TÄTIGKEITSBERICHT

2011/2012

BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT

5. Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht für die Jahre 2011 und 2012

Vorwort

Sie halten nunmehr den 5. Tätigkeitsbericht der bayerischen Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich in Ihren Händen. Schon an den Bezeichnungen der Herausgeber dieser Berichte ist der Einfluss der Europäischen Union auf das Datenschutzrecht erkennbar. Wurden die ersten beiden Berichte noch von der „Regierung von Mittelfranken - Bayerische Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich“ und der dritte Tätigkeitsbericht vom „Landesamt für Datenschutzaufsicht in der Regierung von Mittelfranken“ herausgegeben, stand beim 4. Tätigkeitsbericht und steht nun auch bei dem vorliegenden Tätigkeitsbericht das „Bayerische Landesamt für Datenschutzaufsicht“ (kurz: BayLDA) als Herausgeber im Impressum. Bei der Herausgabe des 4. Tätigkeitsberichts (2009 bis 2010) war das BayLDA organisatorisch noch ein Bestandteil der Regierung von Mittelfranken. Nach der Entscheidung des Europäischen Gerichtshofs vom 9. März 2010 (Az.: C-518/07), durch die die Bundesrepublik Deutschland verpflichtet wurde, die Datenschutzaufsicht auch im nicht-öffentlichen Bereich in völliger Unabhängigkeit auszugestalten, haben das Bayerische Staatsministerium des Innern und das Präsidium der Regierung von Mittelfranken bezüglich der inhaltlichen Amtsführung diese Entscheidung mit sofortiger Wirkung umgesetzt. Dabei wurde das BayLDA in die völlige Unabhängigkeit entlassen. Mit Inkrafttreten der Änderungen des Bayerischen Datenschutzgesetzes zum 1. August 2011 wurde das BayLDA auch in organisatorischer Hinsicht als unabhängige Behörde mit - wie es bei bayerischen Landesämtern üblich ist - einem Präsidenten an der Spitze geschaffen. Der vorliegende Bericht ist deshalb der erste Tätigkeitsbericht einer nicht nur inhaltlich, sondern auch organisatorisch völlig unabhängigen bayerischen Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich.

Wir Mitarbeiterinnen und Mitarbeiter des BayLDA haben trotz der o. g. organisatorischen Änderung nach wie vor im Fokus, dass wir es bei unserer Aufgabenerfüllung - anders als im öffentlichen Bereich - grundsätzlich mit zwei Grundrechtsträgern, d. h. den Unternehmen (verantwortliche Stellen) und den Bürgern (Betroffenen) zu tun haben, deren Rechte und Interessen zu wahren und auszugleichen sind. Wesentliche Änderungen gegenüber den bisherigen Tätigkeitsberichten, außer einer gesteigerten technischen Kompetenz unseres Amtes, sollten Sie in diesem Tätigkeitsbericht deshalb nicht erkennen.

Mit gespannter Erwartung sehen wir auf den laufenden europäischen Rechtsetzungsprozess, der von der Europäischen Kommission mit Vorlage des Entwurfs einer Datenschutz-Grundverordnung am 25. Januar 2011 in Gang gesetzt wurde. Der politische Wille des Europäischen Parlaments und des Europäischen Rates, diese Verordnung noch in der derzeit laufenden Legislaturperiode des Europäischen Parlaments zu verabschieden, scheint ausgesprochen groß zu sein. Welche Regelungen die Verordnung tatsächlich beinhalten wird, steht heute noch nicht fest. Sollte die endgültige Fassung aber in den wesentlichen Punkten dem Entwurf entsprechen, so kann schon heute festgestellt werden, dass nicht nur durch den in Deutschland fast völligen Wegfall der Verpflichtung, betriebliche Datenschutzbeauftragte zu bestellen, sondern auch durch sonstige Aufgaben für die Aufsichtsbehörden im Zusammenhang mit technischen Überprüfungen, Datenpannen und insbesondere Umgang mit Betroffenen aus anderen Mitgliedstaaten und der Koordination mit anderen Aufsichtsbehörden eine erhebliche Mehrarbeit auf die Aufsichtsbehörden zukommen dürfte. Hat sich im Verhältnis der Aufsichtsbehörden innerhalb der EU, ohne dass es dafür eine gesetzliche Regelung gäbe, die Kommunikation auf Englisch als Standard durchgesetzt, bleibt abzuwarten, wie die jeweiligen Aufsichtsbehörden mit Eingaben und Beschwerden von Bürgern anderer Mitgliedstaaten in deren Landessprache umgehen werden.

Die Globalisierung und Vernetzung und damit auch der Datenverkehr haben in den letzten Jahren mit enormen Steigerungsraten zugenommen. Zwangsläufig häufen sich dadurch die datenschutzrechtlichen Fragestellungen. Gleichzeitig ist aber auch festzustellen, dass in der Gesellschaft das Verständnis darüber, wie weit ein staatlich zu schützender Bereich des allgemeinen Persönlichkeitsrechts im privaten Umfeld besteht, einem laufenden Wandel unterzogen ist. Damit umzugehen ist und bleibt spannend. Dies gilt ebenso, wenn Datenschutzbeschwerden als Mittel zum Austragen sonstiger Konflikte erhoben werden oder wenn wie im Bereich des internationalen Datenverkehrs festzustellen ist, dass sich die Realität von den für uns verbindlichen rechtlichen Rahmenbedingungen uneinholbar weit entfernt hat. Zu beachten haben wir auch, dass wir den selbstbestimmenden mündigen Bürger nicht in einem Umfang vor sich selbst oder vor etwas schützen, was er nicht möchte und ihn damit bevormunden.

In diesem Sinne bedanken wir uns bei allen, die uns bei dieser Gratwanderung kritisch begleiten, sei es in persönlichen Gesprächen, bei Sitzungen der Erfa-Kreise oder sonstigen Veranstaltungen. Mit dem vorliegenden Tätigkeitsbericht informieren wir über unsere Arbeit in den letzten beiden Jahren und beziehen damit öffentlich Stellung zu für uns wesentlichen Vollzugsfragen im Datenschutzrecht. Wir bitten um Verständnis, dass wir wegen der leichteren Lesbarkeit im Rahmen der allgemeinen Ausführungen bei geschlechtsspezifischen Bezeichnungen nur die männliche Form verwendet haben. Wir hoffen, dass unsere Ausführungen Ihr Interesse finden und bedanken uns für Ihre Rückmeldungen im Voraus.

Ansbach, im März 2013

Thomas Kranig
Präsident

Inhaltsverzeichnis

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

1.1 Die bayerische Datenschutzaufsichtsbehörde

Aufgaben und Befugnisse der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich ergeben sich aus § 38 des Bundesdatenschutzgesetzes (BDSG). Gemäß § 38 Abs. 6 BDSG bestimmen die Landesregierungen oder die von ihnen ermächtigten Stellen die für die Kontrolle der Durchführung des Datenschutzes zuständigen Aufsichtsbehörden. Im Vollzug der Anforderung aus dem Urteil des Europäischen Gerichtshofs vom 9. März 2010 (Az. C-518/07), in dem u. a. entschieden wurde, dass auch die Datenschutzaufsicht im nicht-öffentlichen Bereich in „völliger Unabhängigkeit“ ausgestaltet sein muss, hat der Bayerische Landtag das Bayerische Datenschutzgesetz geändert und mit Wirkung zum 1. August 2011 in den Art. 34 und 35 BayDSG die Rechtsgrundlage für das Bayerische Landesamt für Datenschutzaufsicht als unabhängige Behörde mit einem Präsidenten an der Spitze geschaffen (GVBl 2011, S. 307). Am 4. August 2011 hat der Bayerische Staatsminister des Innern, Joachim Herrmann, den ersten Präsidenten mit einer Amtszeit von fünf Jahren ernannt.

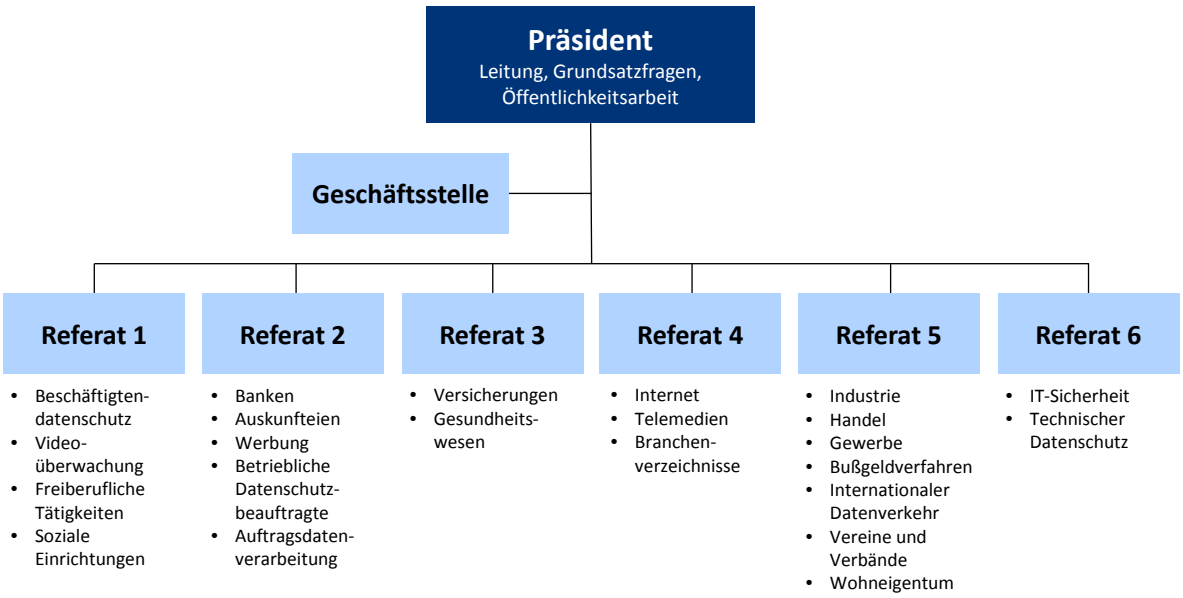
Als Folge der Unabhängigkeit ist das Landesamt nunmehr auch für den Vollzug der Vorschriften über die Datensicherheit zuständig. Die frühere Zuständigkeit des Technischen Überwachungsvereins (TÜV Süd) endete damit.

Neben bekannten Fragen aus der IT-Sicherheit existieren im technischen Bereich auch viele junge Themengebiete wie beispielsweise die Geolokalisierung von Internetnutzern und die Absicherung mobiler Endgeräte. So hat vor allem die starke Marktdurchdringung der Smartphones und Tablets im privaten als auch beruflichen Umfeld im vergangenen Jahr dazu geführt, dass neue datenschutzrechtliche Spannungsfelder wie „Bring your own device“ im IT-Bereich entstanden. Um diese und weitere Aufgaben erfüllen zu können, wurde beim BayLDA ein neues technisches Referat geschaffen und ein Diplom-Informatiker (Univ.) und ein Diplom-Wirtschaftsinformatiker (FH) eingestellt.

Darüber hinaus konnten gegenüber dem vorherigen Berichtszeitraum zwei weitere Stellen im Verwaltungsbereich geschaffen werden, so dass das BayLDA am 1. Januar 2013 über 16 Planstellen verfügt.

1.2 Gesetzliche Grundlage für die Erstellung des Tätigkeitsberichts

Gemäß § 38 Abs. 1 Satz 7 BDSG hat die Aufsichtsbehörde regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen. Der letzte Tätigkeitsbericht für die Jahre 2009 und 2010 wurde der Öffentlichkeit am 13. März 2011 vorgestellt.



2 Allgemeiner Überblick über die Tätigkeit des BayLDA

2.1 Statistik

Neben der Bearbeitung von Beschwerden, in denen Verletzungen von Datenschutzvorschriften geltend gemacht werden, nehmen auch die Beratungsleistungen für Bürger und Unternehmen mittlerweile einen wesentlichen Teil unserer täglichen Arbeit ein.

	2011	2012
Schriftliche Beschwerden	**687**	**719**
davon Verstöße	365	386
davon keine Verstöße	322	333
Beratungen Bürger/Betroffene	**1008**	**959**
Beratungen Unternehmen	**1418**	**1475**
Ordnungswidrigkeitsverfahren	**30**	**144**

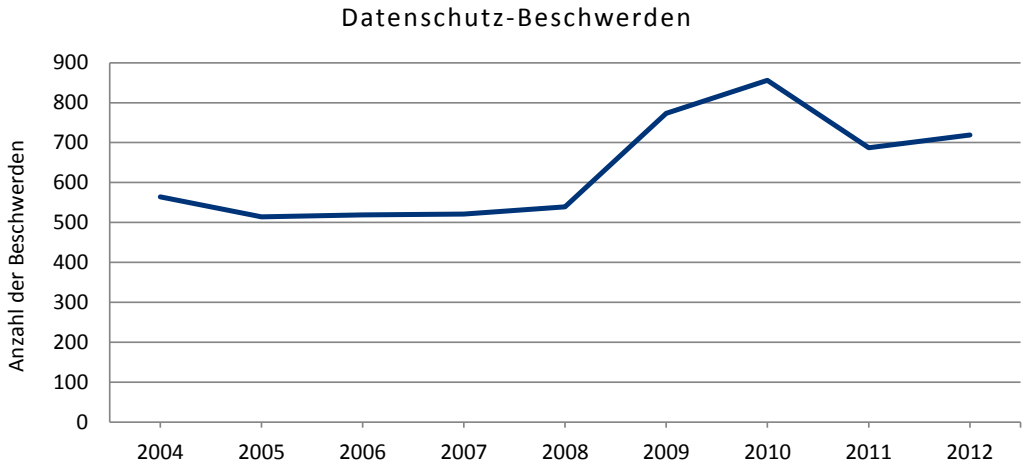
2.1.1 Beschwerden

Die Anzahl der bei uns eingegangenen schriftlichen Beschwerden ist im Vergleich zum vergangenen Berichtszeitraum 2009/2010 zwar insgesamt leicht rückläufig, bewegt sich jedoch nach wie vor auf einem hohen Niveau. Dies zeigt insbesondere der Vergleich zu den Eingaben der davor befindlichen Jahre ab 2004.

Als einen der Gründe, warum die Anzahl der Beschwerden nach 2010 nicht weiter anstieg, sehen wir die Tatsache, dass unsere Beratungen von verantwortlichen Stellen in Bayern erneut deutlich gestiegen sind. Im Vergleich zu den Vorjahren ist in diesem Bereich ein Anstieg von über 23% zu verzeichnen. Somit sehen wir die Unternehmen über datenschutzrechtliche Pflichten besser informiert, weshalb im Rückschluss die Anzahl der Beschwerden nicht weiter anstieg.

Bei über der Hälfte der im Berichtszeitraum erfassten Eingaben lagen ein oder mehrere Verstöße gegen Bestimmungen des Bundesdatenschutzgesetzes zu Grunde. Wir haben in diesen Fällen deshalb die verantwortlichen Stellen - zum Teil verbunden mit Zwangsgeldandrohungen - verpflichtet, den Verstößen abzuhelfen.

Beschwerden erreichten uns auf unterschiedliche Art und Weise: Zunehmend gingen sie per E-Mail ein - jedoch auch über herkömmliche Kanäle wie den Postweg oder per Telefax. Oft wurden wir bereits im Vorfeld telefonisch kontaktiert und über den Inhalt der Beschwerde informiert, so dass wir uns ein erstes Bild über den Sachverhalt machen konnten. Zugeleitet bekamen wir auch Eingaben anderer Einrichtungen - überwiegend Datenschutzaufsichtsbehörden aus anderen Bundesländern - die in unseren Zuständigkeitsbereich fielen. Im Gegenzug gaben wir Beschwerden an andere Institutionen und Datenschutzaufsichtsbehörden ab, für die wir nicht zuständig waren. Diese weitergeleiten bzw. abgegebenen Eingaben sind nicht in unserer Statistik abgebildet, d. h. die hier angegebenen Zahlen spiegeln die tatsächlich vollumfänglich bearbeiteten Datenschutz-Beschwerden wider. Ebenso nicht enthalten sind die 2371 Fälle bezüglich des von uns beanstandeten Einsatzes der Webtracking-Software Google Analytics im Jahr 2012 (siehe Kapitel 4.1.3).



Die eingehenden Beschwerden haben vielfältige Bereiche des Datenschutzes betroffen. In der nachfolgenden Grafik geben wir die Themen der Beschwerden prozentual zur Gesamtanzahl der Beschwerden wieder.

Internet	**14%**
Auskunftsanspruch nach § 34 BDSG	**12%**
Werbung und Adressenhandel	**11%**
Datenübermittlungen	**10%**
Versicherungen	**8%**
Zulässigkeit von Datenerhebungen	**7%**
Videoüberwachung	**7%**
IT-Sicherheit und Technik	**6%**
Datenlöschung	**6%**
Daten im Gesundheitsbereich	**5%**
Arbeitnehmerdatenschutz	**4%**
Daten im Bankenwesen	**3%**
Wirtschaftsauskunfteien	**2%**
Vereine und Verbände	**2%**
Daten von Mietern	**1%**
Tätigkeit von Rechtsanwälten	**1%**
Markt- und Meinungsforschung	**1%**

Wie bereits im vergangenen Tätigkeitsbericht festgehalten, beziehen sich die meisten Eingaben auf den umfassenden Themenkomplex Internet mit den tangierenden Fragen der IT-Sicherheit. Auch die (Nicht-)Erteilung von Auskünften an Betroffene nach § 34 BDSG ist nach wie vor ein häufiger Bestandteil der uns zugetragenen Beschwerden. Ebenso ist als ein Datenschutz-Dauerthema der Bereich „Werbung und Adresshandel“ zu nennen.

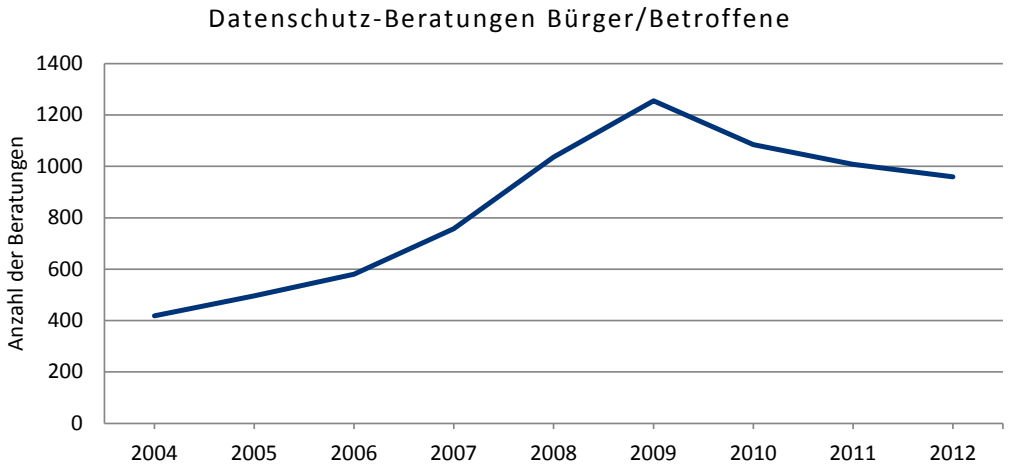
2.1.2 Beratung der Betroffenen

Bürger bzw. Betroffene wenden sich nicht nur mit Beschwerden an uns. In den vergangenen Jahren hatten wir seitens der Bürger auch zahlreiche Anfragen zu datenschutzrechtlichen Themen. Die Anfragen variierten dabei wie die Beschwerden in ihrer Komplexität und Thematik. Wir haben hier durch unsere Beratungsleistung zum jeweiligen Sachverhalt nach bestem Wissen informiert.

Die unten stehende Grafik zeigt, dass für die letzten fünf Jahre ein hohes Niveau mit rund 1.000 Beratungen jährlich gegenüber Bürgern und Betroffenen zu verzeichnen ist. Lediglich im Jahr 2009 gab es eine deutliche Spitze mit insgesamt über 1.200 Beratungen. Dies ist zum Teil darauf zurückzuführen, dass in diesem Jahr mit der Gründung der neuen organisatorischen Struktur als eigenes Landesamt unser Bekanntheitsgrad in der Bevölkerung stieg.

Den Bedarf an Beratungsleistungen haben wir frühzeitig erkannt. Deshalb versuchen wir die Bürger neben unseren mündlichen und schriftlichen Beratungen auch durch unseren Webauftritt sowie Flyer und Informationsblätter über die vielfältigen Datenschutzthemen zu informieren.

Siehe:
www.lda.bayern.de



2.1.3 Beratung der verantwortlichen Stellen und der betrieblichen Datenschutzbeauftragten

Nach § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Auf die Einhaltung der datenschutzrechtlichen Vorschriften bei den verantwortlichen Stellen hat insbesondere der betriebliche Datenschutzbeauftragte (siehe Kapitel 3) hinzuwirken.

Die Beratung der verantwortlichen Stellen und der betrieblichen Datenschutzbeauftragten gemäß § 38 Abs. 1 Satz 2 BDSG stellt einen wichtigen Schwerpunkt unserer Arbeit dar. Komplexe Fallgestaltungen werden uns schriftlich vorgetragen oder in Besprechungen bei uns bzw. in den Unternehmen gezielt erörtert.

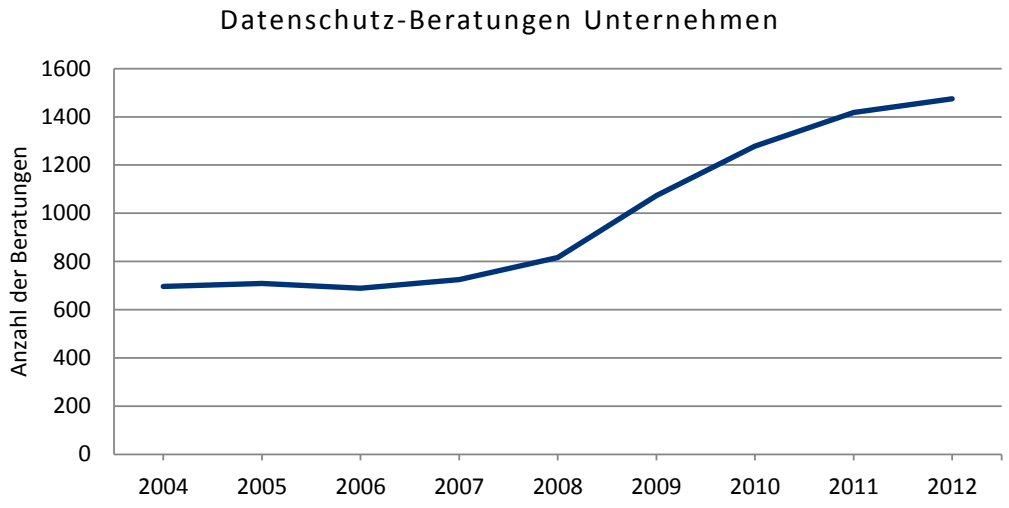
Vielen verantwortlichen Stellen, Datenschutzbeauftragten oder bevollmächtigten Rechtsanwälten ist dabei ein Leitmotiv des BayLDA bekannt, lieber im Beratungsweg zu unterstützen und damit Datenschutzverstöße zu vermeiden, als repressiv dagegen vorgehen zu müssen. Bei über 100 Besprechungen im Berichtszeitraum, an denen Referenten und meistens auch der Präsident seitens des BayLDA teilgenommen haben, wurden Konzepte, Projekte oder Produkte von Unternehmen vorgestellt und in rechtlicher und/oder technischer Hinsicht geprüft.

Die Beratungsanfragen aus dem Kreis der verantwortlichen Stellen sind in den letzten Jahren spürbar gestiegen. Dieser Trend setzte sich 2011 und 2012 konsequent fort. So stieg die Anzahl der Unternehmensberatungen schließlich im Jahr 2012 mit 1475 von uns durchgeführten Beratungen auf mehr als das Doppelte im Vergleich zum Jahr 2007.

Folgende Themen standen bei den Beratungen verantwortlicher Stellen im Vordergrund:

- Internationaler Datenverkehr
- Datenschutz bei Werbung
- Beschäftigtendatenschutz
- Videoüberwachung
- Externe Datenverarbeitung durch Dienstleister
- Datenschutz im Gesundheitswesen
- Datenschutz beim Umgang mit neuen Medien insbesondere des Internets
- IT-Sicherheit und Fragen des technischen Datenschutzes

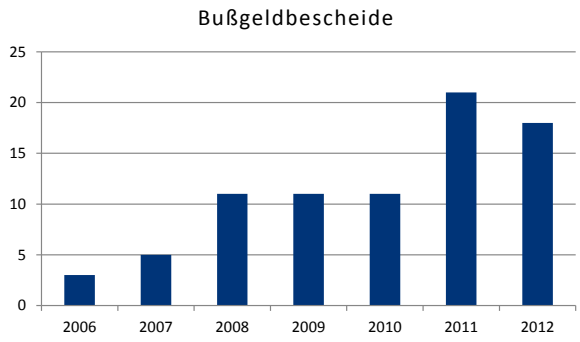
Abschließend gilt festzuhalten, dass wir in dieser Statistik Zahlen unserer Google Analytics Prüfaktion aus dem Jahr 2012 - immerhin über 500 zusätzliche telefonische Beratungen verantwortlicher Stellen - nicht mit eingerechnet haben (siehe Kapitel 4.1.3).



2.1.4 Ordnungswidrigkeitenverfahren und Strafanträge

Im Berichtszeitraum hat das BayLDA insgesamt 174 Ordnungswidrigkeitenverfahren eröffnet, wobei 39 Bußgeldbescheide über insgesamt ca. 37.000 EUR erlassen und drei Strafanträge wegen datenschutzrechtlicher Verstöße gestellt wurden.

Die Anzahl der erlassenen Bußgeldbescheide ist somit in den vergangenen Jahren sprunghaft gestiegen, während die Stellung von Strafanträgen sich weiterhin auf einem niedrigen Niveau bewegt.



2.1.5 Kontrolltätigkeit

Jede Eingabe oder Beschwerde, die plausibel erscheint, wird bearbeitet und mündet in Einzelfällen in eine anlassbezogene Kontrolle, gegebenenfalls mit Ortseinsicht. Wichtig war es uns daneben aber auch, anlasslose Kontrollmaßnahmen in Bereichen durchzuführen, in denen entweder wegen der besonderen Beziehung der Beteiligten (z. B. Arzt-Patient) oder wegen der für die Betroffenen nicht erkennbaren Auswertung (Tracking von Nutzerverhalten im Internet) Beschwerden üblicherweise nur in sehr geringem Umfang erhoben werden.

Bei den hier genannten Kontrollen wurde die Beachtung der datenschutzrechtlichen Vorschriften nach § 38 Abs. 1 Satz 1 BDSG gezielt auf den Prüfstand gestellt. Wir haben aus diesen Kontrollen insbesondere folgende Erkenntnisse gewonnen bzw. Defizite festgestellt:

- Im Gesundheitsbereich ist es notwendig, mehr Sensibilität für die Persönlichkeitsrechte der Patienten zu wecken, insbesondere wenn andere Personen mithören oder Unterlagen bzw. Bildschirminhalte einsehen können.
- Bei Videoüberwachung öffentlich zugänglicher Bereiche sind die Interessen betroffener Personen angemessen zu berücksichtigen, denn grundsätzlich hat jeder das Recht, sich in der Öffentlichkeit unbeobachtet und undokumentiert zu bewegen.
- In einer Vor-Ort-Kontrolle stellten wir eine unzulässige Übermittlung von Finanzdaten in größerem Umfang fest, die wir mit einem Bußgeld in Höhe von 10.000 EUR geahndet haben.
- Im Bereich der Internetnutzungsauswertung haben wir ein großes Informationsdefizit bei den Webseitenbetreibern über die datenschutzrechtlichen Rahmenbedingungen erkannt und versucht, dem durch unsere Beratung abzuhelfen.
- Die Webseitenbetreiber müssen wegen der allgegenwärtigen Hacking-Gefahr, insbesondere dem Ausspähen von Zugangs- sowie von Kreditkarten- und Bankdaten, ihre getroffenen Sicherheitsmaßnahmen laufend im Auge haben und dem aktuellen technischen Stand anpassen.

	2009	2010	2011	2012
Kontrollen ohne Vor-Ort-Besuch			**50**	**13.404**
Banken, Finanzbereich			42	
Webseiten (Google Analytics)				13.404
Videoüberwachung in Bäckerei-Filialen			8	
Kontrollen mit Vor-Ort-Besuch	**10**	**10**	**12**	**20**
Gesundheitsbereich				12
Datenschutzorganisation und Technik	3	3	3	3
Auskunfteien		1	3	2
Internetbezug	4	4	3	
Videoüberwachung	2		2	1
Banken, Finanzbereich	1	2	1	2

2.1.6 Öffentliches Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen

Nach § 38 Abs. 2 BDSG führen wir ein Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen bei verantwortlichen Stellen in Bayern.

Im Wesentlichen sind die folgenden zwei Geschäftsfelder gegenüber uns als Datenschutzaufsichtsbehörde meldepflichtig:

- Datenspeicherung zum Zweck der Übermittlung, also der Handel mit personenbezogenen Daten, wie es bei Wirtschaftsauskunfteien und Adresshändlern der Fall ist, und
- Datenspeicherung zum Zweck der anonymisierten Übermittlung, also die Tätigkeit der Markt-, Meinungs- und Sozialforschungsinstitute.

Uns lagen zum Ende des Berichtszeitraums insgesamt 145 Anmeldungen aus Bayern vor. Wie auch zum Zeitpunkt des letzten Tätigkeitsberichts entfällt etwa die Hälfte dieser Anmeldungen auf Auskunfteien und Adresshändler, die andere Hälfte auf die analysierenden Institutionen der Markt-, Meinungs- und Sozialforschung.

Das bei uns geführte Register über die meldepflichtigen Unternehmen kann nach § 38 Abs. 2 Satz 2 BDSG von jedem eingesehen bzw. kann aus ihm Auskunft erteilt werden.

2.2 Zusammenarbeit mit den anderen Datenschutzaufsichtsbehörden

Die Datenschutzaufsichtsbehörden für den nichtöffentlichen Bereich arbeiten bundesweit in dem in der Regel zwei Mal jährlich tagenden sog. „Düsseldorfer Kreis“ zusammen. Sie hatten bislang diese Treffen als oberstes Beratungsgremium, in dem grundsätzliche Rechtsfragen des Vollzugs in länderübergreifenden Sachverhalten beraten und abgestimmt werden, verstanden. Die Konferenz des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz (Datenschutzkonferenz) hat entschieden, den Düsseldorfer Kreis als einen Arbeitskreis (neben vielen anderen) der Konferenz unterzuordnen. Es bleibt abzuwarten und ist zu hoffen, dass die konkrete Arbeit an der Abstimmung von datenschutzrechtlichen Vollzugsfragen, die den Düsseldorfer Kreis zu einem „Markenzeichen“ gemacht hat, erhalten bleibt und nicht durch (auch, aber nicht in diesem Kreis notwendige) datenschutzpolitische Aktivitäten in den Hintergrund gerät.

In das Gesamtgremium des Düsseldorfer Kreises sind wir ebenso eingebunden wie auch in die dazu gehörenden Arbeitsgruppen Kreditwirtschaft, Auskunfteien/SCHUFA, Versicherungswirtschaft, Internationaler Datenverkehr, Medien, Sanktionen, Beschäftigtendatenschutz und Technik.

Wir arbeiten auch regelmäßig in den für bestimmte Fachfragen eingerichteten sog. ad-hoc-Arbeitsgruppen mit. In den abgeschlossenen ad-hoc-Arbeitsgruppen zum Thema Fahrzeugdatenspeicher und Elektronisches Lastschriftverfahren hatten wir den Vorsitz inne.

Die Ergebnisse der Beratungen werden, sofern Einvernehmen erreicht werden konnte, in Beschlüssen festgehalten. Eine Übersicht über die vom Düsseldorfer Kreis seit 2006 gefassten Beschlüsse finden Sie auf der Homepage des Bundesbeauftragten für Datenschutz und Informationsfreiheit.

Siehe:
www.datenschutz.bund.de

Einmal im Jahr treffen wir uns mit Vertretern der anderen Datenschutzaufsichtsbehörden bei einem Workshop zur Klärung und Abstimmung von konkreten Praxisfragen.

Darüber hinaus nehmen wir regelmäßig an den Sitzungen der Arbeitsgruppe (Subgroup) „International Transfers“ der Artikel-29-Gruppe der Datenschutzaufsichtsbehörden der EU-Mitgliedsstaaten teil.

Nicht vergessen werden sollte schließlich die Zusammenarbeit mit dem Bayerischen Landesbeauftragten für den Datenschutz und seinen Mitarbeitern. Sowohl bei Fragen zur Klärung der Zuständigkeit als auch bezüglich Abstimmungsverhaltens für Bayern in der Datenschutzkonferenz gestaltet sich die Zusammenarbeit kollegial und reibungslos.

2.3 Teilnahme und Mitwirkung bei Veranstaltungen der Wirtschaft und anderer Berufsgruppen

Betriebliche Datenschutzbeauftragte treffen sich unter der Federführung der Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) zum Erfahrungsaustausch in sog. „Erfa-Kreisen“ (Erfahrungsaustausch-Kreisen), um von- bzw. miteinander zu lernen und sich fortzubilden. Diese Arbeitskreise, an denen wir mit entsprechender Einladung regelmäßig teilnehmen, bestehen für Bayern in München, Nürnberg, Würzburg und Coburg und tagen jeweils zwei- bis dreimal im Jahr.

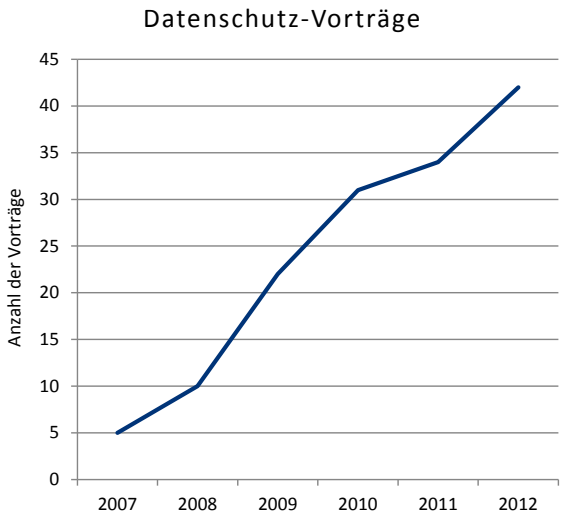
An den halbjährlichen Treffen der Datenschutzbeauftragten der bayerischen Versicherungsunternehmen, einem auf Versicherungsfachfragen ausgerichteten Datenschutz-Arbeitskreis, nehmen wir ebenfalls regelmäßig teil.

Durch Übernahme der Schirmherrschaft unterstützen wir die Aktivitäten des Berufsverbandes der Datenschutzbeauftragten Deutschlands e.V. (BvD) bei dem Projekt „Datenschutz geht zur Schule“. Im Rahmen dieses Projekts gehen betriebliche Datenschutzbeauftragte ehrenamtlich in Schulen, um dort die Schüler im Umgang mit dem Internet und sozialen Netzwerken zu sensibilisieren, sie vor Gefahren zu warnen und ihnen noch den einen oder anderen Tipp zu geben.

Teilgenommen haben wir mit Vorträgen auch an zahlreichen Veranstaltungen von Rechtsanwaltskanzleien, Berufsverbänden oder Unternehmen, bei denen wir sehr häufig auf eine unserer „Zielgruppen“, die betrieblichen Datenschutzbeauftragten, gestoßen sind.

Darüber hinaus waren wir mit Vorträgen u. a. bei folgenden öffentlichen Einrichtungen vertreten: Dienstbesprechungen der jur. Staatsbeamten bei vier Bezirksregierungen, Hochschule Weihenstephan-Triesdorf, IHK Oberbayern, Hochschule Würzburg-Schweinfurt, Fortbildungsinstitut der bayerischen Polizei, Sparkassenakademie, Universität Würzburg, Staatskanzlei Saarbrücken, Lebenshilfe Landesverband Bayern e.V., Verband der Bayer. Bezirke, Technische Universität München, Evangelische Hochschule Nürnberg.

Auf Wunsch und im Zusammenwirken mit Unternehmensverbänden und Datenschutzorganisationen haben wir bei Fortbildungsveranstaltungen, Kongressen und Seminaren Vorträge zu datenschutzrechtlichen Themen gehalten, um auch auf diesem Weg eine Breitenwirkung in der Datenschutzinformation zu erreichen. Im Jahr 2011 wurden von uns 34 Vorträge und im Jahr 2012 insgesamt 42 Vorträge gehalten. Somit ist im Vergleich zu den Vorjahren nach wie vor ein ansteigender Trend zu erkennen.



2.4 Datenschutzfachtagungen und -kongresse

Mehrmals im Jahr besuchen wir Datenschutz-Kongresse, bei denen über die aktuellen Fragen des Datenschutzes und der Datensicherheit in Deutschland referiert und diskutiert wird. Mit eigenen Beiträgen waren wir u. a. auf der IDACON in Würzburg, der DAFTA in Köln, der it-sa in Nürnberg, der Berliner Datenschutzrunde, dem Web-Law-Forum in Zürich sowie dem ePrivacy-Forum in London vertreten.

Im Mai 2012 haben wir zusammen mit dem amerikanischen Generalkonsulat München, dem Bayerischen Landesbeauftragten für den Datenschutz und der Vereinigung der bayerischen Wirtschaft (vbw) den 1. Deutsch-amerikanischen Datenschutztag in München mit Beteiligung von Julie Brill, Commissioner der Federal Trade Commission (FTC), dem Bayerischen Staatsminister des Inneren Joachim Herrmann und dem amerikanischen Generalkonsul Conrad Tribble organisiert.

