vereinbar sind. Der Rat hat diese Ausnahme noch erweitert, indem er solche Zweckänderungen auch bei einem überwiegenden berechtigten Interesse des Verarbeiters zulassen will. Spätestens durch diese Ergänzungen werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

Das Europäische Parlament ist deshalb zu dem bewährten Ansatz der Richtlinie 95/46/EG zurückgekehrt und hat konsequenterweise Art. 6(4) DS-GVO gestrichen. Dies entspricht auch einer frühzeitig erhobenen Forderung der Artikel-29-Gruppe der Europäischen Datenschutzbehörden.

Die Gewährleistung einer starken Zweckbindung ist eine unabdingbare Voraussetzung, um dem Einzelnen ein Höchstmaß an Entscheidungsfreiheit und Transparenz zu ermöglichen.

Die Konferenz lehnt deshalb die vom Rat vorgeschlagene Aufweichung der Zweckbindung entschieden ab und spricht sich auf der Basis des Ratsvorschlages für eine Streichung des Art. 6(4) DS-GVO aus.

5. Keinen datenschutzrechtlichen Freibrief für Statistik, Archive sowie wissenschaftliche und historische Zwecke!

Die Verarbeitung personenbezogener Daten für die im öffentlichen Interesse tätigen Archive, für die Statistik sowie für historische und für Forschungszwecke folgt aufgrund der jeweiligen Eigenarten der genannten Zweckbestimmungen zum Teil besonderen Regelungen. In allen Fällen geht es darum, die Grundrechte auf Datenschutz und Privatsphäre in einen angemessenen Ausgleich zu bringen mit wichtigen - zum Teil ebenfalls grundrechtlich - geschützten Interessen wie der Forschungsfreiheit oder den öffentlichen Interessen an der amtlichen Statistik bzw. der langzeitlichen Verfügbarmachung staatlicher Informationen durch die Archive. Dies wird grundsätzlich auch durch die Datenschutzbeauftragten des Bundes und der Länder

anerkannt. Das geltende Datenschutzrecht hat diesen Ausgleich bisher angemessen hergestellt.

Der Rat geht in seinem Entwurf in verschiedener Hinsicht über diesen Ansatz hinaus und privilegiert die genannten Bereiche in unannehmbarer Weise. Einerseits soll eine Weiterverarbeitung zu den genannten Zwecken gem. Art. 5(1)(b) DS-GVO generell immer möglich sein; die Zweckbindung wird insoweit aufgehoben. Andererseits soll Art. 6(2) DS-GVO die (Weiter-) Verarbeitung zu den genannten Zwecken ermöglichen, ohne dass es der Rechtsgrundlagen des Art. 6(1) DS-GVO bedarf. Dies würde bedeuten, dass eine Verarbeitung zu den genannten Zwecken ohne weitere Rechtsgrundlage – vorbehaltlich mitgliedstaatlicher Sonderbestimmungen in Teilbereichen nach Art. 83 DS-GVO – möglich wäre und die Weiterverarbeitung personenbezogener Daten, die ursprünglich zu anderen Zwecken erhoben worden sind, weitgehend schrankenlos möglich wäre.

Hinzu kommt, dass der gegenständliche Anwendungsbereich der Privilegierung zu weit gefasst ist. Einzig für die Archive im öffentlichen Interesse bestehen insofern keine Bedenken, zumal sich zumindest die staatlichen Archive nach Art. 83 DS-GVO nach dem meist ausdifferenzierten mitgliedstaatlichen Recht zu richten haben. Bei der Privilegierung der statistischen Zwecke differenziert der Ratsentwurf hingegen nicht nach solchen der amtlichen Statistik und sonstigen statistischen Zwecken. Während für erstere im Rahmen von Art. 83 DS-GVO eine Privilegierung nachvollziehbar ist, besteht im Übrigen die Gefahr, dass etwa die Betreiber von sozialen Netzwerken, Suchmaschinen, Analysetools usw. die von ihnen vorgenommene umfassende Profilbildung als statistische Zwecke deklarieren. Vergleichbare Bedenken bestehen auch gegen die Privilegierung der wissenschaftlichen Datenverarbeitung, die vom Rat nicht auf Zwecke der wissenschaftlichen Forschung beschränkt wird, sondern darüber hinausgeht.

Datenschutzrechtliche Grundsätze gelten auch für die Verarbeitung personenbezogener Daten zu Zwecken der öffentlichen Archive, der Statistik sowie für wissenschaftliche und historische Zwecke. Die Konferenz erwartet im Trilog eine differenzierte und ausgewogene Regelung zum Schutze der genannten Interessen, die die Einschränkungen der Grundrechte auf Datenschutz und Privatsphäre auf das unabdingbar Notwendige beschränkt. Jede Verarbeitung zu den genannten Zwecken bedarf einer Rechtsgrundlage im Sinne von Art. 6(1) DS-GVO. Art. 6(2) DS-GVO ist insofern missverständlich und sollte daher gestrichen werden. Darüber hinaus sollte – vergleichbar mit den Archiven – nur die amtliche Statistik privilegiert werden. Profilbildungen in sozialen Netzwerken, Suchmaschinen, durch den Einsatz von Analysetools usw. dürfen nicht privilegiert werden.

6. Die Einwilligung muss die Datenhoheit des Einzelnen sichern!

Recht auf informationelle Selbstbestimmung bedeutet seit jeher, dass der Einzelne grundsätzlich selbst über Preisgabe und Verwendung seiner personenbezogenen Daten entscheiden darf. Daraus folgt unmittelbar, dass der Einzelne grundsätzlich autonom darüber bestimmen kann, ob er eine Verarbeitung seiner personenbezogenen Daten erlaubt oder nicht.

Die Einwilligung ist ein wesentliches Element, um diese Autonomie wirksam zu sichern. Sie ist deshalb in Art. 8 Abs. 2 der EU-Grundrechtecharta ausdrücklich als Legitimation für die Verarbeitung personenbezogener Daten genannt.

Kommission und Parlament haben sich im Bewusstsein dieser Bedeutung dafür entschieden, dass eine Einwilligung nur dann wirksam sein soll, wenn sie ausdrücklich erfolgt. Nur bei einer ausdrücklichen Willensbekundung kann letztlich der Nachweis erbracht werden, dass sich der Einzelne der Tragweite seiner Entscheidung bewusst wird.

Der Rat verabschiedet sich in seinem Entwurf entgegen der Grundrechtecharta von diesem Grundsatz, indem er bereits eine eindeutige Willensbekundung ausreichen lässt. Damit wird es insbesondere den global agierenden Diensteanbietern ermöglicht, durch die Verwendung pauschaler Datenschutzbestimmungen und datenschutzunfreundlicher Voreinstellungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Als datenschutzgerechte Einwilligung kann nur ein Opt-In akzeptiert werden.

Es sollte zudem ein Koppelungsverbot ausdrücklich in den verfügenden Teil der DS-GVO aufgenommen werden. Während Kommission und Parlament dieses in Artikel 7(4) DS-GVO vorsehen, hat es der Rat gestrichen und erwähnt es lediglich in den Erwägungsgründen (EG 34).

Zur wirksamen Gewährleistung des Rechts auf informationelle Selbstbestimmung unterstützt die Konferenz den Ansatz von Kommission und Parlament, dass eine Einwilligung nur dann die Verarbeitung personenbezogener Daten legitimieren kann, wenn sie ausdrücklich abgegeben wird. In Art. 7 DS-GVO sollte darüber hinaus ein Koppelungsverbot ausdrücklich geregelt werden.

7. Rechte der Betroffenen

a. Sicherstellung der Unentgeltlichkeit

Die Entwürfe der Kommission und des Parlaments sehen in Art. 12(4) DS-GVO vor, dass Unterrichtungen der Betroffenen und *die auf Antrag ergriffenen Maßnahmen* zur Umsetzung der Betroffenenrechte unentgeltlich sind. Der Entwurf des Rates sieht dagegen vor, dass lediglich die Informationen gemäß Art. 14 und 14a sowie alle *Mitteilungen* gemäß den Artikeln 16 bis 19 und 32 unentgeltlich zur Verfügung gestellt werden. Damit bleibt unklar, ob auch die Umsetzung der Betroffenenrechte selbst unentgeltlich erfolgen muss oder die verantwortlichen Stellen hierfür ggf. eine Gebühr erheben können. Dafür spricht, dass nur das Auskunftsrecht (Art. 15) ausdrückliche Regelungen zur (Un-)Entgeltlichkeit enthält (vgl. Art. 15(1) und (1b)), die übrigen Betroffenenrechte hingegen nicht.

Die Unentgeltlichkeit der Ausübung und Umsetzung der Betroffenenrechte ist unabdingbare Voraussetzung für die effektive Wahrnehmung des Rechts auf informationelle Selbstbestimmung. Gebühren für die Ausübung schrecken die Betroffenen regelmäßig von der Wahrnehmung ihrer Rechte ab.

Die Konferenz spricht sich für eine unmissverständliche Regelung aus, dass die Ausübung der Betroffenenrechte und deren Umsetzung durch die verantwortlichen Stellen unentgeltlich erfolgen müssen.

b. Keine Einschränkung der Betroffenenrechte!

Die Information der Betroffenen (Art. 14, 14a DS-GVO) versetzt diese in die Lage, Umfang und Risiko der Datenverarbeitung einzuschätzen. Sie ist die wesentliche Bedingung für die Schaffung von Transparenz. Der Entwurf des Rates sieht lediglich die Unterrichtung über die Identität der verantwortlichen Stelle, die Zwecke der Datenverarbeitung und die Rechtsgrundlage vor. Weitergehende Informationen sollen nur dann erforderlich sein, wenn sie unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten.

Die Konferenz lehnt Beschränkungen der Betroffenenrechte ab. Die Formulierungen des Rates führen zu Rechtsunsicherheit und lassen Raum für Interpretationen, die zu einer Absenkung des geltenden Datenschutzniveaus führen.

Die Informationspflichten der Art. 14 und 14a DS-GVO beinhalten im Gegensatz zum Recht auf Auskunft (Art. 15) lediglich allgemeine, abstrakte Informationen über Art, Umfang und Zweck der Datenverarbeitung. Die Informationspflicht führt daher nicht zu exzessiven Bürokratiekosten, weil sie in standardisierter Form gegenüber den Betroffenen erfüllt werden kann. Die vom Europäischen Parlament vorgeschlagenen standardisierten Informationsmaßnahmen unter ergänzender Verwendung von Piktogrammen (Art. 13a) erachtet die Konferenz für erwägenswert.

Die Konferenz spricht sich gegen Einschränkungen der Betroffenenrechte aus und unterstützt die Position des Europäischen Parlaments.

c. Wirksame Begrenzung der Profilbildung sicherstellen!

Die Datenschutzbeauftragten des Bundes und der Länder sind der Auffassung, dass die bisherigen Vorschläge für eine Regelung von Profilbildungen in Art. 20 DS-GVO nicht geeignet sind, um die Bürgerinnen und Bürger im Zeitalter von Big Data, der Allgegenwart des Internets der Dinge und der in alle Lebens-, Privat- und Intimbereiche wie die Gesundheit vordringenden Technologien zur individuellen Datenerfassung und -analyse effektiv vor der Erstellung und Nutzung von Persönlichkeitsprofilen zu schützen.

Die Vorschläge von Kommission, Parlament und Rat zu Art. 20 DS-GVO sind unzureichend, da keiner der Vorschläge die Profilbildung an sich besonderen Zulässigkeitsvoraussetzungen unterwirft, sondern erst das Treffen einer „automatisierten Entscheidung“ (Rat) oder einer „Maßnahme“ (KOM) auf Basis des Profilings bzw. „Profiling, das Maßnahmen zur Folge hat, die rechtliche oder ähnlich erhebliche Auswirkungen auf die Interessen der betroffenen Person hat“ (EP).

Unzulänglich ist insbesondere der Vorschlag des Rates, da er das Phänomen des Profilings in Anlehnung an Art. 15 Abs. 1 der EG-Datenschutzrichtlinie 95/46 auf das Treffen automatisierter Entscheidungen mit Rechtswirkung für den Einzelnen reduziert. Geregelt wird damit lediglich eine spezifische Folge der Datenverarbeitung im Zusammenhang mit der Auswertung von Persönlichkeitsmerkmalen, nicht aber die grundlegende Frage, zu welchen Zwecken und innerhalb welcher Grenzen Persönlichkeitsprofile überhaupt erstellt und genutzt werden dürfen. Zudem beinhaltet dieser Ansatz in der Praxis ein erhebliches Interpretations- und Umgehungspotenzial im Hinblick auf Dienste oder Anwendungen, die keine unmittelbaren Rechtswirkungen gegenüber dem Betroffenen entfalten, wie die Analyse des Nutzerverhaltens im Internet, die Analyse persönlicher Vorlieben durch ein soziales Netzwerk, die Analyse von Bewegungsdaten oder die Analyse der Körperaktivität mittels Apps und Sensoren.

Vor diesem Hintergrund plädieren die Datenschutzbeauftragten des Bundes und der Länder für eine differenzierte Regelung der Profilbildung und -nutzung in der DS-GVO, die folgende Kernelemente beinhalten sollte:

- Statt der Verkürzung auf automatisierte Einzelfallentscheidungen ist ein Ansatz zu wählen, der sämtliche Profilbildungen oder darauf basierende Maßnahmen erfasst. Diesem Ansatz entspricht am ehesten der vom Europäischen Parlament zu Artikel 20 unterbreitete Regelungsvorschlag.
- Ausnahmen vom Verbot der Profilbildung bedürfen eng begrenzter klarer Erlaubnistatbestände. Wegen ihrer hohen Sensitivität sollte zudem festgelegt werden, dass besondere Kategorien personenbezogener Daten nicht in eine Profilbildung einfließen dürfen.
- In jedem Fall sollte die Verarbeitung personenbezogener Daten zu Zwecken des Profilings stets mit einem Höchstmaß an Transparenz und Informiertheit des Betroffenen einhergehen. Der Einzelne muss wissen, wann, zu welchem Zweck und in welcher Form seine Daten im Internet oder bei der Nutzung eines Dienstes auf einem Endgerät zu Profilingzwecken verarbeitet werden und muss hierzu seine ausdrückliche Einwilligung erteilen.
- Zudem sollte eine Verpflichtung zu frühestmöglicher Anonymisierung oder Pseudonymisierung der für die Profilbildung und -auswertung verwendeten Daten bestehen, letzteres flankiert von einem Verbot der (Re-)Identifizierung.

In Anbetracht der wiederholt vom EuGH festgestellten Gefahren, die von Persönlichkeitsprofilen für das Grundrecht auf Datenschutz ausgehen, fordert die Konferenz, die vorliegenden Vorschläge für eine Profilingregelung im Sinne der vorgenannten Eckpunkte substanziell zu verbessern.

8. Die datenschutzrechtliche Verantwortlichkeit gilt für jede Verarbeitung personenbezogener Daten!

Die in Kapitel IV, insbesondere in Art. 22 DS-GVO geregelte Verantwortlichkeit für die Einhaltung der datenschutzrechtlichen Bestimmungen *(Accountability)* gehört zu

den zentralen Grundprinzipien eines modernen Datenschutzrechts. Die für die Verarbeitung Verantwortlichen und die Auftragsdatenverarbeiter sind in jedem Falle und ohne Einschränkungen für die Einhaltung des Datenschutzrechts verantwortlich. Dies gilt ungeachtet der Art, des Umfangs, der Umstände und der Zweck der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für die Betroffenen. Ebenso müssen die für die Verarbeitung Verantwortlichen und Auftragsdatenverarbeiter uneingeschränkt in der Lage sein, die Einhaltung ihrer Pflichten nachzuweisen. Risikobasierte Aspekte dürfen lediglich bei der Frage berücksichtigt werden, welche konkreten Maßnahmen zur Einhaltung der Pflichten zu treffen sind.

Es muss daher klargestellt werden, dass sich ein risikobasierter Ansatz nicht auf das „Ob" und die Nachweisbarkeit, sondern allenfalls auf das „Wie" der Einhaltung der Pflichten beziehen kann. Dies wird im Vorschlag der Kommission am besten verdeutlicht, in dem auf jede Relativierung verzichtet wird.

Die Konferenz spricht sich für den seitens der Kommission für Art. 22 DS-GVO gewählten Ansatz aus, um zu verdeutlichen, dass die Verantwortlichkeit *(„Accountability")* ein tragendes Grundelement des Datenschutzes ist, das als solches einem risikobasierten Ansatz nicht zugänglich ist.

9. Für die Verankerung von Gewährleistungszielen beim technischen und organisatorischen Datenschutz!

Die Verarbeitung personenbezogener Daten bedarf zum Schutz der Grundrechte nicht nur eines rechtlichen, sondern auch eines technischen und organisatorischen Schutzes. Ein modernes Datenschutzrecht muss hierfür Gewährleistungsziele definieren, an denen sich die zu treffenden Maßnahmen auszurichten haben. Dies bedeutet, dass zu den klassischen Gewährleistungszielen der IT-Sicherheit spezifische Ziele hinzutreten müssen, die sich namentlich auf den Schutz personenbezogener Daten beziehen. Deshalb sind die Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit, aber auch Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit in der DS-GVO zu verankern. Während sich Kommission und Rat in ihren Vorschlägen zu Art. 30(2) bzw. 30(1a) DS-GVO im Wesentlichen auf die klassischen Ziele Verfügbarkeit, Integrität und Vertraulichkeit fokussieren, geht der Ansatz des Parlaments in Art. 30(1a) und 30(2) DS-GVO i. V. m. Art. 5(1)(ea) und (eb) am weitesten.

Die Konferenz hält eine konsequente, klare und übersichtliche Verankerung der Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit, Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit in Art. 30 DS-GVO für notwendig. Sie unterstützt insoweit die Zielrichtung des Parlaments, spricht sich allerdings für eine übersichtlichere Gestaltung aus.

10. Guter Datenschutz braucht betriebliche und behördliche Datenschutzbeauftragte!

Ungeachtet der materiell-rechtlichen Bestimmungen hängt das konkrete Datenschutzniveau in Behörden und Unternehmen ganz entscheidend davon ab, welche

Akzeptanz der Datenschutz vor Ort genießt und wie die Datenschutzkultur ausgeprägt ist. Hierzu können die Aufsichtsbehörden für den Datenschutz Impulse liefern und durch Kontrollen und Beratungen einen entscheidenden Beitrag leisten. Diese Aktivitäten bleiben aber notwendigerweise punktuell und sind aufgrund der unterschiedlichen Rollen nicht immer konfliktfrei. Deshalb kommt der Institution der Datenschutzbeauftragten in Unternehmen und Verwaltungen eine hohe Bedeutung zu.

Es ist deshalb erfreulich, dass sowohl Kommission als auch Parlament in Art. 35 DS-GVO die verpflichtende Bestellung interner Datenschutzbeauftragter vorsehen. Allerdings sind die von beiden Institutionen gewählten Kriterien, unter denen eine Bestellung verpflichtend ist, wenig überzeugend.

Bedauerlicherweise hat sich im Rat eine europaweit geltende Verpflichtung zur Bestellung von Datenschutzbeauftragten nicht durchgesetzt. Hierbei wird vor allem mit dem bürokratischen und wirtschaftlichen Aufwand argumentiert. Nach den jahrzehntelangen Erfahrungen in Deutschland überzeugt dieses Argument nicht. Der Compliance-Aufwand für die Unternehmen ist ohne die Einbindung betrieblicher Datenschutzbeauftragter nicht unerheblich; durch deren Einsatz können zudem Sanktionen und Bußgelder oftmals vermieden werden.

> Die Konferenz setzt sich nach wie vor dafür ein, dass eine verpflichtende Bestellung betrieblicher und behördlicher Datenschutzbeauftragter europaweit verbindlich vorgeschrieben wird. Während es für Behörden keine Ausnahmen geben sollte, sollten Unternehmen nicht nur ab einer bestimmten Größe oder einer bestimmten Zahl Betroffener einen Datenschutzbeauftragten bestellen, sondern in jedem Falle auch dann, wenn die Datenverarbeitung mit besonderen Risiken für die Rechte und Freiheiten der Betroffenen verbunden ist.

11. Mehr Kontrolle über Datenübermittlungen an Behörden und Gerichte in Drittstaaten!

Seit den Enthüllungen von Edward Snowden wird intensiv über einen besseren Schutz der personenbezogenen Daten von europäischen Bürgerinnen und Bürgern gegenüber Behörden und Stellen aus Drittstaaten diskutiert. Deshalb hat das Parlament einen spezifischen Art. 43a DS-GVO vorgeschlagen. Dieser stellt klar, dass Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaats, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der EU grundsätzlich weder anerkannt werden noch vollstreckbar sind, wenn dies nicht in internationalen Übereinkommen zur Amts- oder Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der in den Abkommen bezeichneten zuständigen Stellen.

Die Konferenz unterstützt diese Forderung ebenso wie die Artikel-29-Gruppe. Mit der Schaffung einer solchen Regelung wird die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Verhältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Der Rat ist einer entsprechenden Initiative der Bundesregierung bedauerlicherweise nicht gefolgt.

Die Konferenz spricht sich weiterhin dafür aus, eine spezifische Rechtsgrundlage für die Datenübermittlung an Behörden und Gerichte in Drittstaaten zu schaffen, mit der insbesondere im Hinblick auf die nachrichtendienstliche Überwachung mehr Transparenz und Kontrolle geschaffen wird. Sie unterstützt den vom Parlament eingebrachten Vorschlag eines Art. 43a DS-GVO.

Die Zuständigkeit sollte jedoch wie folgt geregelt werden: Haben ersuchender und ersuchter Staat ein Rechtshilfeabkommen oder einen ähnlichen internationalen Vertrag geschlossen, sollte die hierin bezeichnete Stelle für die Entgegennahme und Prüfung eines Ersuchens auf Datenübermittlung zuständig sein. In den Fällen, in denen eine zuständige Stelle nicht vertraglich bestimmt worden ist, kann diese Aufgabe nachrangig in die Zuständigkeit der Datenschutzaufsichtsbehörden fallen.

12. Für eine effektive und bürgernahe Zusammenarbeit der Datenschutzbehörden in Europa

Ein entscheidender Fortschritt der Datenschutz-Grundverordnung soll in einer verbesserten Zusammenarbeit der Datenschutzbehörden in Europa liegen. Um dies zu gewährleisten und auf der anderen Seite den Unternehmen einen Mehrwert zu bieten, hatte die Kommission einen sog. One-Stop-Shop, einen Kohärenzmechanismus und die Einrichtung eines Europäischen Datenschutzausschusses vorgeschlagen.

Auf Vorschlag des Rats soll es eine federführende Datenschutzbehörde geben, die einem Unternehmen am Ort seiner Hauptniederlassung als hauptsächlicher Ansprechpartner zur Verfügung steht, aber auch mit allen anderen – sei es aufgrund weiterer Niederlassungen oder der Betroffenheit ihrer Bürger – betroffenen Aufsichtsbehörden kooperiert. Weiterhin hat der Rat Vorschläge zu einem sog. One-Stop-Shop gemacht, sodass Betroffene sich an die Aufsichtsbehörde und die Gerichte bei ihnen vor Ort wenden können. Um zu verbindlichen Entscheidungen ohne Beteiligung der Kommission zu kommen, schlägt der Rat darüber hinaus vor, den Europäischen Datenschutzausschuss mit verbindlichen Entscheidungsbefugnissen auszustatten. Hierzu ist der Ausschuss mit eigener Rechtspersönlichkeit auszustatten.

Das vom Rat vorgeschlagene Modell ist für die Aufsichtsbehörden komplex, soll aber den Bürgerinnen und Bürgern eine ortsnahe Bearbeitung ihrer Anliegen und den Unternehmen einen Ansprechpartner für länderübergreifende Datenverarbeitungen verschaffen.

Die Konferenz unterstützt die Ziele des Ratsvorschlags zum sog. One-Stop-Mechanismus. Der effiziente Vollzug des Datenschutzrechts darf jedoch nicht durch die Untätigkeit der federführenden Datenschutzbehörde unterlaufen werden. Es ist eine Regelung zu schaffen, wonach die mitgliedstaatlichen Aufsichtsbehörden bei Betroffenheit ihrer Bürger von der federführenden Behörde ein aufsichtsbehördliches Einschreiten verlangen können, dessen Ablehnung zu einer unmittelbaren Überprüfung durch den Europäischen Datenschutzausschuss führt.

Der One-Stop-Shop soll einen ausgewogenen Ausgleich zwischen den verschiedenen Interessen schaffen, eine bürgernahe Bearbeitung von Beschwerden ermöglichen, den Unternehmen klare Ansprechpartner zur Verfügung stellen und durch die Aufwertung des Europäischen Datenschutzausschusses die notwendige Verbindlichkeit und damit Rechtssicherheit aufweisen. Die Konferenz bittet die am Trilog beteiligten Parteien gleichwohl, praktikable Verfahrensregeln festzulegen. Dies betrifft insbesondere die Frage der Verfahrensfristen und der Amtshilfe der Aufsichtsbehörden untereinander.

13. Für einen starken Beschäftigtendatenschutz

Die DS-GVO überlässt die Regelung des Datenschutzes für Beschäftigte in Artikel 82 dem mitgliedstaatlichen Recht. Der Rat und die Kommission legen fest, dass die Mitgliedstaaten dabei den Rahmen der DS-GVO einhalten müssen und verzichten auf konkretere Anforderungen.

Das Europäische Parlament gibt dagegen ganz konkrete Mindeststandards im Verordnungstext vor.

Die Konferenz hält es für wichtig, dass Artikel 82 DS-GVO den Mitgliedstaaten in jedem Falle die Möglichkeit eröffnet, auch über den Standard der DS-GVO hinausgehen zu können. Die Konferenz begrüßt den Ansatz des Parlaments, konkrete Mindeststandards für den Beschäftigtendatenschutz im Verordnungstext selbst vorzusehen.