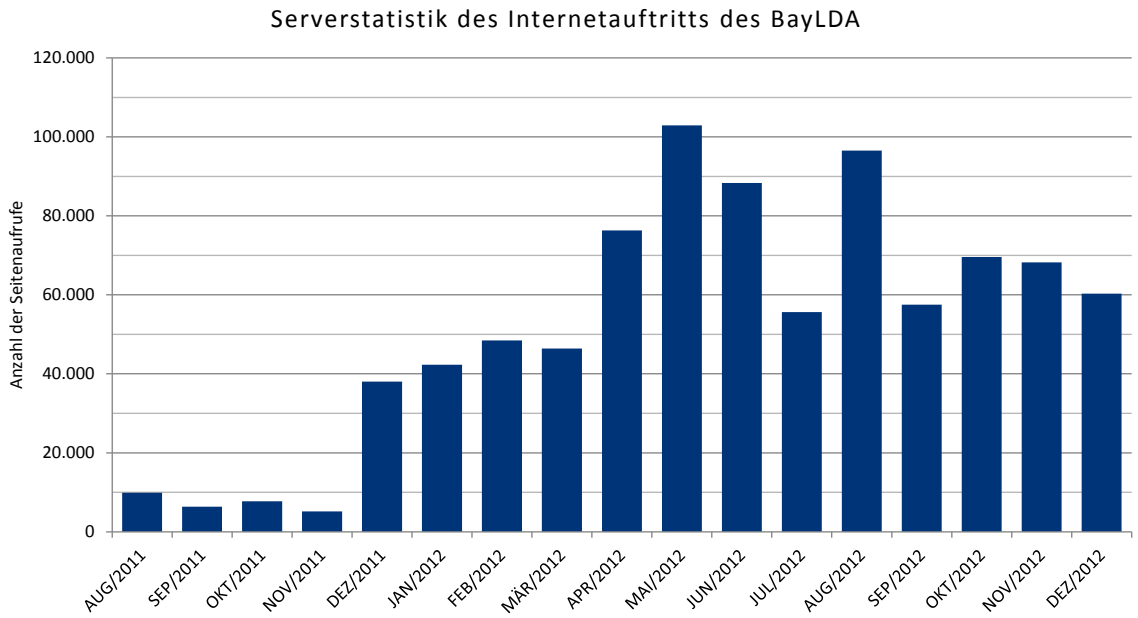
Im Dezember 2012 haben wir in Brüssel zum Entwurf der Datenschutz-Grundverordnung auf dem Podium an einer Diskussion mit Paul Nemitz (EU-Kommission), Jan-Philip Albrecht (EU-Parlament) und BITKOM teilgenommen.

2.5 Öffentlichkeitsarbeit

Die Öffentlichkeitsarbeit ist einer der Schwerpunkte unserer Tätigkeit. In Presse, Rundfunk und Fernsehen haben wir im Berichtszeitraum in zahlreichen Beiträgen regelmäßig zu aktuellen Datenschutzthemen Stellung genommen. Für die wichtige Aufgabe der Öffentlichkeitsarbeit haben wir eine Homepage eingerichtet, die eine Reihe von Dokumenten zu grundsätzlichen Datenschutzfragen und Links zu anderen Datenschutzinformationen umfasst. Daneben halten wir Informationsmaterial zum Datenschutz auch in Papierform bereit.

Siehe:
www.lda.bayern.de

Um erkennen zu können, ob und in welchem Umfang unsere Homepage wahrgenommen wird, erfassen wir ohne sonstige weitere Daten seit August 2011 die Zahl der Zugriffe. Dabei stellten wir fest, dass nach unserer Prüfungsaktion im Zusammenhang mit dem Einsatz von Google Analytics die Zugriffszahlen ab Mai 2012 deutlich in die Höhe gegangen sind und sich ansonsten in einem durchaus zufriedenstellenden Umfang bewegen.



3 Der betriebliche Datenschutzbeauftragte

3.1 Wann eine Bestellung nach § 4f Abs. 1 BDSG nötig ist

Im Regelfall ist ein Datenschutzbeauftragter dann zu bestellen, wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Die Vorschrift in § 4f Abs. 1 BDSG zur Bestellung eines Datenschutzbeauftragten führt immer wieder zu Fragen von Unternehmen, Vereinen und Freiberuflern, ob sie aufgrund ihrer Gegebenheiten einen Datenschutzbeauftragten bestellen müssen oder nicht.

Unklar ist z. B., wann in der Regel mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden, wie dies § 4f Abs. 1 Satz 4 BDSG bestimmt.

Wir vertreten dazu die Auffassung, dass das Merkmal „ständig“ zwar nicht bedeutet, dass eine Person während ihrer gesamten Arbeitszeit mit personenbezogenen Daten umgeht. Es muss aber doch ein erheblicher Teil der Arbeit die Verarbeitung personenbezogener Daten betreffen, wie dies z. B. bei Mitarbeitern der Personalverwaltung, des Marketings oder der Kundenbetreuung der Fall ist.

Beschäftigte, die in erster Linie mit anderen (z. B. technischen) Aufgaben betraut sind und nur völlig untergeordnet mit personenbezogenen Daten umgehen, sind nicht zu berücksichtigen. Nicht zu zählen sind damit insbesondere Handwerker, Monteure, Arbeiter an Produktionslinien etc., die nur gelegentlich bzw. vereinzelt personenbezogene Daten verwenden oder damit in Berührung kommen.

Auch § 4f Abs. 1 Satz 6 BDSG führt, vor allem im medizinischen Bereich, zu Fragen, ob eventuell aufgrund einer notwendigen Vorabkontrolle generell, unabhängig von der Zahl der beschäftigten Personen, ein Datenschutzbeauftragter notwendig ist. Eine Vorabkontrolle als vorgezogene Prüfungsmaßnahme bei sensiblen Daten oder heiklen Datenverarbeitungen ist jedoch dann nicht vorgeschrieben, wenn der Umgang mit personenbezogenen Daten auf der Einwilligung der betroffenen Personen beruht oder für den Vollzug eines Vertragsverhältnisses mit diesen Personen erforderlich ist. Diese Umstände (Einwilligung oder Vertragsbeziehung) sind bei Arztpraxen, Apotheken, Steuerberatern usw. im Allgemeinen gegeben, so dass auch dort die 9-Personen-Grenze an beschäftigten Personen maßgebend ist.

3.2 Unvereinbarkeit mit anderen Aufgaben

Der Datenschutzbeauftragte darf keine sonstigen Funktionen im Unternehmen ausüben, die zu erhöhten Interessenkollisionen mit der Datenschutzkontrolle führen können.

Der Datenschutzbeauftragte muss nach dem Gesetz neben ausreichender Fachkunde auch die erforderliche Zuverlässigkeit besitzen. Hierzu zählt auch, dass er nicht neben der Datenschutzkontrolle noch Zuständigkeiten hat, die zu über das unvermeidliche Maß hinausgehenden Interessenkollisionen führen.

Solchen erhöhten Interessenkollisionen unterliegen regelmäßig die Personen der obersten Leitungsebene eines Unternehmens, wie Inhaber, Vorstände, Geschäftsführer, einschließlich deren Stellvertreter, weil dort der Datenschutz im Rahmen der Gesamtverantwortung dieser Personen für das Unternehmen naturgemäß nur ein Aspekt neben vielen anderen zu berücksichtigenden Unternehmensinteressen sein kann.

Erhöhten Interessenkollisionen sind grundsätzlich auch Personalleiter sowie IT-Leiter und IT-Administratoren ausgesetzt, die in dieser Funktion eine große Verantwortung für die Verarbeitung personenbezogener Daten haben und die in weiten Teilen als Datenschutzbeauftragte ihre eigene Tätigkeit kontrollieren müssten.

Das Gleiche trifft nach Meinung der Datenschutzaufsichtsbehörden auch auf die Geldwäschebeauftragten von Finanzinstituten zu, die in dieser Funktion ebenfalls umfangreich mit personenbezogenen Daten umgehen müssen. Insoweit sehen wir eine neutrale bzw. unabhängige Datenschutzkontrolle als nicht gewährleistet.

Die Rechtsprechung hatte im Jahre 2011 zu zwei Aufgabenkombinationen beim Datenschutzbeauftragten Entscheidungen getroffen, denen wir uns gut anschließen können, weil wir diese Auffassungen bisher schon in Praxisfällen vertreten haben. Zunächst musste sich das Bundesarbeitsgericht mit der Frage befassen, ob die Mitgliedschaft im Be-

triebsrat und dessen EDV-Ausschuss eine Person für das Amt des Datenschutzbeauftragten unzuverlässig macht. In dem Urteil vom 23. März 2011, Az. 10 AZR 562/09, wurde dabei keine grundsätzliche Unvereinbarkeit zwischen diesen beiden Ämtern gesehen. Das Landesarbeitsgericht Hamm hat in einem Beschluss vom 8. April 2011, Az. 13 TaBV 92/10, die Auffassung vertreten, dass allein die Mitarbeit im IT-Bereich (hier: IT-Projektarbeit, Umsetzung von IT-Sicherheitsstandards) nicht die für den Datenschutzbeauftragten gebotene Zuverlässigkeit in Frage stellt. Vorhandene Spezialkenntnisse einer Person böten auch die Chance, jemanden mit ausgewiesener Fachkunde für die Tätigkeit als Datenschutzbeauftragten zu gewinnen.

Wegen der vorhandenen speziellen Fachkunde im rechtlichen oder technischen Bereich sehen wir grundsätzlich auch Beschäftigte in der Revision, der Rechtsabteilung oder der Organisation als mögliche Datenschutzbeauftragte in Unternehmen an.

4 Datenschutz im Internet

4.1 Rechtliche Fragestellungen des Datenschutzes im Internet

4.1.1 Elektronische Verzeichnisse im Internet

Die Aufnahme personenbezogener Daten in ein elektronisches Verzeichnis im Internet ist zulässig, sofern der Datensatz zu diesem Zweck von einem Telekommunikationsunternehmen rechtmäßig übermittelt worden ist und der Betroffene dem nicht widersprochen hat.

Mehrere Bürger haben sich besorgt an uns gewandt, da sie bei der Eingabe ihres Namens in eine Internetsuchmaschine mehrere Suchtreffer zu elektronischen Verzeichnissen erhalten hatten, in denen sie mit Namen, Anschrift und Telefonnummer aufgenommen waren. Mehrheitlich zeigten sie sich hierüber sehr überrascht und baten uns um Unterstützung, um eine umgehende Löschung der Datensätze zu erreichen. In den bei uns anhängig gewordenen Fällen handelte es sich bei den besagten Diensteanbietern um Anbieter von elektronischen Verzeichnissen, die die veröffentlichten Datensätze von Telekommunikationsdiensteanbietern bezogen haben. Diese haben uns gegenüber in ihren Stellungnahmen ausgeführt, dass die Eingabeführer gegenüber ihrem Telekommunikationsanbieter der Aufnahme ihrer Daten in öffentliche Teilnehmerverzeichnisse zugestimmt hätten.

Nach den einschlägigen Vorschriften des Telekommunikationsgesetzes (TKG) können Teilnehmer auf Antrag mit ihrem Namen, ihrer Anschrift und zusätzlichen Angaben wie Beruf, Branche und Art des Anschlusses in öffentliche gedruckte oder elektronische Verzeichnisse eingetragen werden, wobei die Teilnehmer bestimmen können, welche Angaben in den Verzeichnissen veröffentlicht werden sollen (§ 104 TKG). Jedes Unternehmen, das Telekommunikationsdienste für die Öffentlichkeit erbringt und Rufnummern an Endnutzer vergibt, ist verpflichtet, unter Beachtung der anzuwendenden datenschutzrechtlichen Regelungen jedem Unternehmen auf Antrag Teilnehmerdaten zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen zur Verfügung zu stellen (§ 47 TKG).

Aufgrund dieser gesetzlichen Regelung ist es zunächst datenschutzrechtlich zulässig, dass Telekommunikationsunternehmen auf Antrag ihre Datensätze zweckgebunden auch an andere Unternehmen übermitteln, die im Internet elektronische Verzeichnisse anbieten. Eine Aufnahme personenbezogener Daten in derartige elektronische Verzeichnisse hat jedoch dann zu unterbleiben, „wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist“ (§ 29 Abs. 3 Satz 1 BDSG).

Deshalb sollten Personen, die eine Weitergabe ihrer personenbezogenen Daten durch den Telekommunikationsanbieter an Anbieter von elektronischen Verzeichnissen unterbinden wollen, sich an den Telekommunikationsanbieter wenden und einen Widerspruch geltend machen. Dies führt dazu, dass der Datensatz vom Telekommunikationsanbieter künftig nicht mehr an anfragende Unternehmen weitergegeben wird bzw. entsprechend gekennzeichnet wird.

4.1.2 Bing Maps Streetside

Für die Veröffentlichung von Hausansichten in sog. Panoramadiensten ist auf die Anforderungen abzustellen, die vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit federführend für alle Datenschutzaufsichtsbehörden in Deutschland mit der Firma Google vereinbart wurden.

Aufgrund der Tatsache, dass in München eine Tochtergesellschaft von Microsoft, die Microsoft Deutschland GmbH, ansässig ist, hatten sich die deutschen Datenschutzaufsichtsbehörden darauf verständigt, dass wir in Sachen „Bing Maps Streetside“ als zentraler Ansprechpartner für Microsoft fungieren und tätig werden sollen.

Frühzeitig hatte Microsoft das Gespräch mit uns gesucht und uns über ihre Pläne, Straßenansichten aufzunehmen und im Internet zu veröffentlichen, informiert. Die Art des geplanten Internetdienstes war uns bekannt, da sich die Datenschutzaufsichtsbehörden zuvor bereits mit dem vergleichbaren Internetdienst „Google Street View“ der Google Inc. mit Sitz in den USA beschäftigt hatte.

Bereits im Jahr 2008 hat der Düsseldorfer Kreis sich mit der „Bewertung von digitalen Straßenansichten insbesondere im Internet“ befasst. Dabei wurde festgestellt, dass nach den Maßstäben der Vor-

schriften des Bundesdatenschutzgesetzes derartige Dienste nur dann datenschutzrechtlich zulässig sind, wenn die schutzwürdigen Interessen der betroffenen Personen, denen ein Haus gehört oder die es bewohnen, nicht entgegenstehen. Die gefundene Widerspruchslösung ist ein wesentlicher Baustein, der betroffenen Personen dazu verhelfen soll, ihre schutzwürdigen Interessen zu wahren.

Der gefasste Beschluss des Düsseldorfer Kreises lautet wie folgt:

„Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückseigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen."

Siehe:
www.bfdi.bund.de >> Entschließungen >> Düsseldorfer Kreis >> Datenschutzrechtliche Bewertung von digitalen Straßenansichten im Internet (14.11.2008)

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, der seinerseits federführend für die deutschen Datenschutzaufsichtsbehörden hinsichtlich des Internetdienstes „Google Street View" tätig war, hatte als Gesprächsergebnis im Juni 2009 mit der Fa. Google eine Vereinbarung getroffen, die als sog. 13-Punkte-Katalog veröffentlicht wurde. Die dortigen Kriterien waren auch Grundlage der Gespräche zwischen Microsoft und uns zur datenschutzkonformen Einführung und Ausgestaltung von „Bing Maps Streetside". Im Wesentlichen ergab sich daraus, dass bei derartigen Angeboten Gesichter und Kfz-Kennzeichen vor der Veröffentlichung generell unkenntlich gemacht werden. Hausansichten werden unter Einräumung einer angemessenen Widerspruchsfrist auf Wunsch der Betroffenen vor der Veröffentlichung unkenntlich gemacht. Eine Widerspruchsmöglichkeit besteht auch noch nach Veröffentlichung.

Siehe:
www.datenschutz-hamburg.de >> Ihr Recht auf Datenschutz >> Google Street View >> Zusagen von Google

In den Verhandlungen um „Bing Maps Streetside" haben wir einen Schwerpunkt auf die Sicherstellung eines „Vorabwiderspruchsverfahren" gelegt. Microsoft sollte den Bürgern bereits im Vorfeld die Möglichkeit einräumen, einer Internetveröffentlichung ihrer Hausansichten widersprechen zu können. In sehr konstruktiven Gesprächen hat sich Microsoft hierzu bereit erklärt. Nach entsprechender Information hat Microsoft nach eigener Auskunft am 23. Mai 2011 mit den Kamerafahrten begonnen und ein Zeitfenster vom 1. August bis 30. September 2011 bekannt gegeben, in dem es Bürgern aus der ganzen Bundesrepublik möglich gewesen ist, online oder per Brief einen Vorabwiderspruch einzulegen, ohne dass zu diesem Zeitpunkt schon feststand, welche Gebiete Deutschlands von Microsoft bereits befahren wurden oder noch befahren werden und welches Bildmaterial veröffentlicht wird. Eine zeitliche Begrenzung war notwendig, um es Microsoft zu ermöglichen, alle eingegangenen Widersprüche tatsächlich vor einer Veröffentlichung der Bilder zu bearbeiten.

Wir haben uns in dieser Zeit intensiv darum bemüht, die Bevölkerung auf die Möglichkeit des Vorabwiderspruchs aufmerksam zu machen und zahlreiche, meist telefonische Beratungsgespräche geführt. Neben der Veröffentlichung aktueller Informationen in unserem Internetauftritt haben wir stets die Presse auf die neuesten Entwicklungen aufmerksam gemacht. Zudem wurden die Kollegen der anderen deutschen Datenschutzaufsichtsbehörden gebeten, bei den Bürgerinnen und Bürgern in ihrem örtlichen Zuständigkeitsbereich in geeigneter Form Aufklärungsarbeit zu leisten.

Innerhalb des Zeitfensters gingen nach Angaben von Microsoft 80.818 Vorabwidersprüche ein. Bevor der Internetdienst im Dezember 2011 schließlich online ging, haben wir uns bei einem Treffen mit Unternehmensvertretern im Rahmen einer Vorschau anhand konkreter Stichproben von der ordnungsgemäßen Umsetzung der Vorabwidersprüche überzeugt.

Seit Mai 2012 steht „Bing Maps Streetside“ in Deutschland nicht mehr zur Verfügung. Es ist uns nicht bekannt, ob bzw. wann der Dienst für Deutschland wieder online geht. Allerdings fanden auch nach Mai 2012 noch weitere Befahrungen deutscher Städte statt, um Bildmaterial zu gewinnen. Ein eventueller Widerspruch bei Microsoft gegen die Veröffentlichung von Hausansichten ist nach den mit Microsoft getroffenen Vereinbarungen und dem Ablauf der Vorabwiderspruchsfrist nunmehr allerdings erst nach einer Veröffentlichung möglich.

4.1.3 Prüfung des Einsatzes von Google Analytics im Internetauftritt bayerischer Unternehmen

Das Webanalysetool Google Analytics kann von deutschen Webseitenbetreibern unter gewissen Rahmenbedingungen beanstandungsfrei eingesetzt werden.

In unserem Tätigkeitsbericht 2009/2010 hatten wir bereits den Beschluss des Düsseldorfer Kreises vorgestellt, in dem die rechtlichen Anforderungen an eine datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten dargelegt worden sind.

Siehe:
www.bfdi.bund.de >> Entschließungen >> Düsseldorfer Kreis >> Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten

Vor dem Hintergrund dieses Beschlusses hat sich der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit federführend für die Datenschutzaufsichtsbehörden in Deutschland mit der Firma Google darüber verständigt, wie Google Analytics von deutschen Webseitenbetreibern eingesetzt werden soll und in einer Pressemitteilung vom 15. September 2011 vorgestellt, durch welche zu treffenden Maßnahmen ein beanstandungsfreier Betrieb möglich ist. Zentrale Punkte waren:

- Jedem Nutzer muss die Möglichkeit des Widerspruchs gegen die Erfassung von Nutzungsdaten eingeräumt werden. Die Firma Google stellt dafür ein sog. Deaktivierungs-Add-On für den Browser zur Verfügung.
- Auf Anforderung des Webseitenbetreibers löscht Google innerhalb von Europa das letzte Oktett der IP-Adresse vor der systematischen Verarbeitung, so dass darüber keine Identifizierung des Nutzers mehr möglich ist. Konkret bedeutet dies, dass der Webseitenbetreiber (und nicht der Nutzer) im Programmcode auf seiner Webseite die Anonymisierung der IP-Adressen der Webseitenbesucher durch Google konfigurieren muss.
- Der Webseitenbetreiber hat einen Vertrag zur Auftragsdatenverarbeitung mit der Firma Google nach den Vorschriften des Bundesdatenschutzgesetzes abzuschließen.

Nach einer gewissen „Umsetzungsfrist“ hatten wir uns im Frühjahr 2012 dazu entschlossen, den datenschutzkonformen Einsatz von Google Analytics durch Diensteanbieter, die ihren Sitz in Bayern haben, zu überprüfen. Dabei stand von vornherein klar im Vordergrund, nicht etwa durch Verhängung von Bußgeldern die Kasse des Freistaats Bayern aufzufüllen, sondern durch Information und Hilfestellung in verschiedenster Form die bayerischen Diensteanbieter zu unterstützen, den datenschutzrechtlichen Anforderungen für den Einsatz von Google Analytics gerecht zu werden.

Wir hatten für die Prüfung eine eigene Software entwickelt, die es bei Eingabe einer URL u. a. ermöglichte, automatisch zu erkennen,

- ob Google Analytics eingesetzt wird,
- ob die erforderliche Anonymisierung der IP-Adresse durch Einfügen von „anoymizeIP“ in den Programmcode in Auftrag gegeben wird und
- ob die erforderliche Datenschutzerklärung mit Hinweis auf die Widerspruchsmöglichkeit enthalten ist.

Mit Hilfe dieser Software war es möglich, in einem Prüflauf im Mai 2012 bei 13.404 Webseiten bayerischer Anbieter den Einsatz von Google Analytics zu überprüfen. Im Ergebnis ergab die Auswertung, dass auf 2.371 von 2.449 Webseiten, bei denen Google Analytics zum Einsatz kam, dies nicht ent-

sprechend den Vorgaben des Düsseldorfer Kreises geschah.

Wir haben alle 2.371 Webseitenbetreiber angeschrieben, ihnen das Ergebnis der Überprüfung mitgeteilt und zum Teil in dem Schreiben und unter Verweis auf weitergehende Informationen auf unserer Homepage konkret die Schritte aufgezeigt, die jeweils für einen datenschutzgerechten Einsatz vorzunehmen sind.

Die Reaktionen auf die versandten Anschreiben waren vielfältig und unterschiedlichster Natur. Wir hatten enorme Aufklärungsarbeit, vor allem telefonisch und per E-Mail, zu leisten und zahlreiche schriftliche Rückmeldungen zu verarbeiten. Es war festzustellen, dass viele der angeschriebenen Webseitenbetreiber überhaupt nicht (mehr) vom Einsatz von Google Analytics auf ihrer Homepage wussten und der überwiegende Anteil dankbar für die gegebenen Hinweise war. Vielfach wurde angekündigt, sich umgehend der Angelegenheit anzunehmen und für eine Umsetzung der zu ergreifenden Maßnahmen zu sorgen. Allerdings haben auch 247 Webseitenbetreiber keinerlei Reaktion auf unser Anschreiben gezeigt, so dass wir uns mit einem weiteren Schreiben Ende Juni 2012 erneut an diese Webseitenbetreiber gewandt haben.

Bei einem zweiten technischen Prüflauf, der sich nur noch auf die fehlende Implementierung der Anonymisierungsfunktion bezogen hat, haben wir festgestellt, dass in 105 Fällen diese Funktion immer noch nicht in die Webseite eingebunden wurde und hiervon 12 Webseitenbetreiber uns entgegen ihrer gesetzlichen Auskunftspflicht aus § 38 Abs. 3 BDSG zudem keine schriftliche Rückmeldung haben zukommen lassen.

Als Konsequenz wurde gegen diese 105 Webseitenbetreiber im August 2012 ein Bußgeldverfahren eingeleitet und ihnen ein entsprechendes Anhörungsschreiben zugesandt. Auch wenn der Bußgeldtatbestand bereits erfüllt war, haben wir gegenüber den Webseitenbetreibern, die zwar erst auf das Anhörungsschreiben hin, aber dann unverzüglich für eine entsprechende Konfigurierung von Google Analytics gesorgt haben, das Bußgeldverfahren wieder eingestellt. Übrig geblieben sind letztendlich sechs Fälle, die die Anonymisierungsfunktion nicht vorgesehen und sich teilweise zusätzlich auch geweigert haben, Auskunft zu geben. In diesen sechs Fällen haben wir Bußgeldbescheide erlassen, die alle ohne Gerichtsentscheidung unanfechtbar geworden sind.

Die Reaktionen auf diese Prüfaktion waren insbesondere bei den betrieblichen Datenschutzbeauftragten überwiegend sehr positiv. Diese wiesen darauf hin, dass durch unsere Aktion manchen Unternehmen überhaupt erst bewusst geworden sei, dass es eine Datenschutzaufsichtsbehörde gebe und nunmehr in Kenntnis einer drohenden sonstigen Kontrolle den Empfehlungen der Datenschutzbeauftragten über Google Analytics hinaus mehr Gehör geschenkt werde.

4.1.4 Online-Veröffentlichung von behördlichem Schriftverkehr mit personenbezogenen Daten von Behördenmitarbeitern

Die Veröffentlichung behördlichen Schriftverkehrs, der personenbezogene Daten von Behördenmitarbeitern enthält, ist unzulässig, soweit das Interesse des Behördenmitarbeiters am Ausschluss der Veröffentlichung überwiegt. Ebenso bedarf es bei sonstigen Veröffentlichungen personenbezogener Daten von Behördenmitarbeitern einer Interessenabwägung.

Bereits im letzten Tätigkeitsbericht hatten wir die datenschutzrechtliche Relevanz der Veröffentlichung personenbezogener Daten im Internet dargestellt (vgl. dort Ziffer 4.1, S. 22 ff.). Im aktuellen Berichtszeitraum häuften sich nunmehr die Eingaben und Anfragen zu der speziellen Thematik der Veröffentlichung behördlichen Schriftverkehrs und personenbezogener Daten von Behördenmitarbeitern durch nicht-öffentliche Stellen auf deren Webseiten.

Bei der Veröffentlichung behördlichen Schriftverkehrs im Internet (eingescannte Briefe, Screenshots bzw. Kopien von E-Mails) wurden von privaten Webseitenbetreibern personenbezogene Daten von Behördenmitarbeitern in das Internet eingestellt, d. h. etwaige Namen und Kontaktdaten auf den Schriftstücken wurden nicht unkenntlich gemacht bzw. „abgeschnitten“. Ebenso nannten einige Homepagebetreiber - unabhängig von der Veröffentlichung behördlichen Schriftverkehrs - die zuständigen Behördenmitarbeiter im Zusammenhang mit ihrer behördlichen Tätigkeit beim Klarnamen. In beiden Fallgestaltungen brachte die veröffentlichende Stelle entweder im Zusammenhang mit der auf der Webseite veröffentlichten Äußerung oder durch eine direkte Kommentierung auf der Webseite ihre - überwiegend negative -

Meinung zu den Behördenmitarbeitern zum Ausdruck.

Da es sich bei der Veröffentlichung von personenbezogenen Daten im Internet um eine Übermittlung durch den Webseitenbetreiber gem. § 3 Abs. 4 Nr. 3 b BDSG handelt, bedarf es dafür grundsätzlich einer datenschutzrechtlichen Erlaubnis (§ 4 Abs. 1 BDSG). Diese kann entweder in einer Einwilligung oder einer Erlaubnisnorm liegen. Eine Einwilligung in die Veröffentlichung der personenbezogenen Daten außerhalb der Internetpräsenz der Behörde ist regelmäßig nicht gegeben. Eine Erlaubnisnorm kann § 28 Abs. 1 Satz 1 Nr. 2 BDSG sein. Hierbei sind die Interessen der veröffentlichenden Stelle und deren Recht auf Meinungsfreiheit (Art. 5 Abs. 1 GG) mit den Interessen der betroffenen Person und deren Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) gegeneinander abzuwägen.

Oftmals ist ein überwiegendes berechtigtes Interesse der veröffentlichenden Stelle an der direkten oder mittels eines Schriftstückes erfolgten Namensnennung eines Behördenmitarbeiters nicht gegeben. Dem Interesse der veröffentlichenden Stelle an der Veröffentlichung eines Verwaltungsvorganges und dem Interesse der Öffentlichkeit, über diesen Vorgang informiert zu werden, kann regelmäßig auch durch Veröffentlichung einer anonymisierten Version von Schriftstücken, die „einem Mitarbeiter der Behörde XY“ zugeschrieben wird, entsprochen werden.

Dies gilt selbst dann, wenn der Behördenmitarbeiter auf der Homepage der Behörde für jedermann einsehbar vorgestellt wird. Durch die Nennung im Zusammenhang mit einem Schreiben oder der konkreten Tätigkeit des Behördenmitarbeiters erhalten die auf der Homepage veröffentlichten personenbezogenen Daten eine neue Qualität. Von einer bloßen Wiedergabe allgemein zugänglicher Daten kann deshalb nicht (mehr) ausgegangen werden. Gleichwohl kommt es im Kern auf eine Interessenabwägung im Einzelfall an, wobei insbesondere die Position des Behördenmitarbeiters und der Kontext der Veröffentlichung mit einzubeziehen sind. Ebenso sind konkrete Folgen der Veröffentlichung, wie beispielsweise eine Anfeindung oder Gefährdung durch Dritte, bei der Interessenabwägung zu beachten.

Soweit es sich bei der veröffentlichenden Stelle allerdings um ein Unternehmen oder ein Hilfsunternehmen der Presse handelt, welches ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken personenbezogene Daten erhebt, verarbeitet oder nutzt, finden die Regelungen des BDSG lediglich eingeschränkt Anwendung (vgl. § 41 BDSG, § 57 RStV). Insbesondere § 4 Abs. 1 BDSG, der für einen zulässigen Umgang mit personenbezogenen Daten eine Erlaubnis in Form einer Einwilligung oder eines Gesetzes verlangt, kommt in diesem Fall nicht zur Anwendung. Diese Privilegierung gilt für die Presse im verfassungsrechtlichen Sinne, also auch für die elektronische Presse (vgl. Spick-mich-Urteil des BGH vom 23.06.2009, Az.: VI ZR 196/08), aber - jedenfalls nach deutschen Recht - nicht für jeden Blogger im Internet. Anzumerken ist jedoch, dass das datenschutzrechtliche Medienprivileg das Bestehen eventueller zivilrechtlicher Ansprüche unberührt lässt.

4.1.5 Cloud Computing

Cloud Computing ist einer der „Megatrends“ der letzten Jahre im Bereich der elektronischen Datenverarbeitung. Datenschutzrechtlich ergeben sich Probleme insbesondere daraus, dass einerseits eine über mehrere Stufen geteilte Datenverarbeitung stattfindet und anderseits der Auftraggeber häufig nicht weiß und auch keinen Einfluss darauf hat, wo seine Daten verarbeitet werden.

Ein Merkmal des Cloud Computing ist, dass die Daten nicht mehr lokal beim Anwender, sondern ausgelagert bei einem Dienstleister, dem Cloud-Anbieter, gespeichert und verarbeitet werden. Der Anwender greift über das Internet auf die Daten zu. Wesentliches Kennzeichen des Cloud-Computing ist darüber hinaus, dass der Anwender nicht in jedem Falle feststellen kann, wo sich die Daten zu einem bestimmten Zeitpunkt befinden, da der Ort der Speicherung wechseln kann. Wesentliche Fallgruppen des Cloud Computing sind:

- Infrastructure as a Service (IaaS): Hierbei stellt der Cloud-Anbieter den Anwendern IT-Ressourcen, meist Speicherressourcen, Rechenkapazitäten oder Kommunikationsverbindungen zur Verfügung.
- Platform as a Service (PaaS): Der Cloud-Anbieter bietet den Anwendern eine Plattform an, auf der die Anwender eigene Anwendungen entwickeln können. Die Anwender haben meist keine oder allenfalls sehr begrenzte administrative Zugriffsmöglichkeiten auf die Infrastruktur.
- Software as a Service (SaaS): Hier werden dem Cloud-Anwender vom Cloud-

Anbieter nicht nur Infrastruktur und Plattform, sondern auch Anwendungssoftware zur Verfügung gestellt. Der Anwender nutzt die Software üblicherweise über einen Web-Browser oder über spezielle Anwendungsprogramme und hat in aller Regel keinen administrativen Zugriff auf die bereitgestellten Ressourcen.

Cloud-Anwendungen, wie Dropbox, Apple iCloud oder Google Drive, sind auch für Unternehmen oft attraktiv, weil sich Kosten sparen lassen, indem die entsprechenden Ressourcen nicht mehr vom Unternehmen selbst angeschafft, vorgehalten und gewartet werden müssen. Verbunden ist dabei die Erwartung, dass auch entsprechende Einsparungen bei Personalkosten möglich sind.

Soweit Cloud-Anwendungen auch zur Verarbeitung personenbezogener Daten verwendet werden sollen, stellen sich datenschutzrechtliche Fragen, die nur zum Teil neu sind. Die Auslagerung der Verarbeitung personenbezogener Daten an spezialisierte Dienstleister („Outsourcing“) als solche ist nicht neu, vielmehr kennzeichnet diese auch die herkömmliche Auftragsdatenverarbeitung. Darüber hinausgehende Fragestellungen erwachsen vor allem daraus, dass der Anwender in der Regel nicht weiß, an welchen Orten und auf welchen Systemen seine Daten zu einem bestimmten Zeitpunkt verarbeitet werden, insbesondere dann, wenn der Cloud-Anbieter Teile der von ihm zu erbringenden Leistungen bei anderen Unternehmen einkauft. Die Frage einer effektiven Kontrolle der Verarbeitung personenbezogener Daten durch den Auftraggeber ist daher besonders virulent.

Datenschutzrechtlich werden Cloud-Computing-Anwendungen in den meisten Fällen als Auftragsdatenverarbeitung im Sinne von § 11 BDSG einzuordnen sein. Typischerweise bieten Cloud-Anbieter ihre Leistungen, z. B. die Zur-Verfügung-Stellung von Software, am Markt einer grundsätzlich unbeschränkten Anzahl potentieller Kunden an, häufig gerade auch kleineren und mittleren Unternehmen. Damit steht in der Regel eine große Anzahl an Auftraggebern einem einzelnen großen Cloud-Anbieter als Auftragsverarbeiter gegenüber, der nicht selten für Teile seiner Leistungen Unterauftragsverarbeiter (aus dem eigenen Konzern oder konzernfremd, in- oder außerhalb der EU bzw. des EWR) einzuschalten plant. Die maßgebliche datenschutzrechtliche Herausforderung besteht darin, sicherzustellen, dass der Auftraggeber unter diesen Umständen die Verarbeitung noch hinreichend kontrollieren kann. Dies setzt zunächst vor allem die Transparenz der Datenverarbeitungen für den Cloud-Anwender voraus. Des Weiteren müssen vertragliche Regelungen getroffen werden, die auch in einer Cloud-Umgebung den Anforderungen des § 11 BDSG an Auftragsdatenverarbeitung genügen.

Die deutschen Datenschutzaufsichtsbehörden haben bereits 2011 in der „Orientierungshilfe Cloud Computing“ erläutert, unter welchen Voraussetzungen Cloud-Computing-Dienste in datenschutzrechtskonformer Weise eingesetzt werden können.

Siehe:
www.datenschutz-bayern.de >> Themen >> Technik und Organisation >> Vernetzung >> Cloud Computing

Am 1. Juli 2012 hat schließlich die Artikel-29-Gruppe der Datenschutzbehörden der EU-Mitgliedstaaten in einem Arbeitspapier (Working Paper 196) ebenfalls eine ausführliche Stellungnahme zu den datenschutzrechtlichen Anforderungen an Cloud Computing veröffentlicht. Um Wiederholungen zu vermeiden, soll an dieser Stelle auf diese Papiere verwiesen und lediglich stellvertretend auf einige wenige Problemkreise hingewiesen werden, die besondere Schwierigkeiten aufwerfen.

Siehe:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf

Besondere Herausforderungen bereitet auch und gerade beim Cloud Computing die mehrstufige Unterauftragsvergabe (siehe auch Kapitel 12.1). Meist wird der Cloud-Anbieter für seine Leistungen mehrere Unterauftragnehmer einschalten wollen. Dies ist wie bei jeder Auftragsdatenverarbeitung nur auf der Grundlage einer entsprechenden Einwilligung des Cloud-Anwenders zulässig, was vertraglich sichergestellt werden muss. Sollen Unterauftragnehmer im Laufe der Verarbeitung wechseln, muss der Cloud-Anbieter (Auftragsverarbeiter) vertraglich ausdrücklich verpflichtet werden, dem Anwender/Kunden (Auftraggeber) neu hinzukommende Unterauftragnehmer zu nennen, und zwar bevor die Daten an den neuen Unterauftragnehmer weitergegeben werden. Der Auftraggeber muss die Möglichkeit haben, solchen Änderungen, d. h. einer bestimmten Unterbeauftragung, zu widersprechen oder den Vertrag zu beenden. Dies hat die Artikel-29-Gruppe ausdrücklich festgehalten (vgl. WP 196, Nr. 3.3.2 auf Seite 12 unten und Nr. 4.1 auf Seite 25 oben). Diese Anforderung ist für die Praxis häufig kritisch, da Cloud-Anbieter

typischerweise daran interessiert sein dürften, selbst möglichst frei über die Einschaltung und den Wechsel von Unterauftragsverarbeitern zu entscheiden. Datenschutzrechtlich wäre jedoch eine Einschaltung von (bestimmten) Unterauftragnehmern gegen oder ohne den Willen des Auftraggebers nicht hinnehmbar. Andernfalls wäre das zwingende Mindestmaß an notwendiger Kontrolle im Auftragsdatenverarbeitungsverhältnis nicht gewährleistet. Unternehmen, die die Nutzung eines Cloud-Dienstes erwägen, müssen sich daher entsprechende Informationsansprüche und Rechte gegenüber dem Cloud-Anbieter zwingend vertraglich einräumen lassen, auch wenn diese Forderung hinsichtlich ihrer Durchsetzbarkeit gerade gegenüber großen Cloud-Anbietern auf praktische Schwierigkeiten stoßen mag.

Eine weitere praktische Schwierigkeit dürfte nicht selten darin bestehen, dass den Cloud-Anwendern, d. h. den Auftraggebern im Sinne von § 11 BDSG, Kontrollrechte auch gegenüber eingeschalteten Unterauftragsverarbeitern eingeräumt werden müssen (siehe hierzu ausführlich Kapitel 12.2).

Hinzuweisen ist noch darauf, dass für alle Cloud-Angebote, bei denen personenbezogene Daten bei Cloud-Anbietern und/oder Unterauftragnehmern in Drittstaaten ohne angemessenes Datenschutzniveau verarbeitet werden sollen, neben den Anforderungen aus § 11 BDSG die an Datenweitergaben in Drittstaaten ohne angemessenes Datenschutzniveau zu stellenden Anforderungen gemäß §§ 4b, 4c BDSG gelten. Mithin müssen hier z. B. mittels Standardvertragsklauseln ausreichende Datenschutzgarantien bei den Cloud-Anbietern und Unterauftragnehmern in Drittstaaten erbracht werden.

Dabei bestehen auch beim Cloud Computing die unter Nr. 12.1 dieses Berichts näher geschilderten praktischen Schwierigkeiten bei Unterauftragsvergaben durch im EWR niedergelassene Haupt-Auftragsverarbeiter an in Drittstaaten niedergelassene Unterauftragsverarbeiter. Wie bei der „herkömmlichen“ Auftragsdatenverarbeitung ist auch beim Cloud Computing bei dieser Fallgestaltung in der Regel der Direkt-Abschluss eines Standardvertrags zwischen (jedem) Auftraggeber (hier: Cloud-Anwender/Kunde) und (jedem) Drittstaats-Unterauftragsverarbeiter erforderlich, da eine Unterauftragsvergabe durch den im EWR niedergelassenen Haupt-Auftragsverarbeiter (hier: Cloud-Anbieter) im eigenen Namen auf der Basis der Standardvertragsklauseln zur Auftragsdatenverarbeitung nicht möglich ist (siehe Kapitel 12.1).

4.1.6 Identitätsdiebstahl

Nutzer sozialer Netzwerke sollten bei Freundschaftsanfragen entsprechend sensibilisiert sein und gegebenenfalls auf anderem Weg, d. h. persönlich oder per Telefon, nachfragen und nicht jede Anfrage „blind“ akzeptieren. Nicht hinter jeder Freundschaftsanfrage verbirgt sich tatsächlich ein Freund.

Im Zeitalter zahlreicher verschiedener sozialer Netzwerke und ähnlicher Web-Communities besteht die Gefahr, dass sich eine Person bewusst mit Profilinformationen einer anderen Person - von Name über Geburtsdatum bis Profilbild - registriert und Dritten wiederum vortäuscht, die eigentliche Person zu sein. Durch rufschädigende Äußerungen im Web kann die Person den Betroffenen sehr stark in seinem Persönlichkeitsrecht verletzen. Noch problematischer wird es, wenn der Vortäuscher durch den Identitätsdiebstahl auch noch Zugriff auf vertrauliche Informationen des eigentlichen Nutzers erhält oder mit der gestohlenen Identität sogar Einkäufe im Namen des Betroffenen tätigt und somit einen Betrug begeht. Oftmals versucht der „Dieb“ auch, sich mit der gestohlenen Identität die Freundschaft von Personen zu erschleichen, um weitere Informationen zu erhalten. Aufgrund der weiten Vernetzung im Internet und existierenden Personensuchmaschinen lässt sich oft ein umfangreiches Hintergrundwissen über einzelne Personen aufbauen, das eine Täuschung eines vermeintlichen Bekannten und eines neuen Opfers ermöglicht.

Im vergangenen Berichtszeitraum wurden uns bislang nur wenige solcher Fälle gemeldet, die zudem ausschließlich bei Facebook stattfanden. Hier wurden unter falschen Namen mit gestohlenen persönlichen Informationen beleidigende Aussagen getroffen. Den Betroffenen konnte dann geholfen werden, wenn über andere Kanäle herausgefunden werden konnte, wer sich hinter dem falschen Account verbirgt.

Als kleinen Beitrag zur Prävention haben wir den Flyer „Internet - bist du dabei?“ für Kinder und Jugendliche entwickelt, um sie für Gefahren sozialer Netzwerke zu sensibilisieren.

Siehe:
www.lda.bayern.de >> Bürger-Information

4.2 Technische Fragestellungen des Datenschutzes im Internet

4.2.1 Löschung von Daten aus dem Internet

Das Entfernen personenbezogener Daten aus dem Internet stellt sich häufig als anspruchsvolle und manchmal leider auch als unlösbare Aufgabe dar.

Es ist recht einfach, Daten über sich und andere Personen im Web zu veröffentlichen. Zahlreiche Portale bieten an, nach kurzer Registrierung beliebige Daten ins Netz zu stellen. Dabei ermöglichen die wenigsten Webseiten den Nutzern gleich zu Beginn schützende Privatsphäre-Einstellungen so zu treffen, dass der Kreis der zugriffsberechtigten Nutzer eingeschränkt wird. Auf vielen Plattformen ist es sogar ausdrücklich erwünscht, dass möglichst viele Informationen über die eigene Person öffentlich zugänglich sind. Dies hat meist zur Folge, dass diese personenbezogenen Daten dann größtenteils auch über Suchmaschinen zu finden sind. Den betroffenen Nutzern wird dieser Umstand erst bewusst, wenn es tatsächlich zu spät ist: Die eigenen persönlichen Daten stehen für jeden frei zugänglich im Netz. Schon ein simples Suchen nach dem eigenen Namen zeigt sehr schnell, welche Daten auch der Rest der Welt mühelos auffinden kann.

Aus diesem Grund hatten wir zahlreiche Beschwerden zu persönlichen Daten, die aus dem Netz gelöscht werden sollten. Häufig waren es Bilder, die wissentlich in sozialen Netzwerken oder anderen Portalen hochgeladen wurden, die dann für den Nutzer überraschend auch in Suchmaschinen auffindbar waren. Ursache waren zumeist falsch getroffene Account-Einstellungen, die den Kreis der zugriffsberechtigten Personen nicht einschränkten. Die Betroffenen wollten dann oftmals selbst das entsprechende Bild von der eigentlichen Seite löschen, stellten aber nach kurzer Zeit fest, dass sich manche Daten nicht einfach löschen ließen oder über Suchmaschinen noch immer auffindbar waren.

Wir haben den Betroffenen, die sich an uns gewendet haben, dahingehend geholfen, dass wir konkrete Schritte aufgezeigt haben, um ihre Daten aus dem Internet löschen zu lassen. Im Allgemeinen gilt, dass der Betroffene zuerst versuchen muss, über die Webseite seine Daten löschen zu lassen, auf der die Daten veröffentlicht wurden. Bei manchen Plattformen besteht die Möglichkeit, über eigens hierfür eingerichtete Supportstellen gezielten Kontakt mit dem Webseitenbetreiber aufzunehmen und das Löschbegehren vorzutragen. Dies läuft im Internet häufig unter dem Begriff „Abuse“, d. h. Missbrauch melden. Besteht keine Anlaufstelle auf der Webseite, kann der Webseitenbetreiber auch schriftlich mit der exakten URL des zu entfernenden Datums kontaktiert werden, falls keine Löschroutinen vorhanden sind. Wir haben dabei folgende Erfahrung gemacht: Je konkreter die Betroffenen ihr Anliegen beschrieben und begründet hatten, desto höher war die Wahrscheinlichkeit, dass ihrem Begehren direkt nachgegangen wurde. Eine Herausforderung besteht jedoch teilweise darin, dass sich der Betroffene online gegenüber der verantwortlichen Stelle auch als der wirklich Betroffene ausweisen kann. So fordern einige Firmen aus legitimen Gründen weitere Informationen an, um sicherzustellen, dass kein Missbrauch stattfindet und persönliche Daten anderer Personen unberechtigt gelöscht werden.

Sofern es sich um bayerische Webseitenbetreiber handelt, können wir als Aufsichtsbehörde tätig werden und direkt an die verantwortlichen Stellen herantreten, um die Löschung der betroffenen Daten auf der jeweiligen Webseite zu bewirken, falls ein Herantreten des Betroffenen selbst nicht erfolgreich war. Bei ausländischen Webseitenbetreibern existiert dagegen für uns neben der oftmals nicht gegebenen Eröffnung des Anwendungsbereichs des BDSG und den abweichenden gesetzlichen Grundlagen des betroffenen Staates noch die Schwierigkeit, dass es bisweilen nicht möglich ist, an den Betreiber der Webseite oder das Hosting-Unternehmen überhaupt heranzutreten. Das liegt daran, dass es heutzutage problemlos möglich ist, über spezialisierte ausländische IT-Firmen Internetdomains zu registrieren und Webseiten zu betreiben, ohne persönliche Informationen über sich Preis zu geben. Diese ausländischen Dienstleister schützen die Webseitenbetreiber gezielt durch anonyme Angaben und manchen so eine Rückverfolgung für uns schwierig und im Einzelfall sogar unmöglich. So kann zwar stets die IP-Adresse und somit der Server mit den relevanten Daten ermittelt werden, jedoch wird ein weiteres Vorgehen aufgrund der genannten Hindernisse ausgeschlossen.

In den meisten uns gemeldeten Fällen wurden die Daten von der eigentlichen Webseite ohne größere Verzögerung entfernt. Man fand die dort gelöschten Informationen jedoch oftmals noch im Zwischenspeicher (Cache) von Suchmaschinen. Der

Grund dafür liegt darin, dass einerseits Sinn und Zweck von Suchmaschinen ist, öffentlich zugängliche Informationen aus dem Web wiederzugeben und andererseits die Suchmaschinen-Crawler (Programme, die das Internet gezielt analysieren) nur in bestimmten Intervallen die Webseiten nach Änderungen durchsuchen. Erst nachdem der Crawler die betroffene Webseite erneut durchsucht hat, wird der gelöschte Datensatz auch aus den Suchergebnissen der Suchmaschine entfernt. Da dieses Zeitintervall je nach Webseite und Suchmaschine stark variiert und manche Inhalte zeitnah entfernt werden sollten, gab es Fälle, in denen wir die Betroffenen auch dahingehend beraten haben, die Suchmaschinenbetreiber zu kontaktieren, damit die gelöschten Einträge auch aus dem Such-Cache unmittelbar gelöscht werden. Dabei existieren je nach Betreiber unterschiedliche Verfahren, um Ergebnisse gezielt löschen zu lassen. Die meisten Suchmaschinen präsentieren jedoch bereits bei der Anzeige von Suchergebnissen dem Nutzer die Möglichkeit, unangemessene Beiträge entfernen zu lassen.

4.2.2 Datensicherheit bei Webshops

Webshops gehen mit ihren Kundendaten nicht immer sorgsam um, d.h. schützen nicht ausreichend vor unbefugtem Zugriff, lassen unsichere Passworte zu oder übertragen diese unverschlüsselt.

Der Zugang zu einem Webshop erfolgt in der Regel über einen zentralen Login mit Benutzername und Passwort, die in einem kurzen Registrierungsprozess meist durch den Webshop-Kunden eigenständig auf der Shopseite angelegt werden. Viele, insbesondere Besitzer kleinerer Webshops zeigten häufig kein ausgeprägtes Verständnis für die notwendigen Sicherheitsvorkehrungen, um die Daten ihrer Kunden angemessen zu schützen. So erreichten uns beispielsweise Beschwerden betroffener Kunden über frei in Suchmaschinen auffindbare Rechnungen, Bestellungen und Lieferscheine mit persönlichen Daten des Kunden. Ursache hierfür waren nicht ausreichend abgesicherte Verzeichnisstrukturen oder Datenbanken des Webshops.

Auch wurden von uns Defizite im Bereich der Passwortsicherheit festgestellt. Bei manchen Web-Shops konnte man sich aufgrund fehlender Passwortprüfung (siehe auch Kapitel 19.2) mit beliebigen unsicheren Passwörtern wie „123“ registrieren. Zudem wurde das bei der Registrierung eingegebene Passwort in einem uns gemeldeten Fall auch direkt im Klartext zusammen mit dem Benutzernamen per E-Mail an den Nutzer geschickt. Dies ist aus sicherheitstechnischen Gründen ebenso wie eine Speicherung des Passworts im Klartext seitens des Webshop-Betreibers nicht ausreichend.

Des Weiteren haben wir mehrmals die fehlende HTTPS-Verschlüsselung im Browser festgestellt. Wir haben in diesen Fällen von den Unternehmen den Einsatz einer SSL-Verschlüsselung zur sichereren Datenübertragung im Rahmen der Shopnutzung gefordert, da dies unserer Ansicht nach für den Betrieb auch kleinerer Webshops nach § 9 BDSG eine unverzichtbare Voraussetzung darstellt. Der Aufwand dieser Maßnahme liegt in einem zumutbaren Verhältnis zum angestrebten Schutzzweck.

Festzuhalten gilt, dass zwar einige von uns kontaktierte Webshop-Betreiber sich der Wichtigkeit der IT-Sicherheit scheinbar nicht umfänglich bewusst waren, nach unserem Tätigwerden jedoch reagierten und Maßnahmen ergriffen, um auf ein höheres Sicherheitsniveau zu gelangen.

4.2.3 E-Mail-Kommunikation: Spam, Phishing und Scamming

Durch eigene Vorsicht können Gefahren bei der E-Mail-Kommunikation im Umgang mit Spam, Phishing und Scamming in großem Umfang gebannt werden. Vollständig ausschließen kann man diese Gefahren jedoch nicht.

Der elektronische Informationsaustausch findet heutzutage in sehr großem Umfang per E-Mail statt. Aufgrund des in der Regel kostenlosen Service erscheint dieser Kommunikationskanal verlockend, um Empfänger mit unerwünschten Nachrichten zu überhäufen - angefangen von scheinbar harmlosen Werbeangeboten bis hin zu gezielten Betrugsabsichten. Immer wieder erreichten uns Beschwerden von Bürgern über Spam-Nachrichten. Unter Spam versteht man nicht angeforderte kommerzielle E-Mails, ähnlich wie klassische unerwünschte Werbepost im Briefkasten. Teilweise war es technisch nicht möglich, den tatsächlichen Versender der unerwünschten Nachrichten ausfindig zu machen, da einige Versender gefälschte Absenderadressen nutzen oder über ausländische Server agieren, die keinen Rückschluss über den tatsächlichen Spam-Initiator ermöglichen.

Während beim Spammen primäres Ziel ist, die Mailkonten der Nutzer mit Werbemails zu überfluten, werden beim Phishing (engl.: Kunstwort aus password fishing - betrügerisches Entlocken sensibler Daten) gezielte Angriffe auf Passwörter unternommen, um sich Kennwörter zu angeln und sich mit den Zugangsdaten des Opfers in Systeme einzuloggen. Phishing ist daher als Form des Betrugs einzustufen. Oftmals erfolgt dies über die Methodik des sogenannten Social Engineering, bei dem sich Fremde als scheinbar vertrauenswürdige Bekannte ausgeben, um an sensible Daten zu gelangen. In den uns gemeldeten Fällen haben wir neben einer technischen Information an die jeweilige Strafermittlungsbehörde verwiesen.

Als wirkungsvolle Schutzmaßnahme gegen Spam und Phishing empfehlen wir Bürgern, die eigene E-Mail-Adresse grundsätzlich nur denjenigen weiterzugeben, mit denen man einen weitergehenden Kontakt wünscht. Sollte dennoch eine merkwürdig erscheinende Nachricht im Posteingang liegen, gilt es zuallererst den Absender und die zugehörige E-Mail-Adresse zu prüfen, anstatt die Nachricht automatisch zu öffnen. Bei unbekanntem Absender ist besondere Vorsicht geboten. Auch der Betreff der E-Mail-Nachricht sollte genau angesehen werden, da Spam und Phishing-Nachrichten häufig verdächtige Titel tragen. Erscheint die Nachricht bis dahin seriös, sollte der darin enthaltene Text geprüft werden. Besondere Aufmerksamkeit sollte insbesondere den in der E-Mail enthaltenen Links und Dateianhängen gelten. Hinter diesen verbergen sich zuweilen schädliche Links zum Zwecke von Phishing oder Schadcode, um auf dem Gerät Malware zu installieren. Auch wenn die Nachricht möglicherweise neugierig macht, sollte man sie besser löschen, ohne die Dateianhänge zu öffnen.

Vor allem Unternehmen, die uns über ein hohes Spam-Aufkommen informierten, haben wir empfohlen, entsprechende Schutzsoftware einzusetzen. Mittlerweile existieren zahlreiche sehr effektive Produkte, um am E-Mail-Gateway Nachrichten zu filtern. Diese technischen Filtersysteme sortieren unerwünschte Nachrichten aus, in dem eingehende Nachrichten z. B. nach verdächtigen Schlüsselwörtern, bekannten Spam-Absendernamen und -adressen sowie gefährlichen Dateianhängen durchsucht werden. Im Übrigen verweisen wir in diesem Zusammenhang auch auf die Homepage des Bundesamts für Sicherheit in der Informationstechnik (BSI), auf der man sich einen aktuellen Überblick zur Bedrohungslage verschaffen kann.

Siehe:
www.bsi.bund.de

Als Sonderfall treten auch sog. „Scamming"-Versuche (engl.: betrügen) auf. Inhaltlich wurde z. B. in einer elektronischen Nachricht dem Bürger eine Menge Geld versprochen: *„fuer Ihre Zusammenarbeit gebe ich Ihnen 50% des Vermoegens"*. Ziel des Absenders war es, durch sehr hohe Gewinnversprechen den E-Mail-Empfänger zu einer Vorauszahlung zu verleiten, ohne dass später der versprochene Gewinn überwiesen wird. Diese Form des Vorschussbetrugs ist schon lange unter dem Namen „Nigeria Connection" bekannt und tritt in vielfältiger Form in Erscheinung. Die Strafverfolgung im Falle eines finanziellen Schadens ist in solchen Fällen sehr schwierig, da die Täter oft aus dem Ausland agieren. Aus diesem Grund ist zu empfehlen, E-Mails solcher Art gänzlich zu ignorieren und als Spam zu deklarieren, so dass künftige E-Mails dieses Absenders nicht mehr im Posteingang landen. Weitere Informationen zu Scamming finden sich auf den Webseiten der polizeilichen Kriminalprävention.

Siehe:
www.polizei-beratung.de >> Themen und Tipp >> Betrug >> Scamming

4.2.4 Geolokalisierung über IP-Adressen

Durch die IP-Adresse lässt sich eine ungefähre geographische Ortung des Webseitenbesuchers durchführen.

Ein technischer Themenkomplex, der datenschutzrechtlich ein zentrales Element im Rahmen der Reichweitenmessung von Webseiten darstellt und uns in unterschiedlichen Anfragen erreicht hat, ist die Geolokalisierung eines Webseitenbesuchers (auch Geotargeting genannt) über dessen IP-Adresse. Die IP-Adresse wird im Internetprotokoll (IP) grundsätzlich dazu verwendet, den Datenaustausch im Internet, z. B. beim Besuch einer Webseite, zu ermöglichen. Zwar ändert sich die IP-Adresse des Webseitenbesuchers durch das dynamische Vergabeverfahren regelmäßig, bewegt sich aber dennoch meist in einem beschränkten Adressraum. Dies liegt daran, dass je nach geographischem Ort nur ein bestimmtes Segment der IP-Adresse durch den Netzknoten zur Verfügung steht bzw. vom Provider vergeben wird. Da diese IP-Adresspools sich in der Regel nicht ändern, kann nach einmaligem Bekanntwerden der Geoposition einer IP-Adresse davon ausgegangen werden, dass die Geoposition gleich bleibt.

Im Rahmen unserer Tätigkeit erreichten uns mehrmals Anfragen, welche Anforderungen erfüllt werden müssen, um eine geographische Lokalisierung der eigenen Webseitenbesucher über IP-Adressen durchführen zu dürfen. Anwendung findet diese Fragestellung auch bei zugestellten Werbe-E-Mails, deren Inhalte passenden zum Aufenthaltsort des Empfängers ausgewählt werden sollen. Da durch eine IP-Adresse der Besitzer der Adresse und meistens auch der tatsächliche Nutzer herauszufinden ist, haben wir darauf hingewiesen, dass zur Verwendung dieses personenbezogenen Datums im Rahmen der Geolokalisierung die IP-Adresse so gekürzt werden muss, dass eine Anonymisierung stattfindet und somit ein Rückschluss auf den Webseitenbesucher nicht mehr möglich ist. In der Praxis geschieht dies meist durch das „Nullen“ des letzten Oktetts einer 32-stelligen IPv4-Adresse, was wir in den behandelten Fällen als zweckmäßig betrachtet haben. Man spricht dann im Allgemeinen von einer Geolokalisierung mit anonymisierten IP-Adressen. Inwieweit sich dies bei Einführung von IPv6 verändern wird bleibt abzuwarten - letztendlich hängt dies von der konkreten Umsetzung der Provider ab.

4.2.5 Webtracking: Software zur Prüfung von Reichweitenanalysen

Die Entwicklung eines eigenen Tools zur Online-Prüfung von Webtracking-Techniken ermöglicht auch in Zukunft unsere aufsichtliche Tätigkeit hinsichtlich Tracking im World Wide Web wahrzunehmen.

Das Surfen im Internet gehört mittlerweile wie das Fernsehen oder das Zeitunglesen zum täglichen Leben. Neben dem Einkaufen in Webshops werden Informationen gesucht, Kontakte über soziale Netzwerke gepflegt oder Videos auf Plattformen angesehen. Was vielen nicht bekannt sein dürfte, ist, dass viele Webseitenbesuche durch sogenannte Methoden zur Reichweitenmessung erfasst werden.

Die Erfassung des Surfverhaltens der Internetnutzer ist eine weit verbreitete Praxis, von der die Nutzer in der Regel nichts merken und auch nicht wissen, was mit den erfassten Daten geschieht. Da ein manuelles Analysieren einer Webseite zu aufwändig gewesen wäre, haben wir selbst ein kleines Software-Werkzeug zur automatischen Prüfung von vielen Webseiten geschrieben. Nur durch einen Mausklick kann dann eine großangelegte Prüfung mit mehreren tausend Webseiten gestartet werden. Nach einigen Stunden liegen die Ergebnisse vor, die ebenfalls automatisiert ausgewertet werden können. Diese Daten dienen dann auch als Grundlage für die Erstellung von Serienbriefen, mit denen die Webseitenbetreiber über das Ergebnis der Prüfung informiert und ggf. zur Änderung ihrer Programmeinstellungen aufgefordert werden (siehe auch Kapitel 4.1.3).

Die Software ist von der Konzeption einfach gehalten. Sie simuliert einen Browser, der anhand einer URL eine Webseite besucht. Durch Analyse der Webseite wird festgestellt, ob die geprüfte Technik zur Reichweitenanalyse (z. B. Google Analytics) eingesetzt wird. Ebenso werden die Datenschutzerklärungen bewertet. Die Software wurde modular entworfen, so dass die Implementierung einer Prüfroutine für eine neue Methode zur Reichweitenmessung nur wenige Zeilen Quelltext benötigt.

Wir werden diese automatisierten Möglichkeiten einer Online-Prüfung auch zukünftig beibehalten, da wir dadurch mit vergleichbar geringem Aufwand eine Vielzahl an Webseiten analysieren können, um anschließend den bayerischen Unternehmen gezielte Informationen für einen beanstandungsfreien Einsatz von Webtracking-Techniken zu geben.

4.2.6 Schülerdaten im Internet

Ein Softwarefehler in einer Webanwendung zur Bestellung von Schulessen offenbarte personenbezogene Daten von Schülern und Eltern.

Im Rahmen einer Eingabe haben wir eine Webapplikation untersucht, mit der Eltern für ihre Kinder das Essen in der Schule organisieren können. Dazu besaß jede registrierte Familie einen Account mit Zugangsdaten, mit denen die Anwendung über einen Internetbrowser bedient werden konnte. Neben Vor- und Nachname des Kindes waren auch zahlreiche weitere persönliche Informationen in dem System hinterlegt. So konnte man neben der Wohnanschrift des jeweiligen Kindes auch die Namen eines Erziehungsberechtigten einsehen. Zusätzlich war zu jedem Kind neben der Angabe der besuchten Schule auch ein Passfoto des Kindes im System abgespeichert, das im Rahmen der Essensausgabe in der Schule an der Kasse der Kantine angezeigt wird. Auch Informationen zur Befreiung von Zuzahlungen (z. B. bei Empfängern von ALG 2) und Angaben zu bestimmten Essenwünschen (z. B. kein Schweinefleisch) konnten

in der Webanwendung verwaltet werden. Zudem gab es für die Familien die Möglichkeit, vorhandene Abrechnungen und Bestellübersichten zu betrachten.

Grundsätzlich müssen diese Daten ausreichend vor unbefugtem Zugriff im Web abgesichert sein. In dem uns gemeldeten Fall war es jedoch durch Manipulation der URL-Parameter in Form von simplem Hochzählen von IDs auch für Laien möglich, nicht nur die Daten des eigenen Kindes, sondern von vielen anderen Kindern zu sehen. Da z. B. unter dem Webseitenverzeichnis …/essensverwaltung/123/index.html das Kind „Max Mustermann“ zu finden war, konnte man durch Ändern dieser ID auch auf Seiten anderer Kinder wie „Berta Beispiel“ auf …/essensverwaltung/124/index.html usw. gelangen. Als Ausgangspunkt benötigte man lediglich eine gültige ID eines Kindes, um das Muster der URL-Struktur zu erkennen. Da es einen frei zugänglichen Demozugang gibt, konnte man mühelos mit der ID des „Demo-Kindes“ auf Daten anderer Kinder von anderen Schulen zugreifen. Diese Schwachstelle in der Anwendung kommt in Webapplikationen nicht selten vor und wird unter dem Begriff „Mangelnder URL-Zugriffsschutz“ (OWASP Top 10 / 2010) bezeichnet.

Bezüglich der Sensibilität der Daten haben wir noch am selben Tage das Unternehmen, das die Webapplikation entwickelt hat und betrieb, zur Beseitigung der technischen Mängel aufgefordert. Eine formelle Anordnung nach § 38 Abs. 5 BDSG zur Beseitigung des fehlenden Zugangsschutzes war nicht notwendig, da das Unternehmen sehr schnell reagiert und den Fehler in der Software behoben hat. Schäden sind nach unserer Kenntnis bei den Betroffenen nicht entstanden.

4.2.7 Ungewollte Übertragung von Daten an Dritte

Benutzername und Passwort gehen unbeabsichtigt auf die Reise durchs Internet.

Neben dem eigenen Inhalt binden viele Webseiten Inhalte aus Quellen Dritter ein. Dies können Ressourcen wie Grafiken, Java-Script-Codes oder Videos sein. Häufig werden auch Techniken zur Reichweitenmessung oder Werbebanner eingebunden. Bei den meisten dieser Techniken wird ausführbarer Programmcode in Form von JavaScript verwendet. Dieser sammelt zum Beispiel bei Google Analytics Informationen der besuchten Webseite, wertet ggf. die Anonymisierungsfunktion aus und überträgt die Daten an die Server der Drittanbieter. Häufig wird auch die aktuelle URL als Bestandteil dieses Datenpaketes erfasst und übermittelt.

Die Kommunikation im Internet kann über das HTTP-Protokoll abgewickelt werden. Mit diesem kann entweder durch einen GET-Aufruf oder durch einen POST-Aufruf auf eine Aktion eines Webseitenbesuchers reagiert werden. Bei Webseiten, bei denen sich ein Besucher anmelden muss, werden auf diese Weise die Zugangsdaten übermittelt. Wird die Verbindung noch mit einer SSL-Verschlüsselung abgesichert, kann ein hohes Maß an Vertraulichkeit erreicht werden.

Eine Eigenheit eines HTTP-GET-Aufrufs ist, dass dieser die zu übertragenden Daten in Form von URL-Parametern kodiert. Dazu ein kleines Beispiel: Eine Person mit der E-Mail-Adresse „max.mustermann@mailprovider.de“ möchte in seinem Lieblingsonlineshop etwas einkaufen. Die Übertragung erfolgt immer verschlüsselt über eine HTTPS-Verbindung. Nachdem er einige Artikel in seinen Einkaufswagen gelegt hat, gibt er seine E-Mail-Adresse und sein Passwort „XD4&5_!!"gfE@R“, das er besonders sicher gestaltet hat, in die Anmeldemaske ein. Was er nicht weiß, ist, dass sein Lieblingsshop eine Schwachstelle in der Software besitzt. Durch den HTTP-GET-Aufruf steht in der URL seines Browsers nach der Eingabe der Zugangsdaten und Drücken des Einloggen-Buttons: https://www.meinlieblingsshop.de/login.php?user=max.mustermann@mailprovider.de&passwort=XD4&5_!!"gfE@R

Was er ebenfalls nicht weiß, ist, dass sein Lieblingsshop ein Werkzeug zur Reichweitenmessung, z. B. Google Analytics, eingebunden hat. Dieses Programm überträgt auch die aktuelle URL an die Server der Firma Google. Damit werden seine E-Mail-Adresse und sein Passwort an den Anbieter der Drittinhalte geliefert. Er kann nun nur noch hoffen, dass diese Daten vom Drittanbieter nicht aus der URL-Zeichenkette extrahiert und verwendet werden.

Das BayLDA ist dabei, eine Prüfung dieser Seiteneffekte durchzuführen. Bei der Mehrheit der Webangebote, die eine Registrierung erfordern, tritt dieser Seiteneffekt nicht auf, da diese das HTTP-Post-Verfahren verwenden, das keine Parameter in der URL kodiert und damit auch nicht an Drittanbieter übertragen kann. Die Webseiten, die eine Kombination von HTTP-GET-Verfahren bei der Übertragung von Zugangsdaten verwenden sowie Techniken zur Reichweitenmessung einsetzen,

werden vom BayLDA angeschrieben und aufgefordert, das Übertragungsverfahren umzustellen. Als Rechtsgrundlage dient hierfür die Anlage zu § 9 BDSG, die in Ziffer 2 (Zugangskontrolle) einen sicheren Umgang mit Zugangsdaten fordert. Der Aufwand der Umstellung ist relativ gering und kann von einem Softwareentwickler in kurzer Zeit angepasst werden.

4.2.8 Das datr-Cookie von Facebook

Ob das datr-Cookie von Facebook zum Schutz der Facebook-Mitglieder erforderlich ist oder für die Erstellung von Schattenprofilen von Nicht-Mitgliedern von Facebook genutzt wird, ist trotz zahlreicher Untersuchungen noch immer als offen zu bewerten.

Das Thema Facebook, vor allem mit seinen sogenannten Like-Buttons („Gefällt mir"-Schaltflächen), beschäftigte auch uns intensiv. Der Like-Button kann von Telemediendiensteanbietern in deren eigene Webseite eingebunden werden. Klickt ein Nutzer diesen Button, wird dieses Gefallen in dessen Facebook-Account, sofern er existiert, übernommen. Uns beschäftigte aber insbesondere die Frage, wie es mit Nutzern aussieht, die nicht Mitglied bei Facebook sind und damit nicht den Nutzungsbedingungen von Facebook zugestimmt haben. Besucht ein solcher Nutzer eine Webseite mit einem Like-Button, ohne den Button zu klicken, werden keine Cookies von Facebook auf dem Browser des Nutzers abgelegt. Eine Übermittlung der IP-Adresse an Facebook im Rahmen der Internetkommunikation findet zwar statt, ist aber im World Wide Web ein üblicher und technisch zwingend notwendiger Vorgang bei der Vernetzung von Inhalten und damit keine Besonderheit von Facebook. Klickt ein Nicht-Facebook-Mitglied auf den Like-Button, wird dieser auf die Webseite von Facebook mit der Möglichkeit, sich dort zu registrieren, weitergeleitet. Lehnt der Nutzer dies ab, indem er die Facebook Webseite schließt, findet er nach diesem Klick trotzdem ein Facebook-Cookie mit dem Namen „datr" auf seinem Browser vor. Dieses Cookie ist ein permanentes Cookies, das bei Beenden des Browsers nicht automatisch gelöscht wird. Besucht dieser Nutzer im Folgenden weitere Webseiten mit dem Facebook Like-Button, wird die ID dieses Cookies mit der Information, auf welcher Webseite sich der Nutzer befindet, an Facebook übertragen, auch wenn der Nutzer nicht auf den Like-Button klickt. Facebook könnte anhand dieser Informationen ein sogenanntes Schattenprofil mit einer Sequenz derjenigen besuchten Webseiten eines Nutzers erstellen, die auf dessen potentielles Kaufverhalten schließen lassen. Würde sich ein Nutzer zu einem späteren Zeitpunkt dazu entscheiden, sich bei Facebook zu registrieren, wäre es technisch problemlos möglich, dieses Schattenprofil (unter der Voraussetzung, dass der gleiche Browser verwendet wird) der konkreten Person zuzuordnen und dadurch entsprechende Werbung zu schalten.

Nach Aussage von Facebook, die bei einem Besuch eines offiziellen Vertreters von Facebook bei uns bestätigt wurde, soll das Cookie nicht der (Schatten-)Profilbildung dienen. Stattdessen sei dieses Cookie Bestandteil des umfassenden Sicherheitskonzepts von Facebook. So soll es auch dazu beitragen, dass gekaperte Facebook-Accounts, die zum Beispiel durch erfolgreiche Phishing-Angriffe auf die Nutzer entwendet wurden, besser erkannt werden können. Wäre dieses Cookie nicht bei einer Anmeldung bei Facebook vorhanden und deuteten weitere Sicherheitsmerkmale wie die Geolokalisierung der IP-Adresse auf einen systematischen Angriff hin, könnten weitere Merkmale wie die Erkennung auf der Freundesliste für eine Authentifizierung eingesetzt werden.

Nach unserer Auffassung kann dieses Cookie durchaus, wie von Facebook beschrieben, Teil einer umfassenden Sicherheitsstrategie sein. Vom Blick des Datenschutzes aus betrachtet besteht aber auch die Gefahr, dass neben der erhöhten Sicherheit für Facebook-Mitglieder auch ein umfassendes Benutzertracking sowohl von Facebook-Mitgliedern als auch von Nicht-Facebook-Mitgliedern möglich wäre. Der Einsatz dieses Cookies in dem gesamten Sicherheitskonzept ist für uns nicht schlüssig, da das Cookie bei Entwendung durch Hacking-Angriffe wie Session-Hijacking zum Risiko für Facebook-Mitglieder werden kann. Fragwürdig ist auch dessen Gültigkeitsdauer von 24 Monaten, die in einer Größenordnung liegt, die in der Praxis auch von Werkzeugen zum Online-Behavioural-Targeting oder zur Reichweitenanalyse verwendet wird. Da Facebook auf eine standardmäßige Verschlüsselung der Verbindung über HTTPS verzichtet, wird die Möglichkeit, dieses Cookie unrechtmäßig zu entwenden, je nach Angriffsszenario deutlich erleichtert.

Das Setzen dieses Cookies bei Nicht-Facebook-Mitgliedern, die auf einer Webseite auf einen Like-Button klicken, wäre nach unserer Auffassung aus Sicherheitsgründen nicht notwendig, da sich dieser Nutzer gar nicht bei Facebook einloggen würde. Da Cookies auch innerhalb eines Pfades einer Domäne gesetzt werden können, wäre eine Anpassung des

Facebook-Systems derart, dass dieses Cookie zumindest nur nach dem Einloggen gesetzt wird, mit geringem Aufwand möglich. Der Nutzer kann sich vor dieser Form der Schattenprofilbildung am besten schützen, indem die Cookies des Browsers bei Beenden des Browsers gelöscht werden. Dies kann aber bei anderen Webseiten zum Verlust von angenehmen Features (zum Beispiel in einem Webshop eingeloggt bleiben) führen. Facebook-Mitglieder kann bei Löschen der Cookies bei Beenden des Browsers eine Einstufung als potentieller Angreifer ereilen. In diesem Fall müssten beim Einloggen ohne Cookie weitere Sicherheitsmerkmale wie die Freundesliste oder die Mobilfunknummer angegeben werden - die mitunter wieder Informationen über den Nutzer enthalten.

Manchmal kommt es auf diese Weise zu einem Spannungsfeld zwischen Datenschutz mit den Prinzipien der Datensparsamkeit und der IT-Sicherheit, die möglichst viele Daten zur Erkennung von Angriffen speichern und auswerten möchte. Der Einsatz des datr-Cookies als reines Sicherheitsfeature überzeugt uns nicht vollständig, obwohl wir dessen Funktion im Rahmen einer umfassenden Sicherheitsstrategie durchaus sehen.