Im Kontext der Verarbeitung von Beschäftigtendaten sollte es die Datenschutz-Grundverordnung den Mitgliedstaaten ermöglichen, im Sinne einer Mindestharmonisierung auch über das Datenschutzniveau der Verordnung hinauszugehen. Die Konferenz unterstützt den Ansatz des Parlaments, konkrete Mindeststandards festzulegen.

14. Recht auf pseudonyme Internet-Nutzung für alle Menschen in Europa schaffen!

Es gibt zahlreiche gewichtige Gründe, bei der Nutzung von Telemediendiensten auf ein Pseudonym zurückzugreifen: Dazu gehört etwa der Wunsch, einer Profilbildung unter dem realen Namen zu entgehen, sei es um sich vor rechtswidrigen Zugriffen zu schützen, sei es zur Stärkung des Schutzes bei der Nutzung sozialer Netzwerke. Ein Pseudonym kann ferner vor politischer oder rassistischer Verfolgung oder Diskriminierung und sozialer Benachteiligungen etwa wegen der sexuellen Ausrichtung schützen. Pseudonyme können schließlich verhindern, dass die private Nutzung eines Telemediums zur geschäftlichen Kontaktaufnahme durch Dritte missbraucht wird. Das ist gerade bei Berufsgeheimnisträgern wie Ärzten, Seelsorgern, Anwälten oder Sozialarbeitern nicht zuletzt zum Schutz der mit ihnen in Kontakt stehenden Personen von Bedeutung.

Das Recht, in Telemedien grundsätzlich auch unter einem Pseudonym gegenüber anderen Nutzern aufzutreten, stärkt sowohl die informationelle Selbstbestimmung Betroffener als auch die Meinungsfreiheit, ohne eine Verfolgung und Ahndung von

missbräuchlichem Verhalten von unter Pseudonym auftretenden Nutzern durch den Telemedienanbieter auszuschließen.

In der Europäischen Datenschutzgrundverordnung fehlt jedoch im Katalog der Rechte Betroffener eine entsprechende ausdrückliche Regelung.

> Die Konferenz hält es für erforderlich, zum Schutz der Privatsphäre der Telemedienutzer eine Bestimmung aufzunehmen, die zumindest bei zu privaten Zwecken genutzten Telemedien innerhalb der EU ein Recht auf pseudonyme Nutzung verbindlich statuiert.

25.11 Entschließung: Die Datenschutz-Grundverordnung muss in wesentlichen Punkten nachgebessert werden!

26. August 2015

Dies fordern im Namen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder deren gegenwärtiger Vorsitzender, der Hessische Datenschutzbeauftragte Prof. Dr. Michael Ronellenfitsch, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Andrea Voßhoff, sowie die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, Dagmar Hartge vor der Bundespressekonferenz in Berlin.

Die Beratungen über die Datenschutz-Grundverordnung sind mit dem Trilog zwischen Europäischem Parlament, Rat der Europäischen Union und Europäischer Kommission in die entscheidende Phase eingetreten. Für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist es von außerordentlicher Bedeutung, dass die Datenschutz-Grundverordnung im Vergleich zum geltenden Rechtsstand einen verbesserten, mindestens aber dem bisherigen Standard gleichwertigen Grundrechtsschutz gewährleistet. Sie appelliert an die Trilogpartner, bei ihren Verhandlungen insbesondere zu berücksichtigen:

1. Die Datensparsamkeit muss Gestaltungsziel bleiben!

Die Allgegenwärtigkeit der Datenverarbeitung und der Einsatz von Big-Data-Technologien erzeugen eine unvorstellbare Menge (auch personenbezogener) Daten. Deshalb ist das seit vielen Jahren im deutschen Datenschutzrecht verankerte Prinzip der Datenvermeidung und Datensparsamkeit wichtiger denn je. Für eine möglichst grundrechtsschonende Datenverarbeitung müssen sich sowohl Staat als auch Wirtschaft auf das zur Erreichung ihrer im Einklang mit der Rechtsordnung legitimen Zwecke notwendige Maß beschränken. Das Prinzip der Datensparsamkeit muss durch die Datenschutz-Grundverordnung explizit vorgegeben werden.

2. Es darf keine Aufweichung der Zweckbindung geben!

Der Grundsatz der Zweckbindung dient in erster Linie der Transparenz und Vorhersehbarkeit der Datenverarbeitung und stärkt die Autonomie der Betroffenen, indem sie sich darauf verlassen können, dass ihre Daten nur zu Zwecken weiterverarbeitet

werden, zu denen sie erhoben wurden. Insbesondere durch die vom Rat vorgeschlagene Regelung würden Zweckänderungen in einem derart weiten Umfang zulässig, dass das in der Europäischen Grundrechtecharta enthaltene Prinzip der Zweckbindung, preisgegeben wäre. Dies lehnt die Konferenz entschieden ab.

Auch die vom Rat vorgesehenen Privilegierungen für die Datenverarbeitung zu statistischen, historischen und wissenschaftlichen Zwecken, nach denen vom ursprünglichen Erhebungszweck abweichende Verarbeitungen stets nahezu schrankenlos zulässig sind, begegnen erheblichen Bedenken.

3. Die Einwilligung des Einzelnen muss die Datenhoheit sichern!

Recht auf informationelle Selbstbestimmung bedeutet, dass der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten in der Form der Einwilligung entscheiden kann. Die Einwilligung ist aber nur dann ein wesentliches Element zur Gewährleistung der Datenhoheit, wenn sie durch eine ausdrückliche Willensbekundung erfolgt. Einwilligungserklärungen, die – wie der Rat vorschlägt – lediglich unmissverständlich sein müssen, lehnt die Konferenz als unzureichend ab. Letzteres ermöglicht es den global agierenden Diensteanbietern, durch die Verwendung pauschaler Datenschutzbestimmungen und datenschutzunfreundlicher Voreinstellungen weitreichende Datenverarbeitungsbefugnisse ohne ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Damit wird einem Opt-Out als pauschale Möglichkeit der Einwilligung der Weg bereitet.

4. Die Rechte der Betroffenen dürfen nicht eingeschränkt werden!

Die Konferenz spricht sich für umfassende Informationsrechte aus, die die Betroffenen in die Lage versetzen, Umfang und Risiko der Datenverarbeitung einzuschätzen. Die Ausübung ihrer Rechte und die zur Umsetzung ergriffenen Maßnahmen müssen für die Betroffenen unentgeltlich sein. Die Konferenz wendet sich daher gegen die vom Rat vorgesehenen diesbezüglichen Beschränkungen aus.

5. Die Profilbildung muss wirksam begrenzt werden!

Die Konferenz weist erneut auf die Notwendigkeit einer strikten Regelung der Profilbildung hin, die der Zusammenführung und Auswertung personenbezogener Daten über eine Person enge Grenzen setzt. Die vorgesehenen Regelungen greifen hier zu kurz.

6. Effektiver Datenschutz braucht betriebliche und behördliche Datenschutzbeauftragte!

Für die Effektivität der Datenschutzaufsicht kommt den in Deutschland fest etablierten behördlichen und betrieblichen Datenschutzbeauftragten große Bedeutung zu. Die Konferenz setzt sich dafür ein, dass die Bestellung von Datenschutzbeauftragten in Behörden und Unternehmen europaweit verpflichtend ist.

7. Datenübermittlungen an Behörden und Gerichte in Drittstaaten bedürfen einer stärkeren Kontrolle!

Nach den Datenschutzskandalen der jüngsten Zeit ist ein besserer Schutz der personenbezogenen Daten von europäischen Bürgerinnen und Bürgern gegenüber drittstaatlichen Einrichtungen dringend geboten. Nach dem Vorschlag des Parlamentes sollen Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaates, die von einer datenverarbeitenden Stelle die Weitergabe personenbezogener Daten verlangen, in der EU nur auf der Grundlage internationaler Übereinkommen zur Amts- und Rechtshilfe anerkannt und vollstreckt werden.

25.12 Entschließung: Verfassungsschutzreform bedroht die Grundrechte

30. September und 1. Oktober 2015

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die mit dem „Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes" (BR-Drs. 123/15 und 382/15) beschlossene Verfassungsschutzreform ab. Die vorgesehenen Gesetzesänderungen sind in zentralen Punkten verfassungsrechtlich äußerst bedenklich. Das betrifft insbesondere die praktisch unbegrenzten Befugnisse der Verfassungsschutzbehörden, personenbezogene Daten in umfassenden und zentralen Dateien zu speichern.

Das Gesetz sieht u. a. vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem ermöglicht es den Austausch mit Polizeibehörden in einem Maß, welches der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom 24. April 2013, 1 BvR 1215/07) widerspricht. Es schafft weiter die rechtliche Grundlage, das zentrale nachrichtendienstliche Informationssystem (NADIS) von einem reinen Indexsystem zu einem vollumfänglichen Informationssystem auszubauen. Dies geschieht vor allem dadurch, dass nach dem Gesetzeswortlaut zu allen gespeicherten Personen und Objekten zukünftig auch die zugehörigen Dokumente, Bilder, Video- oder Audiomaterial in NADIS gespeichert werden können und sollen. Auf die erheblichen Risiken von Recherchen in solch umfassenden Dateien hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig mit ihrer Entschließung vom 4. November 2010 „Keine Volltextsuche in Dateien der Sicherheitsbehörden" hingewiesen. Das Bundesamt für Verfassungsschutz erhält schließlich in Konkurrenz zu den Ländern operative Zuständigkeiten auch für nicht länderübergreifende gewaltorientierte Bestrebungen. Die Verfassungsschutzbehörden der Länder werden faktisch auf die Rolle von Datenlieferanten für das Bundesamt für Verfassungsschutz reduziert.

Es fehlt nach wie vor an einer umfassenden und systematischen Analyse bisheriger Versäumnisse und Vollzugsdefizite. Diese hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit Beginn der Überlegungen zu einer Reform des Verfassungsschutzes gefordert (Entschließung vom 8. November 2012

„Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben“).

Offen bleibt so insbesondere die Frage, ob die Verfassungsschutzbehörden bestehende Befugnisse in der Vergangenheit richtig angewendet haben. Gleichwohl werden nunmehr die Befugnisse der Verfassungsschutzbehörden noch erweitert.

Bestehende Defizite der rechtsstaatlichen Kontrolle über die Nachrichtendienste löst das Gesetz ebenfalls nicht. Dabei hat vor allem der Abschlussbericht des NSU-Untersuchungsausschusses des Bundestages ein erhebliches Kontrolldefizit aufgezeigt.

Auch hier hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits eine verfassungskonforme Gestaltung der Kontrolle angemahnt (Entschließung vom 9. Oktober 2014 „Effektive Kontrolle von Nachrichtendiensten herstellen!“).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält an ihrer Forderung gegenüber dem Gesetzgeber fest, das Recht der Nachrichtendienste maßvoll und verfassungskonform auszugestalten. Dies ist mit diesem Gesetz misslungen.

Das Gesetz stellt einen weiteren Schritt zur Aushöhlung des Rechts auf informationelle Selbstbestimmung dar.

25.13 Entschließung: Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken

30. September und 1. Oktober 2015

Namhafte Hersteller weit verbreiteter Betriebssysteme (z. B. Apple, Google, Microsoft) bieten in zunehmendem Maße neue Versionen dieser Software an, die im Unterschied zu den herkömmlichen Betriebssystemen auf internetbasierte Cloud-Services zurückgreifen. Die Standardeinstellungen dieser neuen Betriebssysteme führen oftmals dazu, dass zunehmend personenbezogene Daten aller Art vom lokalen Endgerät (Personalcomputer, Laptop, Tablet, Smartphone) an die Betriebssystem-Hersteller oder deren Cloud-Dienste übertragen werden. Dadurch erhält der Hersteller Informationen, die es ihm erlauben, das Verhalten der Benutzer nachzuvollziehen und im Detail zu analysieren.

Mit derartigen Betriebssystemen vollziehen die Hersteller einen Paradigmenwechsel, dessen tatsächliche und mögliche Auswirkungen auf den Umgang mit personenbezogenen Daten längst nicht allen Anwendern, d.h. Benutzern und für den IT-Einsatz Verantwortlichen, klar sein kann. Die Hersteller schaffen sich den Zugang zu einer Vielzahl personenbezogener Daten, sofern die Standardeinstellungen nicht aktiv durch die Anwender verändert werden. Weitreichende Datenverarbeitungsbefugnisse können nicht dadurch gerechtfertigt werden, dass Nutzern auf Basis von AGB oder datenschutzunfreundlichen Voreinstellungen lediglich ein Opt-Out ermöglicht wird.

Insoweit ist es erforderlich, der Datenherrschaft von Nutzern durch technisch unterstützte Einwilligungslösungen zu entsprechen. Solange nicht unabhängige Dritte die Wirkung der Einstellungen auf den Datenschutz geprüft haben, ist selbst nach deren Änderung häufig unklar, wie weit Datenübertragungen tatsächlich eingeschränkt werden, welche Daten im Detail betroffen sind und zu welchen konkreten Zwecken diese Daten erhoben werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Darüber hinaus sind die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben bzw. verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud bzw. an den Hersteller übermittelt werden.

Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten vor der Entscheidung für einen Einsatz zu prüfen, ob für ihr Umfeld zugeschnittene Betriebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als Daten verarbeitende Stelle gerecht werden können.

25.14 Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutz-Richtlinie im Bereich von Justiz und Inneres

29. Oktober 2015

I. Vorbemerkung

Nachdem der Rat der Justiz- und Innenminister am 9. Oktober 2015 seinen Standpunkt zur Datenschutz-Richtlinie im Bereich von Justiz und Inneres (JI-Richtlinie) angenommen hat, beraten Kommission, Parlament und Rat im sogenannten Trilog über ihre verschiedenen Positionen zur JI-Richtlinie mit dem Ziel der gemeinsamen Verabschiedung von JI-Richtlinie und Datenschutz-Grundverordnung (DS-GVO) im Paket zum Jahresende 2015.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Konferenz) hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012[84] mehrfach öffentlich zur Datenschutzreform positioniert. Am 26. August

[84] Mitteilung der Kommission Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg., Ziff. 6.

2015 hat sie zu den Trilogverhandlungen zur DS-GVO Stellung genommen.[85] Sie hat ferner zum gesamten Paket am 11. Juni 2012 eine Stellungnahme abgegeben[86]. Von Anfang an hat sie das Ziel der Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union bereitzustellen" und dabei auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus im Anwendungsbereich der JI-Richtlinie hingewiesen.

Mit dieser Richtlinie wird eine Lücke geschlossen, denn einen Rechtsakt, der die Datenverarbeitung in den Bereichen Polizei und Justiz in der EU umfassend regelt, kennt das EU-Recht bislang nicht. Dies hat die Konferenz in der Vergangenheit immer wieder kritisiert.[87]

Die Konferenz setzt sich für eine Richtlinie ein, die auf möglichst hohem Niveau eine Mindestharmonisierung innerhalb der Europäischen Union herbeiführt. Sie begrüßt insofern die Entwürfe von Rat und Europäischem Parlament, als beide eine Mindestharmonisierung festschreiben. Mit einer Richtlinie verbindet die Konferenz die Erwartung an den deutschen Gesetzgeber und die deutsche Rechtsprechung, weiterhin Impulsgeber für die Schaffung eines effektiven Datenschutzrechts zu bleiben.

Vor diesem Hintergrund bewertet die Konferenz die JI-Richtlinie als einen wichtigen Schritt zur Verbesserung des Datenschutzes in der Europäischen Union. Kernanliegen des Datenschutzes im Bereich der polizeilichen Datenverarbeitung ist es, Grenzen der Erfassung und Speicherung in polizeilichen Dateien zu setzen: Bürgerinnen und Bürgern müssen darauf vertrauen können, nicht in polizeilichen Dateien erfasst zu werden, wenn sie keinen Anlass für eine polizeiliche Speicherung gegeben haben. Rechtmäßig von der Polizei erhobene Daten dürfen nur unter besonderen Voraussetzungen auch für andere polizeiliche Zwecke verwendet werden. Wer beispielsweise Opfer oder Zeuge einer Straftat war, muss darüber hinaus darauf vertrauen können, dass seine Daten nur beschränkt und unter strengen Voraussetzungen von Polizeibehörden verarbeitet werden dürfen. Dieses sind nur einige grundsätzliche Forderungen, die in der JI- Richtlinie zu regeln sind. Dazu stellt die Konferenz mit Bedauern fest, dass die Regelungen dieser Grundanliegen insbesondere in der vom Rat vorgelegten Fassung häufig allgemein bleiben, sich im Wesentlichen in dem Verweis auf das nationale Recht erschöpfen oder gar gänzlich fehlen.

Einen ganz wesentlichen Impuls für das deutsche Datenschutzrecht im Bereich von Polizei und Justiz erwartet die Konferenz von den Regelungen zur Durchsetzung des Datenschutzrechts durch die Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen. Datenschutz muss effektiv durchsetzbar sein. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls

---

85 Trilogpapier der Konferenz zur DS-GVO, abrufbar unter: https://www.datenschutz.hessen.de/entschliessungen.htm

86 Stellungnahmen zur DS-GVO und zur JI-Richtlinie vom 11. Juni 2012; Entschließungen „Ein hohes Datenschutzniveau für ganz Europa" vom 21./22. März 2012 „Europäische Datenschutzreform konstruktiv und zügig voranbringen!" vom 8./9. November 2012, jeweils abrufbar unter: https://www.datenschutz.hessen.de/entschliessungen.htm und https://www.datenschutz.hessen.de/taetigkeitsberichte.htm

87 Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S.3.

mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Bei den im Folgenden angesprochenen Themen handelt es sich um die wichtigsten Punkte, denen sich nach Ansicht der Konferenz die am Trilog teilnehmenden Parteien insbesondere widmen sollten.

Zur besseren Handhabbarkeit orientiert sich diese Stellungnahme an der Struktur der vorliegenden Entwürfe der JI-Richtlinie.

II. Die Vorschläge im Einzelnen

1. Keine Ausweitung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DS-GVO!

Der Anwendungsbereich der JI-Richtlinie kann nicht isoliert betrachtet werden, sondern er bestimmt spiegelbildlich den Anwendungsbereich der DS-GVO. Denn die DS-GVO findet nach deren Art. 2 Abs. 2 lit. e keine Anwendung, soweit die JI-Richtlinie Anwendung findet. Vor diesem Hintergrund sind in der Vergangenheit verschiedene Entwürfe diskutiert worden, die teilweise zu einer deutlichen Ausdehnung des Anwendungsbereichs der JI-Richtlinie führen könnten. Auch die vorgelegte Version des Rates wirft insofern in Art. 1 Abs. 1 JI-Richtlinie Fragen auf, als der Anwendungsbereich der JI-Richtlinie um die Formulierung „zum Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit" erweitert worden ist.

Die Konferenz sieht keine überzeugenden Gründe dafür, von der ursprünglich vorgesehenen Trennung der Anwendungsbereiche der DS-GVO und der JI-Richtlinie wesentlich abzuweichen. Nach dem ursprünglichen Entwurf der Kommission enthält die JI-Richtlinie Regelungen zum "Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung". Der Rat kritisiert, dass damit die präventive Gefahrenabwehr nicht erfasst sei, soweit sie nicht der Prävention einer Straftat diene. Dies führe wiederum dazu, dass die Datenverarbeitung der Polizei unterschiedlichen Rechtsakten unterliege. Um die gesamte Aufgabenerfüllung der Polizei unter einem Rechtsakt – der JIRichtlinie – zusammenzufassen, solle der Anwendungsbereich der Richtlinie entsprechend erweitert werden. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltung unter die Richtlinie zu fassen. Die Ordnungsverwaltung solle der JI-Richtlinie unterfallen, soweit sie Ordnungswidrigkeiten verfolgt. Damit stellt der Rat seine ursprüngliche Argumentation auf den Kopf. Denn diese Ausweitung der JI-Richtlinie führt gerade dazu, dass Ordnungsverwaltungen sodann sowohl der DS-GVO als auch der JI-Richtlinie unterfielen, je nachdem welche Aufgabe sie erfüllten.

Eine solche Ausweitung lehnt die Konferenz ab. Sofern ein Kompromiss gefunden werden muss, der den Anwendungsbereich der JI-Richtlinie für die polizeiliche Datenverarbeitung erweitern soll, muss durch die Formulierung im Gesetzestext und in den Erwägungsgründen sichergestellt sein, dass davon nicht auch noch die Datenverarbeitung der Ordnungsverwaltung erfasst wird. Dies ist nach der vom Rat vorgelegten Fassung nicht der Fall. Die Datenverarbeitung anderer Behörden als der Polizeibehörden sollte weiterhin von der DS-GVO geregelt werden.

Die Konferenz sieht die in der Ratsfassung hinzugefügte Erweiterung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DS-GVO kritisch. Die Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte, wie im Entwurf der Kommission und des Europäischen Parlaments vorgesehen, von der DS-GVO geregelt werden.

2. Die Durchbrechung der Zweckbindung darf nur in engen Grenzen erfolgen!

Die Konferenz hat in ihrer Stellungnahme vom 11. Juni 2012 die Klarstellung gefordert, dass die Regelungen über die Zweckbindung nicht so verstanden werden dürfen, „dass ein einmal im Anwendungsbereich der Richtlinie für einen bestimmten Zweck erhobenes Datum ohne weitere gesetzliche Voraussetzung für jeden anderen von der Richtlinie erfassten Zweck weiterverarbeitet werden darf". Die Bedeutung der Zweckbindung wurde auch durch die Europäische Grundrechtecharta betont, in der sich in Art. 8 Abs. 2 die Zweckbindung als tragendes Prinzip des Datenschutzes findet. In der Richtlinie sollte daher die Zweckbindung (Art. 4 Abs. 1 lit. b JI-Richtlinie) insgesamt strikter gefasst werden[88].

Der Rat hat in seiner Fassung den ursprünglichen Vorschlag der Kommission in Art. 4 Abs. 2 dahingehend ergänzt, dass eine Weiterverarbeitung für einen anderen Zweck innerhalb der JI-Richtlinie zulässig ist, wenn es dafür nach anwendbarem (nationalen) Recht eine Rechtsgrundlage gibt und die Weiterverarbeitung erforderlich und verhältnismäßig ist. Der Entwurf der Kommission enthielt insofern nur allgemeine Regelungen, nach der eine Weiterverarbeitung nicht „unvereinbar" mit dem ursprünglichen Zweck der Erhebung und nicht exzessiv sein dürfe (Art. 4 Abs. 1 lit. b und c).

Die Konferenz bedauert insofern, dass der Entwurf des Rates keine ambitionierteren, strengeren Vorgaben macht. Die vorgeschlagenen Regelungen lassen nach der Auffassung der Konferenz einen zu weiten Rahmen, den auszufüllen ganz weitgehend dem nationalen Gesetzgeber überlassen wird. In Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) sollte der Begriff der Unvereinbarkeit von Datenverarbeitungen konkretisiert werden. Danach liegt eine Unvereinbarkeit vor, „wenn mit der Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen („hypothetischer Ersatzeingriff")[89].

Die Konferenz spricht sich für strenge Vorgaben an die Durchbrechung der Zweckbindung aus und regt insofern an, den Mitgliedstaaten konkrete Vorgaben für die Weiterverarbeitung zu machen. Der Begriff der Unvereinbarkeit in Art. 4 sollte bei Abs. 1 lit. b JI-Richtlinie in der Fassung des Rates wie folgt präzisiert werden: Eine Weiterverarbeitung der personenbezogenen Daten ist als unvereinbar mit dem

88 Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S. 5.
89 BVerfGE 100, 313, 389; ständige Rechtsprechung.

ursprünglichen Erhebungszweck anzusehen, wenn die Daten nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen.

3. Unverdächtige und andere besondere Personengruppen brauchen mehr Schutz!

Der Schutz unverdächtiger Bürgerinnen und Bürger sowie besondere Voraussetzungen für besondere Personengruppen stellen ein Kernanliegen des Datenschutzes im Bereich der Polizei und Justiz dar. Die Konferenz bedauert insofern die ersatzlose Streichung des Art. 5 in der Fassung des Rates und weist ausdrücklich auf die Fassung des Europäischen Parlaments zu Art. 5 hin, der sich an einer Stellungnahme der Art. 29-Gruppe orientiert.

Ziel der von der Art. 29-Gruppe vorgeschlagenen Regelung des Art. 5 ist es sicherzustellen, dass Daten bestimmter Personengruppen (Zeugen, Opfer, Kontaktpersonen etc.) unter strengeren Voraussetzungen mit kürzeren Fristen gespeichert werden und dass darüber hinaus Daten anderer Personen, die nicht einer Straftat verdächtig sind, entweder gar nicht oder nur in sehr begrenzten Fällen gespeichert werden dürfen.

Die Konferenz lehnt die Streichung des Art. 5 der JI-Richtlinie in der Ratsversion ab und unterstützt Art. 5 in der Fassung des Europäischen Parlaments.

4. Datenspeicherungen sind regelmäßig auf ihre Erforderlichkeit und Verhältnismäßigkeit zu überprüfen!

Ungeachtet des Rechts auf Löschung sollten die datenverarbeitenden Stellen verpflichtet sein, die Erforderlichkeit und Verhältnismäßigkeit von Speicherungen in regelmäßigen Abständen zu überprüfen. Eine solche Verpflichtung enthält die Ratsversion im Gegensatz zu Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments nicht. Der Rat beschränkt sich in seinem Entwurf darauf, die Mitgliedstaaten zur Festlegung von Speicher- und Aussonderungsprüffristen in Verfahrensverzeichnissen („records", Art. 23 JI-Richtlinie) zu verpflichten, wenn dies möglich ist. Dies reicht nicht aus. Vielmehr fordert die Konferenz als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

Die Konferenz fordert als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen nach dem Vorbild von Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

5. Moderner Datenschutz braucht umfassende Benachrichtigungspflichten!

Benachrichtigungen gehören zu den datenschutzrechtlichen „Kernrechten" der Betroffenen. Effektiver Rechtsschutz ist nicht möglich, wenn der von einer (heimlichen)

Datenerhebung Betroffene keine Kenntnis von der Erhebung und Speicherung erlangt. Die Kontrolle dieser Datenverarbeitungen ist zwar auch Aufgabe der Datenschutzaufsichtsbehörden, doch sollte auch jede Bürgerin und jeder Bürger in die Lage versetzt werden, die sie oder ihn betreffende polizeiliche Maßnahme überprüfen zu können und überprüfen zu lassen.

Die Konferenz setzt sich daher für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

Zur Wahrung der Rechte des Einzelnen und zur Gewährung effektiven Rechtsschutzes durch Aufsichtsbehörden und Gerichte setzt sich die Konferenz für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

6. Keine Sonderregelung der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren!

Die Konferenz spricht sich für eine möglichst weitgehende einheitliche Regelung der Rechte der Betroffenen im Anwendungsbereich der JI-Richtlinie aus. Demgegenüber enthält Art. 17 hinsichtlich personenbezogener Daten in Gerichtsbeschlüssen oder staatsanwaltschaftlichen Verfahrensakten die Regelung, dass die Ausübung der Betroffenenrechte „im Einklang mit dem einzelstaatlichen Recht" erfolgt. Schon in ihrer Stellungnahme vom 11. Juni 2012 hatte die Konferenz eine Klarstellung zum Regelungsgehalt des Art. 17 JI-Richtlinie gefordert. Leider tragen auch die vorgelegten Fassungen von Europäischem Parlament und Rat nicht dazu bei, die notwendige Klarstellung herbeizuführen. Die Konferenz betont daher noch einmal diese Notwendigkeit, da ansonsten Zweifel an der Anwendbarkeit der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren entstehen können. Zu diesem Zweck ist die Sonderregelung des Art. 17 zu streichen und sind die Betroffenenrechte in strafrechtlichen Ermittlungen einheitlich in der JI-Richtlinie zu regeln.

Die Konferenz spricht sich für eine Streichung des Art. 17 JI-Richtlinie aus, und wiederholt ihre Forderung, dass die in Kapitel III gewährten Betroffenenrechte auch im Bereich des staatsanwaltschaftlichen Ermittlungsverfahrens Anwendung finden.

7. Klarstellung - Datenverarbeitung nach dem Stand der Technik!

Die Konferenz unterstreicht die Bedeutung des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen. Die Verpflichtung, diese Grundsätze zu beachten, wird in Art. 19 JI-Richtlinie jedoch in verschiedener Hinsicht erheblich beschränkt, unter anderem durch Bezugnahme auf „verfügbare Technologie". Dies wird dem notwendigen Grundrechtsschutz nicht gerecht, denn „verfügbar" sind auch veraltete Technologien, die nicht (mehr) die ausreichende Sicherheit bieten.

Demgegenüber stellt der „Stand der Technik" („state of the art") sicher, dass jeweils die modernsten vorhandenen Technologien einzusetzen sind. Der Stand der Technik ist eine im Europäischen Datenschutz handhabbare Definition. Sie findet seit längerem eine bewährte Anwendung in der Praxis und sollte auch in der JI-Richtlinie verwendet werden.

Der an verschiedenen Stellen gebrauchte ungenaue und dem Schutzbedarf personenbezogener Daten nicht gerecht werdende Begriff „verfügbare" Technik bzw. Technologie sollte konsequenter Weise auch in der JI-Richtlinie durch „Stand der Technik" ersetzt werden. Die Konferenz spricht sich insofern für Art. 19 in der Fassung des Europäischen Parlaments aus.

8. Datenschutz-Folgeabschätzung auch im Bereich der JI-Richtlinie!

Bei der Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden sind Datenschutz-Folgeabschätzungen äußerst wichtig, da gerade bei dieser Verarbeitung erhöhte Risiken für den Einzelnen bestehen. Das Europäische Parlament hat eine entsprechende Regelung zur Datenschutz-Folgenabschätzung vorgeschlagen, die jedoch vom Rat abgelehnt wird.

Die vom Europäischen Parlament in Art. 25a vorgeschlagene Bestimmung sieht eine Datenschutz-Folgenabschätzung vor, wenn die Verarbeitungsvorgänge aufgrund ihrer Natur, ihres Anwendungsbereichs oder ihrer Bestimmungszwecke eine konkrete Gefahr für die Rechte und Freiheiten der betroffenen Personen darstellen können. Für die in Art. 25a (2) lit. b erwähnten „biometrischen Daten" gibt es in Art. 3 Abs. 11 des Vorschlags des Europäischen Parlaments eine entsprechende Definition.

In Art. 33 des Entwurfs der Datenschutz-Grundverordnung (Ratsfassung) ist, anders als beim Richtlinien-Vorschlag, nach wie vor eine Datenschutz-Folgenabschätzung vorgesehen. Doch gerade im verarbeitungsintensiven Bereich der Strafverfolgung sind gründliche Sicherheitsvorkehrungen beim Umgang mit personenbezogenen Daten von größter Wichtigkeit, weshalb sich die Konferenz für die Aufnahme einer entsprechenden Regelung in den Richtlinienvorschlag ausspricht.

Die Konferenz setzt sich für eine Regelung der Datenschutz-Folgenabschätzung ein, die sich an Art. 25a des Richtlinien-Vorschlags des Europäischen Parlaments orientiert. In diesem Zusammenhang befürwortet die Konferenz die Wiederaufnahme der Definition der „biometrischen Daten", wie sie vom Europäischen Parlament in Art. 3 Abs. 11 vorgesehen war.

9. Guter Datenschutz braucht behördliche Datenschutzbeauftragte!

Die Konferenz bedauert, dass der Rat es in seiner Version ablehnt, die Mitgliedstaaten zur Schaffung eines behördlichen Datenschutzbeauftragten zu verpflichten, sondern dies stattdessen in deren Ermessen stellt. Die Datenschutzbeauftragten des Bundes und der Länder haben überwiegend sehr gute Erfahrung bei der Zusammenarbeit mit den Datenschutzbeauftragten der beaufsichtigten Behörden gemacht und

halten die interne Kontrolle vor Ort – neben der externen Kontrolle durch die Aufsichtsbehörden – für ein unverzichtbares Element eines flächendeckenden effektiven Datenschutzregimes.

Die Konferenz betont die Bedeutung einer verpflichtenden Bestellung eines behördlichen Datenschutzbeauftragten und spricht sich deshalb für Art. 30 des Vorschlages des Europäischen Parlaments aus.

10. Übermittlungen an Behörden und Gerichte in Drittstaaten bedürfen eines transparenten Verfahrens, der Abwägung im Einzelfall und müssen überprüfbar dokumentiert sein!

Neu an den Regelungen über die Übermittlung personenbezogener Daten in Drittstaaten ist, dass auch im JI-Bereich das Instrument des Angemessenheitsbeschlusses eingeführt werden soll. Die Konferenz ist der Auffassung, dass die geltenden Angemessenheitsbeschlüsse nicht auf den JI-Bereich übertragbar sind. Neben den Übermittlungen in Drittstaaten mit adäquatem Datenschutzniveau wird die Mehrzahl der Übermittlungen weiterhin auf der Grundlage bilateraler Abkommen und nationalen Rechts (im Einzelfall) erfolgen.

Die Konferenz fordert, in Übereinstimmung mit der Rechtsprechung des EuGH Abwägungsklauseln für alle Übermittlungen vorzusehen. Diese sollten die übermittelnde Behörde verpflichten, eine Abwägung zwischen dem Interesse an der Übermittlung und den schutzwürdigen Interessen des Betroffenen vorzunehmen. Die JI-Richtlinie sollte zugleich Dokumentationspflichten festschreiben, um die Kontrolle von Übermittlungen überprüfbar zu machen. Die Konferenz bedauert insofern die Streichung der Dokumentationspflicht in Art. 35 Abs. 2 in der Fassung des Rates. Zudem sollten die Drittstaaten über Verarbeitungsbeschränkungen (Löschfristen etc.) informiert werden.

Die Konferenz spricht sich ebenfalls für eine Art. 43a der Parlamentsfassung der Datenschutz-Grundverordnung entsprechende Regelung aus. Danach sind Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaates, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der EU grundsätzlich weder anerkannt noch vollstreckbar, wenn dies nicht in internationalen Übereinkommen zur Amts- und Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der in den Abkommen bezeichneten Stellen. Die Konferenz erkennt an, dass mit der Schaffung einer solchen Regelung insbesondere die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden wird. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Verhältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Die Konferenz fordert bei jeder Übermittlung in Drittstaaten eine Abwägung im Einzelfall. Des Weiteren muss die JI-Richtlinie sicherstellen, dass Übermittlungen dokumentiert und damit kontrollierbar sind. Deshalb sollte die Dokumentations-

pflicht gem. Art. 35 in der Fassung der Kommission beibehalten werden. Über nationale Verarbeitungsbeschränkungen ist bei jeder Übermittlung zu informieren. Des Weiteren fordert die Konferenz eine Regelung zur Übermittlung personenbezogener Daten an Behörden und Gerichte eines Drittstaates in Anlehnung an Art. 43a der Parlamentsfassung der Datenschutz-Grundverordnung.

11. Befugnisse der Datenschutzbehörden müssen gestärkt werden!

Datenschutz muss effektiv durchsetzbar sein. Die Konferenz erwartet von der Datenschutzreform daher eine Stärkung der Befugnisse der Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen.

Art. 8 Abs. 3 der EU-Grundrechtecharta und Art. 16 Abs. 1 AEUV verlangen vielmehr eine wirksame Durchsetzung der Grundrechte der Bürgerinnen und Bürger. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Datenschutz muss effektiv durchsetzbar sein. Dazu fordert die Konferenz die Stärkung der Befugnisse der Datenschutzbehörden durch die JI-Richtlinie. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

25.15 Entschließung: Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen

6./7. April 2016

Nach vier Jahren intensiver Diskussion ist der Text der Europäischen Datenschutz-Grundverordnung nun zwischen der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union abgestimmt. Mit der Grundverordnung verfügt die EU über ein weiterentwickeltes, einheitliches Datenschutzrecht, das für Unternehmen und Behörden in Deutschland weitgehend Kontinuität gewährleistet. Überall in Europa soll künftig dasselbe Schutzniveau für das Grundrecht auf Datenschutz gelten. Ebenso wird feststehen, dass sich auch außereuropäische Anbieter, die ihre Waren und Dienstleistungen auf dem europäischen Markt anbieten, an das europäische Datenschutzrecht halten müssen.

Wichtige datenschutzrechtliche Prinzipien wie der Grundsatz des Verbots mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz und der Grundsatz der Datensparsamkeit sind in den Verhandlungen weitgehend erhalten geblieben.

Nach der Einschätzung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ist es allerdings zur Erhaltung und Verstärkung des bestehenden Datenschutzniveaus auch im Lichte der jüngeren Entscheidungen des Europäischen Gerichtshofs geboten, die in der Grundverordnung enthaltenen Öffnungs- und Konkretisierungsklauseln zu Gunsten des Rechts auf informationelle Selbstbestimmung zu nutzen. Auch die von der Grundverordnung getroffenen Weiterentwicklungen des Datenschutzes wie beispielsweise die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgeabschätzungen müssen wirksam ausgestaltet werden. Die Konferenz fordert deshalb Bundes- und Landesgesetzgeber auf, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen.

Insbesondere folgenden Regelungen kommt in diesem Zusammenhang hohe Bedeutung zu:

- Schaffung eines Beschäftigtendatenschutzgesetzes, mindestens jedoch Beibehaltung der §§ 3 Abs. 11, 32 BDSG (Art. 88 i.V.m. Erwägungsgrund [EG] 155),
- Beschränkungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (Art. 9 Abs. 4 i.V.m. EG 53, letzte beide Sätze),
- Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden (Art. 58 und 83 Abs. 7 i.V.m. EG 150, vorletzter Satz),
- jedenfalls im öffentlichen Bereich durch die Nennung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit, um einen einfachen, flexiblen und praxistauglichen technischen und organisatorischen Datenschutz zu konkretisieren (Art. 6 Abs. 2, 25, 32),
- Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (Art. 6 Abs. 4),
- Beibehaltung der Verpflichtung in § 4f Abs. 1 BDSG einen betrieblichen Datenschutzbeauftragten zu bestellen (Art. 37 Abs. 4).

25.16 Entschließung: Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!

6./7. April 2016

Die Datenschutzkonferenz tritt für einen effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps ein. Einer repräsentativen Umfrage zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jah-

ren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Am Körper getragene Kleincomputer (sog. Wearables) und auf mobilen Endgeräten installierte Anwendungsprogramme (sog. Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet.

Die digitale Sammlung und Auswertung der eigenen gesundheitsbezogenen Daten können durchaus interessante Informationen für Einzelne bieten, die zu einer besseren Gesundheitsversorgung und einem Zugewinn an persönlicher Lebensqualität beitragen können.

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, so dass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können.

Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwendigen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

- Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen bzw. pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).
- Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.
- Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine

Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungs- und Versicherungsverhältnissen.

- Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.
- Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an.

IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

Die Datenschutzkonferenz fordert den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

25.17 Entschließung: Datenschutz bei Servicekonten

6./7. April 2016

Der IT-Planungsrat hat sich in einem Beschluss in seiner 17. Sitzung im Juni 2015 für eine flächendeckende Verbreitung so genannter Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen. Über diese Konten soll es künftig möglich sein, sich einfach für die Inanspruchnahme von Verwaltungsdienstleistungen auf kommunaler, Länder- und Bundesebene zu identifizieren. Dabei soll der neue Personalausweis mit seiner eID-Funktion eine wichtige Rolle spielen. Eine Projektgruppe des IT-Planungsrates erarbeitet zurzeit die rechtlichen und technischen Rahmenbedingungen für Servicekonten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder nimmt die Aktivitäten des IT-Planungsrates zur Kenntnis, den Zugang zu elektronischen Verwaltungsdienstleistungen zu erleichtern und möglichst medienbruchfrei auszugestalten. Sie weist darauf hin, dass insbesondere die Einrichtung von länderübergreifenden Servicekonten gewichtige verfassungsrechtliche Fragen etwa zum Bund-Länder-Verhältnis und zum Persönlichkeitsrecht aufwerfen. So ist dabei das Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken sowie das grundrechtliche Prinzip der informationellen Gewaltenteilung zu beachten. Servicekonten dürfen die gesetzliche Zuständigkeits- und Aufgabenverteilung der öffentlichen Verwaltung nicht unterlaufen.

Hiervon abgesehen müssen jedenfalls die Datenschutzprinzipien der Datensparsamkeit, der Nichtverkettbarkeit und der Transparenz berücksichtigt werden. Für die Integration von Verwaltungsdienstleistungen heißt insbesondere, dass auch die Schnittstellen zwischen den Systemen so definiert sein müssen, dass

nur die für den vorgesehenen Zweck erforderlichen Daten übertragen werden. Dazu sind folgende Rahmenbedingungen einzuhalten:

- Auch künftig muss es möglich sein, ohne Servicekonto Verwaltungsdienstleistungen in Anspruch zu nehmen.
- Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen muss auch ohne dauerhafte Speicherung identifizierender Daten möglich sein. Für diese Zwecke sollten temporäre Servicekonten eingerichtet werden.
- Bürgerinnen und Bürgern muss die Möglichkeit eingeräumt werden, sowohl einzelne im permanenten Servicekonto dauerhaft gespeicherte, personenbezogenen Daten als auch das Konto selbst löschen zu lassen.
- Soweit Daten aus dem Servicekonto übermittelt werden, müssen diese Übermittlungen durch die Bürger im Servicekonto selbst nachvollzogen werden können.
- Für die Erhebung personenbezogener Daten in behördenübergreifenden Servicekonten ist eine Rechtsgrundlage erforderlich, da sie als Aufgabe verwaltungsorganisationsrechtlich einer Stelle zugewiesen werden muss. Der Staat darf personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben grundsätzlich nur auf der Basis einer klaren Rechtsgrundlage verarbeiten. Da zudem die Bedeutung dieser Servicekonten zunehmen wird und absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von „Digital by Default" eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus.
- Vorbehaltlich weiterer verfassungsrechtlicher Prüfungen ist für die Länder übergreifende Nutzung von Servicekonten eine Rechtsgrundlage erforderlich. Durch die dauerhafte Speicherung identifizierender Daten werden bundesweit nutzbare Servicekonten zu einer digitalen Meldestelle bzw. zu einer zweiten, zentralen Identifizierungsstelle neben den Meldebehörden aufgewertet. Die Rechtsgrundlage muss eindeutige Vorgaben zum Datenumfang, zu Zweckbindungsregelungen, zur Löschung und zur Transparenz der Datenverarbeitung enthalten. Daten der Betroffenen sind alleine zum Betrieb des Serviceportals und zur Erledigung der Verfahren der Nutzer zu verarbeiten. Eine Nutzung dritter Stellen zu anderen Zwecken ist gesetzlich ausdrücklich auszuschließen.
- Bevor Unternehmen verpflichtet werden sollen, die eID-Funktion für Verwaltungsangelegenheiten zu nutzen, ist zu prüfen, ob und unter welchen Voraussetzungen der Einsatz privater digitaler Identifikationsnachweise zu nichtprivaten Zwecken bzw. zur Erfüllung arbeitsvertraglicher Pflichten zulässig ist und inwieweit Arbeitnehmerinnen und Arbeitnehmer hierzu verpflichtet werden können.
- Angesichts des Abhängigkeitsverhältnisses der Arbeitnehmerinnen und Arbeitnehmer im Beschäftigungsverhältnis kann die Nutzung von Servicekonten auf der Basis der privaten eID-Funktion keinesfalls auf der Einwilligungsbasis erfolgen. Auch hierfür ist eine Rechtsgrundlage erforderlich, die die

Datenverarbeitung in Servicekonten vollständig erfasst. Bei der Identifizierung eines bevollmächtigten Beschäftigten dürfen nur die für diese Identifizierung erforderlichen Daten erfasst werden.

Sichere, elektronische Identifizierungsmöglichkeiten können zur Datenschutzkonformität von E-Government- und von E-Commerce-Verfahren beitragen. Die unabhängigen Datenschutzaufsichtsbehörden begrüßen daher Maßnahmen, die zur verstärkten Nutzung der eID-Funktion des neuen Personalausweises beitragen. Dennoch muss den Betroffenen die Möglichkeit gelassen werden, selbst zu entscheiden, ob sie die eID-Funktion freischalten und nutzen wollen. Die Datenschutzkonferenz lehnt daher die angedachte Änderung des Personalausweisgesetzes ab, wonach die eID-Funktion des neuen Personalausweises dauerhaft eingeschaltet wäre und nicht mehr deaktiviert werden könnte. Eine standardmäßige Aktivierung der eID-Funktion wäre allenfalls dann hinnehmbar, wenn den Bürgerinnen und Bürgern ein Opt-In mit Widerrufsmöglichkeit angeboten wird, um die eID-Funktion jederzeit gebührenfrei aktivieren und deaktivieren zu können.

25.18 Entschließung: Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus

6./7. April 2016

Rechtsstaat und Grundrechtsschutz – damit auch Datenschutz – stehen einer effektiven Bekämpfung des Terrorismus nicht entgegen.

Auch nach Brüssel gilt: Datenschutz verhindert nicht, Terroristen und ihre Helfernetzwerke zu erfassen und zu bekämpfen. Das geltende Datenschutzrecht erlaubt deren Daten zu speichern und Informationen wechselseitig auszutauschen. Der Datenschutz kann jedenfalls nicht für etwaige Defizite bei der Nutzung vorhandener Eingriffsbefugnisse sowie für möglicherweise ineffiziente sicherheitsbehördliche Strukturen verantwortlich gemacht werden.

Die häufig reflexartig erhobene Forderung nach weiteren Eingriffsbefugnissen und flächendeckenden Überwachungsmaßnahmen trägt zur Bekämpfung des internationalen Terrorismus nicht bei.

Es kennzeichnet den Rechtsstaat, dass sich jeder in einem fairen Verfahren gegen unberechtigte Verdachtsbehauptungen wehren, Schutz bei Gerichten suchen und auf die Kontrolle der Datenschutzbeauftragten vertrauen darf. Die massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht dem Grundrecht auf Datenschutz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren mehrfach formulierten Appell[90], dass alle neu erwogenen Maßnahmen zur Bekämpfung des internationalen Terrorismus sich daran messen lassen müssen, ob sie

[90] Vgl. Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2001 in Münster - Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg - Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und

für dessen wirkungsvolle Bekämpfung wirklich geeignet, erforderlich und angemessen sind und damit dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen.

25.19 Entschließung: Klagerecht für Datenschutzbehörden: EU-Kommissionentscheidungen müssen gerichtlich überprüfbar sein

20. April 2016

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert den Gesetzgeber auf, umgehend ein eigenständiges Klagerecht für die unabhängigen Datenschutzbehörden vorzusehen. Wenn die unabhängigen Datenschutzbehörden der Auffassung sein sollten, dass eine Entscheidung der EU-Kommission rechtswidrig ist, wären sie gleichwohl an diese gebunden. Sie müssten daher ggf. gegen den rechtsstaatlichen Grundsatz der Gesetzmäßigkeit der Verwaltung verstoßen. Um dies zu verhindern, sind die prozessualen Voraussetzungen dafür zu schaffen, dass die Datenschutzbehörden selbst bestehende Zweifel an der Rechtmäßigkeit einer Kommissionsentscheidung gerichtlich klären lassen können.

Anlass für die obige Aufforderung der Datenschutzkonferenz ist die zwischenzeitliche Vorlage einer Reihe von Dokumenten unterschiedlicher Repräsentanten der US-Administration durch die EU-Kommission am 29. Februar 2016, die für Unternehmen und Behörden Zusagen für den Umgang mit aus der EU übermittelten personenbezogenen Daten enthalten. Im Rahmen eines so genannten EU-US Privacy Shield sollen diese Dokumente Grundlage für eine künftige EU-Kommissionsentscheidung zur Angemessenheit des Datenschutzniveaus in den USA sein und damit als Nachfolgeregelung für die Safe Harbor-Entscheidung dienen. Letztere wurde bekanntlich am 6. Oktober 2015 durch den Europäischen Gerichtshof aufgehoben.

Gegen den „EU-US Privacy Shield" bestehen jedoch nach Auffassung der Artikel-29-Datenschutzgruppe, dem Zusammenschluss der Datenschutzbehörden der EU-Mitgliedstaaten und des Europäischen Datenschutzbeauftragten, erhebliche Bedenken. Die Artikel-29-Dateschutzgruppe hat zum „EU-US Privacy Shield" zuletzt am 13. April 2016 detailliert Stellung genommen. Die Datenschutzkonferenz teilt diese umfassende Analyse und unterstützt die darin enthaltene Forderung an die EU-Kommission, vor einer Beschlussfassung substantielle Nachbesserungen vorzunehmen. Die Datenschutzkonferenz ist der Auffassung, dass auch der „EU-US Privacy Shield" in seiner derzeitigen Form nicht ausreichend ist, das für die Übermittlung personenbezogener Daten in die USA erforderliche „angemessene Datenschutzniveau" in den USA zu gewährleisten.

---

der Länder am 28./29. September 2011 in München - Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden.

Der EuGH stellt in seiner o.g. Entscheidung zur Ungültigkeit von Safe Harbor ausdrücklich klar, dass nach Maßgabe der Datenschutz-Richtlinie der nationale Gesetzgeber für die Datenschutzbehörden Rechtsbehelfe vorzusehen hat, die ihnen bei rechtlichen Zweifeln über eine Angemessenheitsentscheidung die Anrufung nationaler Gerichte ermöglichen, so dass diese den EuGH um eine Entscheidung über die Vereinbarkeit mit den europäischen Grundrechten ersuchen können.

Die Datenschutzkonferenz begrüßt und unterstützt daher ausdrücklich die Bundesratsinitiative der Freien und Hansestadt Hamburg zur zeitnahen Einräumung eines Klagerechts für die Datenschutzaufsichtsbehörden von Bund und Ländern (BR-Drs. 171/16), in der nochmals deutlich gemacht wird, „dass das vom Europäischen Gerichtshof (EuGH in seinem Urteil vom 6. Oktober 2015 (Rechtssache C-362/14) statuierte Klagerecht für Datenschutzaufsichtsbehörden für die Gewährleistung einer effektiven Datenschutzkontrolle von besonderer Bedeutung ist".

25.20 Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht[91]

April 2016

1. Zielsetzung

Immer mehr Bildungsinstitutionen setzen auf die webgestützte Wissensvermittlung und die elektronischen Kommunikationsmöglichkeiten zwischen Lehrenden und Lernenden. Zu diesen Zwecken werden auch an Schulen zunehmend Online-Lernplattformen für den Unterricht eingesetzt. Diese Online-Lernplattformen werden von Schulaufsichtsbehörden, Schulbuchverlagen, Computer- und Softwareherstellern und sonstigen Anbietern bereitgestellt. Die Vorteile werden in der orts- und zeitunabhängigen Nutzung dieser Verfahren gesehen. Allerdings werden dabei zahlreiche Schüler[92]- und Lehrerdaten webbasiert verarbeitet. Die vorliegende Orientierungshilfe richtet sich insbesondere an Schulen, die Online-Lernplattformen als Lernmittel einsetzen wollen. Sie sollen sich einen Überblick darüber verschaffen können, welche datenschutzrechtlichen (Mindest-)Kriterien Online-Lernplattformen erfüllen müssen.

Diese Orientierungshilfe gibt auch den Anbietern von Online-Lernplattformen die Möglichkeit, ihr jeweiliges Produkt so zu gestalten oder anzupassen, dass eine Nutzung durch Schulen zulässig ist.

Online-Lernplattformen sollen den Bildungs- und Erziehungsauftrag der Schule unterstützen, beispielsweise

- Kompetenzorientierung,
- Integration fachlicher, methodischer und sozialer Lernziele,

---

91 Beschlossen auf der 91. DSK am 6./7. April 2016 mit Gegenstimme des Bayrischen Landesbeauftragten für den Datenschutz.

92 Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt eine adäquate weibliche Form gleichberechtigt ein.

- Prozesshaftigkeit des Lerngeschehens,
- Unterstützung von Schülern in Kleingruppen,
- Begabungsgerechte Förderung,
- Erkennen individueller Lernfortschritte und Lernschwierigkeiten,
- Beratung und Lernförderung einzelner Schüler.