5 Auftragsdatenverarbeitung oder Funktionsübertragung

Abgrenzungsfragen zwischen Aufgabenauslagerungen (Funktionsübertragung) und Auftragsdatenverarbeitung

Schon im letzten Tätigkeitsbericht hatten wir die datenschutzrechtliche Abgrenzung bei Outsourcing-Sachverhalten zwischen einer Auslagerung bzw. externen Wahrnehmung von bestimmten Aufgaben und Funktionen eines Unternehmens durch Dritte einerseits und der Inanspruchnahme von weisungsgebundenen Hilfsleistungen im Rahmen einer Auftragsdatenverarbeitung nach § 11 BDSG andererseits aus unserer Sicht erläutert. Verantwortliche Stellen haben im Zweifel Interesse am Vorliegen einer Auftragsdatenverarbeitung, weil diese zu einer Privilegierung der Art führt, dass (weitere) materielle Vorschriften nicht zu prüfen sind, da im Gegenzug der Auftragnehmer nur nach Weisungen des Auftraggebers handeln darf.

Zu den nachfolgenden Sachverhalten wurden häufiger Anfragen zur Abgrenzung von Funktionsübertragung und Auftragsdatenverarbeitung an uns gerichtet.

5.1 Steuerberater und Wirtschaftsprüfer

Steuerberater und Wirtschaftsprüfer sind bei einer Beauftragung nach den insoweit geltenden Fachgesetzen (Steuerberatungsgesetz, Berufsordnung der Wirtschaftsprüfer) als Freiberufler selbständig, unabhängig und eigenverantwortlich tätig. Eine gewerbliche Tätigkeit ist ihnen grundsätzlich untersagt. Das widerspricht der Weisungsgebundenheit für eine Auftragsdatenverarbeitung im Sinne von § 11 BDSG, so dass ein Auftragsdatenverarbeitungsverhältnis für Steuerberater und Wirtschaftsprüfer regelmäßig nicht in Betracht kommt. Sie dürfen von den Mandanten im Rahmen der vertraglichen Beauftragung und der Erforderlichkeit für ihre Tätigkeit im Sinne von § 28 Abs. 1 Satz 1 Nr. 2 BDSG personenbezogene Kunden- und/oder Arbeitnehmerdaten erhalten und unterliegen speziellen strafbewehrten Geheimhaltungsverpflichtungen.

Ein klassischer Fall der weisungsgebundenen Auftragsdatenverarbeitung nach § 11 BDSG ist jedoch regelmäßig die Einschaltung von Dienstleistungsrechenzentren (wie z. B. der DATEV) durch Steuerberater zur IT-technischen Unterstützung.

5.2 Unternehmensberatung und Gutachter-Beauftragung

Die Voraussetzungen einer Hilfstätigkeit in Form einer weisungsgebundenen Auftragsdatenverarbeitung im Sinne von § 11 BDSG liegen dann nicht vor, wenn ein Externer erhebliche eigene intellektuelle (Haupt-)Leistungen erbringt und hierzu mit Daten des Auftraggebers umgeht, wie dies klassisch bei den fachlichen Prüfungsaufgaben eines Unternehmensberaters oder eines externen Gutachters gegeben ist. Hier ist bei der Datenweitergabe vom Auftraggeber an den Externen eine nach § 4 Abs. 1 BDSG zu beurteilende Übermittlung von Daten an einen Dritten gegeben.

Die Inanspruchnahme externer Fachstellen, wie Unternehmensberater oder Gutachter, kann unter Umständen als ein mögliches berechtigtes Interesse einer verantwortlichen Stelle gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG angesehen werden. Die Übermittlung von personenbezogenen Daten (z. B. durch Einsichtnahme) an Externe ist nach dieser Vorschrift jedoch nur zulässig, soweit es für den Prüfungszweck erforderlich ist, die Zweckbindung im Sinne von § 28 Abs. 5 BDSG sichergestellt ist und auch sonst ein angemessener datenschutzrechtlicher Rahmen für die externe Verwendung personenbezogener Daten, insbesondere mittels entsprechender Vertragsgestaltung, durch die verantwortliche Stelle geschaffen wird.

Siehe:
www.lda.bayern.de >> Fachthemen >> Auftragsdatenverarbeitung >> Häufige Fragen (insb. Punkt 2.1 letzter Absatz)

5.3 Internet- und E-Mail-Provider

Die vertragliche Beziehung für reine Internet-Zugangs- oder E-Mail-Dienste (ohne weitere Dienste oder Leistungen mit personenbezogenen Daten) bezieht sich auf eine Telekommunikationsleistung bzw. Telemediendienstleistung (Transportleistung, Zugangsvermittlung) und nicht darauf, Daten im Auftrag im Sinne von § 11 BDSG zu verarbeiten. Es gelten dann die spezialgesetzlichen Regelungen des TKG und/oder des TMG. Andere oder ergän-

zende Leistungen eines Providers dazu, wie das Speichern von Bestellvorgängen, das Archivieren von E-Mails im Auftrag, das Tracking der Internetzugriffe und Seitennutzungen im Auftrag, betreffen regelmäßig den Umgang mit personenbezogenen Daten des Vertragspartners (Auftraggebers) und sind dann grundsätzlich als Datenverarbeitung im Auftrag nach § 11 BDSG einzuordnen.

5.4 „Kreative“ Auftragsdatenverarbeitung

Ein Unternehmen (im Folgenden: Unternehmen A) vermittelte den Abschluss von Strom- und Gaslieferungsverträgen für unterschiedliche Anbieter und war aufgrund dessen im Besitz von Adressdaten und z. T. Telefonnummern der Kunden, denen ein Vertragsabschluss vermittelt worden war. Einige der Kunden erhielten ab einem bestimmten Zeitpunkt Anrufe eines anderen, ihnen unbekannten Unternehmens (im Folgenden: Unternehmen B), das ihnen den Abschluss von Verträgen über ein versicherungsartiges Produkt („Schutzbrief“) für bestimmte haushaltsbezogene Notfallreparaturen und Notfallhandwerkerleistungen anbot. Mehrere solcher Fälle wurden uns bekannt, wobei die Betroffenen jeweils angegeben hatten, keine Einwilligung in die Weitergabe ihrer Daten an ein solches Unternehmen erteilt zu haben.

Unsere Überprüfung ergab, dass das Unternehmen A, das Strom- und Gasverträge vermittelt hatte, die Kontaktdaten der Kunden an das andere Unternehmen B weitergegeben hatte. Das Unternehmen A vertrat die Auffassung, dass das Unternehmen B die Daten hierbei als Auftragsdatenverarbeiter im Sinne des § 11 BDSG erhalten habe und somit keine „Datenübermittlung“ im datenschutzrechtlichen Sinne (§ 3 Abs. 4 Satz 2 Nr. 3 BDSG) vorliege. Die Datenweitergabe bedürfe deshalb keines datenschutzrechtlichen Rechtfertigungstatbestandes nach §§ 4 Abs. 1, 28 ff. BDSG. Hierzu wurde uns ein Dienstleistungsvertrag sowie eine schriftliche „Vereinbarung über Auftragsdatenverarbeitung nach § 11 BDSG“ vorgelegt; letztere entsprach jedenfalls den formalen Anforderungen nach § 11 BDSG. Der Dienstleistungsvertrag wiederum besagte, dass das Unternehmen A dem Unternehmen B Vertriebsrechte im Hinblick auf den o. g. Schutzbrief einräumte; Vertragspartei im Hinblick auf die an Kunden vermittelten Schutzbriefe sollte jedoch allein das Unternehmen B werden.

Bei dieser Sachlage lag nach unserer Bewertung kein Verhältnis einer Auftragsdatenverarbeitung vor. Der Rahmen einer Auftragsdatenverarbeitung war hier deshalb eindeutig überschritten, weil es geradezu Hauptzweck der Datenweitergabe war, dem Unternehmen B die Verwendung der Daten für eigene gewerbliche Zwecke, d. h. zur werblichen Ansprache zwecks Vertriebs des o. g. Schutzbriefs, zur Verfügung zu stellen. Würde man in einem solchen Fall noch eine Auftragsdatenverarbeitung im Sinne von § 11 BDSG annehmen wollen, würden die in § 28 Abs. 3 BDSG geregelten gesetzlichen Voraussetzungen der Übermittlung personenbezogener Daten für werbliche Zwecke leerlaufen. Unseres Erachtens war es daher hier unvertretbar, von einem Verhältnis der Auftragsdatenverarbeitung auszugehen. Zwar hatten die beteiligten Unternehmen offenbar versucht, durch die Einräumung von Schutzbrief-Vertriebsrechten an das Unternehmen B formal eine Art „Herrschaft“ des Unternehmens A über den Geschäftszweck des Schutzbriefvertriebs zu etablieren, wohl um so die Konstruktion einer Auftragsdatenverarbeitung argumentativ stützen zu können. In datenschutzrechtlicher Hinsicht handelte es sich hierbei aber um eine reine Fiktion, da aus dem Dienstleistungsvertrag eindeutig hervorging, dass das finanzielle Eigeninteresse am Vertrieb des Schutzbriefs allein beim Unternehmen B lag. Die Datenübermittlung war daher, jedenfalls soweit Daten jenseits von sog. Listendaten im Sinne von § 28 Abs. 3 Satz 2 BDSG weitergegeben worden waren - beispielsweise Telefonnummern - unzulässig.

Werden personenbezogene Daten zur Verwendung für eigene Geschäftszwecke des Datenempfängers, insbesondere für dessen werbliche Zwecke, weitergegeben, kann hierin nicht ein Verhältnis der Auftragsdatenverarbeitung nach § 11 BDSG gesehen werden. Sofern es sich um eine Weitergabe für werbliche Zwecke handelt, muss diese die für die Datenübermittlung zu Werbezwecken geltenden Voraussetzungen gemäß § 28 Abs. 3 BDSG erfüllen.

6 Rechtsanwälte

6.1 Gegnerlisten

Im Rahmen einer Anordnung haben wir einer Rechtsanwaltskanzlei die Veröffentlichung einer sog. Gegnerliste mit Namen von Personen, die angeblich illegal Pornofilme aus dem Internet heruntergeladen haben, untersagt.

Eine Rechtsanwaltskanzlei hatte angekündigt, eine Auswahl der Gegner aus offenen und anhängigen Mandatsverhältnissen, gegen die ihr ein Mandat zur außergerichtlichen oder gerichtlichen Tätigkeit erteilt worden sei, zu veröffentlichen. Es war allgemein bekannt, dass diese Rechtsanwaltskanzlei im Auftrag der Pornoindustrie mit zahlreichen entsprechenden Abmahnverfahren befasst ist. Die geplante Veröffentlichung auf Gegnerlisten hätte bedeutet, dass die Kanzlei auf ihrer Homepage die Namen von Personen veröffentlicht hätte, gegen die sie wegen angeblich illegalen Herunterladens von Filmen angab, bevollmächtigt zu sein. Die Veröffentlichung von Gegnerlisten hatte neben der Werbung für die eigene Kanzlei hier auch den Zweck, Druck auf die Gegner auszuüben, denen rechtswidriges Verhalten unterstellt wurde. Im Zusammenhang mit der Unterstellung des illegalen Herunterladens von Pornofilmen wäre noch eine erhebliche Prangerwirkung dazu gekommen.

Wir haben der Kanzlei schriftlich mitgeteilt, dass diese geplante Veröffentlichung von Namen natürlicher Personen im Zusammenhang mit dem Vorwurf des illegalen Herunterladens von in erster Linie pornographischen Filmen jedenfalls auch datenschutzrechtlich unzulässig sei und forderten sie auf, schriftlich zu erklären, bis zur rechtlichen Klärung die Namen nicht zu veröffentlichen. Gleichzeitig gaben wir der Kanzlei Gelegenheit zur Stellungnahme vor Erlass des ansonsten angekündigten Verbotsbescheides.

Die Kanzlei hatte innerhalb der gesetzten Frist nicht erklärt, auf die Veröffentlichung zu verzichten. Daraufhin verboten wir der Kanzlei mit einer für sofort vollziehbar erklärten Anordnung, die Namen oder sonstige personenbezogene Daten von Privatpersonen, gegen die sie wegen Urheberrechtsverletzung, insbesondere wegen Herunterladens von Pornofilmen, beauftragt sein soll, im Rahmen einer sog. Gegnerliste auf ihrer Homepage oder sonst im Internet zu veröffentlichen.

Wir haben die Anordnung im Wesentlichen wie folgt begründet: Die Veröffentlichung von Angaben über Privatpersonen, gegenüber denen Forderungen aus vermeintlichen Urheberrechtsverletzungen durch das Herunterladen von Filmen aus dem Internet geltend gemacht werden, auf sog. Gegnerlisten der Rechtsanwaltsgesellschaft im Internet verletzt die betroffenen Personen in ihrem Persönlichkeitsrecht und ist deshalb rechtswidrig. Bei der Veröffentlichung dieser Daten im Internet handelt es sich um eine Übermittlung personenbezogener Daten an Dritte, die nur zulässig ist, wenn entweder eine ausdrückliche Einwilligung der Betroffenen dafür vorliegt oder die Übermittlung auf eine gesetzliche Grundlage gestützt werden kann (§ 4 Abs. 1 BDSG). Hier lag weder eine ausdrückliche Einwilligung der Betroffenen vor noch konnte die Übermittlung auf eine gesetzliche Rechtsgrundlage gestützt werden. Vielmehr bestand ein überwiegendes schutzwürdiges Interesse der Betroffenen, nicht unter Angabe ihres Namens oder sonstiger personenbezogener Daten, die eine Identifizierung ermöglicht hätten, auf diesen Gegnerlisten zu erscheinen.

Es ist bekannt, dass Rechtsanwaltskanzleien ein grundrechtlich geschütztes Recht auf Werbung für ihre Kanzlei haben (Art. 12 Abs. 1 GG). Dass die Veröffentlichung von Gegnerlisten im Internet - neben der möglichen Ausübung von Druck auf die Gegner - diesem Zweck dient, ist unbestritten und grundsätzlich - aus datenschutzrechtlicher Sicht - auch nicht zu beanstanden. Das Bundesverfassungsgericht hat in diesem Zusammenhang in einer Entscheidung, in der es um die Veröffentlichung von Unternehmen ging, festgestellt, dass dieses Recht auf Werbung ohne Einschränkung auch bei der Wahl des Mediums Internet gelte (BVerfG, Beschluss vom 12.12.2007, 1 BvR 1625/06).

Wir sind bei unserer Entscheidung davon ausgegangen, dass der Beschluss des Bundesverfassungsgerichts für private Personen als Betroffene auf Gegnerlisten nur sehr eingeschränkt herangezogen werden kann. Selbst wenn davon auszugehen ist, dass die Rechtsanwaltskanzlei die Namen der Gegner nur in den Fällen erhalten hat, in denen durch gerichtliche Entscheidung Internetprovider verpflichtet worden sind, die Namen ihrer Vertragspartner für die IP-Adressen herauszugeben, die beim illegalen Herunterladen von Daten aus dem Internet benutzt worden sind, erweist sich die Aufnahme dieser Namen auf Gegnerlisten im Internetauftritt der Rechtsanwaltskanzlei als datenschutzrechtlich unzulässig. Im Ergebnis machte es für uns keinen Unterschied, ob es sich um Namen von Personen handelt, die zu einem früheren oder späteren Zeitpunkt zivil- oder strafrechtlich wegen illegalen Herunterladens verurteilt wurden oder

vielleicht noch werden oder ob es sich um Personen handelt, die nachweislich keinen illegalen Download vorgenommen haben bzw. denen eine derartige Handlung nicht nachgewiesen werden kann. Die mit der Aufnahme in zu veröffentlichende Gegnerlisten erfolgende Prangerwirkung führt zu einer unverhältnismäßigen Beeinträchtigung des allgemeinen Persönlichkeitsrechts der Betroffenen. Dies gilt insbesondere in den hier zur Diskussion stehenden Fällen des Vorwurfs des illegalen Downloads von Pornofilmen.

Entgegen ihrer ursprünglichen Ankündigung erhob die Kanzlei keine Rechtsmittel gegen die Anordnung, so dass sie bestandskräftig wurde. Eine Veröffentlichung der Gegnerliste unterblieb.

6.2 Insolvenzverfahren

Bei Rückforderungsklagen wegen zu viel bezahlter Löhne und Gehälter bei Insolvenz des Arbeitgebers können Lohn- und Gehaltslisten der ehemaligen Mitarbeiter, aber nicht deren Bankverbindungen, an das zuständige Gericht übersandt werden.

Zu Beginn des Berichtszeitraums gingen bei uns zahlreiche Beschwerden von betroffenen Arbeitnehmern ein, die monierten, dass der Insolvenzverwalter ihres Arbeitgebers im Rahmen von Klagen auf Rückforderung von Löhnen und Gehältern Lohn- und Gehaltslisten an das Gericht übersandt habe. Die Listen enthielten neben den Namen der Mitarbeiter, deren Löhne und Gehälter sowie deren Bankverbindungsdaten.

Der als Rechtsanwalt tätige Insolvenzverwalter führte dazu aus, dass es zur Begründung der Rückforderungsklagen notwendig gewesen sei, nachzuweisen, wer von den ehemaligen Mitarbeitern des insolvent gegangenen Betriebs noch für welchen Zeitraum Lohn- und Gehaltszahlungen erhalten habe und wer nicht. Aus diesem Grund habe er die Lohn- und Gehaltslisten an das Gericht übersandt.

Als Rechtsgrundlage für die Übermittlung der Lohn- und Gehaltslisten durch den Insolvenzverwalter an das Gericht kam § 28 Abs. 1 Satz 1 Nr. 2 bzw. Abs. 2 Nr. 2a BDSG in Betracht. Danach ist eine Übermittlung personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen der übermittelnde Stelle oder eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass die schutzwürdigen Interessen der Betroffenen an dem Ausschluss der Übermittlung überwiegen.

Im Rahmen der Klagen auf Rückforderung von Löhnen und Gehältern nach §§ 130 und 133 Insolvenzordnung (InsO) ist der Kläger als Insolvenzverwalter u. a. darlegungspflichtig bezüglich des Umstandes, ob der Arbeitsgeber bei Auszahlung der Löhne und Gehälter bereits zahlungsunfähig gewesen ist. In diesem Zusammenhang ist ein detaillierter Vortrag zur Zusammensetzung der Schulden, d. h. auch hinsichtlich der noch bestehenden Lohn- und Gehaltsforderungen, notwendig. Aus diesem Grund bestanden berechtigte Interessen sowohl des Insolvenzverwalters als auch der anderen Insolvenzgläubiger diese Angaben an das Gericht zu übermitteln. Zudem war es erforderlich, die Höhe der noch ausstehenden Löhne im Einzelnen sowie die Namen der Forderungsinhaber darzulegen und in diesem Umfang die Lohn- und Gehaltslisten an das Gericht zu übermitteln. Überwiegende schutzwürdige Interessen der betroffenen ehemaligen Mitarbeiter waren insoweit nicht ersichtlich.

Für eine substantiierte Begründung der Rückforderungsklagen war es jedoch nicht erforderlich, auch die auf den Lohn- und Gehaltslisten befindlichen Kontoverbindungsdaten an das Gericht zu übermitteln. Mangels Erforderlichkeit hätte der Insolvenzverwalter die Lohn- und Gehaltslisten vor der Übermittlung an das Gericht insoweit schwärzen müssen.

7 Versicherungswirtschaft

7.1 Verhaltensregeln

Nach jahrelangen Verhandlungen zwischen dem Gesamtverband der deutschen Versicherungswirtschaft (GDV) und den Datenschutzaufsichtsbehörden konnten Verhaltensregeln für die Versicherungswirtschaft zum Umgang mit den personenbezogenen Daten der Versicherten nach Zustimmung aller Aufsichtsbehörden durch die Berliner Datenschutzaufsichtsbehörde als verbindlich festgestellt werden.

Die Verhandlungen der Aufsichtsbehörden mit dem Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) über die Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft - auch Code of Conduct (CoC) genannt - konnten 2012 mit unserer intensiven Beteiligung erfolgreich abgeschlossen werden und stellte damit den ersten praktischen Anwendungsfall des § 38a BDSG dar.

Nach dieser Vorschrift können Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten. Diese Bestimmung setzt die Regelung in Art. 27 der Europäischen Datenschutzrichtlinie (95/46/EG) in nationales Recht um. Danach sollen Verhaltensregeln nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung des nationalen Datenschutzrechts beitragen.

Die Verhaltensregeln konkretisieren die gesetzlichen Anforderungen für die spezifischen Datenverarbeitungen in der Versicherungswirtschaft und erleichtern damit auch die Umsetzung des Datenschutzrechts durch die Versicherungsunternehmen. Gerade in der Versicherungsbranche, wo in großem Umfang personenbezogene Daten von Versicherten insbesondere zur Antrags-, Vertrags- und Leistungsabwicklung sowie zur Einschätzung des zu versichernden Risikos, zur Prüfung der Leistungspflicht und zur Verhinderung von Versicherungsmissbrauch verarbeitet werden, stellt die Präzisierung der gesetzlichen Vorgaben einen datenschutzrechtlichen Mehrwert und eine Stärkung des informationellen Selbstbestimmungsrechts der betroffenen Versicherten dar.

Die Verhaltensregeln der Versicherungswirtschaft enthalten u. a. Regelungen dazu, welche Anforderungen an die in der Versicherungsbranche übliche gemeinsame Verarbeitung von Daten innerhalb einer Unternehmensgruppe zum Schutz der personenbezogenen Daten zu erfüllen sind. Darüber hinaus wird in den Verhaltensregeln konkretisiert, in welchen Fallkonstellationen bei entsprechender Information des Versicherten ein Datenaustausch mit anderen Versicherern zulässig ist oder ausnahmsweise personenbezogene Daten an Rückversicherer übermittelt werden dürfen.

Alle Datenschutzaufsichtsbehörden haben im Rahmen einer Sitzung des Düsseldorfer Kreises zum Ausdruck gebracht, dass diese Verhaltensregeln ihrer Auffassung nach der Förderung der Durchführung von datenschutzrechtlichen Regelungen dienen und mit dem geltenden Datenschutzrecht vereinbar sind. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit stellte als die für den GDV zuständige Aufsichtsbehörde mit Bescheid vom 2. November 2012 fest, dass die ihm vorgelegten Verhaltensregeln geeignet sind, die Durchführung der datenschutzrechtlichen Regelungen im Sinne des § 38a Abs. 1 BDSG zu fördern. Dadurch, dass alle Datenschutzaufsichtsbehörden diesen Verhaltensregeln zugestimmt haben, haben sie insoweit nach dem Grundsatz der Selbstbindung der Verwaltung für ihren Bereich eine Verbindlichkeit dieser Verhaltensregeln geschaffen. Für die dem GDV angeschlossenen Versicherungsunternehmen bedeutet dies, dass sie dann, wenn sie sich an diese Verhaltensregeln halten, Maßnahmen der Datenschutzaufsicht nicht zu befürchten haben.

7.2 Einwilligungs- und Schweigepflichtentbindungserklärung

In der zweiten Jahreshälfte 2011 konnten die langen Verhandlungen der Aufsichtsbehörden mit der Versicherungswirtschaft über eine neue Einwilligungs- und Schweigepflichtentbindungserklärung erfolgreich abgeschlossen werden.

Eine neue Einwilligungs- und Schweigepflichtentbindungserklärung war insbesondere aufgrund der Entscheidung des Bundesverfassungsgerichts vom 23. Oktober 2006, Az.: 1 BvR 2027/02, notwendig. In dieser Entscheidung stellte das Gericht fest, dass mit der Abgabe einer pauschalen Einwilligungs- und Schweigepflichtentbindungserklärung ein wirkungsvoller informationeller Selbstschutz des

Betroffenen in erheblichem Maße beeinträchtigt werde, da der Betroffene insbesondere nicht absehen könne, von welcher Stelle welche Auskünfte eingeholt werden.

Im Zuge dieser bundesverfassungsgerichtlichen Entscheidung wurde mit der Reform des Versicherungsvertragsgesetzes (VVG) im Jahr 2007 die Regelung des § 213 VVG zur Erhebung personenbezogener Gesundheitsdaten bei Dritten in das Versicherungsvertragsgesetz aufgenommen. Die Neuregelung lässt zwar eine pauschale Einwilligung bei Abgabe der Vertragserklärung zu, jedoch nur, wenn die betroffene Person vor einer Datenerhebung unterrichtet und ihr dabei das Recht eingeräumt wird, dieser konkreten Datenerhebung zu widersprechen. Darüber hinaus ist dem Betroffenen die Möglichkeit anzubieten, jeweils in die einzelne Datenerhebung einzuwilligen. Durch diese Bestimmung sollte im Zusammenhang mit der Datenerhebung bei Dritten die vom Bundesverfassungsgericht geforderte informationelle Selbstbestimmung gewährleistet werden.

Da sich zahlreiche Versicherungsunternehmen in unserem Zuständigkeitsbereich befinden, haben wir uns an den Verhandlungen über die neue Einwilligungs- und Schweigepflichtentbindungserklärung intensiv beteiligt. In der neuen Erklärung, die ab Januar 2013 von den Versicherungsunternehmen eingesetzt wird, finden die oben beschriebenen Vorgaben ihre Berücksichtigung.

Da für den darüber hinausgehenden Umgang mit Gesundheitsdaten, insbesondere durch private Kranken-, Unfall- und Lebensversicherungsunternehmen, weder im Bundesdatenschutzgesetz noch im Versicherungsrecht spezielle Rechtsgrundlagen vorhanden sind, muss die neue Einwilligungs- und Schweigepflichtentbindungserklärung allerdings auch Bereiche abdecken, die in der Branche allgemein anerkannte Datenverarbeitungsvorgänge darstellen (beispielsweise die Datenweitergabe an Rückversicherer).

Für die Umsetzung dieser Einwilligungs- und Schweigepflichtentbindungserklärungen in die einzelnen Vertragsverhältnisse haben wir, wie die meisten Datenschutzaufsichtsbehörden im Bundesgebiet, uns damit einverstanden erklärt, dass die Versicherungsnehmer zunächst über die neuen Erklärungen nur informiert werden müssen und erst im Leistungs- oder Vertragsänderungsfall die Einholung einer formgerechten Einwilligung erfolgen muss.

7.3 Hinweis- und Informationssystem der Versicherungswirtschaft

Im April 2011 ist das neue Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) in Betrieb genommen worden.

Das neue HIS ersetzt das alte Hinweissystem, das insbesondere aufgrund der fehlenden Transparenz gegenüber den Betroffenen nicht den datenschutzrechtlichen Anforderungen entsprach. Die Konzeption des neuen Systems erfolgte in Abstimmung mit den Datenschutzaufsichtsbehörden. Betreiberin des neuen HIS ist die in Baden-Baden ansässige informa Insurance Risk and Fraud Prevention GmbH.

Zweck des Systems ist es, erhöhte Versicherungsrisiken aufzuzeigen und Versicherungsmissbrauch zu verhindern. Dabei melden die Versicherungsunternehmen Informationen ein, die für die Risikobeurteilung im Antragsfall oder für die Sachverhaltsaufklärung im Leistungs- bzw. Schadensfall von Bedeutung sein können. Um ein Funktionieren des Systems zu gewährleisten, kann nicht ausgeschlossen werden, dass für sich allein betrachtete, unverdächtige Vorfälle eingemeldet werden. Beispielhaft kann hier die Einmeldung von Daten zu einem Fahrzeug genannt werden, wenn ein Fahrzeugschaden fiktiv auf der Basis eines Sachverständigengutachtens mit dem Versicherer abgerechnet wird. Allein der Umstand, dass auf Gutachtenbasis abgerechnet wird, was nach den zivilrechtlichen Bestimmungen ohne Weiteres möglich ist, stellt keinen Anhaltspunkt für ein missbräuchliches Verhalten dar. Allerdings kann nur mit der Erfassung derartiger Fälle im Hinweissystem verhindern werden, dass derselbe, tatsächlich nicht reparierte Schaden, gegebenenfalls erneut abgerechnet wird.

Der Betrieb und die Nutzung des neuen HIS erfolgen nach den Regelungen in § 29 BDSG zur geschäftsmäßigen Datenerhebung und -speicherung zum Zwecke der Übermittlung. Eine datenschutzrechtliche Einwilligung der betroffenen Person ist deshalb nicht notwendig. Die Einmeldungen in das HIS durch Versicherungsunternehmen, die dortige Speicherung von Daten sowie das Abrufen von Informationen aus diesem System kann bei Vorliegen der gesetzlichen Voraussetzungen der § 28 Abs. 1 Satz 1 Nr. 2 bzw. Abs. 2 Nr. 2a BDSG sowie § 29 Abs. 1 Satz 1 Nr. 1 bzw. Abs. 2 BDSG erfolgen. Hierbei ist insbesondere vor einer Einmeldung von Daten zu einer Person eine Abwägung der Interessen des Betroffenen und der Versicherungsunter-

nehmen vorzunehmen. Auch ist der Meldegrund zu dokumentieren. Darüber hinaus prüft die Betreiberin des HIS stichprobenartig, ob für Abfragen aus dem HIS ein berechtigtes Interesse der abfragenden Versicherungsunternehmen vorgelegen hat. Zu diesem Zweck und zu Revisionszwecken werden sämtliche Dateneinmeldungen in das System und Datenabrufe sowohl von den Versicherungsunternehmen als auch der Auskunftei protokolliert.

Die Versicherungsnehmer werden bei Vertragsschluss über das Bestehen des HIS allgemein informiert. Ferner benachrichtigt das einmeldende Versicherungsunternehmen die betroffene Person im konkreten Fall, wenn eine Übermittlung ihrer Daten an das Hinweissystem stattfindet (§ 33 BDSG). Die betroffene Person hat dann die Möglichkeit, ihren Anspruch auf Auskunft gemäß § 34 Abs. 1 BDSG gegenüber der Betreiberin des HIS geltend zu machen. Sofern Daten zu der betroffenen Person unzulässigerweise in dem Hinweissystem gespeichert sind, kann gegebenenfalls die Berichtigung oder der Löschung der Daten nach § 35 Abs. 1 und 2 BDSG verlangt werden.

Bei uns gingen bereits zahlreiche Anfragen von Betroffenen ein, die eine Überprüfung der Rechtmäßigkeit der Übermittlung ihrer Daten an das HIS und die dortige Speicherung wünschten. Bei einem Großteil der von uns überprüften Fälle konnten wir keine Datenschutzverstöße feststellen.

7.4 Einschaltung von Detekteien durch Versicherungsunternehmen

Ein Versicherungsunternehmen kann zum Zwecke der Betrugsprävention die dafür erforderlichen Daten eines Versicherungsnehmers einer Detektei datenschutzrechtlich zulässig übermitteln.

Innerhalb des Berichtszeitraums waren wir mit der Frage befasst, wann und unter welchen Voraussetzungen die Weitergabe personenbezogener Daten eines Versicherungsnehmers durch dessen Versicherer an einen Detektiv datenschutzrechtlich zulässig ist.

Zu dem Einsatz von Detekteien kommt es u. a. bei der Regulierung von Sachschadensfällen etwa in der Gebäudebrandversicherung oder im Rahmen der Prüfung von Ansprüchen aus Berufsunfähigkeits- oder Krankentagegeldversicherungen. Nach Angaben der Versicherungswirtschaft werden Detekteien - auch aus Kostengründen - nur in einem kleinen Bruchteil der von der Versicherungswirtschaft zu regulierenden Schadens- und Leistungsfällen zur Aufdeckung von Betrugsfällen eingesetzt.

Eine Übermittlung personenbezogener Daten im Rahmen der Beauftragung einer Detektei kann auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden, 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 Übermittlung überwiegt. Liegen dem Versicherungsunternehmen konkrete Anhaltspunkte für ein missbräuchliches Verhalten eines Versicherungsnehmers vor, so ist grundsätzlich ein berechtigtes Interesse des Versicherungsunternehmens für den Einsatz einer Detektei anzuerkennen, sofern es zur weiteren Aufklärung des verdächtigen Schadensfalles erforderlich ist. Im Rahmen der Interessenabwägung ist hierbei ebenfalls zu berücksichtigen, dass Versicherungsunternehmen auch versicherungsaufsichtlich zur Betrugsabwehr verpflichtet sind. Darüber hinaus liegt die Verhinderung von Versicherungsmissbrauch auch im Interesse der Versichertengemeinschaft, was insbesondere in den oben geschilderten Fallkonstellationen wegen der meist hohen Leistungssummen von Bedeutung ist.

Zwar stellen heimliche Ermittlungsmaßnahmen einen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht eines betroffenen Versicherungsnehmers dar. Überwiegende schutzwürdige Interessen, die einer Übermittlung der hierfür erforderlichen Daten in diesem Zusammenhang an eine Detektei entgegenstehen, sehen wir jedoch bei Vorliegen konkreter Anhaltspunkte für ein betrugsrelevantes Verhalten regelmäßig nicht.

Im Rahmen der Beauftragung einer Detektei hat das Versicherungsunternehmen die Datenübermittlung auf das für den konkreten Ermittlungszweck erforderliche Maß zu beschränken. Eine pauschale Übermittlung der gesamten Schadens- bzw. Leistungsfallakte ist daher nicht zulässig.

Um einen ausreichenden Schutz der personenbezogenen Daten der betroffenen Versicherungsnehmer zu gewährleisten, halten wir es für zwingend erforderlich, dass Versicherungsunternehmen die Detekteien sorgfältig auswählen und Vertragsregelungen vorsehen, die zumindest folgende datenschutzrechtlichen Festlegungen enthalten:

- Konkreter Ermittlungszweck und strikte Zweckbindung
- Geheimhaltungsverpflichtung
- Löschungsverpflichtung nach Auftragsbeendigung
- technische und organisatorische Maßnahmen
- Vertragsstrafen bei Verstoß

Soweit konkrete Anhaltspunkte für ein betrugsrelevantes Verhalten etwa bei Leistungsansprüchen aus Berufsunfähigkeits- oder Krankentagegeldversicherungen gegeben sind, die Einschaltung einer Detektei zur weiteren Sachverhaltsaufklärung erforderlich ist und dieser hierzu Gesundheitsdaten im Sinne von § 3 Abs. 9 BDSG zur Verfügung gestellt werden, kommt als Rechtsgrundlage für diese Datenübermittlung § 28 Abs. 6 Nr. 3 BDSG in Betracht. Aufgrund der Sensibilität dieser Daten hat ein Versicherungsunternehmen in diesem Fall besonders sorgfältig und intensiv zu prüfen, ob eine Übermittlung von Gesundheitsangaben tatsächlich erforderlich ist und wenn ja, welche Gesundheitsinformationen an eine Detektei weitergegeben werden.

Sofern es sich bei den an eine Detektei übermittelten Daten um Angaben zu Kranken-, Unfall- oder Lebensversicherungsverträgen handelt, haben die in den Versicherungsunternehmen tätigen Personen auch die Verschwiegenheitspflicht aus § 203 Abs. 1 Nr. 6 Strafgesetzbuch (StGB) zu beachten.

7.5 Datenübermittlung an Hypothekengläubiger

Eine Datenübermittlung eines Immobilienversicherers an den Hypothekengläubiger ist im Rahmen der Anzeigepflicht nach § 142 Versicherungsvertragsgesetz (VVG) zulässig.

Eine Petentin wandte sich mit der Bitte um datenschutzrechtliche Überprüfung an uns, weil ihr Immobilienversicherer ihrem Kreditgeber, der zugleich Hypothekengläubiger gewesen ist, über einen Beitragsrückstand im Zusammenhang mit dem Immobilienversicherungsvertrag informiert hatte.

Unsere Überprüfung kam zu dem Ergebnis, dass die Datenübermittlung durch das Versicherungsunternehmen an die kreditgebende Bank und Hypothekengläubigerin auf die bereichsspezifische bundesrechtliche Regelung (vgl. § 1 Abs. 3 Satz 1 BDSG) des § 142 Abs. 1 Versicherungsvertragsgesetz (VVG) gestützt werden kann. Danach hat der Versicherer bei der Gebäudeversicherung einem Hypothekengläubiger, der seine Hypothek angemeldet hat, unverzüglich in Textform anzuzeigen, wenn die einmalige oder die erste Prämie nicht rechtzeitig gezahlt oder wenn dem Versicherungsnehmer für die Zahlung eine Folgeprämie eine Frist bestimmt wird. Sinn und Zweck dieser Vorschrift ist es, den Hypothekengläubiger durch diese Anzeige in die Lage zu versetzen, von sich aus dafür Sorge zu tragen, dass weiterhin Versicherungsschutz besteht, etwa indem er den rückständigen Versicherungsbeitrag selbst entrichtet (vgl. Prölss/ Martin, VVG, 28. Aufl., 2010, § 142 Rn. 1).

Im konkreten Fall hatte das Versicherungsunternehmen die Petentin über die Information der kreditgebenden Bank und Hypothekengläubigerin unterrichtet und der Bank nur die erforderlichen Vertragsangaben sowie die Höhe des rückständigen Beitrages übermittelt. Das Vorgehen des Versicherungsunternehmens war damit datenschutzrechtlich zulässig.

7.6 Verweigerung einer Auskunft an Versicherungsnehmer aus Datenschutzgründen

Das Datenschutzrecht steht nicht generell einer Auskunftserteilung aus der Schadensakte eines Versicherungsunternehmens entgegen.

Ein Versicherungsnehmer, der mit seinem Pkw in einen Verkehrsunfall verwickelt war, wandte sich an uns, weil sein Kfz-Haftpflichtversicherer, der den gegnerischen Schaden reguliert und den Versicherungsnehmer im Zuge dessen in seinem Schadensfreiheitsrabatt zurückgestuft hatte, unter Berufung auf den Datenschutz eine Auskunft aus der Schadensakte verweigerte. Grund für das Gesuch auf Einsicht in Schadensakte des Versicherungsunternehmens bzw. die Abrechnungsunterlagen durch den Versicherungsnehmer war dessen Vermutung, dass die Regulierung des gegnerischen Schadens durch den eigenen Haftpflichtversicherer nicht sachgemäß erfolgt und er deshalb zu Unrecht zurückgestuft worden sei.