Ergänzend wird auf die Orientierungshilfe „Cloud Computing" der Arbeitskreise Technik und Medien der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises in der aktuellen Fassung verwiesen, Orientierungshilfe für Online-Lernplattformen im Schulunterricht weil diese besondere Anforderungen für webbasierte Anwendungen bzw. „Datenverarbeitung in der Wolke" aufzeigt.

Soweit die Online-Lernplattformen für andere als schulische Zwecke über das Internet zur Nutzung zur Verfügung stehen, gelten darüber hinaus die Vorschriften des Telemediengesetzes[93] und des Telekommunikationsgesetzes. Sie sind jedoch nicht Gegenstand dieser Orientierungshilfe.

2. Begriffsbestimmungen

Online-Lernplattformen im Sinne dieser Orientierungshilfe sind Softwaresysteme, die den Lehr- und Unterrichtsbetrieb durch die Bereitstellung und Organisation von Lerninhalten ergänzen oder sogar ersetzen. Schulsoftwaresysteme, die für Aufgaben der Schulverwaltung genutzt werden, sind davon systemtechnisch zu trennen.

Die virtuelle Lernumgebung einer Online-Lernplattform kann von der Schule so gestaltet werden, dass Kommunikation, Gruppenarbeit, Aufgabenbearbeitung und Lernkontrollen eingerichtet werden.

Leistungsbewertungen haben einen erhöhten Schutzbedarf. Dieser ist durch entsprechende technisch-organisatorische Maßnahmen abzusichern.

Der Zugriff auf die Software erfolgt ortsunabhängig mittels eines Endgerätes (PC, Tablet etc.) über einen Web-Browser. Die faktische Teilhabe der Schüler ist durch die Schule zu gewährleisten. Jeder Teilnehmer an einem bestimmten Kurs, also z. B. die Schüler einer Klasse oder eines Jahrgangs in einem bestimmten Schulfach, müssen sich vor einer Nutzung zunächst im Onlineverfahren auf der Lernplattform anmelden oder angemeldet werden. Das System stellt dann jedem Nutzer ein personalisiertes Benutzerkonto zur Verfügung. Darüber hinaus muss die Schule bzw. die verantwortliche Lehrkraft die Zugriffsrechte für die einzelnen Nutzer festlegen und die Funktionalitäten auswählen, die die Online-Lernplattform bietet (Bereitstellung von Lerninhalten, Diskussionsforen, Übungsaufgaben etc.).

3. Datenschutzrechtliche Problematik

In aller Regel melden sich die Benutzer solcher Plattformen personalisiert an und ihre Nutzungsbewegungen werden regelmäßig gespeichert. So wird beispielsweise festgehalten, welcher Nutzer wann auf welche Seite zugegriffen hat, sowie ob und mit welchem Ergebnis er sich an welchem Test beteiligt hat. Dadurch können Persönlichkeitsprofile über Schüler und Lehrkräfte erstellt werden.

---

[93] Die Ausnahme des § 11 Abs. 1 TMG greift in diesem Fall nicht.

Die schulrechtlichen Regelungen für die Verarbeitung und Nutzung von personenbezogenen Daten durch die Schule setzen voraus, dass die erhobenen Daten für die Aufgabenwahrnehmung durch die Schule erforderlich sein müssen. Viele Online-Lernplattformen stellen erheblich mehr Möglichkeiten zur Datenauswertung zur Verfügung, als dies für die Aufgabenwahrnehmung erforderlich ist und sind daher entsprechend anzupassen.

Auch beim Einsatz von Online-Lernplattformen benötigen Lehrkräfte die Möglichkeit, den Lernfortschritt einzelner Schüler zu beobachten, um im individuellen Beratungsgespräch oder bei der Planung und Umsetzung von lernförderlichen Interventionen gezielt den Schüler in seiner Lernsituation zu unterstützen. Weitergehende Angaben, z. B. wie oft und zu welchen Zeiten ein Schüler sich in der Online-Lernplattform an bestimmten Aufgaben beteiligt hat, dürfen in diesem Zusammenhang nicht eingesehen werden. Die Schüler und - falls erforderlich - auch die Erziehungsberechtigten sind vor der Nutzung der Online-Lernplattform darüber zu informieren, welche Auswertungsmöglichkeiten die Anwendung bietet und welche Konsequenzen das Nutzerverhalten haben kann.

Fazit:

- Die Online-Lernplattform ist so zu konfigurieren, dass ausschließlich die zur pädagogischen
- Aufgabenerfüllung der Schule erforderlichen Daten erhoben und verarbeitet werden.
- Es bietet sich die Nutzung von Online-Lernplattformen an, die je nach vorgesehenem
- Einsatzszenario modular angepasst werden können.
- Die Betroffenen sind vor der Nutzung der Online-Lernplattform über mögliche Auswertungen umfassend zu informieren.

4. Rechtsgrundlagen

Rechtsgrundlagen für die Verarbeitung personenbezogener Schülerdaten auch in Online-Lernplattformen sind zunächst die jeweiligen Schulgesetze, Schuldatenschutzgesetze und dazu erlassene Rechtsverordnungen. Ergänzend können – je nach Bundesland und Schultyp – die Landesdatenschutzgesetze sowie das Bundesdatenschutzgesetz zur Anwendung kommen.

Die verpflichtende Verwendung einer Lehrplattform kann nur durch oder aufgrund eines Gesetzes vorgeschrieben werden. Denkbar ist beispielsweise die Bestimmung als Lehrmittel durch entsprechende Verordnung. Andernfalls kann es nur auf Basis einer freiwillig erteilten Einwilligung[94] zum Einsatz einer derartigen Plattform kommen.

[94] Es ist zu beachten, dass sich das Einwilligungserfordernis danach richtet, wie einsichtsfähig die Schüler sind. Die Erforderlichkeit der Einbeziehung der Eltern sollte mit dem zuständigen Landesbeauftragten für Datenschutz abgestimmt werden.

Fazit:

Vor dem Einsatz der Online-Lernplattform ist zu prüfen, ob deren Einsatz rechtlich zulässig ist und ob die Schüler und ggf. die Erziehungsberechtigten in die Nutzung der Plattform einwilligen müssen.

5. Verantwortliche Stelle

Bei der Nutzung von Lernplattformen bleibt die Schule – oder je nach Bundesland die Schulaufsichtsbehörde - verantwortliche Stelle für die Datenverarbeitung und -nutzung. Dies setzt voraus, dass sie die Art und Weise der Datennutzung und -verarbeitung maßgeblich bestimmen kann, also „Herrin der Daten" bleibt. Lehrende dürfen im Rahmen der Freiheit der Gestaltung des Unterrichts nur insoweit Lernplattformen im Unterricht einsetzen, als die Schule oder die Schulaufsicht über den Einsatz der jeweiligen Lernplattform entschieden hat.

6. Umfang der Datenverarbeitung

6.1. Erforderliche Daten

Die Schule/Schulaufsichtsbehörde muss festlegen, welche Daten für die Nutzung der Online-Lernplattform zwingend benötigt werden.

6.1.1 Zwingend erforderliche Stammdaten

- Name und Anschrift der jeweiligen Schule und der verantwortlichen Stelle, die, wenn die Schulaufsichtsbehörde diese Aufgaben wahrnimmt, differieren können.
- Stammdaten zur Anlage von Benutzerkonten, die sowohl zur Identifikation des Nutzers im System als auch zum Zwecke der Vergabe von Rollen und Berechtigungen dienen. Es gibt die Möglichkeit, dass der Nutzer selbst die Daten eingibt und anlegt oder dass die Daten durch die Schule erfasst oder geändert werden. Wichtig ist, dass nur Daten eingegeben werden können, die für die sinnvolle Nutzung der pädagogischen Aufgabenerfüllung der Schule erforderlich sind.
- Bei der Benutzerverwaltung durch den Administrator ist zwischen dem Benutzernamen und dem Anmeldernamen zu unterscheiden. Der Benutzername muss den realen Namen (Klarname) des Benutzers enthalten. Der Klarname ist zur Identifikation des Schülers durch betreuende Lehrer erforderlich und muss nicht dem Anmeldenamen entsprechen. Der Anmeldename wird bei der Anmeldung im System verwendet und muss nicht mit dem Benutzernamen identisch sein. Im Gegenteil: die Nutzung von Pseudonymen als Anmeldenamen erhöht die Sicherheit im Vergleich zur Nutzung des Klarnamens. Der Anmeldename kann frei gewählt werden. Es wird die Anmeldung mit Pseudonymen empfohlen, um den Missbrauch des Kontos durch Dritte maßgeblich zu erschweren.
- Die Angabe einer E-Mail-Adresse ist je nach System optional oder zwingend erforderlich. Sie dient insbesondere der Zusendung von Benachrichtigungen

aus den belegten Kursen sowie der Abfrage eines neuen Passworts bei dessen Verlust.

Ein Benutzerkonto kann weitere Informationen enthalten, die die Kommunikation innerhalb des Systems erleichtern, beispielsweise Klassenstufe, Bezeichnung der Lerngruppe, Ausbildungsgang (beispielsweise an berufsbildenden Schulen).

Fazit:

- Bei der Auswahl der Online-Lernplattform ist darauf zu achten, dass die Grundsätze der Datensparsamkeit und Datenvermeidung (z. B. nicht zu viele Stammdaten, Freitextfelder, Kommentarfunktionen) gewährleistet werden.
- Es ist eine pseudonymisierte Nutzerverwaltung der Lernplattform anzustreben.

6.1.2 Optionale Daten

Weitere optionale Daten können im Nutzerprofil auf freiwilliger Basis durch den Benutzer selbst erfasst werden. Bei missbräuchlicher Nutzung einzelner Informationen (beispielsweise im Zusammenhang mit Mobbing) sollten die betreffenden Felder für alle Benutzerkonten deaktiviert werden. Felder wie "Beschreibung'", „Nutzerbild" und "Interessenfelder" verdienen in diesem Zusammenhang besonderes Augenmerk.

Optionale Datenfelder können bei den gängigen Online-Lernplattformen sein:

- Zeitzone: Dieses Feld wird im Regelfall deaktiviert oder mit einem Standardwert belegt, da alle Nutzer in der Regel in der gleichen Zeitzone leben,
- Beschreibung: Hier können Nutzer Angaben zur eigenen Person eintragen. Diese sind innerhalb der Lernplattform, nicht aber öffentlich sichtbar. Dieses Feld ist nicht erforderlich und sollte deaktiviert werden.
- Nutzerbild: Der Nutzer kann eine Grafikdatei (beispielsweise ein Porträtfoto) hochladen, für die er die Urheberrechte besitzt. Dieses Feld ist nicht erforderlich, birgt die Gefahr von Rechtsverstößen und sollte deaktiviert werden.
- Interessenfelder: Hier können Schlagworte zur eigenen Person angegeben werden (beispielsweise Hobbys). Dieses Feld ist nicht erforderlich und sollte deaktiviert werden.
- Webseite: Teilnehmer können hier die URL zu einer eigenen Internetpräsenz angeben. Dieses Feld ist zu deaktivieren.
- Bevorzugte Sprache: Die Einstellung ermöglicht, dass Benutzeroberflächen in anderen Sprachen als Deutsch zur Verfügung stehen. Dieses Feld ist in aller Regel nicht erforderlich und sollte deaktiviert werden.
- Institution, Abteilung: Diese Information wird in der Regel in der Schule nicht verwandt.

Für organisatorische Zwecke können zusätzliche optionale Datenfelder angelegt und gepflegt werden. Dies ist nur zulässig, soweit es für die Aufgabenerfüllung erforder-

lich ist. Zu denken ist hier beispielsweise an die Angabe, an welchen Kursen ein Schüler teilnimmt, damit er Zugang zu den zugehörigen Dokumenten erhält. Nicht hierunter fallen persönliche Angaben wie Hobbies oder private Telefonnummern.

6.1.3 Nutzungsdaten

Bei der Nutzung einer Lernplattform werden automatisch Daten über den Nutzer und seine Aktivitäten erfasst und gespeichert. Diese Logdaten werden auf dem Server abgelegt, sie dürfen ausschließlich für die Überwachung der Funktionsfähigkeit und Sicherheit dieser Systeme sowie bei rechtswidrigem Missbrauch verwendet werden. Ergänzend wird auf die Orientierungshilfe „Protokollierung" des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder in der aktuellen Fassung verwiesen. Näheres sollte in der Nutzungsordnung konkret festgelegt werden.

Nutzungsdaten sind in aller Regel für die Wahrnehmung schulischer Aufgaben nicht erforderlich und sollten daher nur unter klar definierten Voraussetzungen für eindeutig bestimmte Personengruppen zu festgelegten Zwecken einsehbar sein. Nutzungsdaten sind beispielsweise

- Anmeldestatus: Erstlogin im System, letzter Login, Zeitpunkt der Abmeldung,
- Protokollierung von Eingaben oder Änderungen,
- IP-Adressen, genutzte Dienste (z. B. Dateidownloads, Chat).

6.1.4 Pädagogische Prozessdaten

Als pädagogische Prozessdaten werden Informationen bezeichnet, die dem Lehrer die Möglichkeit geben, den individuellen und kollektiven Lernprozess nachzuvollziehen, um didaktische Interventionen zu planen, Unterricht zu reflektieren, zu evaluieren und weiterzuentwickeln sowie individuelle Lernberatung für einzelne Schüler oder kleine Gruppen zu gestalten.

In den verschiedenen Modulen einer Online-Lernplattform werden Prozessdaten generiert, die jeweils für unterschiedliche Personenkreise sichtbar sind. Solche Module sind:

- Forendiskussion: Die Beiträge können den Verfassern zugeordnet und in zeitlicher Struktur geordnet werden. Zudem zeigt die Darstellungsstruktur an, zu welchem Beitrag eine Antwort abgegeben wurde. Diese Informationen sind für alle Nutzer sichtbar. Eine Anzeige noch nicht gelesener Beiträge hingegen ist nur für den jeweiligen Einzelnutzer sichtbar.
- Wiki-Einträge: Ein Wiki ist ein mehrseitiges Dokument, an dem von verschiedenen Verfassern in einem Kurs gearbeitet wird. Durch die Speicherung der Historie ist erkennbar, wer welche Teile an einem Dokument bearbeitet hat. Die Lehrkraft kann dadurch die Beteiligung und die Beiträge Einzelner erkennen. Dies ist für Rückmeldungen und die Bewertung sowie die Förderung sozialer und kommunikativer Aspekte des Lernens wichtig.
- Glossar (Datenbank): Das Glossar stellt eine Sammlung von Informationen in strukturierter Form dar. Es enthält einzelne Texteinträge mit Angaben zum Erstellungszeitpunkt und dem Verfasser. Diese Details sind für alle Nutzer sichtbar.

- Lernobjekte (Aufgaben, Tests): Je nach Art des Objekts sind unterschiedliche Daten nur für Lehrkräfte oder auch für einzelne Schüler sichtbar. Eine Überwachung der außerunterrichtlichen Aktivitäten von Schülern durch Lehrende darf nicht stattfinden. Die Sichtbarkeit der Daten für Lehrende, ist pädagogisch zu begründen und von der Schulleitung bzw. der Schulkonferenz festzulegen.
- SCORM-Module, LTI-Module, Live Classroom, Plagiatsüberprüfung etc.: Bei der Nutzung derartiger Module werden unter Umständen personenbezogene Daten an externe Dienstleister weitergegeben. Dies ist nur im Rahmen von bestehenden Auftragsdatenverarbeitungsverträgen zwischen Schule/Schulträger und Anbieter zulässig und ist datenschutzrechtlich gesondert zu prüfen. Prozessdaten von Lernenden dürfen nur dann für andere Teilnehmer sichtbar sein, wenn dies methodisch oder didaktisch erforderlich ist. Als Beispiel sei die Bewertungsfunktion in einem Diskussionsforum angeführt. Je nach Implementierung erlaubt sie eine schnelle, unter Umständen nonverbale Rückmeldung zu Beiträgen. Da auf diese Weise von Schülern auch unsachgemäße und verletzende Kritik gegenüber Mitschülern geäußert werden kann, ohne dass von Seiten der Lehrenden rechtzeitig eingegriffen werden kann, ist eine solche Funktion nur mit Bedacht zu aktivieren.

6.1.5 Statistische Daten

Die Lernplattformen erlauben die Auswertung statistischer Daten beispielsweise über Art und Umfang der Nutzung. Echte statistische Daten haben aber keinen Personenbezug und sind daher aus datenschutzrechtlicher Sicht unproblematisch. Sollte es sich nicht um echte statistische Daten in diesem Sinne handeln, gelten für sie die jeweiligen Schulgesetze, Schuldatenschutzgesetze und dazu erlassene Rechtsverordnungen der Länder.

6.2. Schriftliche Festlegungen

Vor dem Einsatz der Online-Lernplattform hat die Schule/die Schulaufsichtsbehörde schriftliche Festlegungen zur zulässigen Datennutzung und zum Rollen- und Berechtigungskonzept zu treffen. Außerdem muss dies in das Verfahrensverzeichnis aufgenommen werden.

Die Vorgaben zur Konfiguration und Anwendung der Online-Lernplattform durch die Administratoren, Lehrer und Lehrerinnen kann beispielsweise in Form einer Nutzerordnung geschehen, in der klar geregelt wird, wie die Vertraulichkeit, Integrität, Authentizität, die Nichtverkettbarkeit der Daten und die Intervenierbarkeit des Nutzers entsprechend dem jeweils geltenden Landesrecht vor Ort konkret umzusetzen ist. Hierzu gehören ein Löschkonzept (9.9) sowie die Frage, welche E-Mailadressen verwendet werden (9.2).

Fazit:

Die Grundlagen der Datenverarbeitungsprozesse sind vor dem Einsatz der Online-Lernplattform abschließend in einer Nutzerordnung festzulegen.

7. Notwendige Prüfungen vor Inbetriebnahme

Vor dem Einsatz von Lernplattformen hat die verantwortliche Stelle (Schule oder Schulaufsichtsbehörde) im Zusammenwirken mit ihrem Datenschutzbeauftragten eine Vorabkontrolle nach den jeweils geltenden Landesregelungen durchzuführen. Hierbei sind insbesondere folgende Aspekte zu beachten:

- Einhaltung der ggf. bestehenden landesrechtlichen Regelungen zum Einsatz von Online-Lernplattformen.
- Bei der Anschaffung einer Lernplattform eines externen Dienstleisters ist zu prüfen, ob dieser die datenschutzrechtlichen schulischen Anforderungen erfüllen kann.
- Gestaltung und Auswahl von Datenverarbeitungssystemen nach den Grundsätzen der Datenvermeidung und Datensparsamkeit.
- Beim Einsatz von externen Dienstleistern sind die gesetzlichen Voraussetzungen der zulässigen Auftragsdatenverarbeitung zu beachten.

  Dabei gelten folgende allgemeine Anforderungen:

  - Die Schule/Schulaufsichtsbehörde muss „Herrin der Daten" bleiben. Sie bestimmt, wer die Daten auf welche Weise verarbeitet und nutzt. Sie muss gegenüber dem Auftragnehmer ein Weisungsrecht in Bezug auf die Datenverarbeitung und –nutzung haben und sich vertraglich Kontrollrechte einräumen lassen.
  - Die Allgemeinen Geschäftsbedingungen externer Dienstleister sind unter Beachtung der hier dargestellten Grundsätze zu überprüfen und ggf. vertraglich abzuändern.
  - Mit dem Auftragnehmer ist ein Vertrag zu schließen, der den datenschutzrechtlichen Anforderungen an die Auftragsdatenverarbeitung genügt.
- Es gilt der Grundsatz der Zweckbindung. Danach ist insbesondere zu gewährleisten, dass die Daten der Schüler, Lehrer und Eltern nicht zu Werbezwecken genutzt werden.
- Die von der Schule/Schulaufsichtsbehörde zu erstellenden Nutzungsbedingungen, das Verfahrensverzeichnis und die sonstigen getroffenen technischen und organisatorischen Maßnahmen sind einer datenschutzrechtlichen Prüfung zu unterziehen.

8. Unterrichtungs-, Benachrichtigung-, Schulungs- und Unterweisungspflichten

Schüler, Eltern[95] und Lehrkräfte sind vor dem Einsatz von Online-Lernplattformen ausführlich über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung ihrer Daten zu unterrichten. Sie sind darüber aufzuklären, dass sie jederzeit berech-

[95] Hier ist zu beachten, dass die Eltern möglicherweise bei volljährigen Schülern nach dem geltenden Landesrecht nicht immer eine Zugriffsberechtigung haben dürfen.

tigt sind, das Verfahrensverzeichnis der Lernplattform einzusehen. Sofern die Einwilligung für die Nutzung bestimmter Module erforderlich ist, sind sie ausdrücklich auf deren Freiwilligkeit und das bestehende Widerrufsrecht und dessen Rechtsfolgen zu informieren. Die Einwilligung ist schriftlich einzuholen. Aus der Einwilligung hat hervorzugehen, welche Daten, in welcher Form und zu welchem Zweck verarbeitet werden sollen. Darüber hinaus sind die Nutzer darüber zu informieren, ob und an wen Daten übermittelt werden.

Außerdem sind die Lehrkräfte und Administratoren entsprechend zu schulen und die Schüler entsprechend zu unterweisen.

9. Hinweise zur technischen und organisatorischen Umsetzung

9.1. Passwörter

Die Nutzung einer Online-Plattform erfordert einen passwortgeschützten Zugriff. Passwörter müssen verschlüsselt gespeichert werden. Es muss gewährleistet sein, dass niemand innerhalb der Lernplattform Passwörter im Klartext einsehen kann. Dies gilt auch für Administratoren.

Bei der Vergabe von Passwörtern durch die Schule ist zu gewährleisten, dass bei der ersten Nutzung des Logins der Nutzer sein Passwort ändern muss. Von dieser Regel kann im begründeten Einzelfall abgewichen werden (beispielsweise bei Grundschülern oder Schülern mit speziellem Förderbedarf). Nutzer mit der administrativen Berechtigung zur Bearbeitung der Benutzerkonten im System können für andere Nutzer Passwörter zurücksetzen. Von der Vergabe neuer Passwörter wird abgeraten, da dann der Administrator Kenntnis vom neuen Passwort erlangt. Bei der Passwortgenerierung, dem Passwortgebrauch und der Passwortverwaltung sollte die Maßnahme „M 2.11 -Regelung des Passwortgebrauchs“ der vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten IT-Grundschutz-Kataloge beachtet werden. Dies betrifft insbesondere die Komplexität des Passwortes und die Geheimhaltungspflicht.

Die Passwörter sind nach spätestens 90 Tagen gemäß M 2.11 zu wechseln.

Für die Verwendung von Passwörtern muss eine Vorgabe erfolgen, die die Mindestzahl an Zeichen und deren Zusammensetzung (Zahl der Großbuchstaben, Zahl der Kleinbuchstaben, Zahl der Ziffern und Zahl der Sonderzeichen) festlegt. Bei der Festlegung dieser Vorgaben ist das Alter der Schüler zu beachten, um keine Zugangsprobleme zu schaffen. Ein Passwort soll aber in keinem Falle kürzer als acht Zeichen sein.

9.2. E-Mail-Adresse

Die E-Mail-Adresse ist ein eindeutiger Wert. Soll eine E-Mailadresse innerhalb der Lernplattform zur Verfügung gestellt werden, dann ist sicherzustellen, dass diese E-Mailadresse nicht für mehrere Benutzerkonten verwendet werden kann. Die Verwendung der E-Mail-Adressen ist schriftlich zu regeln.

9.3. Erfassung der Daten des Benutzerkontos und Änderbarkeit

Benutzerkonten können durch Import, manuelle Eingabe oder Anbindung an eine bestehende Datenbank nach Maßgabe der in der Schule verwandten Systeme angelegt werden. Bei einem Import oder einer Anbindung an eine bestehende Datenbank sollte nur der Anmeldename, wie er im bestehenden Datenbestand gespeichert ist, an die Lernplattform übermittelt werden (unidirektionaler Informationsfluss). Dass Passwort muss den Richtlinien aus 9.1 entsprechen und daher evtl. neu vergeben werden. Die Schule oder die Schulaufsichtsbehörde legt die Vorgehensweise in Form von einer Nutzerordnung fest.

9.4. Öffentliche Bereiche

Es ist grundsätzlich möglich, bestimmte Bereiche einer Online-Lernplattform öffentlich zugänglich zu machen. Für diese Bereiche gelten dieselben datenschutzrechtlichen Regelungen wie für andere Internetpräsenzen von Schulen, insbesondere im Hinblick auf die Nennung von Namen oder die Abbildung von Schülern oder Lehrkräften; darüber hinaus gelten das Telemediengesetz und das Telekommunikationsgesetz. Unter Beachtung der einschlägigen Vorschriften muss eine allgemeine Zugänglichkeit immer unterbleiben, sobald dadurch personenbezogene Daten sichtbar werden.

9.5. Suchmaschinen

Bereiche, in denen nutzerspezifische Daten gespeichert werden, dürfen nicht öffentlich angeboten werden. Es ist dafür Sorge zu tragen, dass öffentliche Suchmaschinen (Google, Bing, etc.) keinen Zugriff auf diese Bereiche haben.

9.6. Rollenkonzept

Folgende Rollen sind in einer Online-Lernplattform in der Regel vorgegeben:

- Administrator: Der Administrator hat alle Berechtigungen für sämtliche Bereiche und Inhalte, er kann Benutzerkonten-Einstellungen ändern und systemweite Einstellungen vornehmen.
- Kursverwalter: Der Kursverwalter kann Bereiche anlegen und Berechtigungen vergeben. Das Recht kann auf Teilbereiche (Kurskategorien, beispielsweise Ausbildungsgänge, Fächer, Jahrgangsstufen) beschränkt werden.
- Lehrkraft: Die Lehrkraft kann in bestimmten Bereichen Inhalte pflegen, Teilnehmer zulassen, Lernfortschritte und Lernergebnisse einsehen.
- Teilnehmer: Teilnehmer können in den Bereichen arbeiten, zu denen sie eine Zugangsberechtigung haben, Lerninhalte nutzen und Eingaben tätigen.

In Übereinstimmung mit dem Rollen- und Berechtigungskonzept der Schule können weitere Rollen definiert werden.

Folgende Grundsätze sind bei der Vergabe von Rechten und Rollen zu beachten:

Ein Administrator kann auf alle Bereiche zugreifen. Personen mit Administrationsberechtigungen können daher alle Kurse sowie alle Beiträge der Schüler und Lehrer einsehen. Dies schließt Bewertungen mit ein. Bei der Vergabe von Administrationsrechten muss daher mit besonderer Sorgfalt vorgegangen werden und zwar:

- Jedem Administrator ist ein eigener personenbezogener Benutzeraccount zuzuweisen, d.h. es ist nicht zulässig, dass mehrere Administratoren das gleiche Benutzerkonto (= Gruppenadministratorkonto) nutzen. Der Anmeldename des Administrators muss pseudonym sein, um so eine missbräuchliche Kontosperrung zu verhindern. Das Pseudonym muss so gewählt werden, dass es nicht auf einfachem Weg herauszufinden ist.
- Administratoren, die gleichzeitig noch andere Tätigkeiten wahrnehmen, wie z.B. auch Lehraufgaben, müssen über ein separates Benutzerkonto für diese Zwecke verfügen. Es muss also die Möglichkeit bestehen, einer Person entsprechend ihrer verschiedenen Rollen mehrere Benutzerkonten zuweisen zu können.
- Die Anzahl der Administratorenkonten ist so gering wie möglich zu halten, um das Missbrauchsrisiko zu minimieren (z.B. unbefugte Kenntnisnahme, unkontrollierbare Rechtevergaben, etc.). Eine Vertretungsregelung muss aber gewährleistet sein.
- Administratorenrechte darf nur erhalten, wer innerhalb des Systems entsprechende Aufgaben tatsächlich wahrnehmen muss.
- Alle Aktivitäten der Administratoren sind ausschließlich zu Zwecken der Datenschutzkontrolle für einen Zeitraum von maximal einem Jahr zu protokollieren.

9.7. Zugriffsrechte

9.7.1 Zugriff durch schulinterne Stellen oder Personen

Welche Zugriffsrechte Lehrkräfte, die Schüler, die Schulleitung und der Administrator auf das System erhalten, ist in einem Rollen- und Berechtigungskonzept vorab schriftlich festzulegen. Dabei sind u. a. auch personalvertretungsrechtliche Vorgaben zu beachten.

Mitglieder der Schulleitung und gegebenenfalls Funktionsträger haben das Recht zur Durchführung von Unterrichtshospitationen. Dieses Recht dient der Wahrnehmung der Führungsaufgabe, der Beschaffung von Informationen und Eindrücken zur Unterrichts- und Schulkonzeptentwicklung. In vielen Schulen werden Klassenarbeiten exemplarisch nach der Bewertung und vor der Rückgabe an die Schüler der Schulleitung zur Information und Kenntnisnahme vorgelegt. Gleichwohl dürfen diese Zugriffe nur erfolgen, soweit es für die jeweilige Aufgabe erforderlich ist.

Werden Online-Lernplattformen eingesetzt, so werden sie automatisch zu einem Bestandteil der Unterrichtsarbeit. Damit gelten die schulinternen Vereinbarungen, die im Hinblick auf Hospitationen getroffen wurden, auch hier.

Die Art der Einsichtnahme der Schulleitung in die Arbeit mit einer Online-Lernplattform muss den schulinternen Vereinbarungen entsprechen, wie sie für Unterrichtshospitationen im Klassenraum gelten. Die Nutzer der Lernplattform sind über diese Vorgehensweisen und Vereinbarungen vor Beginn der Nutzung zu informieren. Jede Einsichtnahme wird in derselben Weise dokumentiert, wie dies für Hospitationen im regulären Unterrichtsbetrieb erforderlich und festgelegt ist.

Eine Überwachung der Arbeit mit der Lernplattform durch die Schulleitung oder andere Stellen und Personen ist nicht zulässig. Insbesondere darf auch eine Überwachung der Aktivitäten von Schülern durch Lehrende nicht stattfinden. Etwas anderes gilt, wenn die Plattform für pädagogische Aufgaben, wie organisierte Chats zu bestimmten Themen, Gruppenarbeiten usw. genutzt wird, die einer Benotung unterfallen. In diesem Fall darf die für die Benotung notwendig zu beobachtende Aktivität durch die Lehrkraft überwacht werden. Der Umfang der Daten, die für Lehrende sichtbar sein soll, ist daher pädagogisch zu begründen und von der Schulkonferenz festzulegen. Ebenso wenig dürfen die Aktivitäten von Lehrenden durch Vorgesetzte auf der Online-Lernplattform überwacht werden. Die entsprechenden Regelungen sind in der Nutzerordnung festzulegen.

9.7.2 Zugriff auf die Daten durch schulexterne Stellen oder Personen

Schulexterne haben grundsätzlich keinen Zugriff auf geschützte Bereiche der Online-Lernplattform. Sollte es in begründeten Ausnahmefällen nötig sein, so ist jeder Zugriff dieser Art zuvor durch die verantwortliche Stelle auf seine Rechtmäßigkeit zu prüfen. Die Teilnehmer sind über diesen Zugriff frühzeitig zu informieren. Es ist im Rahmen der datenschutzrechtlichen Vorschriften zulässig, externen Personen, die nicht als Lehrer, Schüler oder Mitarbeiter in der Schulverwaltung tätig sind, einen temporären und begrenzten Zugriff auch auf geschützte Bereiche der Lernplattform zu geben, sofern dies für die Gewährleistung der Funktion des Systems erforderlich ist, beispielsweise bei einer Fernwartung. Hierbei muss mit dem jeweiligen Auftragnehmer ein Vertrag über die Auftragsdatenverarbeitung abgeschlossen werden.

9.8. Datenlöschung

Soweit die Speicherung personenbezogener Daten einer Einwilligung bedarf, werden die gespeicherten Daten der Lehrer und Schüler gelöscht, wenn die Einwilligung widerrufen wird. Die Daten der Schüler in Kursen (letzte Bearbeitung, bearbeitete Lektionen, Fehler, Korrekturanmerkungen u. Ä.) werden jeweils am Ende des laufenden Schuljahres gelöscht. Aufbewahrungsfristen aus den Landesschulgesetzen bzw. zugehörigen Rechtsverordnungen sind ebenfalls zu beachten. Es ist schriftlich festzulegen, wie die Aufbewahrungsfristen eingehalten werden. Ausnahmen sind zulässig beispielsweise bei schuljahresübergreifenden Projekten zur Vorbereitung auf Nachprüfungen, bei abiturrelevanten Kursen und aufgrund von Dokumentationspflichten der Schule. Auch E-Portfolios der Schüler können im Sinne einer Sicherheitskopie während der Zeit des kompletten Schulbesuchs hinterlegt werden. Die übrigen Daten der Schüler und Lehrer werden spätestens am Ende des Schuljahres gelöscht, in dem die Lehrkraft von der Schule abgegangen ist oder der Schüler ausgetreten ist.

Benutzerkonten von Schülern und Lehrern sind nach deren Ausscheiden aus der Schule zu löschen oder wenn diese ihre Einwilligung widerrufen.

Die unter 6.1.3 genannten Log-Daten (z.B. wann welcher Nutzer auf welche Daten zugegriffen hat oder wann welche Funktionen genutzt wurden) fallen auf Serverseite an und ermöglichen es, Probleme beim technischen Betrieb und beim Zugriff der Nutzer im Bedarfsfall zu untersuchen und zu lösen. Die Speicherdauer sollte maximal

zehn Tage betragen. Eine längere Speicherdauer ist nur in begründeten Ausnahmefällen zulässig. Für weitergehende Regelungen zur Protokollierung wird auf die o.g. Orientierungshilfe „Protokollierung“ verwiesen.

Die entsprechenden Regelungen sind in der Nutzerordnung festzulegen.

9.9. Trennung der Datenbanken

Jede Schule wird als eigenständige Organisationseinheit verstanden. Die Daten verschiedener Schulen sind logisch getrennt zu halten und zu verwalten. Es muss mindestens gewährleistet sein, dass Schulen nur auf ihre eigenen Daten zugreifen können. Hierzu wird auf die OH Mandantenfähigkeit des Arbeitskreises Technische und organisatorische Datenschutzfragen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in der jeweils aktuellen Fassung verwiesen.

9.10. Sonstige technische Maßnahmen

Es sollten konkrete Maßnahmen vorgeschlagen werden, die insbesondere den Zugriff externer Stellen auf die Daten verhindern und gewährleisten, dass die Datenübertragung auf den häuslichen Rechner der Lehrkräfte und Schüler sowie je nach Rollenkonzept ggf. der Eltern sicher vor unbefugtem Zugriff erfolgt. Die jeweils zu treffenden Maßnahmen richten sich dabei nach den konkreten Umständen des Einzelfalls. Je nach der Art der betroffenen Daten, dem Personenkreis, der auf sie Zugriff haben soll, dem Ort, an dem die Daten gespeichert werden, differiert das Maß der erforderlichen Sicherheit. Wenn es sich lediglich um eine reine Lernplattform handelt, die nur Informationen für die Schüler zur Verfügung stellt, sind nicht die gleichen hohen Schutzmaßnahmen erforderlich wie bei einer Plattform, auf der Noten abgespeichert werden und auf die in bestimmen Bereichen auch Dritte Zugriff haben.

Die Sicherheitsmaßnahmen betreffen insbesondere drei Punkte: die Datensicherheit auf dem Server, den Schutz des Administratorzugangs und den Schutz der Datenübertragung hin zum Nutzer.

1. Auf dem Server sollten nur Hintergrundsysteme zur Datenspeicherung eingesetzt werden, welche eine automatische Zugriffsrechteverwaltung mitbringen, die durch die Lernplattform auch genutzt werden sollte, d. h. ein Default-Nutzer als einziger Datenzugriffsberechtigter ist nicht zulässig (hier wäre sonst der Datenbestand unter Kenntnis des Default-Nutzers komplett auslesbar). Vor Einsatz einer entsprechenden Lernplattform muss das Programm dahingehend geprüft werden, dass eine voll umfängliche Nutzerverwaltung stattfindet.
2. Der Administratorzugriff ist innerhalb der Lernplattform ein sehr kritischer Punkt. Das Passwort sollte gängigen Sicherheitsvorkehrungen genügen. Es wird hierbei auf die jeweils aktuelle BSI Richtlinie zur Erstellung von Passwörtern verwiesen. In Anbetracht der sehr experimentierfreudigen Natur der Schüler sollte außerdem die Administration nur über für Schüler unzugängliche Rechner erfolgen, da dann ausgeschlossen werden kann, dass Schüler unbemerkt Schadsoftware installieren können, die dann das Administratorpasswort ausspähen könnte. Außerdem ist der Einsatz einer Firewall und aktueller Anti-Viren Software auf dem Server uner-

lässlich. Eine Zweifaktor-Authentisierung, wie sie bei vielen webbasierten Anwendungen Standard ist, wird für administrative Zugriffe bei Anwendungen mit erhöhtem Funktionsumfang (Tests, Hausaufgabenkontrolle, etc.) empfohlen.

3. Die Datenübertragung zwischen Server und Nutzer ist zu verschlüsseln. Je nach Lernplattform ist dabei der Einsatz der Verschlüsselungstechnologie einzeln zu prüfen.

25.21 Entschließung: „Videoüberwachungsverbesserungsgesetz" zurückziehen!

9. November 2016

Das Vorhaben des Bundesministeriums des Innern (BMI), durch ein „Videoüberwachungsverbesserungsgesetz" Änderungen des Bundesdatenschutzgesetzes (BDSG) einzuführen, die künftig privaten Stellen den Betrieb von Videokameras zur Verhinderung von Anschlägen wie in Ansbach und Amokläufen wie in München erleichtern sollen, wird von den unabhängigen Datenschutzbehörden des Bundes und der Länder[96] abgelehnt. Der Gesetzentwurf vermag nicht zu begründen, dass die angestrebte

Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist. Auch die Verlagerung der Verantwortung für diese Aufgabe auf die privaten Betreiber von Einkaufszentren und öffentlichem Personennahverkehr lehnen die unabhängigen Datenschutzbehörden des Bundes und der Länder ab. Nach der nicht abschließenden Aufzählung zielt der Gesetzentwurf überwiegend auf Orte, an denen Betroffene ihre Freizeit verbringen. Gerade in diesen Bereichen, in denen sich Menschen typischerweise zur ungezwungenen Kommunikation, Erholung und Entspannung für längere Dauer aufhalten, gilt es das Persönlichkeitsrecht in besonderem Maße zu schützen.

Gleichwohl lässt es die einschlägige Bestimmung des § 6b BDSG bereits gegenwärtig zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können auch heute Kameras installiert werden, um Personen von Straftaten an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt werden und nach § 6 Abs. 3 Satz 2 BDSG können Videobilder an Polizei-, Ordnungs- und Strafverfolgungs- und Ordnungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Begründung des BMI suggeriert, die Datenschutzaufsichtsbehörden verhinderten angesichts der angespannten Sicherheitslage die Durchführung von Videoüberwachung. Dies trifft nicht zu. Tatsächlich werden

[96] Bei Enthaltung der Bundesbeauftragten für Datenschutz und Informationsfreiheit.

gerade im Bereich der großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs bereits heute zahlreiche Kameras mit ausdrücklicher Billigung der Aufsichtsbehörden betrieben.

Terroristen wie auch irrational handelnde Einzeltäter, vor denen die gesetzliche Regelung schützen soll, nehmen ihren eigenen Tod bei derartigen Anschlägen bewusst in Kauf. Sie werden sich daher von ihren Taten auch nicht durch Videokameras abschrecken lassen.

Hinzu kommt, dass die Betreiber von Videoüberwachungsanlagen bereits heute meistens nicht in der Lage sind, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann. In der Praxis bleibt die Bedeutung der Kameras daher auf eine Speicherung auf Vorrat und für die spätere Strafverfolgung beschränkt.

Auch die mögliche Erhöhung eines faktisch ungerechtfertigten subjektiven Sicherheitsgefühls könnte Grundrechtseingriffe nicht rechtfertigen. Insoweit ist die Regelung, die von den privaten Betreibern eine stärkere Gewichtung des Schutzes von Leben, Gesundheit oder Freiheit der Betroffenen bei der rechtlichen Abwägung fordert, letztlich gar nicht geeignet, das Ziel der gesetzlichen Regelung zu erreichen.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder betonen mit Nachdruck, dass es nicht die Aufgabe privater Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Dies obliegt allein den Sicherheitsbehörden, die über ausreichende landes- und bundesgesetzliche Grundlagen sowohl für die Gefahrenabwehr als auch für die Strafverfolgung verfügen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesinnenminister auf, den Gesetzentwurf zurückzuziehen.

25.22 Entschließung: Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf - Konsequenzen für polizeiliche Datenverarbeitung notwendig

10. November 2016

Die Datenschutzbeauftragten des Bundes und der Länder[97] Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben parallel die bundesweit geführte „Falldatei Rauschgift" (FDR) datenschutzrechtlich geprüft.

Die FDR ist eine bundesweite Verbunddatei, in der Informationen über sichergestellte Drogen und Verstöße gegen das Betäubungsmittelgesetz gespeichert werden. Sie wird auf Grundlage des Bundeskriminalamtgesetzes (BKAG) zentral beim Bundeskriminalamt geführt. Die Polizeien aller Länder und die Zollfahndung haben Zu-

[97] Bei Enthaltung Hamburgs.

griff auf die Datei und können direkt Daten einspeichern und abrufen. Die Datenschutzbeauftragten haben im Rahmen ihrer Kontrollen sowohl die Struktur der Datei als auch Einzelspeicherungen überprüft.

Die Prüfung hat im Wesentlichen folgende Mängel aufgedeckt:

- Vielfach haben die Behörden nicht ausreichend geprüft, ob die Voraussetzungen des § 2 BKAG (Straftat von länderübergreifender oder erheblicher Bedeutung) und des § 8 Abs. 2 BKAG (Negativprognose) vorliegen.
- Verbreitet fehlt es an einer nachvollziehbaren Dokumentation des Vorliegens der gesetzlichen Speicherungsvoraussetzungen.
- Dementsprechend fanden sich in der bundesweit abrufbaren Datei vielfach Speicherungen, die dem Bereich der Bagatellkriminalität zuzuordnen sind. Auch wurden Personen gespeichert, bei denen kein hinreichender polizeilicher Restverdacht festzustellen war.
- Das Ergebnis des jeweiligen Strafverfahrens war bei vielen Einträgen nicht berücksichtigt – entweder aufgrund organisatorischer Mängel oder weil die nach § 482 Abs. 2 Strafprozessordnung (StPO) notwendige Mitteilung der Staatsanwaltschaft unterblieb.

Die Ergebnisse machen deutlich:

1. Es ist wichtig, die konkrete Zwecksetzung jeder Datei in einer Errichtungsanordnung festzulegen. Die Voraussetzungen, wann welche Daten für den jeweiligen Zweck erforderlich sind und welcher Personenkreis erfasst werden darf, müssen genau definiert werden.
2. Bagatellfälle in Verbunddateien zu speichern, ist auch im Hinblick auf die bundesweite Abrufbarkeit der Daten unverhältnismäßig.
3. In der Praxis ist sicherzustellen, dass in Verbunddateien alle Speichervoraussetzungen, vor allem die Negativprognose, durchgehend und gründlich bezogen auf den jeweiligen Einzelfall dokumentiert werden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert, nicht nur in der Falldatei Rauschgift die Mängel zu beheben. Vielmehr fordert sie die Einhaltung der grundlegenden Standards für jedwede Speicherung in Verbunddateien der Polizei. Erst recht ist dies erforderlich vor dem Einsatz der neuen Datei zur Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV), die voraussichtlich im kommenden Jahr die FDR ablösen wird. Die Daten aus der FDR dürfen nicht pauschal übernommen werden.

25.23 Kühlungsborner Erklärung der unabhängigen Datenschutzbehörden der Länder[98]

10. November 2016

Der Vollzug der Europäischen Datenschutz-Grundverordnung (DS-GVO) erfordert eine effektive Organisationsstruktur. Zentrale Bedeutung kommt dabei dem Europäischen Datenschutzausschuss (EDSA) zu, der für alle Aufsichtsbehörden verbindliche Beschlüsse treffen kann und in dem jeder Mitgliedstaat eine Stimme hat.

Die Datenschutzbehörden der Länder fordern den Bundesgesetzgeber auf, bei der gesetzlichen Regelung des Vertreters der deutschen Aufsichtsbehörden im EDSA der Unabhängigkeit aller Aufsichtsbehörden und der Zuständigkeitsverteilung zwischen Bund und Ländern Rechnung zu tragen.

Der Vollzug der Datenschutzregelungen obliegt im föderativen System der Bundesrepublik Deutschland den Datenschutzbehörden der Länder. Die Zuständigkeit des/der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) beschränkt sich auf wenige spezifische Bereiche. Diesem Umstand muss bei der Vertretung der deutschen Aufsichtsbehörden im EDSA nach Artikel 68 DS-GVO Rechnung getragen werden. Die unabhängigen Datenschutzbehörden der Länder setzen sich daher für die folgenden Regelungen ein:

- Die Vertretung der deutschen Aufsichtsbehörden im EDSA kann sowohl durch den/die BfDI als auch eine Landesaufsichtsbehörde erfolgen. Die Stellvertretung obliegt dann dem jeweils anderen.
- Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bestimmt die beiden Vertreter im EDSA.
- Die Vertretung im EDSA hat der nationalen Zuständigkeitsverteilung für den Vollzug Rechnung zu tragen. Die für den Vollzug zuständigen Aufsichtsbehörden müssen die Möglichkeit erhalten, über den Vertreter im EDSA Angelegenheiten einzubringen und ihre jeweiligen Positionen im Verfahren autonom zu bestimmen.

Unter Zugrundelegung dieser Leitlinien ist nach Auffassung der Länder eine effektive Vertretung der unabhängigen Datenschutzbehörden im EDSA möglich.

25.24 Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Die Orientierungshilfe zeigt den datenschutzrechtlichen Rahmen und Regelungsmöglichkeiten der Nutzung des betrieblichen Internet- und E-Mail-Dienstes durch die Beschäftigten auf. Sie soll es den Arbeitgebern und den Beschäftigten erleichtern,

[98] Bei Enthaltung Bayerns.

eine klare Regelung im Unternehmen zu erreichen, soweit eine private Nutzung des Internets und/oder des E-Mail-Dienstes erlaubt sein soll. Zudem enthält diese Orientierungshilfe ein Muster für eine Betriebsvereinbarung/Richtlinie/Anweisung für die private Nutzung von Internet und/oder des betrieblichen E-Mail Postfachs.

Die Anlagen sind der Ausführung im Tätigkeitsbericht nicht beigefügt. Die Orientierungshilfe, einschließlich der Anlagen, ist auf der Internetseite der Landesbeauftragten für Datenschutz und Informationsfreiheit im Saarland abrufbar, unter:

https://datenschutz.saarland.de/themen/beschaeftigtendatenschutz

A. Allgemeines

I. Überblick

„Darf ich am Arbeitsplatz privat das Internet nutzen? Darf ich am Arbeitsplatz private E-Mails versenden?" – diese Fragen haben viele Beschäftigte, die Zugang zum Internet haben.

Für den Arbeitgeber stellen sich ähnliche Fragen: „Darf ich auf das E-Mail-Postfach der Beschäftigten zugreifen, wenn sie ungeplant abwesend sind? Darf ich die Internetnutzung kontrollieren? Welche Gestaltungsmöglichkeiten habe ich im Voraus?"

Datenschutzrechtlich bedeutsam sind in diesem Zusammenhang die anfallenden personenbezogenen Daten, und zwar sowohl der Beschäftigten als auch ihrer Kommunikationspartner und anderer Betroffener (z.B. Dritter, deren Namen in einer E-Mail genannt wird).

Für die Beurteilung der datenschutzrechtlichen Zulässigkeit der E-Mail- und Internetnutzung am Arbeitsplatz ist es sehr relevant, ob den Beschäftigten auch die private Nutzung des Internets und/oder des betrieblichen E-Mail-Postfachs am Arbeitsplatz gestattet worden ist.

Diese Orientierungshilfe stellt einige der hierbei zu beachtenden datenschutzrechtlichen Anforderungen dar und zeigt Regelungsmöglichkeiten auf. Sie richtet sich an die Wirtschaft und kann in der Regel entsprechend für den öffentlichen Dienst angewendet werden. Landesspezifische Vorschriften sind zu beachten.

Im Anhang befindet sich das Muster einer Betriebsvereinbarung und ergänzender Einwilligung, mit der die private Internet- und E-Mail-Nutzung geregelt werden kann. Das Muster kann auch als Beispiel genommen werden, um diese Punkte in eine Anweisung/Richtlinie oder in den einzelnen Arbeitsvertrag aufzunehmen.[99] Dies bietet sich insbesondere dann an, wenn es im Unternehmen keinen

Betriebsrat gibt. Das Muster ist an die konkreten Gegebenheiten im jeweiligen Unternehmen anzupassen; zudem sind jeweils arbeitsrechtliche Fragestellungen zu beachten, die dieses Papier nicht erschöpfend berücksichtigen kann.

[99] Aus Gründen der Übersichtlichkeit wird im Folgenden ausschließlich von der Betriebsvereinbarung gesprochen. Gemeint sind jedoch auch die Anweisung/Richtlinie oder eine Regelung im Arbeitsvertrag.

II. Rechtlicher Rahmen

1. Grundsatz

Soweit der Arbeitgeber Hardware bzw. Software zur Verfügung stellt, dürfen die betrieblichen Internet- und E-Mail-Dienste grundsätzlich nur für die betriebliche Tätigkeit genutzt werden. Eine private Nutzung von Internet und/oder betrieblichem E-Mail-Postfach ist daher nicht erlaubt, es sei denn, der Arbeitgeber hat eine Privatnutzung ausdrücklich z.B. im Arbeitsvertrag oder in einer Betriebsvereinbarung geregelt oder, was überwiegend als möglich angesehen wird, in Kenntnis und Duldung der privaten Nutzung über einen längeren Zeitraum (sog. „betriebliche Übung") konkludent genehmigt.

Dem Arbeitgeber steht es frei, ob er eine Privatnutzung des Internets und/oder des betrieblichen E-Mail-Accounts erlaubt.

2. Gesetzlicher Rahmen

a) BDSG und Arbeitsrecht

Soweit die Nutzung des Internets und/oder des betrieblichen E-Mail-Postfachs ausschließlich zu betrieblichen Zwecken erlaubt ist, richtet sich die Erhebung, Verarbeitung und Nutzung von anfallenden personenbezogenen Daten nach dem Bundesdatenschutzgesetz (BDSG).

Da sich das öffentlich-rechtliche Datenschutzrecht gemäß BDSG, welches Gegenstand dieser Orientierungshilfe ist, und das zivilrechtliche Arbeitsrecht „überlappen", sind parallel arbeitsrechtliche Fragestellungen zu berücksichtigen.

b) TKG und TMG

Wenn der Arbeitgeber den Beschäftigten auch die private Nutzung von Internet und/oder des betrieblichen E-Mail-Postfaches erlaubt, ist zusätzlich das Telekommunikationsgesetz (TKG) bzw. das Telemediengesetz (TMG) zu beachten. Nach Auffassung der Aufsichtsbehörden ist der Arbeitgeber in diesem Fall Telekommunikationsdienste- bzw. Telemediendienste-Anbieter. Dies hat die Konsequenz, dass er an das Fernmeldegeheimnis des § 88 Abs. 2 S. 1 TKG gebunden ist und gemäß § 11 Abs. 1 Nr. 1 TMG den Datenschutzvorschriften des TMG unterliegt. Zugleich bedeutet dies, dass sich der Arbeitgeber bei einer Verletzung des Fernmeldegeheimnisses gemäß § 206 Strafgesetzbuch (StGB) strafbar machen kann.