Eine Erteilung von Auskünften aus der von der Versicherung geführten Schadensakte ist problematisch, soweit in der Akte personenbezogene Daten von geschädigten Dritten enthalten sind, was im Zusammenhang mit der Regulierung eines Kfz-Haftpflichtschadens regelmäßig der Fall ist. Das Datenschutzrecht steht jedoch auch in diesem Fall

nicht generell einer Auskunftserteilung entgegen. Vielmehr kann eine Übermittlung auch von Daten des Geschädigten an den Versicherungsnehmer erfolgen, wenn der Geschädigte eingewilligt hat oder eine gesetzliche Rechtsgrundlage vorhanden ist (§ 4 Abs. 1 BDSG).

Im Rahmen der Prüfung ist zunächst zu unterscheiden, ob es sich um „allgemeine" personenbezogene Daten oder um besondere Arten personenbezogener Daten in Form von Gesundheitsdaten nach § 3 Abs. 9 BDSG des betroffenen Geschädigten handelt.

Als gesetzliche Rechtsgrundlage zur Übermittlung „allgemeiner" personenbezogener Daten des Geschädigten im Rahmen einer Auskunftserteilung an den Versicherungsnehmer kommt § 28 Abs. 2 Nr. 2a BDSG in Betracht. Danach ist eine Übermittlung personenbezogener Daten für einen anderen Zweck zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Besteht auf Seiten des Versicherungsnehmers die Vermutung, dass die Regulierung des gegnerischen Schadens durch den eigenen Kfz-Haftpflichtversicherer nicht sachgemäß erfolgte, obliegt die Beweislast dem Versicherungsnehmer (vgl. Prölss/ Martin, VVG, 28. Aufl. 2010, AKB 2008 A.1.1 Rn. 23). Aus diesem Grund muss der Versicherungsnehmer die Möglichkeit haben, sich Informationen über den Kenntnisstand des Versicherers im Zeitpunkt der Regulierung zu verschaffen, um damit die fehlerfreie Ausübung des Regulierungsermessens des Versicherers überprüfen zu können. Dementsprechend hat der Versicherungsnehmer regelmäßig ein berechtigtes Interesse daran, zu diesem Zweck in die Unterlagen der Schadensregulierung Einsicht zu nehmen.

Ein entgegenstehendes schutzwürdiges Interesse des Geschädigten sehen wir in der Regel nicht, wenn der Versicherungsnehmer Anhaltspunkte für eine unsachgemäße Regulierung vorträgt und er nur anhand dieser Informationen den Verlust seines Schadensfreiheitsrabattes abwehren kann. Insoweit ist ebenfalls zu berücksichtigen, dass aufgrund des Schadensereignisses zwischen dem Schädiger und dem Geschädigten ein gesetzliches Schuldverhältnis nach den zivilrechtlichen Bestimmungen entsteht, so dass der Geschädigte auch damit rechnen kann, dass Informationen zu seiner Person an den Schädiger weitergegeben werden. Sofern der Versicherungsnehmer durch detaillierte Angaben des Versicherers zum geleisteten Entschädigungsbetrag in die Lage versetzt wird, eine ermessensfehlerfreie Regulierung des Versicherers zu überprüfen, hat vor dem Hintergrund des Erforderlichkeitsgrundsatzes eine darüber hinaus gehende Datenübermittlung zu unterbleiben. Allerdings ist insoweit auch dem Versicherungsnehmer bzw. dessen anwaltlichen Vertreter ein gewisser Entscheidungsspielraum einzuräumen. Kommen diese zu dem Ergebnis, dass eine Einsicht in die Abrechnungsunterlagen zur Überprüfung notwendig ist und wird dies substantiiert begründet, halten wir Übermittlung dieser Unterlagen auf der gesetzlichen Grundlage des § 28 Abs. 2 Nr. 2a BDSG für zulässig.

Für eine Übermittlung besonderer Arten personenbezogener Daten, wie z. B. Angaben über Gesundheitsschäden des Unfallgegners, kommt als gesetzliche Regelung § 28 Abs. 8 Satz 1 BDSG in Verbindung mit § 28 Abs. 6 Nr. 3 BDSG in Betracht. Danach ist eine Übermittlung besonderer Arten personenbezogener Daten für andere Zwecke zulässig, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung überwiegt. Macht der Versicherungsnehmer geltend, dass die Schadensregulierung durch den Versicherer unsachgemäß erfolgt ist, dient die Übermittlung von Regulierungsunterlagen, die Daten des Geschädigten enthalten, der Abwehr einer Rückstufung des Schadensfreiheitsrabattes. Im Falle von Gesundheitsdaten sind jedoch aufgrund der Sensibilität dieser Datenart erhöhte Anforderungen an die Erforderlichkeit zu stellen, um den schutzwürdigen Interessen des betroffenen Geschädigten Rechnung zu tragen. Dabei wird es zur Abwehr der Rückstufung nicht erforderlich sein, dass der Versicherungsnehmer detaillierte Gesundheitsdaten, wie sie beispielsweise in ärztlichen Gutachten enthalten sind, zur Kenntnis erhält. Besteht der Versicherungsnehmer auf solche Informationen, hat er hierfür eine besondere Begründung vorzulegen.

8 Banken

8.1 Prüfungsaktion bei bayerischen Banken

In einer schriftlich angelegten Abfrageaktion haben wir im Herbst 2011 stichprobenartig bei 42 Banken bzw. Sparkassen in Bayern die Einhaltung datenschutzrechtlicher Vorschriften überprüft. Die Überprüfungen haben ergeben, dass den datenschutzrechtlichen Anforderungen im Wesentlichen Rechnung getragen wird.

Prüfungsschwerpunkte dieser Abfrageaktion waren vor allem:

- Bestellung und Tätigkeit des Datenschutzbeauftragten
- Verpflichtung der Beschäftigten auf das Datengeheimnis
- Verfahrensverzeichnis für automatisierte Datenverarbeitungen
- Regelungen im Zusammenhang mit extern vergebenen EDV-Dienstleistungen (weisungsgebundene Auftragsdatenverarbeitung)
- Ausgliederung gesamter Fachaufgaben an Dritte
- Technische und organisatorische Sicherungsmaßnahmen zum Schutz personenbezogener Daten

Aufgefallen ist uns dabei, dass auch Banken immer mehr Leistungen von externen Stellen wahrnehmen lassen (siehe dazu auch die nachfolgenden Beiträge unter Kapitel 8.2 und 8.4), wobei einerseits die datenschutzrechtliche Zulässigkeit nach § 4 Abs. 1 BDSG zu prüfen und anderseits auf die Einhaltung der geltenden datenschutzrechtlichen Rahmenbedingungen zu achten ist.

Als positiv haben wir es empfunden, dass wir nach Durchführung dieser Prüfung zu einer sparkasseninternen Fortbildungsveranstaltung eingeladen wurden und die Gelegenheit bekamen, unsere Prüfungsergebnisse darzustellen und mit den Teilnehmerinnen und Teilnehmern der Veranstaltung darüber zu diskutieren.

8.2 Aufgabenausgliederungen bei Banken

Bei Aufgabenausgliederungen ist zu berücksichtigen, dass Kunden und Mitarbeiter von einer Verwendung ihrer Daten grundsätzlich nur bei ihrem Vertragspartner bzw. Arbeitgeber ausgehen und Ausnahmen davon eng begrenzt sind.

Betroffene Bereiche einer Ausgliederung gesamter Fachaufgaben an Dritte im Bankgeschäft sind z. B. die über eine weisungsgebundene EDV-Dienstleistung hinausgehende Inanspruchnahme einer Unternehmensberatung oder einer externen Personalsachbearbeitung, das Outsourcing der gesamten Abwicklung des Wertpapiergeschäfts oder auch die Beauftragung von Inkassounternehmen einschließlich Forderungseinzug. Nicht in allen Fällen der Ausgliederung gesamter Fachaufgaben an Dritte waren hier bei unseren Prüfungen die datenschutzrechtlichen Rahmenbedingungen für die damit verbundene Übermittlung personenbezogener Daten in ausreichender Weise geschaffen, um die Belange der betroffenen Mitarbeiter und Kunden zu wahren.

In einem Fall hatte eine Bank dem von ihr beauftragten Unternehmensberater einen umfangreichen Online-Zugriff auf ihre Kundendatenbestände eingerichtet, was für die Arbeit des Unternehmensberaters viel zu weitgehend war. Wir haben dies mit einem Bußgeld geahndet (siehe hierzu Kapitel 8.4).

Soweit für bestimmte Sachverhalte der Übermittlung personenbezogener Daten bei der Ausgliederung von Aufgaben nicht aufgrund § 4 Abs. 1 BDSG eine förmliche Einwilligung nach § 4a BDSG erforderlich ist, sind die betroffenen Personen zumindest nach § 4 Abs. 3 BDSG über die Aufgabenauslagerungen zu unterrichten. Des Weiteren ist die Zweckbindung für die übermittelten Daten gemäß § 28 Abs. 5 BDSG sicherzustellen. Zur Wahrung der schutzwürdigen Interessen der betroffenen Personen ist nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG auch auf die gebotenen Sicherheitsmaßnahmen zu achten. Hierfür wird regelmäßig eine vertragliche Regelung die geeignete Grundlage sein, die sich inhaltlich an § 11 Abs. 2 Satz 2 BDSG orientieren kann.

8.3 Datenübermittlung an ein verbundenes Unternehmen zur Verwendung in einem Schadensersatzprozess

Bei einer Weitergabe personenbezogener Daten unter gesellschaftsrechtlich verbundenen Unternehmen handelt es sich - sofern es der Sache nach nicht um Auftragsdatenverarbeitung geht - datenschutzrechtlich um eine Übermittlung, da auch verbundene Unternehmen datenschutzrechtlich zueinander „Dritte" sind. Diese Übermittlung ist nur zulässig, wenn eine Einwilligung vorliegt oder eine Rechtsvorschrift sie erlaubt.

Eine Bank übermittelte eine ihr vorliegende detaillierte Übersicht über die Vermögens- und Einkünftesituation eines ihrer Kunden ohne dessen Wissen an ein Tochterunternehmen, das von demselben Kunden wegen behaupteter mangelhafter Risikoaufklärung im Zusammenhang mit der Vermittlung eines Fonds auf Schadensersatz verklagt worden war. Die Daten wurden mit der Intention übermittelt, vom Tochterunternehmen in dem Rechtsstreit als Beleg dafür verwendet zu werden, dass der Kunde mehrere andere Fonds- und weitere Anlageprodukte besaß und damit insoweit über entsprechende Vorerfahrungen verfügt habe. Die Vermögens- und Einkünfteübersicht hatte der Kunde selbst zu einem früheren Zeitpunkt im Wege einer Selbstauskunft seiner Bank zur Verfügung gestellt. Aus ihr ergaben sich u. a. die Depotwerte seiner einzelnen Anlageprodukte, die Werte mehrerer Immobilien sowie Einkünfte aus verschiedenen Einnahmequellen.

Bei der Datenweitergabe handelte es sich trotz der gesellschaftsrechtlichen Verbundenheit der Unternehmen um eine Übermittlung personenbezogener Daten im datenschutzrechtlichen Sinne, da auch verbundene Unternehmen datenschutzrechtlich zueinander „Dritte" sind. Eine Einwilligung lag nicht vor.

Wir haben die Übermittlung als unzulässig bewertet, da die schutzwürdigen Interessen des Kunden gemäß § 28 Abs. 2 Nr. 2 a BDSG der Übermittlung entgegenstanden. Zwar war das Interesse des Tochterunternehmens, potentiell geeignetes Beweismaterial für seinen Rechtsstreit gegen den Betroffenen zu sammeln, für sich gesehen nachvollziehbar, doch überwogen demgegenüber die schutzwürdigen Interessen des Betroffenen am Unterbleiben der Datenübermittlung. Denn die Daten besaßen eine ganz erhebliche Sensibilität, weil sie eine detaillierte und vollständige Aufstellung der finanziellen Verhältnisse des Kunden darstellten. Zudem durfte der Kunde aufgrund des vertraglich vereinbarten sog. Bankgeheimnisses einen vertraulichen Umgang der Bank mit seinen Daten erwarten. Die gesellschaftsrechtliche Verbundenheit der beteiligten Unternehmen und das Beweisgewinnungsinteresse des Tochterunternehmens vermochten diese schutzwürdigen Interessen des Kunden nicht aufzuwiegen.

Was das Beweisgewinnungsinteresse angeht, war hierbei noch folgendes zu berücksichtigen: Zwar erschien es denkbar, dass Mitarbeiter der „Mutter"-Bank von dem Tochterunternehmen als Zeugen in dem zwischen dem Tochterunternehmen und dem Betroffenen anhängigen Rechtsstreit benannt werden würden, so dass es nicht ausgeschlossen war, dass die in Rede stehenden Daten bzw. ein Teil hiervon auf diesem Wege zu einem späteren Zeitpunkt zur Kenntnis der Tochtergesellschaft gelangen könnten. Dies führte aber zu keiner anderen datenschutzrechtlichen Beurteilung der vorliegenden Datenübermittlung. Dem Tochterunternehmen stand es nämlich frei, aus seiner Sicht geeignete Zeugen für den Rechtsstreit zu benennen sowie ggf. eine Beweisaufnahme durch Vorlage von bei Dritten vorhandenem Beweismaterial zu beantragen, wobei es in der Entscheidung des erkennenden Gerichts lag, bestimmte Beweiserhebungen zuzulassen bzw. anzuordnen. Dieser Umstand kann aber nicht die hier stattgefundene Datenübermittlung rechtfertigen, da zum Übermittlungszeitpunkt gerade nicht feststand, ob und ggf. welche der entsprechenden Daten unter Anwendung der zur Verfügung stehenden zivilprozessualen Instrumente tatsächlich in den Rechtsstreit eingebracht werden würden. Eine gewissermaßen prophylaktisch erfolgende Übermittlung der Daten - mit Blick auf theoretisch denkbare Beweiserhebungen im anhängigen Rechtsstreit - haben wir angesichts der Sensibilität der Daten als unzulässig bewertet.

8.4 Datenübermittlung an einen externen Unternehmensberater

Bei der Einschaltung eines Unternehmensberaters ist sicherzustellen, dass er nur soweit auf die personenbezogenen Daten des Unternehmens zugreifen kann, wie es zur Erfüllung seines Auftrags unbedingt erforderlich ist. Die Einräumung einer weitergehenden Zugriffsmöglichkeit ist - unabhängig davon, ob vom Unternehmensberater tatsächlich darauf zugegriffen wurde - unzulässig.

Ein Kreditinstitut hatte einen externen Unternehmensberater damit beauftragt, Möglichkeiten zur Optimierung der Geschäftsstrukturen und -prozesse im Privat- und Geschäftskundenvertrieb zu untersuchen. In diesem Zusammenhang richtete das Institut in seinem IT-System für den Berater ein spezielles Laufwerk ein und räumte ihm hierauf Zugriffsrechte ein. In das Laufwerk wurde ein großer Umfang weitgehend personenbezogener Daten bereitgestellt. Dem Berater war über mehrere Monate hinweg jederzeit der Abruf dieser Daten möglich. Zu den Daten zählten Angaben zu Kreditrahmen, Kreditausnutzung, Überziehungshöhe und -dauer, Guthabens- und Vermögenshöhe, Depotumsätze und Depotgesamthöhe einer großen Anzahl von Kunden. Ebenfalls in das Laufwerk eingestellt wurden personenbezogene Daten zu den Salden einer dreistelligen Anzahl solcher Kreditnehmer, die als Grundlage der sog. Meldungen zur Eigenmittelausstattung an die Deutsche Bundesbank gemäß der Solvabilitätsverordnung heranzuziehen waren.

Das Institut hatte den Umfang der bereitzustellenden personenbezogenen Daten nicht am Maßstab der Erforderlichkeit im Hinblick auf den konkreten Beratungsauftrag näher überprüft. Es konnte auch keine organisatorischen Vorkehrungen dafür vorweisen, dass es in derartigen Fällen eine spezifische Erforderlichkeitsprüfung durchführt. Aufgrund der konkreten Gegebenheiten war davon auszugehen, dass für die Erfüllung des Beratungsauftrags die Bereitstellung von Daten ohne Personenbezug jedenfalls weitgehend ausgereicht hätte.

Wir haben das Vorgehen als unbefugte Bereithaltung personenbezogener Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bewertet, da dem Berater der Zugriff auf weit mehr personenbezogene Daten eröffnet wurde, als dieser aufgrund seines konkreten Auftrags tatsächlich benötigte, was gerade auch dadurch untermauert wurde, dass der Berater - mangels Erforderlichkeit - keineswegs tatsächlich Zugriff auf alle bereitgestellten Daten genommen hat. Schon die Bereithaltung der Daten als solche erfüllt den Ordnungswidrigkeitentatbestand gemäß § 43 Abs. 2 Nr. 2 BDSG.

Es lag auch kein Verhältnis einer Auftragsdatenverarbeitung nach § 11 BDSG vor. Denn Dienstleister, die aufgrund ihrer spezifischen Kenntnisse und Fähigkeiten eigenständig und unabhängig Leistungen erbringen, die sich nicht in der praktisch-technischen Durchführung von Datenverarbeitungsvorgängen erschöpfen, sind keine Auftragsdatenverarbeiter. Dies ist etwa bei Rechtsanwälten, Wirtschaftsprüfern, Steuerberatern oder Bilanzbuchhaltern anerkannt (Gola/Schomerus, BDSG, 11. Aufl., 2012, § 11, Rn. 11) und gilt daher auch für den damit in der Regel vergleichbaren Fall eines externen Unternehmensberaters (siehe auch Kapitel 5.1 und 5.2).

Das Institut meinte, der Berater sei in die internen Organisationsabläufe in vergleichbarer Weise wie ein eigener Mitarbeiter oder ein Leiharbeitnehmer eingegliedert gewesen, so dass die Daten innerhalb der verantwortlichen Stelle verblieben seien. Dieser Auffassung sind wir nicht gefolgt. Nach der arbeitsgerichtlichen Rechtsprechung ist entscheidendes Kriterium für die Bejahung eines Arbeitsverhältnisses die Unterwerfung unter die Weisungsbefugnis eines anderen (BAG, Urt. v. 21.01.1999 - 2 AZR 648/97). Ein (faktisches) Arbeitsverhältnis oder ein einem Leiharbeitsverhältnis vergleichbares Verhältnis hätte daher nur dann angenommen werden können, wenn sich der Berater umfassend dem Weisungsrecht des Instituts unterworfen hätte. Dies ist jedoch bei derartigen freiberuflich erbrachten Dienstleistungen eines Unternehmensberaters typischerweise gerade nicht der Fall (siehe auch Kapitel 5.1 und 5.2).

9 Auskunfteien

9.1 Ermittlung von Score-Werten

Score-Werte, die auf einer geringen Datenbasis berechnet werden, können für die betroffenen Personen zu ungerechtfertigten Benachteiligungen führen.

Scorewerte zur Risikoabschätzung bezüglich eines bestimmten zukünftigen Verhaltens von Personen werden hauptsächlich im Finanzdienstleistungssektor errechnet, also von Banken und Wirtschaftsauskunfteien, um insbesondere für das anonyme Massen-, das Online- oder sonstige Fernabsatzgeschäft Anhaltspunkte für Entscheidungen mit finanziellen Ausfallrisiken zu finden.

Mit der zum 1. April 2010 in Kraft getretenen BDSG-Novelle wollte der Gesetzgeber die in Teilen nicht nachvollziehbare und intransparente Verfahrensweise von Scoring-Verfahren insbesondere bei den Auskunfteien verbessern.

Die neuen Bestimmungen in § 28b BDSG zur Regelung bzw. Einschränkung der Scoring-Verfahren (z. B. Verbot des reinen Anschriften-Scorings) und in § 34 BDSG (erweiterte Auskunftsrechte der betroffenen Personen auch zum Zustandekommen und zur Bedeutung der Scorewerte „einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form“) sollten die Rechte der Bürgerinnen und Bürger stärken und ihren Informationsstand erweitern.

§ 28b Nr. 1 BDSG fordert, dass die für das Scoring genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Score-Werte erheblich sind. In diesem Rahmen ist jedoch nicht zu prüfen, ob die Score-Ergebnisse eine hohe Prognosegenauigkeit aufweisen oder nicht. Auch Verfahren mit geringer Aussagekraft können daher die Anforderungen des § 28b Nr. 1 BDSG erfüllen.

Das führt dazu, dass die Scorewerte von Auskunfteien, die nur auf eine vergleichsweise geringe Datenbasis zurückgreifen können, zwar nach den Vorgaben von § 28b Nr. 1 BDSG errechnet werden, die tatsächliche Bonitätssituation einer Person bzw. deren Zahlungsausfallrisiko aber hin und wieder nicht treffen. Dies ist insbesondere dann der Fall, wenn die Bewertung der Wohnverhältnisse einer Person sowie des Wohnumfeldes (Anschriftendaten) mit erheblichem Gewicht in die Scoreberechnung einfließen und sonst nur das aus dem Vornamen entnommene Geschlecht einer Person sowie das aufgrund des Vornamens geschätzte Alter für die Score-Berechnung zur Verfügung stehen.

So hatte z. B. eine Beamtin in einer großen bayerischen Stadt in einem bekanntermaßen überwiegend finanzschwachen Stadtteil eine Wohnung geerbt und ist dort eingezogen. Ohne dass irgendwelche negativen Bonitätsmerkmale vorlagen, wurde die Beamtin von einer Auskunftei vor allem wegen des finanzschwachen Wohnumfelds in eine schlechte Score-Klasse eingestuft. Weil die betreffende Auskunftei in einem anderen Bundesland ansässig ist, haben wir den Vorgang zur weiteren Bearbeitung an die dortige Aufsichtsbehörde abgegeben.

Wegen verschiedener nachvollziehbarer Beschwerden von betroffenen Personen bei den Datenschutzaufsichtsbehörden und den Verbraucherschutzverbänden, die darauf gerichtet waren, dass im konkreten Fall der Scorewert wegen mangelnder Datenbasis die reale Situation völlig verfehlt, haben die Datenschutzaufsichtsbehörden in der Sitzung der Arbeitsgruppe „Auskunfteien“ des Düsseldorfer Kreises im November 2012 eine Nachbesserung der gesetzlichen Regelung für Scorewertberechnungen angeregt.

9.2 Speicherung eines Negativmerkmals „Datenschutz-Beschwerdeführer“

Hat sich ein Betroffener über ein Unternehmen in der Vergangenheit bei der Datenschutzaufsichtsbehörde beschwert, darf das Unternehmen diesen Umstand jedenfalls nicht in allen Fällen als „Negativmerkmal“ zu dem Betroffenen hinzuspeichern.

Ein Betroffener wollte sich als Teilnehmer bei einer alljährlich stattfindenden Sportveranstaltung anmelden, nachdem er daran bereits im Vorjahr teilgenommen hatte. Sein Versuch, sich beim Veranstalter mit seinem Namen online anzumelden, scheiterte jedoch - für ihn zunächst ohne ersichtlichen Grund. Als er beim Veranstalter nachfragte, wurde ihm mitgeteilt, dass seine Anmeldung nicht erwünscht sei, weil er sich im Vorjahr über das Unternehmen bei der Datenschutzaufsichtsbehörde beschwert habe.

Das von uns zur Stellungnahme aufgeforderte Unternehmen bestritt die Darstellung nicht und erklärte, dass keine weiteren Geschäftsbeziehungen zu dem Betroffenen gewünscht seien. Es vertrat die Auffassung, dass es ihm mit Blick auf den Grundsatz der Vertragsfreiheit möglich sein müsse, einen erneuten Vertragsabschluss mit dem Betroffenen wegen negativer Erfahrungen in der Vergangenheit abzulehnen, wozu auch die frühere Beschwerde bei der Datenschutzaufsichtsbehörde gehöre.

Bei der datenschutzrechtlichen Bewertung des Falles ist zu berücksichtigen, dass es der zivilrechtliche Grundsatz der Vertragsfreiheit jedermann erlaubt, grundsätzlich seine Lebensverhältnisse durch Verträge eigenverantwortlich zu gestalten. Dieses Recht ist neben natürlichen Personen auch Unternehmen zuzugestehen. Von der Vertragsfreiheit umfasst ist - sofern keine ausdrücklichen gesetzlichen Ausnahmen wie etwa aufgrund des Allgemeinen Gleichbehandlungsgesetzes bestehen - auch das Recht, den Abschluss von Verträgen mit bestimmten Personen abzulehnen. Datenschutzrechtlich wirkt sich dies auf die Interessenabwägung gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG dahingehend aus, dass ein Unternehmen grundsätzlich berechtigt ist, den Namen von Personen, mit denen keine Geschäftsbeziehung eingegangen werden soll, zu speichern (unternehmensinterne „Schwarze Liste“), um in solchen Fällen vom Recht auf Vertragsfreiheit effektiv Gebrauch machen zu können.

Im vorliegenden Fall hatte das Unternehmen zum Eingabeführer den Hinweis hinzugespeichert, dass sich dieser im Vorjahr bei der Datenschutzbehörde über das Unternehmen beschwert hatte. Die Speicherung dieses Merkmals ist nach unserer Auffassung dann zulässig, wenn die frühere Beschwerde von vornherein offensichtlich unbegründet bzw. aussichtslos war oder sogar als willkürlich oder böswillig zu bewerten ist. Denn in solchen Fällen erscheint es nachvollziehbar, wenn das Unternehmen mit dem Betroffenen künftig keine Geschäftsbeziehung mehr eingehen möchte und dies intern gerade (auch) mit einer unter derartigen Umständen eingelegten früheren Datenschutzbeschwerde begründet. War hingegen - wie es in dem von uns überprüften Sachverhalt der Fall war - die frühere Beschwerde aus Sicht eines durchschnittlichen Betroffenen nachvollziehbar oder zumindest vertretbar, sehen wir die Speicherung der früheren Beschwerdeeinlegung als unzulässig an, selbst wenn in dem damaligen Fall ein datenschutzrechtlicher Verstoß im Ergebnis nicht vorlag; natürlich muss gleiches erst recht gelten, wenn die frühere Beschwerde berechtigt war, weil ein Verstoß tatsächlich vorlag. Denn für diese Fälle ist die gesetzgeberische Entscheidung zu berücksichtigen, jedermann die Anrufung der Datenschutzaufsichtsbehörde zu ermöglichen, der der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten in seinen Rechten verletzt worden zu sein, ohne dass der Beschwerdeführer eine solche Rechtsverletzung bereits bei der Anrufung der Aufsichtsbehörde glaubhaft machen oder in besonderer Weise plausibel darlegen müsste (§ 38 Abs. 1 Satz 8 i. V. m. § 21 Satz 1 BDSG). Da der Gesetzgeber mithin die Anrufung der Datenschutzaufsichtsbehörde bewusst „niederschwellig“ ermöglichen wollte, wäre es unverhältnismäßig und diskriminierend, wenn verantwortliche Stellen die Anrufung der Behörde auch dann als Negativmerkmal zu einem Betroffenen hinzuspeichern dürften, wenn die Anrufung im konkreten Fall aus Sicht eines durchschnittlichen Betroffenen vertretbar bzw. zumindest nicht offensichtlich unbegründet war.

10 Werbung und Adressenhandel

10.1 Übergangsregelung nach § 47 Nr. 2 BDSG

Die Übergangsfrist für alte Datenbestände, die für Zwecke der Werbung verarbeitet oder genutzt werden, ist am 31. August 2012 abgelaufen.

Die am 1. September 2009 in Kraft getretenen engeren Regelungen im BDSG für die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung sind nach Ablauf der dreijährigen Übergangsregelung ab 1. September 2012 nun auf alle betreffenden Datenbestände anzuwenden.

Das bedeutet insbesondere, dass

- nach § 28 Abs. 3 Satz 4 BDSG bei einer Übermittlung von Daten für Zwecke der Werbung die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen muss,
- nach § 28 Abs. 3 Satz 5 BDSG bei einer Nutzung von Daten für fremde Werbezwecke („Empfehlungswerbung“) bei der werblichen Ansprache die für die Nutzung der Daten verantwortliche Stelle, also, wer der Eigner der Kontaktdaten ist, eindeutig erkennbar sein muss und
- nach § 28 Abs. 3 Satz 2 Nr. 1 BDSG für die Neukundenwerbung bei Verbrauchern nur noch Anschriftendaten aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen und nicht mehr Anschriftendaten aus sonstigen allgemein zugänglichen Quellen (wie beispielsweise aus Zeitungsanzeigen oder dem Impressum eine Homepage) oder aus Befragungen dritter Personen erlangte Kontaktdaten (für sogenannte Freundschaftswerbung) verwendet werden dürfen.

Soweit diese genannten Voraussetzungen für die Altdaten nicht vorliegen, sind die Datenbestände zu löschen oder für eine werbliche Verwendung zu sperren.

10.2 Anwendungshinweise für den werblichen Umgang mit personenbezogenen Daten

Eine Ad-hoc-Arbeitsgruppe „Werbung und Adresshandel“ der Datenschutzaufsichtsbehörden hat sich unter unserer Leitung mit der Erarbeitung von Anwendungshinweisen zu den BDSG-Regelungen für den werblichen Umgang mit personenbezogenen Daten befasst. Aufgenommen wurden in dieses Papier Empfehlungen, soweit sie einstimmig oder von einer großen Mehrheit mitgetragen wurden. Die Ergebnisse sind auf unserer Homepage veröffentlicht.

Siehe:
www.lda.bayern.de >> Fachthemen >> Werbung - Hinweise zur Anwendung der BDSG-Vorschriften

10.3 Besondere Einzelfälle

Im Folgenden werden einige Einzelfälle aus dem Berichtszeitraum dargestellt, die typische Fragestellungen von Anfragen und Beschwerden aus dem Werbungsbereich betreffen.

- Ein Autohaus hatte auf einer Jubiläumsbroschüre für werbliche Zwecke unzulässigerweise die Familiennamen und Vornamen seiner Kunden aufgedruckt. Bei selteneren Namen und infolge des örtlichen Bezugs war ein Teil der Kunden bestimmbar.
- Wegen wiederholter Werbung trotz vorliegenden Widerspruchs der betroffenen Personen und wegen fehlenden Hinweises auf das Werbewiderspruchsrecht in der Werbung haben wir gegen die Verantwortlichen jeweils Bußgeldverfahren eingeleitet.
- Eine dritte Person (Täter) hatte auf einer Firmen-Homepage für einen anderen Bürger missbräuchlicherweise dessen Adressdaten eingetragen und eine Werbezusendung angefordert. Über das Auskunftsrecht bei der Firma zu gespeicherten Daten nach § 34 BDSG konnte der andere Bürger die IP-Adresse des Täters zu der missbräuchlichen Bestellung des Werbematerials in Erfahrung bringen, um darüber dessen Identität aufzuklären. Wir hatten hier auf die Beschwerde des betroffenen Bürgers hin dafür gesorgt, dass er diese Auskunft auch erhält. Denn zu-

nächst hatte die Firma für sich keine solche Auskunftspflicht gesehen, weil sich die fraglichen Daten primär auf die dritte Person, den Täter, bezögen.

- Ein Verlag hatte dem Mitarbeiter eines Unternehmens ohne dessen ausdrücklicher Einwilligung Werbung per Fax zugesandt. Die Nutzung der Fax-Nummer für die Werbezusendung war nach den Regelungen von § 28 Abs. 3 BDSG und § 7 Abs. 2 Nr. 3 UWG unzulässig. Allein aus einer bestehenden Kundenbeziehung kann kein Einverständnis eines Kunden mit einer Bewerbung per Fax abgeleitet werden, denn das UWG fordert auch für business-to-business-Werbung per Fax eine ausdrückliche Einwilligung.
- Nach § 28 Abs. 4 Satz 2 BDSG sind die betroffenen Personen bei der werblichen Ansprache sowie bei vertraglichen oder vergleichbaren Beziehungen über ihr Widerspruchsrecht gegen die werbliche Verwendung ihrer Daten zu unterrichten. Damit von einer Unterrichtung im Sinne des Gesetzes ausgegangen werden kann bzw. der Zweck der Unterrichtung erreicht wird, muss der entsprechende Hinweistext für die betroffenen Personen unschwer zur Kenntnis genommen werden können und darf nicht innerhalb vieler anderer Informationen versteckt oder vergleichsweise kleingedruckt sein. In den eingegangenen Beschwerdefällen haben die verantwortlichen Stellen im Zuge unserer Befassung mit der Angelegenheit in allen Fällen für Abhilfe gesorgt.

11 Handel und Dienstleistung

11.1 Aufzeichnung von Telefongesprächen

Eingehende Telefonate unter Notfallrufnummern von Gasversorgungsunternehmen dürfen aufgezeichnet werden, wenn die Betroffenen zu Beginn des Gesprächs über den Aufzeichnungszweck informiert werden.

Mehrere Bürger fragten uns, ob es zulässig sei, dass eingehende Anrufe bei Störungsannahmestellen von Gasversorgungsunternehmen aufgezeichnet werden.

Im Rahmen unserer Überprüfung teilten die betroffenen Unternehmen mit, dass die Störungsannahmestelle zur Entgegennahme von telefonischen Hinweisen auf Störungen im Gasversorgungsnetz diene. Bereits kleine Schäden an Gasleitungen könnten erhebliche Sicherheitsrisiken mit sich bringen. Die Mitarbeiter des Gasversorgungsunternehmens müssten den Störfallmeldungen unverzüglich nachgehen. Es sei daher unerlässlich, eingehende Anrufe aufzuzeichnen, um (akustische) Verständnis- oder Übertragungsfehler so weit wie möglich auszuschließen. Anrufer seien häufig sehr aufgeregt, so z. B. bei Gasgeruch, und ihre Angaben (z. B. zu Straßennamen) daher bisweilen unklar. Mit Hilfe des Gesprächsmitschnitts habe der Mitarbeiter die Möglichkeit, durch nochmaliges Abhören die Angaben zu überprüfen.

Als zweiten Grund für die Aufzeichnung gaben die Unternehmen Beweissicherungsbedürfnisse an: Da bei größeren Störfällen neben den Mitarbeitern des Gasversorgers vorsorglich auch Feuerwehr und z. T. Polizei benachrichtigt würden, könne es bei missbräuchlicher Nutzung der Störfallrufnummer bzw. ungerechtfertigter Alarmierung zu Regressforderungen kommen. Daher sei es für den Gasversorger wichtig, durch den Gesprächsmitschnitt zu dokumentieren, aufgrund welchen Anrufs er die Alarmierung anderer Stellen vorgenommen hat.

In den von uns überprüften Fällen wurden die Anrufer zu Beginn des Telefonats darauf hingewiesen, dass das Gespräch aufgezeichnet werde, um die Störungsmeldung zu dokumentieren und besser nachvollziehen zu können.

Die Unternehmen verwiesen auch auf ein Arbeitsblatt „Technische Regeln“ des Deutschen Vereins des Gas- und Wasserfaches e. V. (DVGW), demzufolge Gas- und Wasserversorgungsunternehmen jede eingehende Störungsmeldung nachvollziehbar zu dokumentieren hätten, wobei dies „evtl. zusätzlich“ durch Tonbandmitschnitt erfolgen könne. Das Arbeitsblatt sieht eine Aufbewahrung der dokumentierten Daten bis zur endgültigen Klärung der Schadensursache vor, mindestens aber für sechs Jahre. Die Länge der Aufbewahrungsfrist begründete der DVGW, den wir um eine Stellungnahme ersucht hatten, damit, dass es bei Unfällen mit Sach- und/oder Personenschäden zu zeitintensiven gerichtlichen Verfahren zur Abklärung der Ursachen kommen könne. Bei der Erarbeitung der „Technischen Regeln“ sei man aufgrund praktischer Erfahrungen davon ausgegangen, dass solche Verfahren bis zu 6 Jahren dauern können.

Nach § 49 Abs. 1 des Gesetzes über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz / EnWG) müssen Energieanlagen unter Gewährleistung der technischen Sicherheit und Beachtung der allgemein anerkannten Regeln der Technik errichtet und betrieben werden, wobei gemäß § 49 Abs. 2 Nr. 1 EnWG die Einhaltung der allgemein anerkannten Regeln der Technik vermutet wird, wenn bei Anlagen zur Erzeugung, Fortleitung und Abgabe von Gas die technischen Regeln des DVGW e. V. eingehalten werden.

Im Ergebnis erachten wir das Aufnehmen der eingehenden Telefonate als solches für datenschutzrechtlich zulässig aufgrund berechtigter Interessen der Versorgungsunternehmen gemäß § 28 Abs. 1 Satz 1 Nr. 2 und berechtigter Interessen Dritter gemäß § 28 Abs. 2 Nr. 2 Buchst. a BDSG. Mit Blick auf die drohenden - unter Umständen erheblichen - Schäden für Personen und Sachwerte im Fall unrichtig verstandener Angaben von Anrufern überwiegt das berechtigte Interesse der potentiell von einem Schadensereignis Betroffenen daran, dass die Angaben des Anrufenden durch nochmaliges Abhören überprüft werden können. Daneben vermag nach unserer Bewertung auch das Interesse an der Dokumentation zur Sicherung der Beweislage mit Blick auf etwaige Regressforderungen die Speicherung gemäß § 28 Abs. 2 Satz 1 Nr. 2 BDSG zu rechtfertigen. Dem steht nach unserer Auffassung auch nicht die Strafvorschrift des § 201 StGB (Verletzung der Vertraulichkeit des Wortes) entgegen, da die Aufzeichnung in diesen Fällen aus den genannten Gründen nicht „unbefugt“ in Sinne von § 201 StGB ist.

Daneben ist zumindest diskussionswürdig, die Aufzeichnung mit einer Einwilligung des Anrufenden zu begründen, wobei an eine konkludent erteilte Einwilligung durch Gesprächsfortsetzung

nach entsprechender Aufklärung über den Aufzeichnungszweck gedacht werden könnte. Jedoch setzt die Annahme einer datenschutzrechtlichen Einwilligung eine freie Entscheidung des Betroffenen voraus. Daraus wird in der datenschutzrechtlichen Diskussion meist gefolgert, dass Betroffenen insoweit eine „Ausweichmöglichkeit“ angeboten werden müsse (etwa, die Meldung auf anderem Wege zu machen), was aber bei Notfallanrufen in aller Regel nicht möglich sein wird. Daher ist zumindest fragwürdig, ob die Konstruktion einer konkludenten Einwilligung in solchen Fällen tragfähig ist, so dass aus unserer Sicht mehr für eine Rechtfertigung der Aufzeichnung auf Grundlage der o. g. Rechtsvorschriften anstatt einer Rechtfertigung mittels Einwilligung spricht.

Was die Dauer der Speicherung und Nutzung betrifft, wird man unterscheiden müssen: Die Verwendung der Daten zur Überprüfung der Angaben der Anrufenden zwecks Vermeidung von Verständnisfehlern rechtfertigt lediglich eine kurzfristige Speicherung und Nutzung. Eine mehrjährige Speicherung zur Sicherung der Beweislage erscheint mit Blick auf die mögliche Dauer gerichtlicher Auseinandersetzungen grundsätzlich als vertretbar.

11.2 Aushänge von Kfz-Kennzeichen und Namen von Kunden in Kfz-Werkstätten

Kfz-Händler und -Werkstätten dürfen Namen von Kunden und dazugehörige Kfz-Kennzeichen nicht ohne Einwilligung der Betroffenen im Wege von Aushängen oder Bildschirmanzeigen im Verkaufsraum oder auf dem Werkstattgelände veröffentlichen.

Mehrere Eingaben im Berichtszeitraum betrafen Kfz-Werkstätten und -Händler, die die Kundennamen und Kennzeichen der Fahrzeuge, die zum Kundendienst oder einer Reparatur abgegeben oder nach einem Kundendienst oder einer Reparatur abgeholt werden konnten, auf Bildschirmen im Verkaufsraum oder als Aushang an der Einfahrt der Werkstattgaragen - z. T. verbunden mit einer „Begrüßung“ der Kunden - veröffentlichten. Andere anwesende Personen konnten damit diese Daten zur Kenntnis nehmen.

Diese von den Unternehmen im Gedanken der Serviceorientierung oder der Kundenbindung begründete Praxis ist nicht datenschutzkonform, da das Aushängen von Namen und Kfz-Kennzeichen zu einer Übermittlung personenbezogener Daten im Sinne von § 3 Abs. 4 Satz 2 Nr. 3b BDSG führt. Die Übermittlung ist zur Begründung, Durchführung oder Beendigung des Werkstattvertrags nicht erforderlich, so dass eine Rechtfertigung nach § 28 Abs. 1 S. 1 Nr. 1 BDSG ausscheidet. Die schutzwürdigen Interessen der Betroffenen am Unterbleiben der Übermittlung ihrer Daten überwiegen gegenüber dem Interesse des Unternehmens an einer freundlichen bzw. positiven Außendarstellung gegenüber dem Kunden, so dass die Übermittlung auch nicht auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden kann. Die schutzwürdigen Interessen der Betroffenen überwiegen aber auch, sofern die Motivation für den Aushang vornehmlich in der Serviceorientierung, namentlich der Vereinfachung der Abläufe für den Kunden beim Abholen seines Fahrzeugs liegen sollte. Denn auch für diesen Fall kann nicht schlicht unterstellt werden, dass alle betroffenen Kunden mit der Bekanntgabe ihres Namens und des Kennzeichens ihres Kfz an andere Anwesende einverstanden sind, was gerade auch daraus ersichtlich ist, dass es diesbezüglich zu Beschwerden bei der Datenschutzaufsichtsbehörde kam.

11.3 Veröffentlichung von Daten zum Standort und zur Leistung von Anlagen zur Erzeugung von Strom aus erneuerbaren Energien

Elektrizitätsversorgungsunternehmen dürfen und müssen nach dem Gesetz für den Vorrang Erneuerbarer Energien (Erneuerbare-Energien-Gesetz - EEG) auf ihren Internetseiten die Adressen von Anlagen zur Erzeugung von Strom aus erneuerbaren Energien sowie die an die Anlagenbetreiber für den eingespeisten Strom geleisteten Vergütungen veröffentlichen.

Im Berichtszeitraum fragten mehrere Eingabeführer, ob es zulässig sei, dass Elektrizitätsversorgungsunternehmen auf ihren Internetseiten die Adressen von Anlagen zur Erzeugung von Strom aus erneuerbaren Energiequellen, z. B. Photovoltaikanlagen oder Biogasanlagen, und die an den jeweiligen Anlagenbetreiber für den von ihm in das Stromnetz eingespeisten Strom geleisteten Vergütungszahlungen veröffentlicht hatten.

Derartige Veröffentlichungen sind zulässig, weil sie seit dem 1. Dezember 2006 in § 52 EEG vorgeschrieben sind. Wie sich aus einer Zusammenschau der Vorschriften der §§ 52 in Verbindung mit 45 - 49 EEG ergibt, müssen Netzbetreiber und Elektrizitätsversorgungsunternehmen auf ihren Internetseiten insbesondere Standort und Leistung der jeweiligen Anlage sowie die für die jeweilige Anlage gemäß dem EEG geleisteten Vergütungszahlungen veröffentlichen. In der Gesetzesbegründung (BT-Drs. 16/2455, Seite 11) heißt es dazu:

„Die Vorschrift dient v. a. der Transparenz der gegenüber Elektrizitätsversorgungsunternehmen und von diesen gegenüber Letztverbrauchern geltend gemachten Vergütungsansprüche. (…) Die Veröffentlichungspflicht führt (…) zu einer erheblichen Steigerung der Transparenz des Systems der Strom- und Kostenwälzung. Die Verpflichtung steht im Interesse aller Beteiligten, da so unberechtigten Vorwürfen hinsichtlich Missbrauchs und überhöhter Zahlungen auf allen Ebenen des Gesetzes entgegnet werden kann."

Dass unter dem „Standort" der Anlage die Adresse zu verstehen ist, ist ebenfalls der Gesetzesbegründung zu entnehmen, denn in der BT-Drs. 16/2455 (Seite 10) heißt es:

„Standort ist der Ort, an dem die Anlage sich befindet. Er wird insbesondere gekennzeichnet durch die genaue Angabe der Adresse bzw. des Flurstücks, des Ortsnamens und der Postleitzahl"

Gesetzgeberisches Ziel war es, durch die Veröffentlichung die Transparenz im Hinblick auf den so genannten (Kosten-)Wälzungsmechanismus für Strom aus erneuerbaren Energien zu verbessern. Hintergrund ist, dass das EEG bestimmte Vergütungshöhen für eingespeisten Strom aus erneuerbaren Energien vorsieht, die an den Anlagenbetreiber zu leisten sind. Die hierdurch entstehenden Kosten sind nach dem sog. Wälzungsmechanismus des EEG letztlich von allen Stromkunden zu tragen. Da die Vergütung nicht durch eine Behörde im Wege eines (gerichtlich überprüfbaren) Bescheides festgesetzt wird, sondern sich direkt aus dem Gesetz ergibt, bestehen im Gegenzug zivilrechtliche Klagemöglichkeiten für alle Akteure, d. h. grundsätzlich auch für andere Stromkunden. Um diese Klagemöglichkeiten nutzen zu können, müssen die Beteiligten - so jedenfalls die Intention des Gesetzgebers - die Möglichkeit haben, in Erfahrung zu bringen, an welcher Stelle und somit durch welche Anlage die jeweiligen Kosten entstanden sind. Dritte sollen deshalb nachvollziehen können, welche Vergütung im Verhältnis zwischen dem jeweiligen Netzbetreiber und dem Betreiber einer Anlage im Sinne des EEG geflossen ist.

Dass uns dennoch immer wieder Anfragen zu diesem Thema erreichen, zeigt, dass die gesetzliche Veröffentlichungspflicht in der Bevölkerung noch nicht allgemein bekannt ist.

11.4 Kopieren von Personalausweisen

Das Kopieren von Personalausweisen ist für die Feststellung der Identität in aller Regel nicht erforderlich und damit datenschutzrechtlich unzulässig. Zur Identitätsfeststellung genügt in den meisten Fällen eine Einsichtnahme in den Ausweis.

Wiederholt beschwerten sich Kunden darüber, dass Unternehmen darauf bestanden haben, eine Kopie des Personalausweises des Kunden anzufertigen und zu den Geschäftsunterlagen zu nehmen. Die Beschwerden betrafen Unternehmen verschiedenster Branchen. So wollten in mehreren Fällen Handelsunternehmen von Kunden, die Waren online vorbestellt hatten, bei der Warenabholung im Ladengeschäft Personalausweiskopien anfertigen. In einem anderen Fall verlangte ein Hotel von Kunden nicht lediglich die nach Art. 23 Abs. 2 in Verbindung mit Art. 24 des Bayerischen Meldegesetzes vorgeschriebene Ausfüllung eines Meldescheins, sondern kopierte zusätzlich noch die Personalausweise.

Im Gesetz findet sich zwar kein ausdrückliches Verbot des Kopierens von Personalausweisen oder Reisepässen. Nach Auffassung des Bundesministeriums des Innern (BMI) ist jedoch ein grundsätzliches Kopierverbot aus dem Eigentum des Bundes an (Pässen und) Personalausweisen, der Existenz einiger spezieller Erlaubnistatbestände (z. B. im Geldwäschegesetz) sowie indirekt aus § 14 Personalausweisgesetz - PAuswG - ableitbar.

Das Kopieren stellt eine Erhebung und Verarbeitung personenbezogener Daten gemäß § 3 Abs. 3 und Abs. 4 Nr. 1 BDSG dar. Diese sind gemäß § 4 Abs. 1 BDSG nur zulässig, wenn sie im Einzelfall auf eine Rechtsvorschrift oder auf eine Einwilligung des Betroffenen gestützt werden können. Mit Blick auf das Eigentum des Bundes an den Personalausweisen ist indessen mindestens zweifelhaft, ob sich die Anfertigung einer Personalausweiskopie alleine auf die Einwilligung des Betroffenen stützen ließe; im Ergebnis wäre damit für die Kopieerstellung

eine Rechtsvorschrift als Rechtsgrundlage erforderlich. Als zulässiger Zweck des Kopierens von Personalausweisen kommt gegenüber nicht-öffentlichen Stellen ausschließlich die Identifizierung in Betracht. Soweit im konkreten Fall mangels Einschlägigkeit eines speziellen gesetzlichen Erlaubnistatbestands (wie z. B. § 8 Abs. 1 Satz 3 Geldwäschegesetz - GwG - oder § 95 Abs. 4 Telekommunikationsgesetz - TKG) lediglich eine generalklauselartige gesetzliche Datenerhebungsbefugnis - insbesondere § 28 Abs. 1 Satz 1 Nr. 2 BDSG - in Betracht kommt, ist sorgfältig zu prüfen, ob die Anfertigung der Kopie tatsächlich „erforderlich“ ist. Betroffene sind darauf hinzuweisen, dass Daten, die nicht zur Identifizierung benötigt werden (darunter insbesondere die auf dem Ausweis aufgedruckte sog. Zugangs- sowie die Seriennummer) auf der Kopie geschwärzt werden können und sollen.

Um in den von uns untersuchten Fällen die Identität der Person überprüfen zu können, die die Ware online vorbestellt hat, genügt es für das Unternehmen, sich den Personalausweis vorzeigen zu lassen. Dies sieht auch § 20 PAuswG ausdrücklich vor, wonach der Ausweisinhaber den Ausweis bei öffentlichen und nichtöffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden kann. Hingegen ist das Kopieren des Ausweises für die Identitätsfeststellung nicht notwendig. Um zu dokumentieren, dass der Ausweis vorgelegen hat, reicht es aus, wenn der befasste Mitarbeiter einen entsprechenden Vermerk anfertigt. Damit ist das Kopieren des Personalausweises jedenfalls dann, wenn - wie im Handel oder Dienstleistungsbereich in aller Regel der Fall - dessen Vorzeigen zur Identifizierung ausreichen würde, nicht erforderlich. Das Kopieren war damit in den von uns überprüften, eingangs genannten Fällen im Handel und in der Hotellerie unzulässig.

Anders kann es sein, wenn der Betroffene nicht persönlich bei dem Unternehmen vorspricht und somit ein bloßes Vorzeigen des Ausweises nicht in Betracht kommt. Hier kann es im Einzelfall als vertretbar angesehen werden, vom Betroffenen die Zusendung einer Personalausweiskopie anzufordern. In diesen Fällen muss der Betroffene aber auf die Möglichkeit der Schwärzung der im konkreten Fall nicht benötigten Daten hingewiesen werden.

Eine Reihe von Eingabeführern fragte nach der Zulässigkeit des Kopierens des Personalausweises in sog. Handy-Shops. Insoweit kann § 95 Abs. 4 TKG als spezialgesetzlicher Erlaubnistatbestand eingreifen, demzufolge Anbieter von Telekommunikationsdiensten im Zusammenhang mit dem Begründen und dem Ändern des Vertragsverhältnisses sowie dem Erbringen von Telekommunikationsdiensten nicht nur die Vorlage eines amtlichen Ausweises verlangen dürfen, wenn dies zur Überprüfung der Angaben des Teilnehmers erforderlich ist, sondern den Ausweis auch kopieren dürfen. Allerdings muss der Diensteanbieter die Kopie unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Teilnehmers vernichten. Wenn die Identitätsprüfung - wie häufig - unmittelbar vor Ort erfolgen kann, dürfte allerdings die Anfertigung einer Ausweiskopie auch in solchen Fällen nicht erforderlich sein, jedenfalls aber muss die Kopie unverzüglich nach Feststellung der o. g. Angaben vernichtet werden.

11.5 Kundenbefragungen durch Energieversorgungsunternehmen

Kundenbefragungen in personenbezogener Form zu Energieverbrauchsgewohnheiten setzen weitgehend die Einholung datenschutzrechtlich wirksamer Einwilligungen voraus. Geht es Unternehmen nur um die Gewinnung statistischer Parameter, werden vielfach Befragungen in anonymisierter Form ausreichend sein. Sofern eine Verwendung personenbezogener Daten für Werbezwecke beabsichtigt ist, sind die Wertungen des § 28 Abs. 3 BDSG bereits bei der Datenerhebung zu beachten.

Ein örtlicher Energieversorger verteilte im Wege einer nichtpersonalisierten Wurfsendung an alle Haushalte einer Gemeinde einen Fragebogen und bat um Beantwortung von Fragen zu den im Haushalt genutzten Heizsystemen einschließlich Energiequellen (Strom, Heizöl, Solarkollektoren, etc.), der jeweiligen Wärmeleistung der Heizsysteme und dem Jahresverbrauch, ferner zum Jahresstromverbrauch und zur beheizten Wohnfläche. Die Befragten wurden gebeten, ihre Namen und Adressen auf den zurückzusendenden Fragebogen einzutragen. Im Anschreiben gab das Unternehmen an, die Befragung diene der Gewinnung eines Überblicks über die örtlichen Energieverbrauchsgewohnheiten und werde als Grundlage für die weiteren Entscheidungsprozesse im Hinblick auf strategische Ausrichtung und Planung des Unternehmens Verwendung finden. Langfristig werde die „Energieautarkie“ der betreffenden Gemeinde angestrebt. Die Angaben würden ausschließlich zu statistischen Zwecken verwendet.

Die Befragung stellt in dieser Form eine datenschutzrechtlich unzulässige Erhebung personenbezogener Daten dar. Das Interesse des Unternehmens an der Gewinnung einer Datenbasis für seine strategisch-unternehmerische Planung ist als solches zwar verständlich. Allerdings konnte das Unternehmen im Rahmen unserer Überprüfung nicht nachvollziehbar darlegen, weshalb hierfür keine anonymisierten Daten ausreichten. Damit fehlte bereits ein berechtigtes Interesse im Sinne von § 28 Abs. 1 Satz 1 Nr. 2 BDSG an der Erhebung personenbezogener Daten. Vielfach - und nach unserer Bewertung so auch im vorliegenden Fall - wird es in derartigen Fällen ausreichen, rein statistische Daten zu erheben, mithin den Kunden Fragebögen zur Verfügung zu stellen, die keinen Rückschluss auf die Identität des Antwortenden zulassen.

Die Rücksendung der ausgefüllten Fragebögen konnte auch nicht als (konkludente) Einwilligung in die Erhebung der erfragten personenbezogenen Daten ausgelegt werden, denn eine datenschutzrechtliche Einwilligung erfordert gemäß § 4a Abs. 1 Satz 3 BDSG grundsätzlich die Schriftform. Bei schriftlichen Umfragen wie vorliegend wird man in aller Regel keine Ausnahme vom Schriftformerfordernis anerkennen können, weil eine Unterschrift ohne weiteres erbeten werden könnte. Damit wäre gemäß § 126 Abs. 1 BGB für eine rechtswirksame Einwilligung die Unterschrift des jeweiligen Betroffenen oder eine mit qualifizierter elektronischen Signatur versehene Erklärung (§§ 126 Abs. 3, 126a BGB) erforderlich gewesen, woran es im überprüften Fall fehlte.

Das Versorgungsunternehmen hat nach der Mitteilung des Überprüfungsergebnisses und entsprechender Aufforderung durch unsere Behörde umgehend alle Daten, die einen Personenbezug ermöglichten, unkenntlich gemacht.

In einem anderen Fall fragte ein Energieversorger in einem als Gewinnspiel gestalteten Fragebogen nach Einstellungen der Befragten zum Thema Energie, etwa nach der Meinung zu einzelnen Energiequellen. Darüber hinaus wurde aber auch nach Interessen, Freizeitbeschäftigungen und persönlichen Wertvorstellungen gefragt. Am Ende des Fragebogens wurde in Textform erläutert, dass der Betroffene mit der Rücksendung des Fragebogens dem Unternehmen die Einwilligung in die Erhebung, Verarbeitung und Nutzung der erhobenen personenbezogenen Daten erteile. Zweck des Fragebogens sei die Erbringung von an die Kundenbedürfnisse angepassten Leistungen sowie die bedarfsgerechte Information über Produkte. Eine Unterzeichnung der ausgefüllten Fragebogen wurde nicht erbeten.

Wir haben die Datenerhebung auch in diesem Fall als unzulässig bewertet. Hauptzweck der Erhebung war es bei verständiger Würdigung, mittels der erfragten Informationen in einem gewissen Umfang „Profile“ der Betroffenen zu bilden, um diesen spezifisch auf sie zugeschnittene Werbung zukommen zu lassen.

Auch in diesem Fall wurden keine datenschutzrechtlich wirksame Einwilligungen der Betroffenen eingeholt, da keine Unterzeichnung der Fragebogen durch die Betroffenen erfolgte und es damit an der nach § 4a Abs. 1 Satz 3 BDSG erforderlichen Schriftform der Einwilligung fehlte.

Die Datenerhebung konnte nicht auf eine Rechtsvorschrift gestützt werden. Da § 28 Abs. 3 BDSG lediglich die Verarbeitung und Nutzung, nicht jedoch die Erhebung personenbezogener Daten für Werbezwecke regelt, war die Datenerhebung an § 28 Abs. 1 und 2 BDSG zu messen. Im Ergebnis konnte sie auf keinen der gesetzlichen Erhebungstatbestände gestützt werden, auch nicht auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Bei der hierbei gebotenen Interessenabwägung war maßgeblich zu berücksichtigen, dass die geplante Verarbeitung und Nutzung der erhobenen Daten für Werbezwecke nicht auf einen gesetzlichen Zulässigkeitstatbestand nach § 28 Abs. 3 BDSG hätte gestützt werden können. Zum einen gingen die Kategorien der erhobenen Daten deutlich über die sog. Listendaten im Sinne von § 28 Abs. 3 Satz 2 BDSG hinaus. Zum anderen griff insoweit auch nicht die gesetzliche Hinzuspeicherungsbefugnis nach § 28 Abs. 3 Satz 3 BDSG. Unternehmen dürfen zwar nach dieser Vorschrift zum Zweck der Eigenwerbung zu den sog. Listendaten grundsätzlich weitere Daten hinzuspeichern, wodurch ihnen nach der Gesetzesbegründung (BT-Drs. 16/12011, Seite 32) ermöglicht werden soll, den eigenen Kundendatenbestand zu selektieren, um die Kunden gezielter ansprechen zu können. Jedoch stellt § 28 Abs. 3 Satz 3 BDSG keine eigene Datenerhebungsbefugnis dar, sondern setzt nach der Gesetzesbegründung gerade voraus, dass das Unternehmen die hinzu zu speichernden Daten nach einer anderen Rechtsgrundlage rechtmäßig erhoben oder übermittelt bekommen haben muss. Letzteres war aber bezüglich der vorliegend per Fragebogen erfragten Daten nicht der Fall, da diese Daten gerade erst im Wege der Befragung, deren Zulässigkeit zur Beurteilung anstand, erhoben wurden und somit nicht bereits anderweitig aufgrund einer gesetzlichen Befugnis rechtmäßig erhoben worden waren. Da somit das

Unternehmen die per Fragebogen erhobenen Daten nicht für werbliche Zwecke hätte verwenden dürfen, konnte die Erhebung dieser Daten nicht auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden, da mangels einer datenschutzrechtlich zulässigen Verwendungsmöglichkeit für diese Daten ein berechtigtes Interesse an der Datenerhebung nicht anerkannt werden konnte.

11.6 Erhebung von personenbezogenen Daten eines Interessenten durch Makler

Ein Makler darf schon vor Zusendung eines Exposés, worum er von einem Interessenten per E-Mail gebeten wurde, diesen Interessenten in Verbindung mit einem Hinweis auf die Voraussetzungen des Entstehens seines Provisionsanspruchs auffordern, Name und Anschrift anzugeben.

Der Eingabeführer (Interessent) hatte in einem Internetportal ein Inserat über eine Mietwohnung gelesen und bat den inserierenden Makler per E-Mail um Zusendung des Exposés zu der Wohnung. In seiner Antwort per E-Mail teilte der Makler mit, dass er das Exposé zuschicken werde, sofern der Interessent vorab seine Kontaktdaten (Name und Adresse) mitteilt. In derselben E-Mail informierte der Makler den Interessenten noch darüber, dass für den Fall, dass aufgrund seiner Vermittlung ein Mietvertrag über die Wohnung zustande kommen würde, ein Provisionsanspruch seinerseits gegen den Interessenten fällig werde.

Der Interessent beschwerte sich bei uns darüber, dass der Makler ihn noch vor Zusendung des Exposés um die Angabe von Name und Adresse ersucht hatte. Wir haben das Vorgehen des Maklers aus folgenden Gründen als zulässig erachtet:

Gemäß § 10 Abs. 1 der Makler- und Bauträgerverordnung (MaBV) treffen den Makler „von der Annahme des Auftrags an“ bestimmte Aufzeichnungs- und Unterlagensammelpflichten. Gemäß § 10 Abs. 2 Nr. 1 MaBV müssen aus den Aufzeichnungen und Unterlagen insbesondere „der Name und Vorname oder die Firma sowie die Anschrift des Auftraggebers“ ersichtlich sein. Unter „Auftraggeber“ ist hierbei der Verbraucher zu verstehen, d. h. im vorliegenden Fall der Mietinteressent, nicht der Vermieter (vgl. Landmann/Rohmer, Kommentar zur Gewerbeordnung und anderen Vorschriften, 60. EL, Februar 2012, § 10 MaBV, Randziffer 5).

Die Pflicht zur Aufzeichnung des Namens des Verbrauchers besteht somit „von der Annahme des Auftrags an“. Nach der Rechtsprechung und Literatur wird hierunter der Zeitpunkt verstanden, in welchem der Wohnungsmakler einem Kunden die Vermittlung von Verträgen oder den Nachweis der Gelegenheit zum Vertragsabschluss zusagt. Vorliegend kam es mithin zunächst auf die Frage an, ob zwischen dem Interessenten und dem Makler zum Zeitpunkt, in dem der Makler den Interessenten zur Angabe von Name und Adresse aufforderte, im Rechtssinne bereits ein Maklervertrag zustande gekommen war.

Der Zeitpunkt des Zustandekommens eines Maklervertrags ist oft nicht ganz einfach festzustellen. Nach der Rechtsprechung kann von einem Vertragsabschluss durch schlüssiges Verhalten nur dann die Rede sein, wenn dem Interessenten die eindeutige Provisionsforderung des Maklers bekannt ist und er daraufhin in diesem Wissen weiterhin wesentliche Maklerdienstleistungen in Anspruch nimmt (BGH, NJW-RR 1996, 114; OLG Schleswig-Holstein, Urt. v. 21.07.2006 - Az. 14 U 55/06). Hingegen ist in der Entgegennahme von Maklerdiensten durch einen Interessenten nicht ohne weiteres der Abschluss eines Maklervertrages zu erblicken (BGH, NJW-RR 1999, 361; BGH, NJW-RR 1996, 114), vielmehr ist es Sache des Maklers, im Hinblick auf das Zustandekommen des Maklervertrages für klare Verhältnisse zu sorgen, etwa durch ein ausdrückliches Provisionsverlangen (BGH, NJW-RR 1996, 114).

Damit lag im vorliegenden Fall ein Vertragsschluss weder in der E-Mail-Anfrage des Interessenten noch in der Antwort-E-Mail des Maklers. Vielmehr wäre ein Maklervertrag erst zustande gekommen, wenn der Interessent im Anschluss an den Erhalt der E-Mail, in welcher der Makler über das Entstehen seines Provisionsanspruchs informierte, weiterhin Leistungen des Maklers in Anspruch genommen hätte.

Dennoch haben wir es im Ergebnis als datenschutzrechtlich zulässig erachtet, dass der Makler den Interessenten bereits in seiner ersten E-Mail um Angabe von Name und Anschrift ersucht hat. Denn aufgrund der Tatsache, dass der Makler in derselben E-Mail bereits über das Entstehen seines Anspruchs auf Maklerprovision für den Fall des Zustandekommens der Vermietung informiert hat, konnte der Interessent in Kenntnis dieser Information frei darüber entscheiden, ob er unter diesen Umständen die Maklerleistungen weiterhin in Anspruch nehmen wollte. Bringt ein Interessent nach Erhalt dieser Information sein fortbestehen-

des Interesse an den Maklerleistungen zum Ausdruck, kommt nach der Rechtsprechung gerade durch diese Interessensbekundung der Maklervertrag zustande und entsteht damit gleichzeitig die o. g. gesetzliche Verpflichtung des Maklers, Name und Anschrift des Interessenten zu speichern.

Selbst wenn es denkbar wäre, den Makler darauf zu verweisen, die Adressdaten des Interessenten durch ein weiteres, gesondertes Schreiben erst zu erfragen, nachdem der Interessent ab Kenntnis des Provisionsverlangens sein fortbestehendes Interesse an der Maklerleistung zum Ausdruck gebracht hat, ist nach unserer Auffassung die Erfragung der Daten des Interessenten bereits in demselben Schreiben, in dem der Makler über seine Provisionsforderung informiert, gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG als zulässig zu bewerten. Wenn ein Interessent in Kenntnis des Provisionsverlangens kein Interesse an den Maklerleistungen (mehr) hat, kann er von einer Fortsetzung des Kontakts schlicht Abstand nehmen und muss dann auch nicht seine Daten angeben. Hingegen hat er gemäß § 10 Abs. 1, Abs. 2 Nr. 1 MaBV kein rechtlich schutzwürdiges Interesse daran, Maklerleistungen - hierzu zählt auch bereits die Zusendung eines Exposés - ohne Angabe seines Namens und seiner Anschrift zu erhalten, nachdem ihn der Makler bereits über seine Provisionsforderung aufgeklärt hat.

11.7 Speicherung von Kundendaten bei Warenumtausch im Handel

Handelsunternehmen dürfen bei aus Kulanz ermöglichten Warenrückgaben Kundendaten zum Zweck der Verfolgung etwaiger Rechtsansprüche im Falle einer Vertragsstörung speichern. Sofern dabei auch Beschäftigtendaten dazu gespeichert werden, dürfen diese unter den Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG genutzt werden.

Einige Handelsunternehmen bieten Kunden die Möglichkeit der freien Rückgabe gekaufter Waren innerhalb eines begrenzten Zeitraums an, ohne dass dafür in rechtlicher Hinsicht ein Rückgabegrund vorliegen muss. Diesbezüglich erreichten uns immer wieder Anfragen dazu, ob Unternehmen anlässlich einer Warenrückgabe personenbezogene Daten des Kunden erheben und speichern dürfen.

Die Unternehmen begründen die Speicherung der Kundendaten in der Regel damit, dass sich nach Rückgabe der Ware bisweilen herausstelle, dass die Ware beschädigt sei. In solchen Fällen müsse die Identität des Kunden für eine etwaige zivilrechtliche Auseinandersetzung mit Letzterem bekannt sein.

Ferner führen einige Unternehmen an, die Umtauschdaten in bestimmten Fällen nutzen zu wollen, um zu verifizieren, ob tatsächlich ein realer Umtauschvorgang stattgefunden habe. Es gebe Fälle, in denen Kassenmitarbeiter Umtauschvorgänge fingiert und Geld aus der Kasse entnommen hätten. Im Verdachtsfall müsse es daher möglich sein, den Vorgang zu rekonstruieren. So teilte uns das Unternehmen in dem von uns bearbeiteten Fall mit, dass zu diesem Zweck zu den „Umtauschdaten“, d. h. den Kundendaten sowie den Daten, die sich auf die Ware beziehen, auch Daten zu der Identität des jeweiligen Mitarbeiters (insbesondere an der Kasse) hinzugespeichert würden, der den Umtausch abgewickelt habe.

Im Einzelnen haben wir die Erhebung und Speicherung der Umtauschdaten zu den beiden o. g. Zwecken datenschutzrechtlich wie folgt bewertet:

Was die Aufdeckung von Missbrauchsfällen durch Mitarbeiter betrifft, handelt es sich um eine Frage des Beschäftigtendatenschutzes. Die Aufdeckung eines - zunächst nur theoretisch denkbaren - Missbrauchs, für den es jedoch bezogen auf einen konkreten Umtauschvorgang (noch) keine tatsächlichen Anhaltspunkte gibt, vermag die Speicherung oder Nutzung der Umtauschdaten für sich gesehen nicht zu rechtfertigen, denn nach § 32 Abs. 1 Satz 2 BDSG erfordert die Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten zur Aufdeckung von Straftaten tatsächliche Anhaltspunkte auf eine Straftat des Beschäftigten.

Die Erhebung und Speicherung kann aber zunächst auf § 28 Abs. 1 S. 1 Nr. 2 BDSG gestützt werden, soweit sie der Durchsetzung etwaiger zivilrechtlicher Ansprüche gegen den Kunden z. B. bei beschädigter Ware dient. Durch die Rückgabe der Ware entsteht zivilrechtlich ein sog. Rückgewährschuldverhältnis. Im Falle einer rechtlichen Störung in diesem Verhältnis, etwa wenn die Ware beschädigt ist, ist für das Unternehmen die Kenntnis der Identität des Kunden erforderlich, um etwaige zivilrechtliche Ansprüche gegen ihn durchsetzen zu können. Als Dauer der zulässigen Verarbeitung und Nutzung für diesen Zweck erscheint grundsätzlich ein Zeitraum von bis zu sechs Monaten ab Umtausch als vertretbar, da sich etwaige Störungen in

diesem Zeitraum in aller Regel gezeigt haben werden. Nach Ablauf von sechs Monaten sind die Umtauschdaten grundsätzlich zu sperren (§ 35 Abs. 2 Satz 1 Nr. 3 BDSG), da ihre Kenntnis für die Erfüllung dieses Speicherzwecks nicht mehr erforderlich ist. Dies bedeutet u. a., dass nach diesem Zeitraum die Umtauschdaten nicht mehr im normalen „Tagesgeschäft“ durch Personal einsehbar sein dürfen. Sollen die Daten nach ihrer Sperrung noch genutzt werden, wäre dies nur noch unter den engen Voraussetzungen des § 35 Abs. 8 BDSG zulässig, d. h. etwa wenn dies zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist.

Sollen die gespeicherten Umtauschdaten im Zeitraum vor ihrer Sperrung zum Zweck der Aufdeckung etwaiger Missbrauchsfälle durch Beschäftigte genutzt werden, ist dies nur nach Maßgabe von § 32 Abs. 1 Satz 2 BDSG zulässig. Voraussetzung sind damit insbesondere tatsächliche Anhaltspunkte für den Verdacht einer Straftat eines Beschäftigten. Unzulässig wäre es somit, gespeicherte Umtauschdaten ohne tatsächliche Anhaltspunkte für einen Straftatverdacht auszuwerten, insbesondere etwa mit dem Ziel, durch die Auswertung überhaupt erst einmal Anhaltspunkte auf etwaige Missbräuche zu gewinnen. Unzulässig wäre ferner etwa die Nutzung bei einem Verdacht auf solche arbeitsvertraglichen Pflichtverletzungen, die keine Straftatqualität haben.

11.8 Weitergabe von Kundendaten an ein Subunternehmen

Ob die Weitergabe von Kundendaten bei Dienst- oder Werkverträgen an einen Subunternehmer zulässig ist, ergibt sich in erster Linie aus der zivilrechtlichen Rechtslage. Möchte ein Betroffener keine Weitergabe seiner Daten, empfiehlt sich meist, dies ausdrücklich mitzuteilen. Unberührt davon bleibt die datenschutzrechtliche Informationspflicht verantwortlicher Stellen im Hinblick auf mögliche Datenempfänger oder -empfängerkategorien.

Ein Kunde beschwerte sich darüber, dass ein Gartenbaubetrieb, den er mit Baumschneidearbeiten in seinem Garten beauftragt hatte, seine Adressdaten an einen Subunternehmer weitergegeben hatte. Dies stellte er fest, als an dem für die Durchführung der Arbeiten vereinbarten Termin anstelle von Mitarbeitern des Gartenbaubetriebs lediglich der Inhaber des Subunternehmens erschien. Der Kunde trug auch vor, dem Gartenbaubetrieb bei der Auftragserteilung ausdrücklich mitgeteilt zu haben, keine Einschaltung von Subunternehmern zu wünschen.

Der Inhaber des Gartenbauunternehmens bestritt uns gegenüber, dass der Kunde seinem Unternehmen die Einschaltung von Subunternehmern untersagt habe. Er habe angenommen, dass der Auftraggeber keine Einwände gegen die Einschaltung des Subunternehmers haben würde. Er begründete dies damit, dass derselbe Subunternehmer bereits in der Vergangenheit einmal im Auftrag des Gartenbaubetriebs für denselben Kunden tätig gewesen sei, ohne dass der Kunde dies moniert habe. Auf diesen Einwand hin erwiderte der Kunde, dass er bei jenem früheren Auftrag nicht gewusst habe, dass es sich bei der die Arbeiten durchführenden Person um einen eigenständigen Subunternehmer gehandelt habe, vielmehr sei er davon ausgegangen, dass ein Mitarbeiter des Gartenbauunternehmens bei ihm gearbeitet habe.

Der Fall zeigt auch die Grenzen der Aufklärungsmöglichkeiten der Datenschutzaufsichtsbehörde auf. Es standen sich widersprechende Aussagen der Beteiligten darüber im Raum, ob der Kunde dem Gartenbaubetrieb die Einschaltung von Subunternehmern untersagt hatte oder nicht. Eine abschließende Aufklärung dieser Frage war uns nicht möglich. Wir verwiesen daher allgemein darauf, dass gemäß § 267 Abs. 1 BGB ein Schuldner für die Erbringung einer Leistung einen Dritten einschalten dürfe, sofern er nicht in eigener Person zu leisten habe. Eine persönliche Dienstleistungspflicht des Schuldners bestehe als gesetzliche Ausnahme etwa gemäß § 664 Abs. 1 Satz 1 BGB grundsätzlich bei Beauftragten oder gemäß § 613 BGB im Zweifel bei Dienstleistungsverpflichteten, erst recht bei sog. höchstpersönlichen Leistungen, d. h. wenn es auf die besonderen Fähigkeiten der betroffenen Person ankomme. Von einer (höchst-) persönlichen Leistungspflicht konnte im vorliegenden Fall jedoch nicht ausgegangen werden, da der Vertrag über Baumschneidearbeiten einen Werkvertrag darstellt und es sich auch nicht aus der Natur dieser Arbeiten ergibt, dass sie nur vom beauftragten Unternehmen selbst erbracht werden sollten.

Sofern die Einschaltung eines Subunternehmers nach bürgerlichem Recht zulässig ist, bringt dies mit sich, dass diejenigen Kundendaten an den Subunternehmer weitergegeben werden dürfen, die zur Auftragserfüllung nötig sind, im vorliegenden Fall somit jedenfalls die Kundenadressdaten.

Die Datenübermittlung kann in diesem Fall auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG gestützt werden.

Damit konnten wir im Ergebnis nur feststellen, dass die Zulässigkeit der Datenübermittlung im vorliegenden Fall davon abhängt, ob der Kunde dem Gartenbaubetrieb die Einschaltung eines Subunternehmers verboten hatte. Da der Kunde diesen Beweis nicht erbringen konnte, haben wir nicht positiv die Unzulässigkeit der Adressdatenübermittlung festgestellt. Wir haben dem Gartenbauunternehmen aber mitgeteilt, dass es den Kunden gemäß § 4 Abs. 3 Satz 1 Nr. 3 BDSG darüber hätte informieren müssen, dass seine (Adress-)Daten an Subunternehmer weitergegeben werden. Der Gartenbaubetrieb konnte nicht belegen, einen solchen Hinweis gegeben zu haben. Wir haben daher gefordert, dass diese Information künftig in die schriftlichen Auftragserteilungsbögen aufgenommen wird und im Falle telefonischer oder mündlicher Auftragsvergabe der Hinweis ebenfalls erteilt wird.