Zum rechtlichen Hintergrund: Das Fernmeldegeheimnis kann sich auch auf E-Mails erstrecken, die auf einem Server des jeweiligen Diensteanbieters zwischen- oder endgespeichert sind. Daher wird auch der „ruhende" E-Mail-Verkehr erfasst, bei dem ein „dynamischer" Telekommunikationsvorgang nicht (mehr) stattfindet (BVerfG, 16. Juni 2009, 2 BVR 902/06). Solange also E-Mails im Herrschaftsbereich des jeweiligen Diensteanbieters verbleiben, folgt die Schutzbedürftigkeit der Kommunikationspartner aus dieser Einschaltung eines Dritten.

Einige Gerichte vertreten demgegenüber die Auffassung, dass Arbeitgeber, die die private Nutzung des Internets und/oder eines betrieblichen E-Mail-Postfachs gestatten oder dulden, nicht als Diensteanbieter im Sinne des TKG bzw. TMG anzusehen sind und daher nicht dem Fernmeldegeheimnis unterliegen.[100]

Solange jedoch diese Frage nicht höchstrichterlich oder durch den Gesetzgeber eindeutig geklärt ist, sollten Arbeitgeber zur Vermeidung etwaiger Strafbarkeit davon ausgehen, Diensteanbieter zu sein. Hiervon geht auch die vorliegende Orientierungshilfe aus.

Auf die Verpflichtung des Arbeitgebers, die Beschäftigten über die Erstellung von Einzelverbindungsnachweisen und deren Kenntnisnahme gem. § 99 Abs. 1 Satz 4 TKG zu informieren, wird hingewiesen.

B. Ausschließlich betriebliche Nutzung

I. Internet

1. Der Arbeitgeber hat grundsätzlich das Recht, anhand von Protokolldaten stichprobenartig[101] zu prüfen, ob das Surfen der Beschäftigten betrieblicher Natur ist. Dazu ist es in einem ersten Schritt zulässig und ausreichend, wenn sie für diesen Zweck zunächst nur eine Auswertung des Surfverhaltens ohne Personenbezug vornehmen, d.h. insbesondere auch ohne Einbeziehung der IP-Adresse und anderer Daten zur Identifizierung der einzelnen Beschäftigten. Grundsätzlich ist datenschutzfreundlichen Maßnahmen zur Begrenzung der Internetnutzung – z. B. Nutzung von black- und/oder whitelists – der Vorzug zu geben. Für die Erstellung solcher black- bzw. whitelists können hinsichtlich der Internetnutzung wirksam anonymisierte Protokolldaten herangezogen werden. Eine personenbezogene Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung der Beschäftigten unter den Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG bei konkretem Missbrauchsverdacht im verhältnismäßigen Rahmen zulässig. Danach können zur Aufdeckung von Straftaten personenbezogene Daten der Beschäftigten erhoben, verarbeitet oder genutzt werden, wenn folgende Voraussetzungen vorliegen: Es müssen zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die Betroffenen im Beschäftigungsverhältnis eine Straftat begangen haben. Zudem muss die Maßnahme zur Aufdeckung erforderlich sein. Letztlich darf nicht das schutzwürdige Interesse der Betroffenen überwiegen; insbesondere dürfen Art und Ausmaß nicht unverhältnismäßig sein.

---

[100] Hessischer VGH, 19.5.2009, AZ: 6 A 2672/08.Z; LAG Niedersachsen, 31.5.2010, AZ: 12 Sa 875/09; LAG Berlin-Brandenburg, 16. Februar 2011, AZ: 4 Sa 2132/10; VG Karlsruhe, 27. Mai 2013, AZ: 2 K 3249/12; VGH Baden-Württemberg, 30. Juli 2014, 1 S 1352/2013. Die genannten Gerichte haben zudem zum Teil die Auffassung vertreten, dass der Schutz des Fernmeldegeheimnisses jedenfalls in dem Moment endet, in dem der Empfänger in der Weise Zugriff auf die E-Mails in seinem betrieblichen E-Mail Postfach hat, dass er entscheiden kann, ob er sie im zentralen Posteingang belässt oder auf einen lokalen Rechner verschiebt/löscht.

[101] Zum Umfang von Stichproben wird auf die arbeitsrechtliche Rechtsprechung, insbesondere BAG, Beschluss vom 9. Juli 2013 - 1 ABR 2/13 (A) - verwiesen.

2. Soweit im Zusammenhang mit der Nutzung des Internets personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren gespeichert werden, dürfen diese Daten auch nur zu diesen Zwecken genutzt werden (§ 31 BDSG). Eine Nutzung dieser Daten zur Verhaltens- und Leistungskontrolle der Beschäftigten ist nicht erlaubt.

II. Nutzung des betrieblichen E-Mail-Accounts

1. Ein- und ausgehende betriebliche E-Mails der Beschäftigten darf der Arbeitgeber zur Kenntnis nehmen. Beispielsweise kann er verfügen, dass die Beschäftigten ihm jede für den Geschäftsgang relevante oder fest definierte ein- oder ausgehende E-Mail einzeln zur Kenntnis zuleiten. Eine durch den Arbeitgeber eingerichtete automatisierte Weiterleitung aller ein- und ausgehenden E-Mails an einzelne Vorgesetzte ist, sofern arbeitsrechtlich nicht statthaft, auch datenschutzrechtlich mangels Erforderlichkeit unzulässig (Verbot der permanenten Kontrolle).

2. Für den Fall der Abwesenheit kann eine Weiterleitung der E-Mail in Betracht kommen. Allerdings sollte im Hinblick auf die schutzwürdigen Belange der Beschäftigten die Verwendung eines Abwesenheitsassistenten vorgezogen werden. Aufgrund der schutzwürdigen Belange der Beschäftigten stellt dieses Vorgehen das mildeste Mittel dar. Nur wenn eine Abwesenheitsmitteilung nicht ausreicht, kann eine Weiterleitung in Betracht gezogen werden.

   Auf bereits empfangene bzw. versandte betriebliche E-Mails darf der Arbeitgeber nur zugreifen, wenn dies für betriebliche Zwecke erforderlich ist.

3. E-Mails dürfen von dem Arbeitgeber nicht weiter inhaltlich zur Kenntnis genommen werden, sobald ihr privater Charakter erkannt wurde. Etwas anderes kann im Falle erforderlicher Maßnahmen der Missbrauchskontrolle gelten.

4. a) Zur Missbrauchskontrolle gelten die Ausführungen zu B I 1 entsprechend.

   b) Zur Regelung des § 31 BDSG (besondere Zweckbindung erhobener Daten) gelten die Ausführungen zu B I 2 entsprechend.

C. Private Nutzung

I. Internet

1. Ist die private Nutzung des Internets erlaubt (oder gilt sie als erlaubt, s.o.[102]), wird der Arbeitgeber hinsichtlich der privaten Nutzung zum Diensteanbieter im Sinne des TKG und unterliegt den Datenschutzbestimmungen des TMG. Er ist daher grundsätzlich zur Wahrung des Fernmeldegeheimnisses verpflichtet. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen (Protokolldaten), ist dem Arbeitgeber nur mit Einwilligung der betreffenden Beschäftigten erlaubt. Dies betrifft insbesondere die Daten, aus denen sich ergibt, welche Internetseiten welche Beschäftigten wann aufgerufen haben.

[102] Siehe A II 1.

Ausnahmen gelten allerdings gemäß §§ 88 Abs. 3, 91 ff. TKG (z.B. erforderliche Maßnahmen zum Schutz der technischen Systeme, d.h. zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen).

2. Der Arbeitgeber kann die Erlaubnis einer Privatnutzung an Bedingungen knüpfen: Es bieten sich insbesondere Regelungen zum zeitlichen Umfang der Privatnutzung an. Auch konkrete Verhaltensregeln sollten vor Beginn der privaten Nutzung getroffen werden. Der Arbeitgeber braucht in diesem Zusammenhang eine Einwilligung der Beschäftigten, die sich darauf bezieht, dass diese mit Zugriffen des Arbeitgebers (wie unter 1. beschrieben) einverstanden sind. Die Einwilligung erstreckt sich also auf Art und Umfang von Zugriffen und Kontrollen. Diese Kontrollen umfassen die Einhaltung der Nutzungsregelungen (zeitlicher Umfang bzw. Inhalt der Nutzung).

3. Zur Einwilligung: Auf der „ersten Stufe" sollte eine Betriebsvereinbarung abgeschlossen werden. In dieser sollte der Gegenstand der späteren, individuellen Einwilligungen umrissen werden. Sodann sind auf dieser Grundlage die individuellen Einwilligungen der einzelnen Beschäftigten einzuholen.

4. Die Einwilligung sollte gesondert erklärt werden. Den Beschäftigten ist vor der Einwilligung Gelegenheit zu geben, die Betriebsvereinbarung zur Kenntnis zu nehmen.

5. Zum weiteren Inhalt einer Betriebsvereinbarung: Es ist zu empfehlen, sämtliche Fragen zur Privatnutzung in der Betriebsvereinbarung zu regeln. In der Betriebsvereinbarung sollten daher die Nutzungsregelungen (zeitlicher Umfang, Verhaltensregeln) und die Zugriffsmöglichkeiten (Einwilligung, insbesondere zu Art und Umfang von Kontrollen) eindeutig festgehalten sein.

6. Auf der Grundlage der Einwilligung darf eine Protokollierung der Internetnutzung sowie eine Auswertung der Protokolldaten entsprechend B.I. stattfinden. Eine personenbezogene Auswertung von Protokolldaten darf jedoch nur bei einem konkreten Verdacht erfolgen. In Betracht kommt insbesondere der Verdacht eines Verstoßes gegen in der Betriebsvereinbarung festgeschriebene Verhaltensvorschriften bzw. den festgelegten Umfang der erlaubten Privatnutzung. Eine personenbezogene Kontrolle ist nur zulässig, wenn sie verhältnismäßig ist.

7. Beschäftigte, die diese Bedingungen nicht akzeptieren wollen, können ihre Einwilligung ohne jeden arbeitsrechtlichen Nachteil verweigern. Eine Privatnutzung ist dann nicht erlaubt. Da für diese Beschäftigten im Ergebnis nur die betriebliche Nutzung erlaubt ist, gelten für sie die Ausführungen unter B.I.

II. Nutzung des betrieblichen E-Mail-Accounts

1. Ist die private E-Mail-Nutzung erlaubt (oder gilt sie als erlaubt, s.o.[103]), ist der Arbeitgeber gegenüber den Beschäftigten und ihren Kommunikationspartnern zur Einhaltung des Fernmeldegeheimnisses verpflichtet.

   Der Schutz des Fernmeldegeheimnisses gilt, solange der Übermittlungsvorgang andauert und die E-Mail noch nicht in den ausschließlichen Herrschaftsbereich des Empfängers gelangt ist. Dies ist beispielsweise der Fall, wenn sie sich noch in einem E-Mail-Postfach auf dem Server im Zugriffsbereich des Arbeitgebers befindet. Der Abschluss des Übermittlungsvorgangs hängt von den technischen Gegebenheiten, insbesondere dem verwendeten Übertragungsprotokoll, ab. Solange Nachrichten - wie bei Verwendung des „IMAP-Protokolls" - auf einem zentralen E-Mail-Server des Arbeitgebers oder eines Providers verbleiben und bei jedem Zugriff durch die Beschäftigten erneut heruntergeladen werden, ist der Übermittlungsvorgang nicht beendet. Dies hat zur Folge, dass der Arbeitgeber grundsätzlich ohne Einwilligung der jeweiligen Beschäftigten nicht auf deren betriebliches E-Mail-Postfach zugreifen darf.

   Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist dem Arbeitgeber grundsätzlich nur mit Einwilligung der betreffenden Beschäftigten erlaubt. Allerdings gelten gemäß §§ 88 Abs. 3, 91 ff. TKG die dort geregelten Ausnahmen (z.B. erforderliche Maßnahmen zum Schutz der technischen Systeme, d.h. zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen).

2. Der Arbeitgeber kann die Erlaubnis zur privaten Nutzung des betrieblichen E-Mail-Postfachs an Bedingungen knüpfen: In Betracht kommen Nutzungsregelungen (insbesondere zum zeitlichen Umfang; ggf. auch Verhaltensregeln) und Zugriffsmöglichkeiten des Arbeitgebers. Hierfür ist wiederum eine Einwilligung der Beschäftigten einzuholen. Wie schon bei der privaten Internetnutzung geht es hierbei zum einen um die Möglichkeit von Kontrollen (bezogen auf die o.g. Nutzungsregelungen). Die Einwilligung sollte sich daher auf Art und Umfang solcher etwaiger Kontrollen beziehen.

   Im Gegensatz zur privaten Internetnutzung steht jedoch bzgl. des privaten Mailverkehrs eine andere Zugriffsmöglichkeit im Vordergrund: Im gemeinsamen betrieblichen Interesse sollte eindeutig im Vorfeld festgelegt werden, ob bzw. wie der Arbeitgeber auf die betrieblichen Mails im gemischt-privat-betrieblichen Postfach zugreifen kann.

   Die Ausführungen unter C. I. 2-6 gelten hierfür entsprechend.

3. Der Arbeitgeber sollte also klare Vorgaben machen, welche Einstellungen die Beschäftigten vorzunehmen haben, wenn sie - geplant oder nicht geplant - abwesend sind (z.B. Abwesenheitsnotiz).

4. Wurden diese Einstellungen nicht vorgenommen (etwa weil es bei einer ungeplanten Abwesenheit nicht möglich war oder weil es vergessen wurde),

[103] Siehe A II 1.

darf ein Zugriff auf das betriebliche E-Mail-Postfach der betroffenen Beschäftigten, soweit dies für betriebliche Zwecke erforderlich ist, nur mit deren vorab eingeholter Einwilligung erfolgen.

5. Ein Zugriff auf bereits vor der Abwesenheit der jeweiligen Beschäftigten eingegangenen E-Mails ist ebenfalls nur zulässig, soweit dieser für betriebliche Zwecke erforderlich ist und vorab Einwilligungen der Beschäftigten eingeholt wurden.

6. Haben Beschäftigte im Zusammenhang mit der betrieblichen E-Mail-Nutzung in die Regelungen zur privaten Mailnutzung eingewilligt, sind sie darauf hinzuweisen, dass im Zusammenhang mit einer Archivierung (z.B. gem. § 257 HGB, § 147 AO) auch eine Archivierung ihrer privaten E-Mails erfolgen kann. Den Beschäftigten sollte jedoch Gelegenheit gegeben werden, private Mails zu löschen oder an ihren privaten Account weiterzuleiten.

D. Regelungen für Geheimnisträger

„Geheimnisträger" in diesem Sinne sind Beschäftigte, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden (Betriebsrat, Jugend- und Ausbildungsvertretung, betrieblicher Datenschutzbeauftragter, Betriebsarzt, Gleichstellungsbeauftragte u.a.) und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen.

I. Internet

Grundsätzlich besteht keine Kontrollbefugnis des Arbeitgebers bzgl. der Internetnutzung der o.g. „Geheimnisträger", z.B. der Betriebsräte.

II. Nutzung des betrieblichen E-Mail-Accounts

Bei den „Geheimnisträgern" muss eine Kenntnisnahme des Arbeitgebers von den Verkehrs- und Inhaltsdaten ausgeschlossen werden. Es empfiehlt sich, für diese Stellen nicht personalisierte funktionsbezogene Postfächer (z.B. Betriebsrat@Unternehmen.de) einzurichten und diese von Kontrollen bzw. Auswertungen auszunehmen.

Neben den Belangen der „Geheimnisträger" selbst, sind in gleichem Maße die schutzwürdigen Belange der einzelnen Beschäftigten, die mit dem jeweiligen „Geheimnisträger" kommunizieren, zu beachten. Auch insofern sind Vorkehrungen zu treffen. Es ist daher dafür zu sorgen, dass E-Mails der Beschäftigten von bzw. an den jeweiligen „Geheimnisträger" (ggf. aufgrund einer einschlägigen Betreffzeile) von dem Arbeitgeber nicht zur Kenntnis genommen werden. Den Beschäftigten sollte daher empfohlen werden, derartige Kommunikation über andere Wege (z.B. private E-Mail-Adresse, schriftlich oder telefonisch) zu führen. So kann eine Kenntnisnahme der Verkehrs- und Inhaltsdaten durch den Arbeitgeber vollkommen ausgeschlossen werden.

E. Empfehlungen der Aufsichtsbehörden

1. Es wird empfohlen, über die betriebliche und/oder private Nutzung des Internets und des betrieblichen E-Mail-Accounts eine schriftliche Regelung zu

treffen, in der die Fragen des Zugriffs, der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig festgelegt werden.

Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

2. Sofern der Arbeitgeber seinen Beschäftigten die Möglichkeit zur Nutzung des betrieblichen E-Mail-Accounts für private E-Mail-Kommunikation ermöglichen möchte, sollte er bedenken, dass er dann an das Fernmeldegeheimnis gebunden ist. Dies führt in der Praxis regelmäßig zu erheblichen Konflikten, nämlich dann, wenn der Arbeitgeber für den Geschäftsablauf auf das betriebliche Postfach der Beschäftigten zugreifen möchte. Es wird daher empfohlen, dass der Arbeitgeber den Beschäftigten lediglich die private Nutzung des Internets anbietet, welche auch die Nutzung von Webmail-Diensten (wie z.B. web.de; gmx.de; yahoo.de etc.) umfasst. Anstatt der Nutzung der betrieblichen E-Mail-Accounts sollten die Beschäftigten dann auf die ausschließliche Nutzung privater Web-Mail-Accounts für private Nachrichten verwiesen werden. Das jeweilige betriebliche Postfach wird dann weiterhin ausschließlich betrieblich genutzt (vgl. B II).

3. Wenn der Arbeitgeber seinen Beschäftigten die private Nutzung des betrieblichen E-Mail-Accounts erlaubt hat (vgl. C II) und für den Geschäftsablauf auf das betriebliche Mailpostfach der einzelnen Beschäftigten zugreifen möchte, hat er Folgendes zu beachten: E-Mails mit erkennbar privatem Inhalt dürfen von dem Arbeitgeber nur in dem Umfang zur Kenntnis genommen werden, wie dies von der Einwilligung gedeckt und unerlässlich ist, um sie von den betrieblichen E-Mails zu trennen. Dasselbe gilt für solche E-Mails, die der Kommunikation der Beschäftigten mit „Geheimnisträgern" (Betriebsrat, Jugend- und Ausbildungsvertretung, Schwerbehindertenvertretung, Gleichstellungsbeauftragte u.a.) dienen. Dies ist durch eine entsprechende Verfahrensgestaltung zu gewährleisten. Wenn sich im Rahmen der Sichtung aus dem Absender und/oder Betreff einer E-Mail Anhaltspunkte dafür ergeben, dass es sich um eine geschützte und dem Privatbereich zuzurechnende E-Mail handelt, ist der Vertreter der Arbeitgeber oder die von dem Arbeitgeber bestimmte Person nicht berechtigt, den Inhalt der E-Mail zur Kenntnis zu nehmen, zu verarbeiten oder zu nutzen.

4. Wenn Beschäftigte das Unternehmen verlassen, sollte darauf geachtet werden, dass die persönliche betriebliche E-Mail-Adresse schnellstmöglich deaktiviert wird.

5. Ergänzende Hinweise lassen sich den Orientierungshilfen „Protokollierung" und „zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet" entnehmen.

F. Spamfilter und Virenschutz

Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, wenn sie Inhalte aufweisen, die zu Sicherheitsrisiken auf Rechnern oder im Netzwerk führen können (Virenfilterung). Davon zu unterscheiden ist die Ausfilterung bzw. Veränderung von „Spam-Mails".

Beim Verfahren zur Behandlung von Spam-Mails ist § 303 a StGB zu beachten.

1. Spamfilter

Über eine zentrale Spam-Filterung ist im Vorfeld zu unterrichten. Es gibt eine Vielzahl an Möglichkeiten zur Abwehr unerwünschter Nachrichten (Spam), die in verschiedensten Kombinationen und Ausprägungen eingesetzt werden können. Aus den in Betracht kommenden Varianten sollte die datenschutzfreundlichste gewählt werden. Zugleich sollte folgenden Grundsätzen Rechnung getragen werden:

- Filter, die Header oder Inhalt elektronischer Post automatisch auf unerwünschte Nachrichten
- (Spam) prüfen, sollten erst an einem Punkt eingesetzt werden, der außerhalb der Reichweite des Fernmeldegeheimnisses liegt.
- Die (zentrale) Markierung spamverdächtiger Nachrichten ist dabei der zentralen Löschung von E-Mails ohne Kenntnis des Empfängers vorzuziehen.
- Um Verletzungen von Vertraulichkeit und Integrität zu vermeiden, sollten die Empfänger der Nachrichten in größtmöglicher Autonomie selbst über den Umgang mit den an sie gerichteten E-Mails entscheiden können.

2. Virenschutz

Das Herausfiltern und Untersuchen von virenverseuchten E-Mails mit Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist hinsichtlich privater E-Mails nur in dem in § 100 TKG festgelegten Umfang gestattet.

26 Düsseldorfer Kreis der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

26.1 Beschluss: Nutzung von Kameradrohnen durch Private

15./16. September 2015

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Drohnen kommen als unbemannte Luftfahr-zeuge nicht nur in Krisengebieten oder in der Landwirtschaft zum Einsatz, sondern werden immer häufiger auch von Privaten für die Freizeitbeschäftigung gekauft und im nachbarschaftlichen Umfeld eingesetzt. Da können durchaus Begehrlichkeiten aufkommen: ein unbeobachteter Blick in den Garten des Nachbarn, auf die Sonnenterrasse oder in sonstige nicht einfach zugängliche Orte.

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

Auch wenn der Betrieb von Drohnen durch Privatpersonen zu Zwecken des Sports oder der Freizeitgestaltung mit Ausnahme von § 16 Abs. 1 Nr. 1 LuftVO keiner luftverkehrsrechtlichen Erlaubnis der zuständigen Landesluftfahrtbehörde bedarf und im Hinblick auf § 1 Abs. 2 Nr. 3 des Bundesdatenschutzgesetzes (BDSG) außerhalb des datenschutzrechtlichen Regelungsregimes erfolgen kann, sind Verwendungen von Drohnen mit Videotechnik denkbar, die in den Anwendungsbereich des BDSG fallen. In solchen Fällen sind Drohnen nur im Rahmen von datenschutzrechtlichen Erlaubnisnormen zu betreiben, wobei deren Voraussetzungen in der Mehrzahl der Fälle wegen des regelmäßigen Überwiegens von Interessen Betroffener nicht gegeben sind. Dies ist insbesondere dann der Fall, wenn die Aufnahmen für eine Veröffentlichung im Internet stattfinden oder ein zielgerichteter Drohneneinsatz zur kontinuierlichen Beobachtung öffentlich zugänglicher Räume im Sinne des § 6b BDSG erfolgt. Wenn solche Drohnen innerhalb des Anwendungsbereiches des BDSG betrieben werden und hierbei unbefugt Daten erhoben oder verarbeitet werden, kann die zuständige Behörde hierfür ein Bußgeld von bis zu 300.000 Euro verhängen.

Jedoch sind auch außerhalb des Anwendungsbereiches des BDSG rechtliche Rahmenbedingungen zu beachten. So sind auch hier das Recht am eigenen Bild, das

Grundrecht der Betroffenen auf informationelle Selbstbestimmung im Besonderen sowie das Persönlichkeitsrecht im Allgemeinen zu wahren.

Dem mit dem Drohneneinsatz verbundenen Eingriff in das allgemeine Persönlichkeitsrecht Betroffener kann neben den Möglichkeiten der zuständigen Aufsichts- oder Bußgeldbehörde auch zivilrechtlich begegnet werden. Vor allem 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. Dem Betroffenen kann in solchen Fällen ein Abwehranspruch aus § 823 in Verbindung mit § 1004 Abs. 1 des Bürgerlichen Gesetzbuches (BGB) analog zustehen. Auch das Kunsturhebergesetz (KUG), welches das Recht am eigenen Bild – als besondere Ausprägung des allgemeinen Persönlichkeitsrechts – schützt, kann tangiert sein (§§ 22, 23 KUG), sofern eine Verbreitung oder Veröffentlichung der Aufzeichnungen erfolgt.

Die Strafverfolgungsbehörden können eingeschaltet werden, wenn durch den Drohneneinsatz die Verwirklichung von Straftatbeständen droht, wie beispielsweise bei der Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche (§ 201a des Strafgesetzbuches (StGB)), mithin Bereiche der Intimsphäre (im Einzelnen dazu: Bundestagsdrucksache 15/2466, S. 5.) oder der Aufzeichnung des nichtöffentlich gesprochenen Wortes (§ 201 StGB).

Der Düsseldorfer Kreis fordert daher Drohnenbetreiber auf, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Private Nutzer dürfen Drohnen mit Foto- oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann.

26.2 Orientierungshilfe: Videoüberwachung in öffentlichen Verkehrsmitteln

16. September 2015

Datenschutzgerechter Einsatz von optisch-elektronischen Einrichtungen in Verkehrsmitteln des öffentlichen Personennahverkehrs und des länderübergreifenden schienengebundenen Regionalverkehrs.

1. Vorbemerkung

Die Datenschutzbeauftragten des Bundes und der Länder sowie die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich hatten unter Beteiligung des Verbandes Deutscher Verkehrsunternehmen (VDV) im Jahre 2001 Empfehlungen zur Videoüberwachung in öffentlichen Verkehrsmitteln abgestimmt.

Unter Berücksichtigung der Erfahrungen aus der Anwendungspraxis sowie auch der technischen Entwicklungen auf dem Gebiet der Videoüberwachungstechnik der letzten Jahre halten die Aufsichtsbehörden eine Fortschreibung dieser Empfehlungen nunmehr für geboten. Zudem wurde der Anwendungsbereich der ursprünglich nur

für den öffentlichen Personennahverkehr (ÖPNV) geltenden Orientierungshilfe auf den länderübergreifenden schienengebundenen Regionalverkehr (SPNV) erweitert.

Im Spannungsfeld zwischen den berechtigten Interessen der Verkehrsunternehmen an einer Videoüberwachung und dem informationellen Selbstbestimmungsrecht ihrer Fahrgäste und Beschäftigten soll dieses Dokument eine datenschutzrechtliche Orientierung für den zulässigen Einsatz von Videoüberwachungseinrichtungen in öffentlichen Verkehrsmitteln geben.

2. Zulässigkeit der Videoüberwachung

Maßgebliche Vorschrift für die Prüfung der Zulässigkeit von Videoüberwachungsanlagen in öffentlichen Verkehrsmitteln ist § 6b des Bundesdatenschutzgesetzes (BDSG), sofern der Verkehrsbetrieb nicht öffentlich-rechtlich betrieben wird und deshalb die Zulässigkeit des Kameraeinsatzes nach Maßgabe des jeweiligen Landesdatenschutzgesetzes zu beurteilen ist.

Soweit Kameras auch Arbeitsplätze von Beschäftigten der Verkehrsunternehmen in öffentlichen Verkehrsmitteln miterfassen (z.B. Fahrerarbeitsplätze), findet neben dieser Vorschrift ggf. auch § 32 BDSG Anwendung. Zweckmäßig ist auch der Abschluss einer Betriebsvereinbarung.

2.1. Videoüberwachung in Fahrgastbereichen

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume, zu denen auch die Fahrgastbereiche in öffentlichen Verkehrsmitteln gehören, mit optisch-elektronischen Einrichtungen nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der davon betroffenen Personen überwiegen.

2.1.1 Wahrnehmung des Hausrechts oder berechtigter Interessen

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann zur Wahrnehmung des Hausrechts oder berechtigter Interessen insbesondere zur Verhinderung oder Verfolgung von Gewalt gegen Personen und Beförderungseinrichtungen sowie zur technischen Fahrgastsicherheit in Betracht kommen.

Eine Videobeobachtung (sog. Monitoring) kann erfolgen, um Personen davon abzuhalten, Rechtsverstöße zu begehen (z.B. Gewalt gegen Beschäftigte, Sachbeschädigungen an Beförderungseinrichtungen). Dieser Überwachungszweck wird auf direkte Weise erreicht, wenn das Geschehen in Echtzeit durch interventionsbereites Personal beobachtet und dadurch im Notfall ein schnelles Eingreifen möglich wird. -

Ist die Videoüberwachung als reine Aufzeichnungslösung ausgestaltet (sog. Black-Box-Lösung), so kann sie eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung von Schadensersatzansprüchen zu ermöglichen (Beweissicherung). Voraussetzung ist, dass eine Gefahrenlage schlüssig dargelegt werden kann bzw. dass Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit Straftaten zu rechnen ist. Insoweit sind konkrete Tatsachen zu fordern, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vor-

kommnisse (z.B. Missbrauch von Notbrems- oder Notrufeinrichtungen) in der Vergangenheit. Ratsam ist es daher, entsprechende Ereignisse sorgfältig zu dokumentieren (Datum, Art und Ort des Vorfalls, Schadenshöhe) oder etwaige Strafanzeigen aufzubewahren.

2.1.2 Erforderlichkeit der Videoüberwachung

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist stets einzelfallbezogen zu prüfen, ob sie für den verfolgten Zweck tatsächlich erforderlich ist. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn die Überwachung geeignet ist, das festgelegte Ziel zu erreichen, und es hierfür kein milderes, in die Rechte der Betroffenen weniger einschneidendes Mittel gibt.

Wenn der Zweck ausschließlich in der Beobachtung des Geschehens in Echtzeit zur direkten Intervention besteht, ist nur eine Monitoring-Lösung geeignet; eine reine Black-Box-Ausgestaltung der Videoüberwachung eignet sich wiederum zur Aufklärung von Straftaten.

Vor dem Einsatz einer Videoüberwachungsanlage müssen sich die Verkehrsunternehmen insbesondere mit zumutbaren alternativen Methoden auseinandersetzen, die in das informationelle Selbstbestimmungsrecht der Fahrgäste weniger eingreifen.

So kann der regelmäßige Einsatz von Personal dem Schutzbedürfnis der Fahrgäste ebenso gut Rechnung tragen wie der Einsatz von Überwachungskameras. Auch die Verwendung besonders widerstandsfähiger Sitze/Sitzbezüge sowie eine spezielle Oberflächenbeschichtung können Vandalismusschäden vorbeugen. Zudem kann eine nur temporäre Videoüberwachung (z.B. nur zu bestimmten Tages- bzw. Nachtzeiten) oder der Kameraeinsatz nur auf besonders gefährdeten Linien oder beschränkt auf schlecht einsehbare Fahrgastbereiche ausreichen. Denkbar ist es, zu Zeiten oder auf Linien, in denen eine permanente Videoüberwachung nicht erforderlich ist, die Möglichkeit einer anlassbezogenen Aktivierung der Videoüberwachung durch einen Notfallschalter für den Fahrzeugführenden oder das Begleitpersonal vorzusehen.

Nicht erforderlich ist eine Videoüberwachung zur Abwehr von Haftungsansprüchen gegen das Verkehrsunternehmen. Der Einsatz von Kameras kann nicht damit begründet werden, dass die Aufzeichnungen benötigt werden, um (unberechtigte) Ansprüche von Fahrgästen wegen Sturzverletzungen oder Beschädigungen persönlicher Gegenstände infolge (angeblich) starker Bremsungen o.Ä. abzuwehren. Zunächst ist der Betroffene in der Pflicht, seine Schadensersatzansprüche zu begründen und den Nachweis zu erbringen, dass sein Sturz unter den gegebenen Umständen für ihn unvermeidbar war und durch das Verkehrsunternehmen verursacht worden ist. Videoaufnahmen zum Beweis des Gegenteils bedarf es daher nicht.

Schließlich ist eine Videoüberwachung allein zur Steigerung des subjektiven Sicherheitsgefühls der Fahrgäste unter dem Gesichtspunkt der Erforderlichkeit nicht geboten.

Ist unter Berücksichtigung dieser Kriterien die Erforderlichkeit einer Videoüberwachung insgesamt oder im vorgesehenen Umfang zu verneinen, so ist der Einsatz von Videokameras unzulässig, ohne dass es noch auf die Frage ankommt, ob ihr schutzwürdige Interessen der Betroffenen entgegenstehen.

2.1.3 Beachtung der schutzwürdigen Interessen der Betroffenen

Auch wenn eine Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen im Einzelfall erforderlich sein sollte, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen.

Vorzunehmen ist eine Abwägung zwischen den berechtigten Interessen der Verkehrsunternehmen und dem informationellen Selbstbestimmungsrecht der von einer Videoüberwachung betroffenen Fahrgäste. Dabei darf die Intensität der Grundrechtsbeschränkung aufgrund der Überwachungsmaßnahme nicht außer Verhältnis zu dem Gewicht des Überwachungsinteresses stehen. Bei der Abwägung sind die Gesamtumstände jedes Einzelfalls maßgeblich. Entscheidend ist insbesondere die Eingriffsintensität der jeweiligen Maßnahme. Diese wird durch Art und Umfang der erfassten Informationen (Informationsgehalt und Informationsdichte), durch Anlass und Umstände der Erhebung (zeitliches und räumliches Ausmaß des Videoeinsatzes), durch den betroffenen Personenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt.

So stellt eine zeitlich und räumlich lückenlose Überwachung des Fahrgastraumes, der sich die Fahrgäste nicht entziehen können, einen intensiveren Eingriff dar als eine nur zeitweilige Beobachtung, die nur Teilbereiche des Raumes erfasst. Dasselbe gilt hinsichtlich der typischen Aufenthaltsdauer der Fahrgäste im Verkehrsmittel: je länger der Beförderungsvorgang andauert, desto intensiver ist der von einer Videoüberwachung ausgehende Eingriff in das Recht auf informationelle Selbstbestimmung der Fahrgäste. Die informationelle Selbstbestimmung wird zudem besonders intensiv bei der Überwachung von Bereichen betroffen, in denen Menschen typischerweise miteinander kommunizieren. Hinzu kommt, dass die Fahrgäste häufig auf die Nutzung öffentlicher Verkehrsmittel angewiesen sind und nur bedingt auf andere Verkehrsmittel ausweichen können. Zudem wird durch eine Videoüberwachung in öffentlichen Verkehrsmitteln eine Vielzahl von Personen betroffen, die durch ihr Verhalten keinerlei Anlass für eine solche Überwachungsmaßnahme bieten.

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann daher nur zum Schutz von Rechtsgütern erheblichen Gewichts gerechtfertigt sein.

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist im Rahmen einer abwägenden Einzelfallprüfung nach Strecken, Tageszeiten und Fahrzeugbereichen zu differenzieren und gemäß § 6b BDSG entsprechend zu beschränken. Maßstab für eine Differenzierung können beispielsweise die Anzahl von Vorkommnissen, Schadenshöhe sowie Art von Ereignissen in der Vergangenheit (Sachbeschädigung, Missbrauch von Notrufeinrichtungen etc.) sein. Eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereichs ist daher nach § 6b BDSG in aller Regel unverhältnismäßig und somit unzulässig. Bei der Beschaffung einer Videoüberwachungseinrichtung sollte darauf geachtet werden, dass die technischen Möglichkeiten für eine Differenzierung bestehen.

Da sich die Intensität des von einer Videoüberwachung ausgehenden Eingriffs in das informationelle Selbstbestimmungsrecht der Fahrgäste durch eine längere Aufenthaltsdauer in überwachten Bereichen deutlich erhöht, kann auf längeren Strecken - wie beispielsweise dem länderübergreifenden Bahnbetrieb - eine Videoüberwachung nur auf Streckenabschnitten mit häufigen und schwerwiegenden Eingriffen in

Rechtsgüter erheblichen Gewichts in Betracht kommen. Nur geringfügige oder vereinzelt auftretende Beeinträchtigungen dieser Rechtsgüter können dort keine Videoüberwachung der Fahrgastbereiche rechtfertigen. Eine solche kann aufgrund ihrer hohen Eingriffsintensität auf längeren Streckenabschnitten allenfalls in Ausnahmefällen erfolgen.

2.2. Videoüberwachung von Beschäftigten

Sofern in öffentlichen Verkehrsmitteln auch Arbeitsplätze von Beschäftigten von optisch-elektronischen Einrichtungen erfasst werden (z.B. der zum Zutritt für Fahrgäste hin offene Fahrerplatz in Bussen), ist Folgendes zu beachten:

In Fällen, in denen die Erfassung der Arbeitsplätze der Beschäftigten lediglich eine Nebenfolge der zulässigen Überwachung des Publikumsverkehrs darstellt, ist das Einrichten von sog. Privatzonen, d.h. das dauerhafte Ausblenden von Bereichen, in denen sich nur die Beschäftigten aufhalten, erforderlich. Vorzugsweise ist die Kamera jedoch so zu installieren, dass sich kein ständiger Arbeitsplatz im Erfassungsbereich befindet.

Wird ausschließlich der Fahrerarbeitsplatz (z.B. der durch eine Tür vom Fahrgastraum getrennte Fahrzeugführerstand) durch Kameras erfasst, richtet sich die datenschutzrechtliche Zulässigkeit einer solchen Maßnahme nach § 32 BDSG. Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten der Beschäftigten durch eine Videoüberwachungsanlage kann allerdings in der Regel nicht auf § 32 Abs. 1 Satz 1 BDSG gestützt werden. Denkbar ist zwar eine offene Videoüberwachung zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber seinen Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Davon kann bei einem abgeschlossenen Fahrerarbeitsplatz jedoch in aller Regel nicht ausgegangen werden. Selbst wenn in Ausnahmefällen hier eine Videoüberwachung in Betracht kommen sollte, ist der Erfassungsbereich der Kamera auf den sicherheitsrelevanten Bereich zu beschränken und der Beschäftigte ist auszublenden.

Im Übrigen dürfen personenbezogene Daten eines Beschäftigten insbesondere mittels Videoüberwachung nur zur Aufdeckung einer Straftat nach Maßgabe des § 32 Abs. 1 Satz 2 BDSG erhoben, verarbeitet oder genutzt werden. Erforderlich sind hier zu dokumentierende tatsächliche Anhaltspunkte, die den Verdacht begründen, dass der Beschäftigte 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. Liegen diese Voraussetzungen vor, ist eine Videoüberwachung gleichwohl nur für einen befristeten Zeitraum zulässig, sofern diese Maßnahme das einzige Mittel zur Überführung eines der Begehung von Straftaten konkret verdächtigten Beschäftigen darstellt. Eine dauerhafte Videoüberwachung von Beschäftigten ohne konkreten Verdacht ist hingegen datenschutzwidrig. Insbesondere dürfen Kameras nicht zur Kontrolle von Arbeitsleistungen, Sorgfalt und Effizienz verwendet werden.

Vor diesem Hintergrund muss das Verkehrsunternehmen nicht zuletzt auch dafür Sorge tragen, dass mittels der in den Fahrzeugen installierten Kameras keine Überwachung des in den Betriebshöfen mit der Reinigung, Reparatur und Wartung beauftragten technischen Personals erfolgen kann. Dies kann beispielsweise durch den

Einbau diesbezüglicher Werkstattschalter oder die Kopplung des Kamerabetriebs an die Eingabe einer Linienkennung erreicht werden.

3. Maßnahmen vor Einrichtung einer Videoüberwachung

Die Verantwortung für eine datenschutzgerechte Videoüberwachung liegt auch dann beim Verkehrsunternehmen, wenn es Fahrzeuge mit eingebauter Videoüberwachungstechnik, die von anderer Seite, z.B. von der die Verkehrsleistung beauftragenden lokalen Nahverkehrsgesellschaft (LNVG) zur Verfügung gestellt worden sind, verwendet. Daher obliegt es auch dem Verkehrsunternehmen, vor der Inbetriebnahme von Videoüberwachungskameras den damit verfolgten Zweck in einer Verfahrensbeschreibung festzulegen.

3.1. Betrieblicher Datenschutzbeauftragter

Der oder die betriebliche Datenschutzbeauftragte des Verkehrsunternehmens ist über die geplante Einrichtung einer Videoüberwachung rechtzeitig zu unterrichten, da hier die Zuständigkeit für die Durchführung der Vorabkontrolle liegt (§ 4d Abs. 5 und 6 BDSG). Er oder sie trägt außerdem dafür Sorge, dass eine Beschreibung des Verfahrens "Videoüberwachung" mit den Angaben nach § 4e Satz 1 Nrn. 1 bis 8 BDSG auf Antrag jedermann in geeigneter Weise verfügbar gemacht wird.

3.2. Information der Fahrgäste

An jedem Fahrzeug, das videoüberwacht wird, müssen Hinweisschilder/Piktogramme/Displays außen die Videoüberwachung kenntlich machen (vgl. § 6b Abs. 2 BDSG).

Der Hinweis ist so anzubringen, dass der Fahrgast ihn beim Eintritt in den überwachten Bereich im normalen Blickwinkel hat und nicht erst von ihm gesucht werden muss, auch bei geöffneten Türen. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen.

Durch geeignete Maßnahmen muss die verantwortliche Stelle mit Anschrift erkennbar sein. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte wenden kann. Daher ist die verantwortliche Stelle mit ihren Kontaktdaten explizit zu nennen.

3.3. Dienstanweisung

Erforderlich ist eine Dienstanweisung, in der alle mit der Videoüberwachung zusammenhängenden Fragen und Probleme geregelt werden.

In der Dienstanweisung müssen unter anderem auch die zu benutzenden Datenträger, auf denen die Speicherung der Bilddaten erfolgen soll, festgelegt werden. Außerdem müssen die besonderen Gründe festgelegt werden, aufgrund derer die Beweis sichernden Bilder der Aufzeichnung entnommen und auf einen neuen Datenträger übertragen werden dürfen sowie wann die Aufzeichnung zu löschen ist. Die Beschäftigten, die Zugang zu den Aufzeichnungen haben, müssen mit ihrer Funkti-

onsbezeichnung (nicht namentlich) bestimmt werden. Schließlich soll die verantwortliche Person bestimmt sein, die eine zu Beweiszwecken identifizierte Person zu benachrichtigen hat (§ 6b Abs. 4 BDSG).

3.4. Mitbestimmung durch die Betriebs- / Personalvertretung

Bei der Videoüberwachung von Beschäftigten handelt es sich regelmäßig um eine Maßnahme, die zur Überwachung des Verhaltens und der Leistung der Beschäftigten geeignet ist. Ihre Einführung und Anwendung unterliegt gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) der Mitbestimmung durch den Betriebsrat. In einer Betriebsvereinbarung sollte deshalb darauf hingewirkt werden, dass die Datenerhebung und die Auswertung in so engen Grenzen gehalten werden wie möglich. Dabei werden folgende Punkte als Bestandteil einer Betriebsvereinbarung festzulegen sein:

- Gegenstand der Datenerhebung, -verarbeitung oder -nutzung
- Art und Umfang der erhobenen, verarbeiteten oder genutzten Daten
- Zweckbeschreibung
- Datenvermeidung- und Datensparsamkeit
- Empfängerin und/oder Empfänger der Daten
- Rechte der Betroffenen
- Löschungsfristen
- Beschreibung der technischen und organisatorischen Maßnahmen (Anlage zu § 9 Abs. 1 BDSG), insbesondere Erstellung eines Berechtigungskonzepts.

Eine solche Betriebsvereinbarung wird dazu beitragen, die Erfüllung der gemeinsamen Aufgaben von Arbeitgeberin bzw. Arbeitgeber und Betriebsrat sicherzustellen, die freie Entfaltung der Persönlichkeit der im Betrieb Beschäftigten zu schützen und zu fördern (§ 75 Abs. 2 BetrVG).

In Unternehmen ohne Betriebsrat sollten Arbeitgeberinnen und Arbeitgeber Regelungen in Dienstanweisungen treffen.

4. Durchführung einer zulässigen Videoüberwachung

4.1. Löschungspflicht

Bei der nicht anlassbezogenen Aufzeichnung in einer Black-Box erfolgt – sofern kein Vorkommnis festgestellt wird – die Löschung der Aufzeichnung ohne Kenntnisnahme der aufgezeichneten Bilder unverzüglich.

Die Frist beginnt spätestens, wenn sich das Verkehrsmittel nicht mehr im täglich festgelegten Einsatz befindet und eine Überprüfung etwaiger Vorkommnisse durch eine verantwortliche Person möglich ist. Die Löschung soll daher im Regelfall nach 48 Stunden erfolgen. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, wenn beispielsweise das Verkehrsmittel nicht innerhalb dieser Frist zu einem Ort zurückkehren kann, an dem festgestellte und aufgezeichnete Vorfälle gesondert gesichert werden können.

Im Falle einer anlassbezogenen Aufzeichnung (ob mit oder ohne Historie) erfolgt die Löschung unverzüglich nach Prüfung der Bilder zum Zwecke der Beweissicherung; hierzu geeignete Bilder werden auf einem neuen Datenträger gespeichert und die Übrigen unverzüglich gelöscht.

4.2. Unterrichtungspflicht

Werden die Kameraaufnahmen einer bestimmten Person zugeordnet, ist diese Person darüber zu unterrichten (§ 6b Abs. 4 BDSG). Zweck dieser Regelung ist es, der identifizierten Person die Überprüfung der Rechtmäßigkeit der Datenverarbeitung und die Verfolgung ihrer Rechte zu ermöglichen. Inhaltlich geht die Unterrichtungspflicht über die Hinweispflicht hinaus. Die Unterrichtung hat über die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verarbeitenden Stelle zu erfolgen.

4.3. Übermittlung von Videosequenzen an Polizei und Staatsanwaltschaft

Nach § 6b Abs. 3 Satz 2 BDSG können gespeicherte Videoaufnahmen zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten an Polizei oder Staatsanwaltschaft herausgegeben werden.

Können bzw. müssen angeforderte Videosequenzen zulässigerweise an Polizei oder Staatsanwaltschaft herausgegeben werden, so müssen der Grund der Übermittlung, Art und Umfang der übermittelten Videodaten, Speichermedium sowie der Zeitpunkt der Übergabe und der Name der die Daten im Empfang nehmenden Person dokumentiert werden (vgl. Anlage zu § 9 BDSG).

4.4. Ausschreibungen

In Ausschreibungen, insbesondere durch die Verkehrsgesellschaften der Länder als Aufgabenträger für den schienengebundenen Personennahverkehr (SPNV), sind die Grundsätze dieser Orientierungshilfe zu beachten. Ausschreibungen, die z.B. pauschal eine „möglichst umfassende" Videoüberwachung fordern, entsprechen diesen Grundsätzen nicht und richten sich auf Videoüberwachungsmaßnahmen, die mit § 6b BDSG nicht zu vereinbaren sind.

4.5. Überprüfung der Rechtmäßigkeitsvoraussetzungen

Verkehrsunternehmen, die in ihren Fahrzeugen eine Videoüberwachungsanlage betreiben, sind verpflichtet, die rechtlichen Voraussetzungen für deren Betrieb in regelmäßigen Abständen zu überprüfen. Insbesondere die Frage der Erforderlichkeit der Maßnahme ist zu evaluieren. Lassen sich zum Beispiel nach Ablauf eines Jahres, in dem die Kameras in Betrieb waren, keine Tatsachen (mehr) feststellen, welche die Annahme rechtfertigen, dass das überwachte Objekt gefährdet ist, oder wurde der mit der Überwachung angestrebte Zweck nicht erreicht, darf die Videoüberwachungsanlage nicht weiter betrieben werden. Das Ergebnis der Überprüfung sollte dokumentiert werden.

26.3 Beschluss: Videoüberwachung in Schwimmbädern

10. August 2015

Zusatz zur Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen" des Düsseldorfer Kreises vom 19. Februar 2014, Stand: 10. August 2015.

Da der Besuch von Schwimmbädern auch mit einigen Risiken verbunden sein kann, greifen viele Betreiber zum Hilfsmittel der Videoüberwachung, sei es, beispielsweise, um den Aufbruch von Spinden oder die unsachgemäße Benutzung der Rutsche zu verhindern. Schwimmbäder, die sich in öffentlicher Trägerschaft befinden, sind nach dem geltenden Landesrecht zu prüfen.

Ansonsten findet das Bundesdatenschutzgesetz (BDSG) Anwendung, weshalb die in der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen" des Düsseldorfer Kreises (OH Videoüberwachung) beschriebenen Grundsätze für diese Schwimmbäder anwendbar sind.

Der Großteil der in Schwimmbädern befindlichen Kameras überwacht Bereiche, die für die Kunden zugänglich sind. Für diese öffentlich zugänglichen Räume beurteilt sich die datenschutzrechtliche Zulässigkeit nach § 6b BDSG.

Da sich die Schwimmbadbesucher im Schwimmbad zum Zweck der Freizeitgestaltung aufhalten, genießen sie besonderen Schutz (vgl. OH Videoüberwachung) und die Prüfung des Vorliegens der gesetzlichen Voraussetzungen bedarf besonderer Sorgfalt. Nach § 6b BDSG muss die Videoüberwachung zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Unabhängig von der Frage eines berechtigten Interesses oder der befugten Hausrechtsausübung ist eine Videoüberwachung jedenfalls nicht erforderlich zur Verhinderung des unberechtigten Zutritts zu Bereichen, für die ein zusätzliches Entgelt (z.B. zum Saunabereich) zu entrichten ist. Dies kann durch andere geeignete Maßnahmen, wie hohe Drehkreuze oder Schranken ohne unverhältnismäßigen Aufwand verhindert werden.

Besonderes Augenmerk ist auf das erforderliche Maß der Überwachung zu richten: Sofern die übrigen Voraussetzungen vorliegen, ist der Aufnahmebereich der Kamera ausschließlich auf den Bereich (z. B. Kassenautomaten) zu richten, den der Zweck der Videoüberwachung betrifft. Zur Sicherung von Beweisen im Falle von Einbrüchen reicht eine Videoaufzeichnung außerhalb der Öffnungszeiten.

Zur Abwehr von den mit dem Baden verbundenen Gefahren ist eine Videoaufzeichnung nicht erforderlich. Im Ausnahmefall kann eine reine Beobachtung („verlängertes Auge") zulässig sein, wenn sie der Unterstützung der Badeaufsicht an besonders gefährlichen oder unübersichtlichen Orten dient. Die Gefährlichkeit dieser Stellen muss sich aufgrund objektiver Anhaltspunkte ergeben, beispielsweise, weil es bereits konkrete Vorfälle gegeben hat oder Erfahrungswerte für eine erhöhte Gefährlichkeit (wie z. B. bei Sprungtürmen, Rutschen, Kinderbecken) sprechen. Nicht ausreichend

ist die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser. Der Einsatz von Videoüberwachungstechnik kann kein Ersatz für Aufsicht durch Personal sein!

Eine Videoaufzeichnung ausschließlich zum Ausschluss des Haftungsrisikos gegenüber Ansprüchen von Badegästen ist aufgrund der überwiegenden schutzwürdigen Interessen der von der Videoüberwachung Betroffenen unzulässig. Es ist nicht verhältnismäßig, einen derartigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung für eine große Zahl von Personen hinzunehmen, nur, damit das Schwimmbad im Zweifel die Möglichkeit hat, seine Haftung auszuschließen. Eine Haftung unterliegt zudem der Beweispflicht des Geschädigten. Die Rechtsprechung fordert keinen Nachweis der hinreichenden Wahrnehmung der Verkehrssicherungspflicht mit Videoaufzeichnungen[104].

Schutzwürdige Interessen der Betroffenen überwiegen immer, wenn die Intimsphäre des Betroffenen berührt ist, weswegen eine Videoüberwachung von Personen in Sanitärräumen, Umkleidekabinen oder Umkleidebereichen und in der Sauna generell unzulässig ist.