11.9 Aufnahme von Dauerkartenkäufern in eine Liste

Selbst wenn personenbezogene Daten allein zum (vermeintlichen) Vorteil eines Kunden erhoben und gespeichert werden, müssen die Betroffenen hinreichend über den Datenerhebungs- und -verwendungszweck informiert werden.

Der Veranstalter einer auf längere Dauer angelegten Veranstaltung bot den Besuchern alternativ zum Erwerb von Einzeleintrittskarten Dauerkarten für einen beliebig häufigen Besuch an. Die Karten sollten durch den Erwerber selbst mit seinem Namen und einem Lichtbild versehen werden. An den Kartenverkaufsstellen wurden die Namen und Adressen der Erwerber von Dauerkarten in eine handschriftliche Liste eingetragen. Ein Kunde stellte bei uns die Frage nach der Zulässigkeit dieser Listeneintragung.

Auf unsere Nachfrage erklärte der Veranstalter, dass die Namen und Adressen ausschließlich dazu dienten, dass der Kunde im Falle des Verlusts seiner Dauerkarte den Kartenerwerb nachweisen könne. Dem Kunden würde in diesem Fall eine neue Dauerkarte ausgestellt. Für andere Zwecke würden die Daten nicht verwendet. Schriftliche vertragliche Regelungen - etwa in AGB - zum Vorgehen im Falle des Verlusts der Dauerkarte waren nicht getroffen worden.

Da der Kunde die Karte (unter anderem) durch Beschriftung mit seinem Namen selbst personalisieren sollte, und auch keine schriftlichen vertraglichen Regelungen über die Verwendung der Adressdaten nachweisbar waren, war die Erhebung der Namen und Adressen nicht zur Begründung, Durchführung oder Beendigung der jeweiligen Vertragsbeziehung erforderlich, so dass § 28 Abs. 1 Satz 1 Nr. 1 BDSG als Rechtsgrundlage hierfür nicht in Betracht kam. Wäre das vom Unternehmen dargelegte Vorgehen bei Kartenverlust ausdrücklich vertraglich vereinbart worden, wäre eine datenschutzrechtliche Rechtfertigung nach dieser Vorschrift denkbar gewesen.

Die Kunden waren offenbar - entgegen § 4 Abs. 3 Nr. 2 BDSG - jedenfalls nicht in allen Fällen hinreichend über den Zweck der Speicherung ihrer Adressdaten informiert worden. Selbst wenn daher, wie vom Unternehmen vorgetragen, die Daten zum rechtlichen Vorteil der Kunden verwendet werden sollten, konnte jedenfalls in den Fällen mangelnder Information die Datenerhebung und -verwendung schon aus diesem Grund auch nicht auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden, weil jedenfalls nicht nachweisbar war, dass den Betroffenen die Möglichkeit zur Geltendmachung von Einwänden gegen die Datenerhebung und damit zur Artikulierung ihrer schutzwürdigen Interessen im Sinne von § 28 Abs. 1 Satz 1 Nr. 2 BDSG eröffnet worden war.

Damit hätten gemäß § 4 Abs. 1 BDSG Einwilligungen der Betroffenen eingeholt werden müssen, was wiederum nach § 4a Abs. 1 Satz 2 BDSG deren hinreichende Information über den Zweck der Erhebung, Speicherung und Nutzung ihrer Adressdaten vorausgesetzt hätte. Zwar könnte es bei einer solchen „Einwilligungslösung“ auf den ersten Blick denkbar erscheinen, angesichts der Vorteilhaftigkeit der Datenspeicherung für die Betroffenen nach § 4a Abs. 1 Satz 3 BDSG eine mündliche Einwilligungserteilung genügen zu lassen. Jedoch müsste auch dann jedenfalls die hinreichende Information der Betroffenen erfolgen und aus Nachweisbarkeitsgründen dokumentiert werden, weil eine rechtswirksame Einwilligung voraussetzt, dass der Betroffene weiß, worin er einwilligt. Aus Gründen der Nachweisbarkeit ist darüber hinaus aber auch die Erteilung der Einwilligungen selbst in schriftlicher Form eindeutig empfehlenswert.

12 Internationaler Datenverkehr

Im Berichtszeitraum hat die Anzahl der Anfragen zu Sachverhalten mit internationalem Bezug deutlich zugenommen. Dies ist zweifellos der sich stetig verstärkenden Internationalisierung von Arbeits- und Geschäftsprozessen von Unternehmen und Unternehmensgruppen geschuldet. Der internationale Datenverkehr wirft zahlreiche z. T. sehr komplexe datenschutzrechtliche Fragen auf, aufgrund derer bei Datenschutzbeauftragten und Unternehmen oft erheblicher Beratungsbedarf besteht.

In besonderer Weise hervorzuheben ist der ungebrochene Trend zum Outsourcing datenverarbeitender Dienste, aber auch von Soft- und Hardwarewartung und -pflege an spezialisierte Dienstleister. Eine Übermittlung personenbezogener Daten kann auch bei Arbeiten der IT-Wartung und Pflege häufig nicht ausgeschlossen werden, selbst wenn sie nicht den eigentlichen Zweck des Outsourcings ausmacht. Häufig möchten Unternehmen für solche Dienstleistungen - etwa gemäß dem sog. follow-the-sun-Prinzip - Unternehmen einschalten, die (auch) außerhalb der EU bzw. des EWR ansässig sind.

Das derzeit noch geltende europäische Datenschutzrecht stößt angesichts der Praxisentwicklungen merklich an seine Grenzen. So decken die wichtigsten für den Austausch personenbezogener Daten mit Drittstaaten zur Verfügung stehenden Rechtsinstrumente, namentlich die sog. Standardvertragsklauseln der Europäischen Kommission, nicht alle relevanten Fallgestaltungen ab. Besondere Schwierigkeiten bereitet insoweit die mehrstufige Auftragsvergabe. Hier erfordern einige Fallgestaltungen in datenschutzrechtlicher Hinsicht einen faktisch kaum mehr leistbaren Verfahrensaufwand. Der auch hieran erkennbare Reformbedarf im europäischen Datenschutzrecht bildet einen Hintergrund für den von der EU-Kommission Anfang 2012 vorgelegten Vorschlag einer europäischen Datenschutz-Grundverordnung.

12.1 Erhebliche Probleme bei der Einschaltung von Drittstaats-Unterauftragsverarbeitern

Die Tatsache, dass Auftragsdatenverarbeiter mit Sitz in einem Drittstaat ohne angemessenes Datenschutzniveau auf der Basis eines Standardvertrages selbst Unterauftragsdatenverarbeiter in einem solchen Drittstaat einschalten können, Auftragsdatenverarbeiter aus der EU, dem EWR-Raum oder aus einem (von der EU-Kommission anerkannten) Drittstaat mit angemessenen Datenschutzniveau dagegen nicht, stellt sich als ein derzeit unlösbares Problem einer „Inländerdiskriminierung“ dar.

In unserem letzten Tätigkeitsbericht haben wir darauf hingewiesen, dass die ab dem 15. Mai 2010 zur Verfügung stehenden Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern (KOM-Beschluss 2010/87/EU) nach ihrem eindeutig definierten Anwendungsbereich nur anwendbar sind, wenn der erste in der Auftragskette eingeschaltete Auftragsdatenverarbeiter (Hauptauftragsverarbeiter) seinen Sitz in einem Drittstaat ohne angemessenes Datenschutzniveau hat. Der Standardvertrag erlaubt in diesen Fällen gemäß seiner Klausel 11 Abs. 1 die Erteilung von Unteraufträgen durch den Hauptauftragsverarbeiter im eigenen Namen, was die Unterauftragsvergabe in der Praxis deutlich erleichtert.

Hat der Hauptauftragsverarbeiter hingegen seinen Sitz in der EU, im EWR oder in einem Drittstaat mit angemessenem Datenschutzniveau (Andorra, Argentinien, Australien, Färöer-Inseln, Guernsey, Israel, Isle of Man, Jersey, Kanada, Neuseeland, Schweiz und Uruguay), ist der Standardvertrag nicht anwendbar. In diesen Fällen ist für die Einschaltung eines Drittstaats-Unterauftragnehmers der direkte Abschluss eines Standardvertrags zwischen dem (EU-/EWR-)Auftraggeber - als Datenexporteur - und dem im Drittstaat ansässigen Unterauftragnehmer - als Datenimporteur - erforderlich („Direktvertragslösung“), wobei zivilrechtlich eine Stellvertretung des Auftraggebers durch den Hauptauftragsverarbeiter möglich ist. Dieses Direktvertragserfordernis führt insbesondere für bereits laufende Auftragsverarbeitungsverhältnisse zu erheblichen praktischen Umsetzungsproblemen, erst recht, wenn der Hauptauftragsverarbeiter personenbezogene Daten für eine Vielzahl von Auftraggebern verarbeitet, und ihm nicht bereits

zu Beginn der Geschäftsbeziehung seitens jedes Auftraggebers eine Vollmacht zum (Direkt-) Abschluss der Standardvertragsklauseln in Vertretung des jeweiligen Auftraggebers mit möglichen Unterauftragnehmern erteilt worden ist. Die nachträgliche Einholung einer Willenserklärung jedes einzelnen Auftraggebers dürfte in der Praxis Schwierigkeiten aufwerfen und nicht selten scheitern.

Die deutschen Aufsichtsbehörden haben diese schon lange bestehende Problematik kürzlich erneut intensiv diskutiert und festgehalten, dass nach geltendem deutschen Datenschutzrecht davon ausgegangen werden muss, dass ein in der EU, im EWR oder in einem Drittstaat mit angemessenem Datenschutzniveau ansässiger Hauptauftragsverarbeiter einen Unterauftrag an einen Drittstaats-Unterauftragnehmer nicht im eigenen Namen erteilen kann, jedenfalls aber für die Datenübermittlung an den Unterauftragnehmer zusätzlich eine Mitwirkung des Auftraggebers erforderlich ist. Außerhalb des Standardvertrags, der für diese Fallgestaltung nach oben Gesagtem gerade nicht anwendbar ist, und sofern der Drittstaats-Unterauftragsverarbeiter nicht safe-harbor-zertifiziert ist, bedarf eine Übermittlung personenbezogener Daten in einen Drittstaat ohne angemessenes Datenschutzniveau gemäß § 4c Abs. 2 Satz 1 BDSG einer Genehmigung der Aufsichtsbehörde. Datenübermittler und damit Adressat einer Übermittlungsgenehmigung kann aber nach deutschem Recht nur eine verantwortliche Stelle - mithin der Auftraggeber - sein, nicht hingegen ein Auftragsdatenverarbeiter. Damit bleibt es dabei: spätestens für die Einholung der Datenexportgenehmigung ist zur Einschaltung des Drittstaats-Unterauftragsverarbeiters eine aktive Mitwirkung des Auftraggebers erforderlich. Insbesondere vermag somit auch die Vergabe des Unterauftrags im Wege des Abschlusses eines „Nicht-Standardvertrags“ (ad-hoc-Vertrags) durch den EU-/EWR-Auftragnehmer im eigenen Namen mit dem Drittstaats-Unterauftragnehmer (siehe WP 176, Nr. I.3., das allerdings offen lässt, welcher Beteiligte den Unterauftrag bei Verwendung eines ad-hoc-Vertrages erteilen kann) bei Geltung des BDSG das Verfahren nicht zu vereinfachen.

Siehe:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_de.pdf

Die für den Datenexport in diesem Falle gemäß § 4c Abs. 2 Satz 1 BDSG erforderliche Genehmigung könnte nur einer verantwortlichen Stelle - nicht jedoch einem Auftragsverarbeiter - erteilt werden. Spätestens für die Einholung der Genehmigung wäre somit - wie bei der o. g. „Direktvertragslösung“ - doch eine Mitwirkung des Auftraggebers erforderlich, mit der Konsequenz der bereits dargestellten praktischen Schwierigkeiten. Selbst wenn man daran denken sollte, vor dem Datenexport eine Art „Muster-Unterauftragstext“ durch die Aufsichtsbehörden abstrakt vorab „genehmigen“ zu lassen, bliebe jeder Auftraggeber verpflichtet, zusätzlich einen entsprechenden Antrag auf Exportgenehmigung auf der Grundlage eines solchen Unterauftrags zu stellen.

Dies ist gerade anders als in der vom Standardvertrag 2010/87/EU abgedeckten Fallgestaltung, d. h. bei Sitz des ersten Auftragsverarbeiters in einem Drittstaat ohne angemessenes Datenschutzniveau, da gemäß Klausel 11 Abs. 1 des Standardvertrags die Unterbeauftragung durch den Hauptauftragsverarbeiter im eigenen Namen zulässig ist, wenn auch nur auf Grundlage einer vorherigen schriftlichen Einwilligung des Auftraggebers, die allerdings zunächst auch in allgemeiner Form (d. h. ohne schon anfängliche Benennung des konkreten Unterauftragnehmers) erteilt werden kann (vgl. WP 176, Nr. II.1). Zu fordern ist in diesen Fällen lediglich, dass der Hauptauftragsverarbeiter dem Auftraggeber vor der Datenweitergabe an den Unterauftragnehmer die Identität des letzteren nennt und dem Auftraggeber insoweit ein Widerspruchsrecht eingeräumt wird (vgl. Nrn. 3.3.2 und 4.1 des WP 196 „Cloud Computing“ der Artikel-29-Gruppe).

Siehe:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf

Eine direkte Vertragsbeziehung zwischen Auftraggeber und Unterauftragnehmer oder auch nur ein Aktivwerden des Auftraggebers (jenseits der vorherigen generellen Einwilligung in die Vergabe von Unteraufträgen durch den Hauptauftragsverarbeiter) ist mithin in diesen Fällen gerade nicht gefordert, was die praktische Umsetzung erheblich erleichtert.

Damit ist die Einschaltung von Drittstaats-Unterauftragnehmern jedenfalls unter rein verfahrenspraktischen Gesichtspunkten mit größeren Schwierigkeiten verbunden, wenn der Haupt-Auftragsverarbeiter innerhalb der EU, des EWR oder in einem Drittstaat mit angemessenem Datenschutzniveau ansässig ist als wenn er seinen Sitz in einem Drittstaat ohne angemessenes Datenschutzniveau hat. Dieses auf den ersten Blick möglicherweise überraschende Ergebnis folgt letztlich

aus dem eindeutig definierten (und begrenzten) Anwendungsbereich des Standardvertrags sowie der o. g. Rechtslage nach dem BDSG.

Gespräche mit den Aufsichtsbehörden anderer EU-Mitgliedstaaten haben gezeigt, dass die Rechtslage in den meisten Mitgliedstaaten offensichtlich derjenigen des BDSG entspricht. Lediglich in einigen wenigen Mitgliedstaaten scheint es - anders als nach deutschem Recht - möglich zu sein, dass ein Auftragsdatenverarbeiter als Datenexporteur fungiert und demgemäß die Erteilung von Datenexportgenehmigungen auch an Auftragsverarbeiter in Betracht kommt - ohne dass der Auftraggeber noch aktiv werden müsste. Nach deutschem Datenschutzrecht und wohl auch der Rechtslage in der Mehrzahl der EU-Mitgliedstaaten ist allerdings ein solches Vorgehen nicht möglich.

Damit bleibt es dabei: Gegenwärtig kann für eine Unterauftragsvergabe in Drittstaaten ohne angemessenes Datenschutzniveau im Falle des Sitzes des Hauptauftragsverarbeiters in der EU, im EWR oder in einem Drittstaat mit angemessenem Datenschutzniveau faktisch nach wie vor nur die o. g. „Direktvertragslösung“ angeboten werden. Zwar mag als theoretische Alternative hierzu der Abschluss eines „Nicht-Standardvertrags“ durch den Auftragsverarbeiter im eigenen Namen mit dem Unterauftragsverarbeiter in Betracht kommen. Diese Lösung dürfte aber in aller Regel kaum zur Verfahrensvereinfachung gegenüber der Direktvertragslösung führen, sondern vielmehr aufgrund der in diesem Fall bestehenden Genehmigungsbedürftigkeit des Datenexports sogar noch aufwändiger sein.

12.2 Kontrollrechte des Auftraggebers bei gestufter Auftragsdatenverarbeitung

Bei einer gestuften Auftragsdatenverarbeitung, d. h. Einschaltung von Unterauftragnehmern, müssen die Kontrollrechte des Auftraggebers, die er gegenüber seinem unmittelbaren Auftragnehmer haben muss, auch gegenüber den Unterauftragnehmern vorgesehen werden.

In unserer Beratungspraxis wurden wir immer wieder gefragt, ob bei der Einschaltung von Unterauftragsverarbeitern dem Auftraggeber immer ausdrücklich auch eigene Kontrollbefugnisse gegenüber den Unterauftragnehmern eingeräumt werden müssten, oder ob insoweit eine Kontrolle durch den (Haupt-)Auftragsverarbeiter ausreichend sei.

Die Frage betrifft Sachverhalte mit internationalem Bezug gleichermaßen wie reine Inlandssachverhalte, ist aber im internationalen Datenverkehr offensichtlich von besonderer praktischer Relevanz, weil hier häufig große (oft US-amerikanische) Auftragsverarbeiter Teile eines Auftrags zur Verarbeitung personenbezogener Daten an weitere Dienstleister als Unterauftragnehmer vergeben möchten. Nicht selten wird es hier um Fälle der IT-Wartung und -Pflege oder des technischen „Supports“ (Help-Desk) gehen, bei denen eine Kenntnisnahme des Dienstleisters von personenbezogenen Daten nicht ausgeschlossen werden kann und auf die daher gemäß § 11 Abs. 5 BDSG die gesetzlichen Regelungen zur Auftragsdatenverarbeitung entsprechende Anwendung finden. Es stellt sich mithin die Frage, ob der (z. B. US-) Auftragsverarbeiter mit den von ihm vorgesehenen Unterauftragsverarbeitern vertraglich regeln muss, dass den (in solchen Fällen oft zahlreichen) deutschen Kundenunternehmen derartige Kontrollrechte gegenüber den Unterauftragnehmern zustehen.

Auf Kontrollrechte des Auftraggebers kann auch bei derartigen „gestuften“ Auftragsverhältnissen nicht verzichtet werden. Der Auftraggeber bleibt gemäß § 11 Abs. 1 Satz 1 BDSG, unabhängig davon, wo die Auftragsverarbeitung stattfindet und wie viele (Unter-)Auftragsverarbeiter in der Auftragskette eingeschaltet sind, für die Verarbeitung datenschutzrechtlich stets verantwortlich. Gemäß § 11 Abs. 2 Satz 2 Nr. 7 BDSG müssen daher in jedem Vertrag zur Auftragsdatenverarbeitung Regelungen zu den Kontrollrechten des Auftraggebers getroffen werden. Um seine datenschutzrechtliche Verantwortung effektiv wahrnehmen zu können, muss der Auftraggeber daher sicherstellen, dass ihm auch gegenüber Unterauftragsverarbeitern ausdrücklich solche Kontrollrechte eingeräumt werden. Dies gilt unabhängig vom geographischen Ort der unterbeauftragten Datenverarbeitungen und selbst dann, wenn die Unterauftragsvergabe durch den (Haupt-)Auftragsverarbeiter erfolgt (zu Letzterem siehe Kapitel 12.1). Freilich ist es zulässig, dass die Auftragskontrolle beim Unterauftragsverarbeiter in der Praxis (vornehmlich) durch den Haupt-Auftragsverarbeiter für den Auftraggeber oder auch durch die Vorlage geeigneter Zertifikate durchgeführt wird. Eigene Kontrollrechte des Auftraggebers dürfen aber nicht ausgeschlossen und müssen vielmehr gegenüber dem Unterauftragsverarbeiter vertraglich ausdrücklich festgeschrieben werden. Bei Ver-

wendung des Standardvertrags zur Auftragsverarbeitung (Beschluss Nr. 2010/87/EU-Kommission vom 05.02.2010) ergibt sich dies aus dem Standardvertragstext selbst, da gemäß Klausel 11 Abs. 1 Satz 1 des Standardvertrags bei Unterauftragserteilungen sichergestellt werden muss, dass dem Unterauftragnehmer dieselben Pflichten auferlegt werden, wie sie bereits für den Haupt-Auftragnehmer gelten, und somit auch die Pflicht, Kontrollen des Auftraggebers gemäß Klausel 5 f zu dulden.

In der Praxis mag dieses Erfordernis nicht selten zu Schwierigkeiten führen, gerade bei Fällen mit Drittstaatsbezug und wenn große IT-Dienstleister als Haupt-Auftragsverarbeiter fungieren, da solche Dienstleister u. U. eigene vorformulierte Texte zur Unterauftragsvergabe verwenden möchten, die nicht immer auf die Anforderungen des europäischen bzw. deutschen Datenschutzrechts zugeschnitten sind. Fragen der faktischen Verhandlungsstärke der beteiligten Akteure sind aber aus Sicht des deutschen Datenschutzrechts nicht entscheidend. Eigene Kontrollbefugnisse des Auftraggebers auch bei (ggf. mehrfacher) Unterauftragsvergabe sind jedenfalls unverzichtbar, da der Auftraggeber andernfalls seine datenschutzrechtliche Verantwortung nicht wahrnehmen könnte.

12.3 Binding Corporate Rules (BCR)

Binding Corporate Rules (BCR - Verbindliche Unternehmensregelungen zum Datenschutz) sind eines der möglichen Instrumente zur Herstellung eines angemessenen Datenschutzniveaus bzw. ausreichender Datenschutzgarantien bei Datenempfängern in Drittstaaten ohne angemessenes Datenschutzniveau im Sinne von § 4b Abs. 2, Abs. 3 und § 4c Abs. 2 BDSG.

Immer mehr Aufsichtsbehörden in Deutschland und in der EU erhalten Anfragen von Unternehmensgruppen bzw. Konzernen, die Interesse an der Einführung von BCR für den Export personenbezogener Daten aus dem EWR an Gruppen- bzw. Konzernmitglieder außerhalb des EWR haben. Da Unternehmensgruppen häufig Mitgliedsunternehmen in mehreren EU-/EWR-Mitgliedstaaten haben, die gleichermaßen derartige Datenübermittlungen beabsichtigen, besteht ein nachvollziehbares Bedürfnis nach einer koordinierten Anerkennung von BCR zwischen allen betroffenen Datenschutzaufsichtsbehörden. Hierzu haben die Aufsichtsbehörden im EWR bereits vor Jahren ein Kooperationsverfahren etabliert und entwickeln dieses laufend fort. Demnach ist der Antrag auf Anerkennung von BCR bei der im EWR federführenden Aufsichtsbehörde zu stellen. Die Kriterien für die Bestimmung der Federführung im Anerkennungsverfahren sind im WP 107 der Artikel-29-Gruppe festgelegt; vorrangiges Kriterium ist hierbei der Sitz der europäischen Unternehmenszentrale. Die federführende Behörde ist zunächst alleiniger Ansprechpartner der Unternehmensgruppe und prüft den vorgelegten BCR-Entwurf, bis dieser nach ihrer Überzeugung die von der Artikel-29-Gruppe an BCR gestellten Anforderungen erfüllt (die Anforderungen finden sich in den WP 74, 108, 153, 154 und 155). Diese Anforderungen enthalten letztlich alle maßgeblichen Datenschutzgrundsätze und Betroffenenrechte gemäß der EU-Datenschutzrichtlinie und ferner Verpflichtungen zur Implementierung bestimmter Maßnahmen zur Sicherstellung der effektiven Geltung und Wirksamkeit der BCR in der Unternehmensgruppe.

Das BCR-Anerkennungsverfahren ist laufend weiterentwickelt worden. Inzwischen praktizieren die Datenschutzaufsichtsbehörden von 21 der 30 EWR-Staaten eine sog. „Gegenseitige Anerkennung“ (mutual recognition) von BCR. Hierbei verzichten sie auf eine eigene, gesonderte Prüfung eines BCR-Entwurfs und vertrauen insoweit auf die Prüfung der federführenden Aufsichtsbehörde. Vereinbart ist, dass die federführende Aufsichtsbehörde zwei weitere Behörden im EWR als Co-Prüfer am Verfahren beteiligen kann. Das mutual-recognition-Verfahren hat zu einer merklichen Verkürzung der Dauer der BCR-Anerkennungsverfahren beigetragen.

Detaillierte Informationen zu den Anforderungen an BCR und zum BCR-Anerkennungsverfahren, die Liste der an der Gegenseitigen Anerkennung teilnehmenden Mitgliedstaaten sowie eine Übersicht zu den Unternehmensgruppen, die bereits erfolgreich Anerkennungsverfahren abgeschlossen haben, sind auf der Homepage der Europäischen Kommission abrufbar.

Siehe:
http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

Im Berichtszeitraum haben nunmehr erstmalig auch wir als federführende Aufsichtsbehörde im EWR Anträge auf EWR-weite Anerkennung von BCR erhalten. Die Verfahren dauern derzeit noch an. Unsere bisherigen Erfahrungen mit diesen Verfahren sind positiv. Daneben haben wir in drei

weiteren - zwischenzeitlich abgeschlossenen - Verfahren, deren Federführung der Aufsichtsbehörde eines anderen Mitgliedstaates oblag, als Co-Prüfer mitgewirkt.

In unserer Beratungspraxis zu BCR haben einige Fragen eine besondere Rolle gespielt, die hier kurz angesprochen werden sollen:

Für die konkreten Exporte personenbezogener Daten auf der Basis von BCR sind jedenfalls in einer Reihe von Mitgliedstaaten - bzw. in Deutschland in einigen Bundesländern sowie im Zuständigkeitsbereich des Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) - zusätzlich zu den (aufsichtsbehördlich anerkannten) BCR noch Übermittlungsgenehmigungen der jeweils örtlich zuständigen Aufsichtsbehörden erforderlich. Dies bedeutet: Die konzern- bzw. gruppenangehörigen Gesellschaften in diesen Mitgliedstaaten und Bundesländern sowie die der aufsichtlichen Zuständigkeit des BfDI unterfallenden Gesellschaften müssen nach Abschluss des BCR-Anerkennungsverfahrens bei den jeweils für sie zuständigen Aufsichtsbehörden entsprechende Genehmigungsanträge stellen. Eine Übersicht dazu, in welchen Mitgliedstaaten und Bundesländern dies erforderlich ist, findet sich ebenfalls auf der Homepage der Kommission bei dem angegebenen Link unter „table of national administrative requirements“. Wir erachten derartige Genehmigungen für Datenexporte aus Bayern nicht für erforderlich.

Siehe:
http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

Unternehmensgruppen, die Interesse an BCR haben, sollten sich so frühzeitig wie möglich über BCR informieren. Hierzu ist eine Konsultation der auf der Homepage der EU-Kommission zur Verfügung gestellten Materialien zu BCR, insbesondere der o. g. Arbeitspapiere der Artikel-29-Gruppe, unerlässlich. Auch eine frühe Kontaktaufnahme mit den Aufsichtsbehörden ist sehr empfehlenswert. Auf diese Weise können mögliche Missverständnisse oder Fehlerwartungen an BCR frühzeitig ausgeräumt werden, etwa dazu, ob BCR für die betreffende Unternehmensgruppe angesichts der in Rede stehenden Umgänge mit personenbezogenen Daten überhaupt das passende Instrument sind.

Zu beobachten ist, dass Unternehmensgruppen die Konsequenzen von BCR im Hinblick auf die Haftung für Verstöße gegen die BCR anfänglich bisweilen nicht zutreffend beurteilen. An BCR interessierte Unternehmensgruppen sollten daher gleich zu Beginn ihrer Überlegungen den Anwendungsbereich der BCR intern belastbar - d. h. unter Einbeziehung der Geschäftsleitung - klären. Hierzu sollten der Geschäftsleitung insbesondere die Fragen der Haftung bei Verstoß gegen die BCR erläutert werden. Auf dieser Grundlage sollte die Gruppe dann entscheiden, ob sie bereit ist, die geplanten BCR auf alle Umgänge mit personenbezogenen Daten durch die gruppenangehörigen Gesellschaften weltweit anzuwenden, d. h. unabhängig von der Herkunft der Daten, oder ob insoweit eine Beschränkung auf Daten erfolgen soll, die aus dem EWR stammen. Zwingend ist jedenfalls die Anwendung auf Datenumgänge bei den Gruppenmitgliedern außerhalb des EWR, sofern es sich um personenbezogene Daten handelt, die von Gruppenmitgliedern aus dem EWR dorthin übermittelt worden sind (vgl. WP 155, Nr. 1). Durch frühzeitige Abstimmung der Frage des Anwendungsbereichs mit der Geschäftsleitung, insbesondere unter Darlegung der Haftungsfragen, können - u. U. zeitintensive - Nachbesserungen eines BCR-Entwurfs in diesem Punkt vermieden werden.

Siehe:
Filip Alexander, Binding Corporate Rules (BCR) aus der Sicht einer Datenschutzaufsichtsbehörde, ZD 2/2013, S. 51 ff.

13 Beschäftigtendatenschutz

13.1 Löschung von Bewerberdaten (AGG-Fristen; Vorhalten der Daten über diese Fristen hinaus)

Ein Arbeitgeber hat die Daten von Bewerbern nach sechs Monaten ab Zugang des Ablehnungsschreibens zu löschen. Möchte der Arbeitgeber die Daten über diesen Zeitpunkt hinaus speichern, bedarf es der Einwilligung des Bewerbers.

Ein Beschwerdeführer hatte sich bei einem Unternehmen erfolglos beworben. Nach Abschluss des Bewerbungsverfahrens verlangte er eine Bestätigung über die Löschung der Daten, erhielt diese vom Unternehmen aber nicht.

Personenbezogene Daten, die für eigene Zwecke verarbeitet werden, sind nach § 35 Abs. 2 Nr. 3 BDSG zu löschen, wenn ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Ein Arbeitgeber kann die Bewerberdaten über die tatsächliche Dauer des Bewerbungsverfahrens hinaus benötigen, bis er nicht mehr mit Ansprüchen wegen Diskriminierung nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) oder anderen Ansprüchen rechnen muss.

Nach § 15 Abs. 4 AGG muss ein solcher Anspruch auf Schadensersatz innerhalb einer Frist von zwei Monaten geltend gemacht werden, wenn nicht die Tarifvertragsparteien etwas anderes vereinbart haben. Die Frist beginnt bei einer Bewerbung mit dem Zugang der Ablehnung. Da aber auch noch andere zivilrechtliche Unterlassungs- bzw. Schadensersatzansprüche geltend gemacht werden können (siehe § 15 Abs. 5 AGG), ist es sachgerecht, einen mehrmonatigen „Sicherheitszuschlag“ einzuräumen. Wir halten es somit für vertretbar, wenn ein Unternehmen die Bewerberunterlagen bis zu sechs Monate ab Abschluss des Bewerbungsverfahrens noch vorhält.

Ein Anspruch auf eine Bestätigung der Löschung ergibt sich aus § 35 BDSG nicht.

Möchte der Arbeitgeber die Daten über den oben genannten Zeitpunkt hinaus vorhalten, weil er den Bewerber zwar nicht für die ausgeschriebene Stelle berücksichtigt hat, ihn aber dennoch für interessant hält und bei künftig zu besetzenden Stellen in die Auswahl einbeziehen möchte, ist das Einverständnis des Betroffenen erforderlich. Eine „Widerspruchslösung“ halten wir dabei für akzeptabel. Das Unternehmen könnte seine Absicht im Ablehnungsschreiben ansprechen und sollte aus Gründen der Rechtsklarheit ein konkretes Datum nennen, bis zu dem ein Widerspruch erklärt sein müsste.

13.2 Speicherdauer bei Initiativbewerbung

Bei einer Initiativbewerbung darf ein Arbeitgeber die Bewerberdaten grundsätzlich auch nicht länger speichern als in einem Bewerbungsverfahren zu einer ausgeschriebenen Stelle, es sei denn die Beteiligten haben etwas anderes vereinbart.

Ein Beschwerdeführer trug vor, ein Unternehmen, bei dem er sich aktuell beworben hatte, habe ihm erklärt, es gebe Abweichungen zu einer früheren Bewerbung. Das Unternehmen habe die Daten aus der früheren Bewerbung, bei der es sich um eine Initiativbewerbung gehandelt habe, mindestens zwei Jahre vorgehalten. Eine Einwilligung für eine so lange Speicherung habe er dem Unternehmen nicht gegeben.

Nach § 35 Abs. 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Häufig wird die Situation für den Bewerber bei einer Initiativbewerbung nicht anders sein als bei einer Bewerbung auf eine ausgeschriebene Stelle. Der Bewerber wird eine größere Zahl von beiden Arten von Bewerbungen verschickt haben und davon ausgehen, dass sich in überschaubarer Zeit klärt, ob er eine Stelle erhält. Für diese Fälle erscheint es deshalb sachgerecht, eine Speicherfrist von ebenfalls bis zu sechs Monaten, wie bei einer ausgeschriebenen Stelle, anzunehmen. Anders wäre es, wenn der Bewerber erklärt hat, mit einer längeren Speicherung einverstanden zu sein, bis das Unternehmen für ihn eine geeignete Stelle gefunden hat oder das Unternehmen eine solche Absicht dem Bewerber mitteilt und dieser damit einverstanden ist.

Das Unternehmen speicherte die Daten länger als sechs Monate, obwohl der Beschwerdeführer kein Einverständnis erklärt hatte. Wir haben dies als unzulässig bewertet.

13.3 Vorlage sämtlicher Arbeitsverträge an potentiellen Erwerber eines Unternehmens

Einem potentiellen Erwerber eines Unternehmens dürfen Arbeitsverträge der „normalen" Mitarbeiter nur in anonymisierter Form zur Verfügung gestellt werden. Bestimmte Angaben aus Arbeitsverträgen leitender Mitarbeiter, die für den Wert des Unternehmens von Bedeutung sind, dürfen personenbezogen übermittelt werden.

Ein betrieblicher Datenschutzbeauftragter eines Unternehmens fragte an, ob es datenschutzrechtlich zulässig sei, wenn ein potentieller Erwerber sämtliche Arbeitsverträge vorgelegt bekommen möchte, um sich einen Überblick über die Verhältnisse im Unternehmen verschaffen zu können.

Rechtsgrundlage dürfte wohl nicht § 32 Abs. 1 Satz 1 BDSG sein, da die Datenübermittlungen nicht unmittelbar die Durchführung der Beschäftigungsverhältnisse zwischen derzeitigem Arbeitgeber und seinen Mitarbeitern betreffen, sondern § 28 Abs.1 Satz 1 Nr. 2 BDSG. Danach ist eine Datenübermittlung für eigene Zwecke zulässig, wenn sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass die schutzwürdigen Interessen der Betroffenen überwiegen.

Ein berechtigtes Interesse des derzeitigen Arbeitgebers ist anzunehmen, wenn ohne die Weitergabe der Daten ein Verkauf nicht verwirklicht werden könnte. Es kommt also darauf an, inwieweit der Interessent ein gewichtiges Interesse an bestimmten Daten hat. Bei „normalen" Mitarbeitern kann ein solches gewichtiges Interesse nicht angenommen werden, so dass insoweit nur eine Übermittlung in anonymisierter Form in Betracht kommen kann. Anders dürfte es sich bei Personal aus der Leitungsebene verhalten. Eine Übermittlung von Daten, die für den Wert des Unternehmens von Bedeutung sind, also insbesondere Angaben zu Gehältern, Pensionsverpflichtungen, Kündigungsmodalitäten, Qualifikationen von Personal aus der Leitungsebene ist in personenbezogener Form vertretbar (so auch Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl. Rn. 1226ff). Eine Vorlage der gesamten Arbeitsverträge ginge zu weit, da diese noch weitere Angaben enthalten, die ein potentieller Erwerber zu diesem Zeitpunkt nicht zu wissen braucht, so dass hier das schutzwürdige Interesse des betroffenen Personenkreises überwiegt.

13.4 Archivierung von E-Mails bei erlaubter Privatnutzung - Besonderheiten bzgl. E-Mails an Betriebsrat, Datenschutzbeauftragten und Betriebsarzt

Wenn in einem Unternehmen die private E-Mail-Nutzung erlaubt wird, muss für eine Archivierung der E-Mails, soweit keine Trennung in dienstliche und private Mails möglich ist, eine Einwilligung der Mitarbeiter eingeholt werden. Die Archivierung von E-Mails, die an den Betriebsarzt, den Betriebsrat oder den Datenschutzbeauftragten gerichtet sind, muss in einer Weise erfolgen, dass sie dem Zugriff des Arbeitgebers entzogen bleiben.

In einem Unternehmen ist die private E-Mail-nutzung unter der Bedingung erlaubt, dass die Mitarbeiter mit stichprobenartigen Kontrollen des Arbeitgebers einverstanden sind. Der Fragesteller möchte nun wissen, ob auch bezüglich der Archivierung der E-Mails eine Einwilligung erforderlich ist und wie es um den Datenschutz der Absender von privaten E-Mails an einen dienstlichen Account bestellt ist.

Wir teilten mit, dass die gesetzlichen Aufbewahrungsvorschriften des Handelsgesetzbuches und der Abgabenordnung nur für dienstliche E-Mails gelten. Da der Übermittlungsvorgang in diesem Zeitpunkt jedenfalls abgeschlossen ist, gilt nicht mehr das Fernmelde-, sondern das Datenschutzrecht. Soweit keine Trennung von dienstlichen und privaten E-Mails möglich ist (dies wäre bei Einrichtung von zwei getrennten E-Mail-Adressen der Fall), muss auch für die Archivierung von E-Mails bei erlaubter Privatnutzung wegen der hohen Schutzwürdigkeit der Mitarbeiterinteressen eine Einwilligung eingeholt werden.