Eine Videoüberwachung kann im Einzelfall zur Sicherung von Beweismitteln bei nachgewiesenen Spindaufbrüchen zulässig sein, sofern nicht gleichzeitig Bänke/Ablageflächen oder Umkleidebereiche erfasst werden. Voraussetzung ist, dass den Badegästen eine echte Wahlmöglichkeit eingeräumt wird, in welchen Bereich sie sich begeben. Dabei sind Bereiche, die videoüberwacht werden, von solchen, in denen keine Überwachung stattfindet, erkennbar zu trennen, beispielsweise durch farbige Markierung des Fußbodens.

Unverhältnismäßig und damit nicht zulässig ist jedenfalls die Videoüberwachung aufgrund von Bagatellschäden (z.B. Beschädigung von Haartrocknern).

Darüber hinaus sind die in der OH Videoüberwachung unter Ziffer 2.2 benannten Maßnahmen (z.B. Verfahrensverzeichnis, Vorabkontrolle, Hinweisbeschilderung) zu beachten. Dazu gehört auch, Bildschirme so zu positionieren, dass sie nicht für Dritte einsehbar sind.

---

[104] OLG Koblenz, Beschluss vom 7. Mai 2010, Az.: 8 U 810/09: Der Betreiber genügt seiner Verkehrssicherungspflicht, wenn durch Hinweisschilder mit ausformulierten Warnhinweisen oder mit Piktogrammen auf die Problempunkte eindeutig hingewiesen wird; LG Münster, Urteil vom 17. Mai 2006, Az.: 12 O 639/04:
Der Betreiber eines Schwimmbads genügt seiner Verkehrssicherungspflicht, wenn er einen Bademeister bereitstellt, der sein Augenmerk auch - wenn auch nicht ununterbrochen - auf die besonderen Schwimmbadeinrichtungen (hier: ins Nichtschwimmerbecken führende Kinderrutsche) richtet.

26.4 Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen

März 2016

Diese Orientierungshilfe enthält Hinweise zur datenschutzgerechten Formulierung und Gestaltung von schriftlichen Einwilligungserklärungen nach § 4a Bundesdatenschutzgesetz (BDSG) und elektronischen Texten nach § 13 Abs. 2 und Abs. 3 des Telemediengesetzes (TMG). Einwilligungen in Übermittlungen in Drittstaaten werden von dieser Orientierungshilfe nicht erfasst. Ergänzend sind gegebenenfalls die gesetzlichen Regelungen zu Allgemeinen Geschäftsbedingungen zu beachten.

In der täglichen Praxis der Datenschutzaufsichtsbehörden fällt immer wieder auf, dass in Antragsvordrucken von Firmen, Versicherungen, Banken, und anderen neben den vom Leistungsanbieter fest vorgegebenen Vertragsbedingungen die eventuell dazu ergänzend vorgesehenen datenschutzrechtlichen Einwilligungserklärungen nicht den Erfordernissen des § 4a BDSG entsprechen oder aber als „Einwilligungen" bezeichnete Texte vielmehr in Wirklichkeit als unabdingbare Vertragserklärungen bzw. allgemein geltende Geschäftsbedingungen einzustufen sind. Muss eine (AGB-rechtlich zulässige) Erklärung abgegeben bzw. Vertragsbedingung akzeptiert werden, um einen Vertrag abzuschließen, hat die betroffene Person also gar keine freie Wahlmöglichkeit, so handelt es sich nicht um eine datenschutzrechtliche Einwilligung nach § 4a BDSG, sondern um ein Vertragsangebot, das angenommen oder abgelehnt werden kann. Die mögliche Erlaubnis für den Datenumgang ergibt sich dann nicht aus § 4a BDSG, sondern aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG.

1. Überschriften

Bereits die Überschriften bringen häufig nicht klar genug zum Ausdruck, ob hier vom Antragsteller oder Kunden neben seiner hauptsächlichen Erklärung, beispielsweise dem Versicherungsantrag oder seiner Teilnahmeerklärung, noch zusätzlich eine datenschutzrechtliche Einwilligung abverlangt wird. Dies soll anhand einiger Negativbeispiele für Überschriften aufgezeigt werden:

- Datenschutzerklärung,
- Datenschutz,
- Datenschutzklausel,
- Hinweis zum Datenschutz,
- Erklärung zum Datenschutz,
- Erklärung zur Datenverarbeitung.

Im Gegensatz dazu weisen folgende dem § 4a BDSG entsprechende Positivbeispiele für Überschriften den Unterzeichnenden darauf hin, dass er mit Unterzeichnung eine datenschutzrechtliche Einwilligung abgibt:

- Einwilligungserklärung Datenschutz,
- Datenschutzrechtliche Einwilligungserklärung,
- Datenschutzrechtliche Einwilligungsklausel,
- Einwilligungserklärung nach dem Bundesdatenschutzgesetz.

2. Eindeutigkeit

Auch die Erklärung selbst ist zuweilen nicht eindeutig genug vorformuliert. So reicht es nicht aus, wenn sie mit den Worten beginnt: „Mir ist bekannt, dass ...". Hier ist dem Kunden nicht bewusst, dass er eine zusätzliche Erklärung abgibt.

Die notwendige Klarheit besteht nur, wenn die Formulierung den Erklärungscharakter eindeutig zum Ausdruck bringt, wie es in folgenden Positivbeispielen aufgezeigt wird:

- Ich willige ein, dass ...
- Ich bin einverstanden, dass ...
- Mit der Unterschrift geben Sie Ihre Einwilligung, dass ...
- Durch Ihre Unterschrift wird die vorstehende Einwilligungserklärung mit den auf der Rückseite abgedruckten näheren Erläuterungen zur Datenverarbeitung und Datennutzung für ... (Zweck) Bestandteil des Antrages.

Weiter muss es sich um eine bewusste Erklärung der betreffenden Person selbst handeln (Opt-In). Schon von der verantwortlichen Stelle im Sinne einer Zustimmung vorangekreuzte Einwilligungstexte oder nur mit einer Streich-/Abwahl-Möglichkeit versehene „vorgegebene Zustimmungen" (Opt-Out) genügen dem grundsätzlich nicht.

3. Freiwilligkeit

Eine wirksame datenschutzrechtliche Einwilligung im Sinne von § 4a BDSG liegt nur dann vor, wenn diese freiwillig abgegeben werden und auch jederzeit widerrufen werden kann. Eine unter Druck oder Zwang abgegebene datenschutzrechtliche Einwilligung ist unwirksam.

4. Hervorhebung

In zahlreichen vorformulierten Einwilligungserklärungen fehlt es an der gemäß § 4a Abs. 1 Satz 4 BDSG und - bei Einwilligung in Werbung - gemäß § 28 Abs. 3a Satz 2 BDSG erforderlichen besonderen Hervorhebung gegenüber anderen Textpassagen, zum Beispiel durch:

- Fettdruck, Schriftart oder Schriftgröße,
- farbliche Gestaltung der Schrift oder des Hintergrundes oder
- eine Umrahmung der Erklärung.

5. Platzierung

Die datenschutzrechtliche Einwilligungserklärung gehört als besondere beziehungsweise zusätzliche Willensäußerung der betroffenen Person in hervorgehobener Form (siehe unter Ziffer 4) grundsätzlich insgesamt auf das eigentliche Antragsformular und dort in aller Regel unmittelbar vor die Unterschrift, die dann sowohl die Hauptsacheerklärung (beispielsweise den Versicherungsantrag) als auch die datenschutzrechtliche Einwilligungserklärung abdeckt.

Denkbar ist aber auch bei längeren Einwilligungstexten eine besonders hervorzuhebende aussagekräftige Kurzfassung mit den wesentlichen Inhalten der datenschutzrechtlichen Einwilligungserklärung bei der Unterschrift mit einem Hinweis auf den beispielsweise auf der Rückseite oder auf einer Anlage enthaltenen erläuternden Text (siehe letztes Positivbeispiel unter Ziffer 2.).

Besonders datenschutzfreundlich - und in einzelnen Fallkonstellationen zwingend erforderlich (beispielsweise bei der beabsichtigten Übermittlung von Gesundheitsdaten) - ist es, wenn im Formular für die datenschutzrechtliche Einwilligung eine gesonderte Unterschrift vorgesehen ist.

Jedenfalls ist zur Sicherstellung der Eindeutigkeit und Freiwilligkeit (siehe Ziffern 2 und 3) erforderlich, dass die Einwilligungserklärung für ihre Gültigkeit ausdrücklich angenommen werden muss (beispielsweise durch ein Ankreuzen).

6. Trennung

In manchen Formularen werden die Datenschutzhinweise und -informationen nach § 4 Abs. 3 BDSG zu unabdingbaren Vertragsinhalten beziehungsweise allgemein geltenden Geschäftsbedingungen mit einer auf freiwilliger Basis abgefragten datenschutzrechtlichen Einwilligungserklärung nach § 4a BDSG vermischt. Unter der Überschrift „Datenschutzhinweise" beginnt der Text mit Hinweisen und geht dann im weiteren Verlauf unvermittelt in eine Einwilligungserklärung über.

Dem Betroffenen wird hier nicht deutlich genug vor Augen geführt, dass er eine datenschutzrechtliche Einwilligungserklärung abgeben soll. Die reinen Informationen über Datenverarbeitung auf der Grundlage von Gesetz beziehungsweise Vertrag auf der einen Seite und die freiwillige datenschutzrechtliche Einwilligungserklärung auf der anderen Seite müssen textlich getrennt dargestellt werden. Eine mangelnde Trennung kann dazu führen, dass die Einwilligung als solche nicht erkannt wird und deshalb unwirksam sein kann.

7. Klare Zuordnung

Die ansonsten korrekt gestaltete datenschutzrechtliche Einwilligungserklärung soll nicht mit Datenverwendungen aufgebläht werden, die gar nicht einwilligungsbedürftig sind, da sie bereits auf Grund eines Gesetzes oder einer sonstigen Rechtsvorschrift zulässig sind.

Es ist vielmehr eine klare Zuordnung zur Einwilligung einerseits und zu den Datenschutzinformationen nach § 4 Abs. 3 BDSG andererseits vorzunehmen. Ist es rechtlich strittig, ob eine Datenverwendung einer Einwilligung bedarf, bestehen keine Bedenken, sie unter Beachtung der oben genannten Formvorschriften „vorsichtshalber" in die Einwilligungserklärung mit einzubeziehen.

8. Einwilligung bei besonderen Arten personenbezogener Daten

Soweit sich die Einwilligung auf besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) beziehen soll, ist bei der formularmäßigen Gestaltung der Erklärung § 4a Abs. 3 BDSG zu beachten, das heißt die Einwilligung muss ausdrücklich auch für diese besonderen Arten personenbezogener Daten erklärt werden.

9. Inhalt von Einwilligungen

Der Text der Einwilligungserklärung muss die betroffene Person klar und allgemein verständlich über die zu verarbeitenden Daten und den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten durch die verantwortliche Stelle informieren, und muss, soweit nach den Umständen des Einzelfalls erforderlich, auf

eventuelle Folgen der Verweigerung der Einwilligung hinweisen (§ 4a Abs. 1 Satz 2 BDSG).

Auf die grundsätzlich gegebene Widerrufsmöglichkeit der Einwilligung ist hinzuweisen; im Bereich der Telemedien ist ein solcher Hinweis durch § 13 Abs. 3 TMG sogar ausdrücklich vorgeschrieben (siehe bei Nr. 10).

Wenn im Rahmen der Verarbeitung auch Datenübermittlungen an Dritte in Betracht kommen, sind die Datenübermittlungen mit deren Zweckbestimmung und die Empfänger der Daten transparent zu erläutern.

Eine undifferenzierte, nicht mehr überschaubare Darstellung einer großen Anzahl genannter Datenempfänger kann den Transparenzanforderungen widersprechen und nach der zivilrechtlichen Rechtsprechung zu einer Unwirksamkeit der Einwilligung führen.

10. Einwilligung bei Telemedienangeboten

Wird eine Einwilligung elektronisch im Rahmen eines Telemedienangebotes eingeholt (beispielsweise auf einer Webseite), so sind gemäß § 13 Abs. 2 und Abs. 3 TMG einige Besonderheiten zu beachten:

Danach muss der Diensteanbieter sicherstellen, dass

- der Nutzer die Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen und
- mit Wirkung für die Zukunft widerrufen kann.

Der Nutzer muss zudem vor Erklärung der Einwilligung auf sein jederzeitiges Widerrufsrecht hingewiesen werden, wobei diese Information für den Nutzer jederzeit abrufbar sein muss. Diese Unterrichtung kann beispielsweise in der Datenschutzerklärung erfolgen.

11. Werbeeinwilligungen

Hierzu wird auf die ergänzenden Regelungen in § 28 Abs. 3a und 3b BDSG hingewiesen. Siehe insoweit auch die Ziffern 2 und 4 der Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke.[105]

[105] Vgl. Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke, Stand: September 2014, unter: https://www.lda.bayern.de/media/ah_werbung.pdf.

27 Konferenzen der Informationsfreiheitsbeauftragten des Bundes und der Länder

27.1 Entschließung: Auch Kammern sind zur Transparenz verpflichtet!

30. Juni 2015

Immer wieder verweigern sich berufsständische Kammern den Transparenzanforderungen der jeweiligen Informationszugangsgesetze. Berufsständische Kammern nehmen hoheitliche Aufgaben auf Bundes- und Länderebene wahr. Für die jeweiligen Berufsgruppen besteht eine gesetzliche Pflicht zur Mitgliedschaft, die Kammern sind für Berufszulassungen zuständig und haben oft weitgehende Sanktionsmöglichkeiten.

Informationen, die im Rahmen ihrer Tätigkeit anfallen, unterfallen den Informationszugangsgesetzen von Bund und Ländern. Dies gilt auch für Jahresabschlüsse und Angaben zu Einnahmen, Ausgaben und Rückstellungen der Kammern. Für die Verpflichtung der Kammern ist es unerheblich, ob Antragstellende Kammermitglieder sind und welche Motive zur Antragstellung führten. Öffentlich-rechtliche Körperschaften befinden sich in weiten Bereichen nicht in Konkurrenz zu Marktteilnehmern – Wettbewerbsnachteile können sich zumeist nicht ergeben. Folglich stehen schutzwürdige Betriebs- und Geschäftsgeheimnisse einem Informationszugang in der Regel nicht entgegen.

Ansprüche auf Informationszugang sind unverzüglich, spätestens jedoch innerhalb der in den Informationszugangsgesetzen des Bundes bzw. der Länder genannten Fristen zu erfüllen. Eine Entscheidung darf nicht auf Gremiensitzungen verschoben, sondern sollte im Rahmen der regulären Geschäftsführung getroffen werden. Im Übrigen sind transparenzpflichtige Informationen der berufsständischen Kammern in den bereits vorhandenen Informationsregistern zu veröffentlichen.

Die Informationsfreiheitsbeauftragten in Deutschland fordern daher die berufsständischen Kammern auf, ihren Transparenzverpflichtungen nachzukommen.

27.2 Entschließung: Mehr Transparenz bei den Verhandlungen über das Transatlantische Freihandelsabkommen (TTIP)!

30. Juni 2015

Die Bundesregierung hat sich dafür ausgesprochen, noch im Jahr 2015 das geplante Freihandelsabkommen (Transatlantic Trade and Investment Partnership, TTIP) zwischen der EU und den Vereinigten Staaten von Amerika zu verabschieden. Mit dem geplanten Abkommen würde die derzeit weltgrößte Freihandelszone entstehen.

Seit der Aufnahme der Verhandlungen zwischen der EU und den USA im Jahr 2013 wurden deren Intransparenz und der spärliche Informationsfluss kritisiert. Als Reaktion auf diese Kritik hat die EU-Handelskommissarin Cecilia Malmström im November 2014 mehr Transparenz versprochen. In diesem Rahmen hat sich die Europäische Kommission dazu verpflichtet, die Öffentlichkeit darüber zu informieren, mit wem sich ihre führenden Politiker und höheren Beamten treffen und einen erweiterten Zugang zu Dokumenten im Zusammenhang mit den Verhandlungen über eine transatlantische Handels- und Investitionspartnerschaft mit den Vereinigten Staaten zu ermöglichen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) sieht diese Initiative als einen wichtigen ersten Schritt hin zu mehr Offenheit und mahnt deren Fortführung und Ausweitung dringlich an. Sie hebt die Notwendigkeit größtmöglicher Transparenz in den Verhandlungen für eine lebendige öffentliche Debatte hervor, in der die Bürgerinnen und Bürger vollständig über die Auswirkungen auf ihr tägliches Leben informiert werden. Die Informationsfreiheitsbeauftragten fordern im Sinne von Open Government Data, der Öffentlichkeit neben zusammenfassenden und erläuternden Informationen vermehrt Originaldokumente zur Verfügung zu stellen, um es den Bürgerinnen und Bürgern zu ermöglichen, sich eine eigene Meinung von den Inhalten und dem Ablauf der Verhandlungen zu bilden. Hierzu gehören auch Informationen über die Positionen und Forderungen der USA sowie von Lobbyisten. Eine umfassende Offenlegung von Informationen zu TTIP auf EU- sowie auf Bundes-Ebene soll so früh und so weit wie möglich erfolgen. Erst wenn Originaldokumente aus den Bereichen Umwelt-, Arbeitnehmer- und Verbraucherschutz bekannt sind, kann beurteilt werden, ob es zu einer Absenkung europäischer Standards kommt.

Die IFK fordert die Bundesregierung und die Europäische Kommission dazu auf, in den Verhandlungen mit den USA darauf zu bestehen, dass für Streitigkeiten zwischen den Handelspartnern öffentlich tagende hoheitliche Gerichte geschaffen werden. Nur dadurch kann die notwendige Transparenz gewährleistet werden.

27.3 Entschließung: Informationsfreiheit 2.0 – endlich gleiches Recht in Bund und Ländern![106]

4. Dezember 2015

Vor zehn Jahren hat der Deutsche Bundestag das Informationsfreiheitsgesetz verabschiedet und damit für solche Länder, die bislang noch kein derartiges Gesetz kannten, ein Beispiel gegeben. Inzwischen besteht in elf Ländern ein Recht auf Zugang zu Verwaltungsinformationen, ohne dass die Antragsteller ihr Einsichtsinteresse begründen müssen.

Trotz einer flächendeckenden Entwicklung hin zu mehr Verwaltungstransparenz besteht weiterhin Handlungsbedarf. So zeigen weder Bayern noch Hessen Bestrebungen, Informationsfreiheitsgesetze zu schaffen. Die niedersächsische Landesregierung hat zwar beschlossen, einen Entwurf vorzulegen, berät aber noch über die Einzelheiten. In Sachsen soll bis spätestens 2019 ein Informationsfreiheitsgesetz geschaffen werden. Indes enttäuscht der lange erwartete Gesetzentwurf der baden-württembergischen Landesregierung durch viele überflüssige Einschränkungen. Das brandenburgische Beispiel zeigt, dass auch die Novellierung vorhandener Gesetze dazu dienen kann, das Rad durch die Schaffung neuer Ausnahmen zurückzudrehen. Die Umsetzung der Evaluation des Informationsfreiheitsgesetzes des Bundes steht noch aus. Ob dort – ebenso wie bereits in den Transparenzgesetzen von Hamburg und Bremen – Verwaltungen verpflichtet werden, bestimmte Informationen von sich aus im Internet zu veröffentlichen, ist ungewiss. In Rheinland-Pfalz tritt zum 01. Januar 2016 als erstem Flächenland ein solches Transparenzgesetz in Kraft. Es umfasst auch das im Übrigen bundesweit eingeführte Recht auf Zugang zu Umweltinformationen. Auch in Thüringen und Nordrhein-Westfalen ist laut Koalitionsvertrag beabsichtigt, das derzeitige Informationsfreiheitsgesetz zu einem Transparenzgesetz fortzuentwickeln.

Nach Auffassung der Informationsfreiheitsbeauftragten sollten moderne Regelungen über den Informationszugang in Form effektiver Transparenzgesetze

1. der herkömmlichen Informationserteilung auf Antrag eine Pflicht der Verwaltung zur proaktiven Veröffentlichung von Informationen in Open-Data-Portalen zur Seite stellen,
2. Ausnahmen vom freien Zugang zu Informationen nur in einem unbedingt erforderlichen Maß enthalten,
3. neben klassischen Verwaltungen auch Unternehmen der öffentlichen Hand einbeziehen und
4. der vorhandenen Rechtszersplitterung auf dem Gebiet der Informationsfreiheit entgegenwirken und das Umweltinformationsrecht mit dem Informationsfreiheitsrecht zusammenführen.

[106] Bei Stimmenenthaltung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Sowohl bei der Novellierung vorhandener als auch bei der Schaffung neuer Regelungen muss die Erhöhung der Transparenz oberstes Ziel sein. Nach Auffassung der Informationsfreiheitsbeauftragten gibt es keinen vernünftigen Grund dafür, dass einige Länder noch immer kein Recht auf voraussetzungslosen Zugang zu Informationen haben.

Die Informationsfreiheit hat dort, wo sie eingeführt wurde, zu mehr staatlicher Transparenz, einer besseren Informiertheit der Bürger und einer offeneren Verwaltungskultur geführt. Transparenzgesetze und Open-Data-Plattformen im Internet haben diese Wirkung in erfreulicher Weise befördert. Die Befürchtung von Kritikern, dass Verwaltungen von einer Antragsflut überrannt würden, hat sich nicht bewahrheitet.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Gesetzgeber in Bund und Ländern auf, die positiven Erfahrungen mit der Informationsfreiheit in Deutschland anzuerkennen und die Einheitlichkeit der Lebensbedingungen auch im Bereich der Verwaltungstransparenz herzustellen.

27.4 Entschließung: Auch die Verwaltungen der Landesparlamente sollen Gutachten der Wissenschaftlichen Dienste proaktiv veröffentlichen!

28. April 2016

Nach der aktuellen Rechtsprechung des Bundesverwaltungsgerichts (Urteil vom 25. Juni 2015, Az.: 7 C 1/14) muss die Bundestagsverwaltung auf Antrag Zugang zu den Ausarbeitungen der Wissenschaftlichen Dienste gewähren.

Wie der Deutsche Bundestag inzwischen bekannt gab, bedarf es derartiger individueller Anträge seit dem 18. Februar 2016 nicht mehr, denn die Bundestagsverwaltung veröffentlicht generell die Ausarbeitungen der Wissenschaftlichen Dienste nunmehr vier Wochen nach Auslieferung an die auftraggebenden Abgeordneten, damit diese zunächst die Möglichkeit haben, die Gutachten exklusiv nutzen zu können, proaktiv im Internet. Dabei werden die Namen der Auftraggeber nicht bekannt gegeben.

Die Entscheidung zur proaktiven Veröffentlichung ist im Sinne von Open Data und Transparenz nachdrücklich zu unterstützen, da es ein großes öffentliches Interesse an den Ausarbeitungen der Wissenschaftlichen Dienste gibt. So lagen infolge der neuen Rechtsprechung des Bundesverwaltungsgerichts der Bundestagsverwaltung in kürzester Zeit weit über 2.000 Informationszugangsanträge vor. Die individuelle Bearbeitung dieser Anträge hätte in aller Regel viel Zeit gebunden und unnötig hohe Personal- und Sachkosten verursacht. Durch die Entscheidung werden die Kosten sowohl für die Verwaltung als auch für die Bürgerinnen und Bürger deutlich gesenkt. Die Ausarbeitungen stehen der interessierten Öffentlichkeit zukünftig schnell und einfach zur Verfügung.

Vor diesem Hintergrund fordert die Konferenz der Informationsfreiheitsbeauftragten in Deutschland die Verwaltungen der Landesparlamente auf, dem Beispiel der Bundestagsverwaltung in Sachen Transparenz und Open Data zu folgen. Dabei sind et-

waige Ausschlussgründe (insbesondere durch Schwärzung der Namen der Auftraggeber) sowie landesrechtliche Vorgaben zu berücksichtigen. Auch die Verwaltungen der Landesparlamente sollten Ausarbeitungen der jeweiligen Wissenschaftlichen Dienste bzw. der Gesetzgebungs- und Beratungsdienste unabhängig von individuellen Zugangsanträgen im Internet veröffentlichen, soweit dies nicht bereits geschieht.

27.5 Entschließung: GovData: Alle Länder sollen der Verwaltungsvereinbarung beitreten und Daten auf dem Portal bereitstellen!

15. Juni 2016

„GovData – das Datenportal für Deutschland" ist eine Anwendung des IT-Planungsrats, die auf der Grundlage einer Verwaltungsvereinbarung vom Bund und mehreren Ländern betrieben wird. Das Portal bietet einen einheitlichen zentralen Zugang zu offenen Verwaltungsdaten aus Bund, Ländern und Kommunen. Ziel ist es, diese Daten möglichst flächendeckend zur Verfügung zu stellen und sie an einer zentralen Stelle auffindbar und so einfacher nutzbar zu machen. GovData dient damit nicht nur der Information der Bürgerinnen und Bürger, sondern fördert zugleich auch die Transparenz und Akzeptanz des Verwaltungshandelns. Es stellt der Wirtschaft darüber hinaus Verwaltungsdaten zur Entwicklung neuer Geschäftsmodelle zur Verfügung.

Bislang beteiligen sich jedoch an dem Bund-Länder-Online-Portal noch nicht alle Länder. Viele Daten, an deren Veröffentlichung ein großes öffentliches Interesse besteht, sind noch nicht abrufbar. Das immense wirtschaftliche Potential von Open Data bleibt ungenutzt.

Sowohl für die Wirtschaft als auch für die Zivilgesellschaft ergeben sich erhebliche Vorteile durch einen freien Zugang zu den öffentlichen Daten der Verwaltung. Der Umfang und die Qualität der in GovData zur Verfügung gestellten Daten müssen verbessert und der Nutzwert des Portals weiter erhöht werden.

Daher appelliert die Konferenz der Informationsfreiheitsbeauftragten in Deutschland an die verbleibenden Länder, der Verwaltungsvereinbarung beizutreten, und fordert alle Vereinbarungspartner zur verstärkten Bereitstellung von Daten auf.

28 Stichwortverzeichnis