Bei Archivierung auch privater E-Mails ist gegenüber den Absendern nichts veranlasst. Einen besonderen Schutz der Absender privater E-Mails sehen wir nicht. Wenn jemand eine private E-Mail an einen dienstlichen E-Mail Account versendet, muss er sich darüber im Klaren sein, dass möglicherweise auch andere Personen als der Adressat die Mail lesen und dass solche Mails auch archiviert

werden könnten. Der gleiche Standard an Privatheit wie bei Versendung an eine private E-Mail Adresse kann in einem solchen Fall nicht erwartet werden.

Die E-Mails, die an den Betriebsrat, den Betriebsarzt oder den betrieblichen Datenschutzbeauftragten gerichtet sind, müssen dem Zugriff des Arbeitgebers entzogen bleiben, weil nur so diese Stellen die Vertraulichkeit wahren können, zu der sie verpflichtet sind. Dies muss konsequenterweise nicht nur für den Kommunikationsvorgang, sondern auch für die Archivierung von E-Mails gelten. Es sind also Lösungen zu suchen, die dies berücksichtigen. Dies kann z. B. eine Archivierung in verschlüsselter Form oder in der Weise sein, dass z. B. nur Betriebsrat, Betriebsarzt, Datenschutzbeauftragter zugreifen können und nicht der Arbeitgeber.

13.5 Herausgabe von Daten über runde Geburtstage und Jubiläen an Betriebsrat

Wenn der Betriebsrat eines Unternehmens die Herausgabe von Mitarbeiterdaten über runde Geburtstage, Jubiläen usw. von der Personalabteilung begehrt, ist dies nur zulässig, wenn die Mitarbeiter über diese beabsichtigte Herausgabe informiert werden und ihnen eine Widerspruchsfrist eingeräumt wird.

Die Personalabteilung eines Unternehmens möchte an den Betriebsrat die Daten von Mitarbeitern über runde Geburtstage, Jubiläen (10, 15, 25 und 50 Jahre Betriebszugehörigkeit), Tag der Eheschließung und Geburt eines Kindes zum Zweck der Gratulation und Übergabe eines Geschenks herausgeben. Wir wurden gefragt, ob bzw. unter welchen Voraussetzungen dies möglich sei.

Die Herausgabe der Daten ist eine Nutzung, weil der Betriebsrat nicht Dritter ist, sondern Bestandteil des Unternehmens. Auf gesetzlicher Rechtsgrundlage dürfte die Weiterleitung wohl nicht möglich sein. Das Interesse des Betriebsrats kann als nicht besonders gewichtig angesehen werden, während andererseits entgegenstehende Interessen einzelner Beschäftigter nicht auszuschließen sind (vor allem bei weiblichen Beschäftigten kann es häufiger Vorbehalte gegen die Preisgabe der Altersangabe geben; die Altersangabe lässt ferner u. U. Rückschlüsse darauf zu, wie schnell oder langsam jemand befördert wurde). Für erforderlich, aber auch ausreichend halten wir es, dass die Mitarbeiter über die Weitergabe der entsprechenden Daten informiert werden und ihnen ausdrücklich eine bestimmte Frist eingeräumt wird, innerhalb der sie der Weitergabe widersprechen können („Widerspruchslösung“, so auch Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl. Rn. 940ff).

13.6 Abgleich von Mitarbeiterlisten mit EU-Terrorlisten (allgemein, nicht AEO)

Abgleiche von Mitarbeiterlisten mit den sogenannten „Terrorlisten“ (Mitarbeiterscreening) sind datenschutzrechtlich vertretbar, wenn die Grundsätze der Transparenz und der Verhältnismäßigkeit eingehalten werden.

Nach den EG-Verordnungen Nr. 2580/2001 und Nr. 881/2002 dürfen juristische Personen den im Anhang zu den Verordnungen jeweils aufgeführten Personen, Gruppen oder Organisationen - es handelt sich um Terrororganisationen und -verdächtige - keine Gelder oder wirtschaftliche Ressourcen zur Verfügung stellen. Die Verordnungen gelten in jedem Mitgliedsstaat unmittelbar. Verstöße dagegen, auch fahrlässige, stellen eine strafbare Handlung nach § 34 Außenwirtschaftsgesetz (AWG) dar. Das bedeutet, dass Unternehmen keine der gelisteten Personen als Mitarbeiter beschäftigen dürfen, weil sie durch die Lohnzahlung gegen das oben dargestellte Verbot verstoßen würden. Ihrer Verpflichtung können die Unternehmen durch Abgleiche ihrer Mitarbeiterliste mit den Listen im Anhang der EG-Verordnungen nachkommen.

Datenschutzrechtlich sind diese Abgleiche zulässig, wenn sie von einer gesetzlichen Rechtsgrundlage oder einer Einwilligung gedeckt sind. Eine Einwilligung der Mitarbeiter dürfte mangels Freiwilligkeit (wegen des sozialen Abhängigkeitsverhältnisses) als Grundlage ausscheiden. Da die Verordnungen selbst nur die abstrakte Verpflichtung, keine Leistungen zu gewähren, aber keine Befugnisnorm für eine konkrete Maßnahme zur Umsetzung der Verpflichtung enthalten, ist insoweit auf die Regelungen des BDSG zurückzugreifen. In Betracht kommt § 28 Abs. 1 Nr. 2 BDSG. Danach ist eine Datennutzung oder -verarbeitung zulässig, wenn sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen am Ausschluss der Nutzung über-

wiegen. Nach Auffassung des Bundesfinanzhofes ist § 32 Abs. 1 Satz 1 BDSG die zutreffende Rechtsgrundlage (Urteil vom 19.06.2012, VII R 43/11). Danach ist die Datennutzung oder -verarbeitung durch den Arbeitgeber zulässig, wenn sie für die Durchführung des Beschäftigungsverhältnisses erforderlich ist.

Das überwiegende berechtigte Interesse des Arbeitgebers bzw. die Erforderlichkeit für die Durchführung des Beschäftigungsverhältnisses ist in der Verpflichtung des Unternehmens aus der EG-Verordnung bzw. in dem Bemühen, eine Bestrafung nach § 34 AWG wegen einer unzulässigen Gehaltsüberweisung zu verhindern, zu sehen. Im Hinblick darauf, dass das Persönlichkeitsrecht der Mitarbeiter durch den Abgleich betroffen ist, müssen allerdings gewisse Maßgaben erfüllt werden:

So sind die Mitarbeiter über die Abgleiche zu informieren. Der betriebliche Datenschutzbeauftragte ist in die Maßnahme einzubinden, ebenso der Betriebsrat, soweit dies nach dem Betriebsverfassungsgesetz vorgesehen ist. Der Grundsatz der Verhältnismäßigkeit ist zu beachten, d. h. die Abgleiche dürfen nicht in zu kurzen Abständen durchgeführt werden. Wir halten bei Mitarbeitern grundsätzlich einen Abgleich einmal pro Jahr für ausreichend. Schließlich ist es wichtig, dass im Falle eines Treffers sehr sorgfältig vorgegangen und geklärt wird, ob es sich zweifelsfrei um eine auf der Liste befindliche Person handelt oder um einen Fall zufälliger Namensgleichheit. Dazu ist dem Betroffenen Gelegenheit zu eigenen Darlegungen zu geben.

13.7 Bild auf Betriebs- oder Werksausweis

Das Versehen eines Werksausweises mit einem Bild des jeweiligen Mitarbeiters kann für die Durchführung des Beschäftigungsverhältnisses erforderlich sein, so dass es keiner Einwilligung des Mitarbeiters bedarf.

Ein Unternehmen möchte einen Werksausweis einführen, der Vor- und Zunamen sowie ein Bild des jeweiligen Mitarbeiters enthalten soll. Zweck des Ausweises ist, dass die Mitarbeiter von Handwerkern oder Gästen unterschieden werden können und für Kunden identifizierbar sind. Das Unternehmen hat angefragt, ob hinsichtlich des Bildes eine Einwilligung der Mitarbeiter erforderlich ist.

Eine Einwilligung der Mitarbeiter wäre nach dem Kunsturhebergesetz erforderlich, wenn die Bilder verbreitet oder öffentlich zur Schau gestellt werden würden. Das ist hier aber nicht der Fall. Der Ausweis und damit auch das Bild werden vom Mitarbeiter nur einem sehr begrenzten Personenkreis gezeigt, dem gegenüber er sich als Mitarbeiter des Unternehmens zu erkennen geben möchte.

Die Zulässigkeit auch der Verwendung des Bildes richtet sich somit nach dem Bundesdatenschutzgesetz. Die Verwendung des Bildes ist für die Durchführung des Beschäftigungsverhältnisses erforderlich, weil nur so der aus Sicht des Arbeitgebers nachvollziehbare und sachlich berechtigte Zweck (Identifizierung) verwirklicht werden kann.

13.8 Zugriff des Arbeitgebers auf E-Mail-Account verdächtiger Mitarbeiter

Ein Arbeitgeber ist berechtigt, bei einem begründeten Verdacht eines schwerwiegenden Verstoßes auch auf die Inhalte der an den verdächtigen Mitarbeiter gerichteten dienstlichen E-Mails zuzugreifen. Bei solchen Zugriffen des Arbeitgebers in Abwesenheit des betroffenen Mitarbeiters sollten aus Beweisgründen mindestens zwei Personen beteiligt sein, von denen - wenn vorhanden - einer der betriebliche Datenschutzbeauftragte sein sollte (Vier-Augen-Prinzip).

In einem Unternehmen, in dem die private E-Mail-Nutzung erlaubt ist, wurde zu einem bestimmten Zeitpunkt festgestellt, dass Dateien, die auf Unternehmenssystemen gespeichert waren und Geschäfts- und Betriebsgeheimnisse enthielten, nicht mehr auffindbar waren. Es ergaben sich Verdachtsmomente, dass ehemalige Mitarbeiter noch vor ihrem Ausscheiden diese an andere Unternehmen weitergeleitet und von den Unternehmenssystemen gelöscht hatten. Darauf erhielt ein IT-Mitarbeiter den Auftrag, die verloren gegangenen Dateien, soweit als möglich, wieder herzustellen.

Nach Mitteilung des Unternehmens habe der IT-Mitarbeiter bei Zugriffen auf Fileserver festgestellt, dass die entsprechenden Dateien gelöscht worden seien. Er habe dann versucht, in den dienstlichen E-Mail-Accounts der ausgeschiedenen Mitarbeiter anhand von ausgewählten Suchbegriffen, die den konkret laufenden Projekten zuzuordnen waren,

die Dateien aufzufinden. Die Suchbegriffe seien so ausgesucht worden, dass sie nicht mit privaten Inhalten verwechselt werden konnten. Sofern am Betreff oder an Hand anderer Merkmale erkennbar gewesen sei, dass es sich um private Inhalte handeln könnte, habe der IT-Mitarbeiter darauf nicht zugegriffen. Im Zuge dieser Maßnahme habe sich dann bestätigt, dass die ausgeschiedenen Mitarbeiter die E-Mails mit diversen Anhängen an andere Unternehmen, darunter ein Konkurrenzunternehmen, weitergeleitet hatten.

Gegen die Durchsuchung des E-Mail-Accounts wandten sich einige der ausgeschiedenen Mitarbeiter mit einer Eingabe an uns und trugen vor, aus bestimmten Äußerungen der Unternehmensleitung ergebe sich, dass diese auf die Inhalte sämtlicher E-Mails, auch der privaten, zugegriffen habe, was wegen der erlaubten Privatnutzung eine Verletzung des Fernmeldegeheimnisses darstelle.

Nach § 4 Abs. 1 BDSG ist ein Datenumgang nur zulässig, wenn er entweder durch eine gesetzliche Rechtsgrundlage gedeckt ist oder die betroffene Person eingewilligt hat. Nach § 32 Abs. 1 Satz 1 BDSG ist ein Datenumgang des Arbeitgebers mit Mitarbeiterdaten zulässig, wenn es für die Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

Bei der hier vorliegenden Situation, dass verschwundene dienstliche Dateien gesucht wurden, um eine Weiterbearbeitung laufender Projekte zu ermöglichen, lagen wichtige dienstliche Gründe vor. In einem solchen Fall hat der Arbeitgeber das Recht, auch bei erlaubter privater E-Mail-Nutzung auf die Inhalte der dienstlichen E-Mails der betreffenden Mitarbeiter zuzugreifen. Da es sich um E-Mails handelte, bei denen der Übermittlungsvorgang jeweils abgeschlossen war, galt nicht mehr das Fernmelde-, sondern das Datenschutzrecht. Die Zugriffe auf die Inhalte der dienstlichen E-Mails waren bei der gegebenen Sachlage für die Durchführung des Beschäftigungsverhältnisses erforderlich (§ 32 Abs. 1 Satz 1 BDSG).

Seinen Angaben zufolge achtete der Arbeitgeber darauf, dass er auf private Mails nicht zugriff. Er wählte spezielle Suchbegriffe, bei denen davon auszugehen war, dass sie in privaten Mails nicht vorkommen. Diesbezüglich sahen wir es allerdings als problematisch an, dass die Maßnahme nur durch eine Person (IT-Mitarbeiter) durchgeführt wurde, so dass es für den Arbeitgeber schwierig war, nachzuweisen, dass er private Mails unangetastet ließ. Wir halten in solchen Fällen deshalb die Beteiligung des betrieblichen Datenschutzbeauftragten für angezeigt, damit das Vier-Augen-Prinzip gewahrt ist.

Von diesem Aspekt abgesehen hielten wir die Vorgehensweise des Unternehmens für datenschutzrechtlich vertretbar. Derartige Situationen können vermieden werden, wenn im Zuge des Ausscheidens von Mitarbeitern diese aufgefordert werden, bis zum Zeitpunkt des Ausscheidens sämtliche private Mails zu löschen, was wir bei entsprechenden Beratungen grundsätzlich empfehlen.

13.9 Kontrollsoftware auf Arbeitsplatzrechner eines Mitarbeiters

Sind keine ausreichenden technischen und organisatorischen Maßnahmen umgesetzt, so ist der Einsatz einer Spionage-Software zur Mitarbeiterüberwachung nicht zulässig.

Wenn der Verdacht besteht, dass ein Mitarbeiter durch unerlaubte Zugriffe auf das Arbeitszeitprogramm Arbeitszeitbetrug begangen haben könnte, fehlt es an der Erforderlichkeit einer am PC des Mitarbeiters ohne sein Wissen angebrachten Kontrollsoftware, wenn der Arbeitgeber es vorher versäumt hatte, Benutzernamen für jede einzelne Person zu vergeben. In einem solchen Fall wäre nämlich ermittelbar, von welchem Gerät aus die Zugriffe erfolgten. Wenn die Kontrollsoftware bei Zugriff auf das Arbeitszeitprogramm aktiviert wird und dann eine gewisse Zeit läuft und damit auch unter Umständen andere Inhalte, z. B. aus der Betriebsratstätigkeit oder private E-Mails aufnimmt, ist diese Maßnahme unverhältnismäßig.

Eine Eingabe einer Gewerkschaft betraf ein Unternehmen, das eine Gruppenkennung für ein Zeiterfassungssystem nutzte. Diese war allen Mitarbeitern der der IT-Abteilung wie auch externen IT-Dienstleister bekannt. Zu einem bestimmten Tag wurde festgestellt, dass am Vortag bei der Zeiterfassung eines Betriebsratsmitglieds für einen etwa einen Monat zurückliegenden Tag nachträglich mit dieser Gruppenkennung eine Änderung des Arbeitszeitkontos vorgenommen wurde. Daraufhin wurde eine umfassende Überprüfung des Arbeitszeitkontos dieses Betriebsratsmitglieds für den Zeitraum der letzten rund eineinhalb Jahre vorgenommen. Dabei stellten sich - jeweils mit der Gruppenkennung erfolgte - Änderungen am Arbeitszeitkonto dieses Betriebsratsmitglieds von insgesamt über 100 Stunden heraus. Eine Lokalisie-

rung, von welchem Rechner aus die Einträge vorgenommen wurden, war nicht möglich. Deshalb entschloss sich die Unternehmensleitung, auf dem Computer des verdächtigten Betriebsratsmitglieds ohne dessen Wissen eine Kontrollsoftware zu installieren, um damit feststellen zu können, ob bzw. dass von diesem Rechner der Zugriff stattfindet. Das Kontrollprogramm wurde aktiviert, wenn ein Zugriff auf das Arbeitszeitprogramm erfolgte, lief dann fünf Minuten lang, wobei es im Sekundentakt eine Grafik vom aktiven Bildschirmfenster des PCs fertigte, und schaltete sich anschließend wieder ab. Das bedeutete, dass auch E-Mails zur Betriebsratstätigkeit oder private E-Mails - die Privatnutzung war im Unternehmen geduldet - betroffen sein konnten, sobald das Betriebsratsmitglied auf das Arbeitszeitprogramm zugriff. Mit Hilfe der Kontrollsoftware wurde dann festgestellt, dass von dem Rechner des verdächtigten Betriebsratsmitglieds mit der Gruppenkennung der IT-Abteilung eine nachträgliche Änderung seines Arbeitszeitkontos vorgenommen wurde.

Nach § 32 Abs. 1 Satz 2 BDSG dürfen zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende 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 am Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Angesichts der Tatsache, dass mehrere Personen diese Gruppenkennung nutzten, was seitens des Unternehmens einen Verstoß gegen die Datensicherheit darstellt (Zugangskontrolle, Nr. 2 der Anlage zu § 9 BDSG), fehlt es hier bereits deshalb an der Erforderlichkeit der Datenerhebung. Wären persönliche Zugangsdaten vergeben worden, wäre es zu der vorliegenden Situation gar nicht gekommen, weil dann feststellbar gewesen wäre, wer die Änderungen vorgenommen hat. Das Unternehmen hätte also zuallererst die eigenen Mängel der IT-Systeme zum Ausschluss möglicher Manipulationen beseitigen müssen.

Die getroffene Maßnahme ist aber auch unverhältnismäßig, da neben der Aufzeichnung des Arbeitszeitprogramms auch Inhalte anderer Anwendungen durchgeführt wurden, die innerhalb der Aufzeichnungszeit genutzt wurden. Es wäre technisch leicht möglich gewesen, das Kontrollprogramm so zu entwickeln, dass nur die Inhalte des Arbeitszeitprogramms aufgezeichnet werden.

Aus diesem Grund haben wir dem Unternehmen mitgeteilt, dass die getroffene Maßnahme datenschutzrechtlich unzulässig war und haben infolge dessen ein Bußgeldverfahren gegen die verantwortliche Stelle eingeleitet.

13.10 Personenbezug bei Mitarbeiterbefragungen

Mitarbeiterbefragungen über sensible Daten müssen so erfolgen, dass auch unter Berücksichtigung von Zusatzwissen keine Rückschlüsse auf einzelne Personen bei den Auswertungen möglich sind.

Im Themenkomplex von Umfragen erreichten uns im Berichtszeitraum Anfragen sowohl von Unternehmen, die eine Mitarbeiterbefragung bei externen Dienstleistern in Auftrag gaben, als auch von potentiellen Teilnehmern. Gemeinsamer Schwerpunkt war die Frage, ob die jeweilige Mitarbeiterbefragung tatsächlich anonym durchgeführt werden kann oder ob ein Rückschluss auf einzelne Mitarbeiter möglich sei. Inhaltlicher Fokus der Umfragen war das Gesundheits- und Stressbild der Beschäftigten im betrieblichen Umfeld.

In allen Fällen galt es neben der eigentlichen Befragung auszuschließen, dass durch zusätzliches Wissen über die Mitarbeiter das - isoliert betrachtet - anonyme Ergebnis doch zu einer personenbezogenen Auswertung wird. Aus diesem Grund haben wir die uns gemeldeten Fälle individuell untersucht.

Neben der Befragung an sich spielte auch die Art der Auswertung eine wesentliche Rolle. Hierbei kam es zu einer Aggregierung der Rücklaufdaten, d. h. die Ergebnisse der Teilnehmer wurden in Auswertungsgruppen zusammengefasst. Wichtig dabei war es für uns, die Kriterien zur vorgenommenen Gruppierung und die Mindestanzahl der Personen pro Auswertungsgruppe näher zu betrachten. Eine Mindestanzahl von drei Personen pro Gruppe war dabei für uns nicht ausreichend, um einen Rückschluss auf einzelne Teilnehmer auszuschließen.

In den uns bekannten Fällen war die auswertende Stelle zudem stets extern, d. h. nicht die verantwortliche Stelle selbst. Wir haben dabei geprüft, dass der Dienstleister sicherstellt, dass die verant-

wortliche Stelle keinen Zugang zu den Rohdaten der Auswertung erhält.

Besonders interessant wurde die Fragestellung in technischer Hinsicht in einem uns gemeldeten Fall einer Online-Mitarbeiterbefragung. Hierbei kamen neben den Daten, die im Rahmen der Befragung selbst erhoben wurden, weitere Daten ins Spiel, wie z. B. IP-Adresse, Benutzername, Passwort, Browser Fingerprint und Cookies, die einen Personenbezug grundsätzlich ermöglichen können. Da es zu einer Erhebung personenbezogener Daten kam, die online erfolgte, musste auch auf eine verschlüsselte Datenübertragung per SSL geachtet werden. Die Bewertung von Online-Befragungen gestaltet sich daher für uns etwas komplexer.

Festzuhalten bleibt, dass pauschale Antworten über die datenschutzrechtliche Zulässigkeit von Mitarbeiterbefragungen nicht möglich sind, da das Spektrum potentiellen Zusatzwissens über die Befragten fallspezifisch variiert. Bei Online-Befragungen wächst die Gefahr, dass über technische Aspekte eine Identifizierung einzelner Personen und somit der Verlust der Anonymität der Betroffenen ermöglicht wird.

14 Gesundheitswesen und Soziales

14.1 Datenschutz in der Arztpraxis

Ein Schwerpunkt unserer Tätigkeit für sog. anlasslose Prüfungen für das Jahr 2012 war der „Datenschutz in der Arztpraxis". Die Prüfungstätigkeit in diesem Bereich werden wir auch im Jahr 2013 fortsetzen.

Der Grund für diese Prüfungen lag nicht darin, dass viele oder erhebliche Datenschutzverstöße durch Arztpraxen bekannt geworden wären. Allerdings bestehen wegen der besonderen Sensibilität von Patientendaten und dem notwendigen Schutz des Vertrauensverhältnisses zwischen Arzt und Patient erhöhte Anforderungen an einen sorgsamen Umgang mit diesen sensiblen Daten. Vor dem Hintergrund der strafbewehrten ärztlichen Schweigepflicht gewinnt das Thema Datenschutz und Datensicherheit auch für Ärzte und ihre Mitarbeiter eine besondere Bedeutung.

Hinzukommen die Entwicklungen der modernen Informations- und Kommunikationstechnik, die eine zunehmende Vernetzung von Arztpraxen, Krankenhäusern, Apotheken sowie anderen medizinischen Dienstleistern und Patienten ermöglichen. Dies trägt zu einer besseren medizinischen Versorgung der Patienten bei, da den behandelnden Stellen die erforderlichen Informationen zu ihren Patienten zeitnah zur Verfügung stehen und dadurch beispielsweise Doppeluntersuchungen eines Patienten vermieden werden können. Neben den Chancen neuer Informationstechniken sind jedoch auch die mit dem Austausch großer Datenmengen verbundenen erhöhten Risiken für die übertragenen und in den Arztpraxen verarbeiteten Patientendaten zu beachten, z. B. durch unbefugte Zugriffe von außen.

Das Hauptanliegen im Rahmen unserer Prüfungstätigkeit war bzw. ist dabei nicht, Verstöße festzustellen, um Bußgelder zu verhängen. Ziel ist es vielmehr, die einzelne Praxis gegebenenfalls auf Versäumnisse hinzuweisen und sie zu unterstützen, den Umgang mit personenbezogenen Daten zu verbessern. Darüber hinaus wollen wir uns einen Einblick verschaffen, wie es „in der Praxis“ läuft.

Im Rahmen unserer Prüfungen vor Ort in den Praxen haben wir insbesondere festgestellt, dass in vielen Praxen im Eingangs- und Empfangsbereich die Daten anderer Patienten ohne Weiteres zur Kenntnis genommen werden konnten, etwa durch einsehbare Bildschirme, auf dem Empfangstresen abgelegte Patientenunterlagen oder durch im Empfangsbereich wartende Patienten. Diese Missstände können durch einfache organisatorische Maßnahmen, wie etwa die Umpositionierung des Bildschirms, das Aufkleben einer Sichtschutzfolie auf den Bildschirm, das Entfernen von Sitzgelegenheiten in Hörweite des Empfangstresens und/oder das Einrichten einer Diskretionszone abgestellt werden.

Auch kam es vor, dass Daten von Patienten, die zuvor in dem Behandlungszimmer untersucht worden sind, noch für den nachfolgenden Patienten auf Bildschirmen von medizinischen Geräten, wie dem Ultraschallgerät, sichtbar waren.

Ferner haben wir bei unseren Prüfungen festgestellt, dass die Arztpraxen in den meisten Fällen mit Datenträgerentsorgungsunternehmen und IT-Dienstleistern, die die technische Ausstattung der Arztpraxis betreuten, keine Verträge über eine Datenverarbeitung im Auftrag gemäß § 11 BDSG geschlossen hatten. Nach § 11 Abs. 5 BDSG gelten die Regelungen zur Auftragsdatenverarbeitung (§ 11 Abs. 1 bis 4 BDSG) entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Diese Voraussetzungen liegen bereits dann vor, wenn im Rahmen der (Fern-)Wartungstätigkeit personenbezogene Daten zur Kenntnis genommen werden können. Im Rahmen unserer Prüfungen und Informationsveranstaltungen mussten wir die Ärzte allerdings auch auf die unbefriedigende rechtliche Situation hinweisen, dass selbst bei Vorliegen von Verträgen über eine Datenverarbeitung im Auftrag und der Erfüllung der Kontrollpflichten aus § 11 BDSG eine rechtliche Grauzone im Hinblick auf die mögliche Verletzung der ärztlichen Schweigepflicht nach § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) besteht. Denn nach der bisher herrschenden Meinung stellt § 11 BDSG weder eine Befugnis zur Offenbarung von Patientendaten gegenüber dem Dienstleister dar noch gilt ein Auftragsdatenverarbeiter als berufsmäßig tätiger Gehilfe im Sinne von § 203 Abs. 3 Satz 2 StGB.

Im Zuge der Prüfung der technischen und organisatorischen Maßnahmen war zu berücksichtigen, dass es sich bei Gesundheitsdaten um besondere Arten personenbezogener Daten, d. h. um Daten mit einer erhöhten Schutzbedarfsklasse handelt.

Nach den Regelungen in § 9 BDSG i. V. m. der Anlage zu § 9 BDSG ergab sich daraus bei den technischen Maßnahmen ein hohes und im Einzelfall sogar sehr hohes Sicherheitsniveau. Im Alltag der ärztlichen Beschäftigung existieren deshalb immer wieder Spannungsfelder zwischen einerseits schneller und unkomplizierter Patientenversorgung und anderseits ausreichenden Schutzmaßnahmen der sensiblen personenbezogenen Daten.

Bei der Begutachtung des Zutrittsschutzes stellten wir in den Arztpraxen fest, dass die Praxis- und Serverräume meist gut vor unbefugtem Zutritt geschützt waren. In manchen Arztpraxen wurden die Patientendaten jedoch in nicht abgeschlossenen oder überhaupt nicht verschließbaren Schränken im Eingangsbereich unzureichend vor unberechtigter Kenntnisnahme abgeschirmt. Im Rahmen der Untersuchung einzelner Arbeitsplätze wurde ebenso auffällig, dass vermehrt Gruppenkennungen für alle Mitarbeiter anstelle von einzelnen Benutzerkennungen verwendet werden. Dies führt zu einer nicht mehr möglichen personenbezogenen Protokollierung von Änderungen im Patientenmanagementsystem und einer fehlenden Geheimhaltung von Passwörtern. Durchgängige Berechtigungskonzepte, wie sie in anderen Branchen im IT-Bereich existieren, fehlten überwiegend in den Arztpraxen. Unter dem Fokus der Weitergabekontrolle erkannten wir zudem eine teilweise fehlende Verschlüsselung und unzureichende Absicherung von Backup-Medien. So wurden in den konkreten Fällen USB-Datenträger, die zur Datensicherung verwendet wurden, ohne ausreichenden Schutz - zum Teil auch außerhalb der Arztpraxis - aufbewahrt.

Um den Ärzten die notwendigen Informationen für einen sicheren Umgang mit Patientendaten an die Hand zu geben, haben wir im Rahmen von mehreren bayernweiten Informationsveranstaltungen, die wir in Kooperation mit den Ärztlichen Kreis- und Bezirksverbänden angeboten und durchgeführt haben, die rechtlichen und technischen Grundlagen für den Umgang mit Patientendaten im Praxisalltag dargestellt sowie über unsere Prüfungserfahrungen berichtet. Diese Vortragsreihe wird im Jahr 2013 fortgesetzt.

14.2 Datenübermittlung an mit- oder weiterbehandelnde Ärzte

Die Weitergabe von Patientendaten an einen mit- oder weiterbehandelnden Arzt ist, wenn es sich tatsächlich um eine Mit- oder Weiterbehandlung handelt, auch ohne schriftliche Einwilligung des Patienten zulässig.

Im Rahmen unserer Informationsveranstaltungen „Datenschutz in der Arztpraxis“ und durch bei uns eingegangene Anfragen von Ärzten haben wir festgestellt, dass in den Arztpraxen eine große Unsicherheit darüber besteht, unter welchen Voraussetzungen eine Übermittlung von Patientendaten an andere Ärzte zulässig ist. Häufig wurde die Frage aufgeworfen, ob für eine solche Datenübermittlung stets eine schriftliche Einwilligung des Patienten notwendig sei. Entscheidend für die Beantwortung dieser Frage ist, ob die Weitergabe der Patientendaten für die weitere Behandlung erforderlich ist und an einen mit- oder weiterbehandelnden Arzt erfolgt. Im Einzelnen gilt folgendes:

Soweit keine spezialgesetzlichen Vorschriften, insbesondere aus dem Sozialgesetzbuch (SGB) V zur gesetzlichen Krankenversicherung, einschlägig sind, finden auf die Verarbeitung von Patientendaten durch niedergelassene Ärzte die Bestimmungen des Bundesdatenschutzgesetzes Anwendung.

Bei Patientendaten handelt es sich um sog. besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG in der Form von Gesundheitsdaten. Für diese gelten nach § 28 Abs. 6 bis 8 BDSG spezielle Regelungen. Nach § 28 Abs. 7 Satz 1 und 2 BDSG ist das Übermitteln von Gesundheitsdaten zulässig, wenn dies zum Zweck der Behandlung erforderlich ist, die Verarbeitung der Daten durch Personen erfolgt, die der ärztlichen Schweigepflicht oder einer entsprechenden Geheimhaltungspflicht unterliegen und die Datenübermittlung auch nach den geltenden Geheimhaltungspflichten zulässig ist. Die datenschutzrechtliche Vorschrift knüpft somit die Zulässigkeit des Umgangs mit Patientendaten an die ärztliche Schweigepflicht.

Die Regelungen zur ärztlichen Schweigepflicht in § 9 Abs. 4 der Berufsordnung für die Ärzte Bayerns sehen vor, dass für den Fall, dass mehrere Ärzte gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln, diese insoweit

von der Schweigepflicht befreit sind, als das Einverständnis des Patienten vorliegt oder anzunehmen ist. Das Einverständnis des Patienten in die Weitergabe von Informationen liegt vor bzw. kann angenommen werden, wenn bestimmte Behandlungsunterlagen für seine weitere Behandlung durch einen anderen Arzt erforderlich sind, der Patient im Rahmen der Untersuchung hierüber informiert worden ist und einer Weitergabe zugestimmt bzw. in Kenntnis der erfolgenden Datenübermittlung dieser nicht widersprochen hat. Eine schriftliche Einwilligungserklärung ist in diesem Fall nicht erforderlich. Dies gilt unabhängig davon, ob es sich bei dem weiterbehandelnden Arzt um einen Haus- oder Facharzt handelt.

Anders ist der Fall zu beurteilen, wenn der überweisende Arzt nicht der weiterbehandelnde Arzt ist, wenn z. B. der Orthopäde den Patienten an einen Kardiologen überweist und der Kardiologe den Patienten vollständig kuriert. In diesem Fall ist eine Rückinformation an den „bloß“ überweisenden Orthopäden für die weitere Behandlung des Patienten nicht erforderlich, weshalb die Übermittlung, z. B. des Arztbriefes, grundsätzlich der schriftlichen Einwilligung des Patienten nach § 4a Abs. 1 und 3 BDSG bedarf.

Handelt es sich bei dem überweisenden, jedoch nicht weiterbehandelnden Arzt, um den Hausarzt, so ist bei gesetzlich versicherten Patienten für die Übermittlung von Patientendaten des weiterbehandelnden Arztes an den Hausarzt die Spezialvorschrift des § 73 Abs. 1b Satz 2 SGB V einschlägig. Danach darf der weiterbehandelnde Arzt mit schriftlicher Einwilligung des Patienten Gesundheitsdaten an den Hausarzt auch nur zu Dokumentationszwecken übermitteln. Diese Vorschrift soll in erster Linie die Fälle erfassen, in denen ein Hausarzt in der ihm nach dem SGB V zugedachten „Lotsenfunktion“ eine zentrale Patientendokumentation außerhalb eines konkreten Behandlungsverhältnisses führt (vgl. Krauskopf, Soziale Krankenversicherung, § 73 SGB V, Rn. 8).

Soweit Patientendaten im Rahmen eines krankenhausärztlichen Behandlungsverhältnisses an einen mit- oder weiterbehandelnden Arzt übermittelt werden, ist die Spezialvorschrift des Art. 27 Abs. 5 Bayerisches Krankenhausgesetz (BayKrG) einschlägig. Danach ist eine Übermittlung von Patientendaten an Dritte u. a. zulässig im Rahmen des Behandlungsverhältnisses oder wenn die betroffenen Personen eingewilligt haben. Eine Offenbarung von Patientendaten an Vor-, Mit- oder Nachbehandelnde ist zulässig, soweit das Einverständnis des Patienten anzunehmen ist.

Ist die Übermittlung der krankenhausärztlichen Behandlungsdaten für die weitere ambulante Behandlung des Patienten erforderlich, so kann das Einverständnis des Patienten in die Datenübermittlung angenommen werden, wenn er dieser nicht ausdrücklich widerspricht. Eine schriftliche Einwilligungserklärung des Patienten ist nicht notwendig.

Soweit eine Datenübermittlung für die weitere Behandlung des Patienten nicht erforderlich ist, kann das Einverständnis in eine Übermittlung seiner Patientendaten regelmäßig nicht angenommen werden, so dass, wie oben dargestellt, grundsätzlich die schriftliche Einwilligung des Patienten einzuholen ist.

Eine Übermittlung von Patientendaten der Krankenhäuser an vorbehandelnde Notärzte und Verlegungsärzte ist zulässig, wenn diese Daten im Einzelfall zur Evaluation des Erfolgs ihrer Vorbehandlung erforderlich sind. Liegen diese Voraussetzungen vor, darf das behandelnde Krankenhaus ohne Einwilligung des Patienten die hierzu erforderlichen Patientendaten weitergeben (Art. 47 Abs. 3 Satz 1 Bayerisches Rettungsdienstgesetz (BayRDG)).

14.3 Hausarztzentrierte Versorgung

Die im Zuge der Einschreibung und Abrechnung der hausarztzentrierten Versorgung (§ 73 SGB V) in Bayern praktizierten und von uns geprüften Datenumgänge unter Beteiligung von Patient, Hausarzt, Rechenzentrum und Krankenkasse sind datenschutzrechtlich zulässig.

Kern der hausarztzentrierten Versorgung ist die zentrale Koordinierungsfunktion des Hausarztes, der für den gesetzlich versicherten Patienten als „Lotse“ im Gesundheitssystem fungieren soll. Die gesetzlichen Regelungen zur hausarztzentrierten Versorgung finden sich in § 73b Sozialgesetzbuch (SGB) V. Die Teilnahme an dieser besonderen hausärztlichen Versorgungsform ist sowohl für den Versicherten als auch den Leistungserbringer (Hausarzt) freiwillig. Entscheidet sich ein Versicherter für die Teilnahme an dieser Versorgungsform, erklärt er sich verbindlich gegenüber seiner Krankenkasse bereit, einen Facharzt nur auf Überweisung seines Hausarztes aufzusuchen und sich an seinen Hausarzt ein Jahr zu binden, den er innerhalb dieser Zeit nur aus wichtigem Grund wechseln kann (vgl. § 73b Abs. 3 SGB V). Der an der hausarztzentrierten Versorgung teilnehmende Hausarzt

erhält zur Verbesserung der Versorgungsqualität und zur Kostensenkung bestimmte Vorgaben.

Mit den datenschutzrechtlichen Fragen, die im Rahmen der Durchführung von Verträgen zur hausarztzentrierten Versorgung gemäß § 73b Abs. 4 Satz 1 SGB V des Bayerischen Hausärzteverbandes e. V. mit den Krankenkassen aufgetreten sind, waren wir während des Berichtszeitraums sowohl in rechtlicher als auch in technischer Hinsicht intensiv befasst.

14.3.1 Rechtliche Überprüfung

Anfang des Jahres 2011 ging es dabei zunächst um die Frage, wie insbesondere eine datenschutzkonforme Gestaltung der Verträge zur hausarztzentrierten Versorgung hinsichtlich der Abrechnung der ärztlichen Leistungen unter Berücksichtigung der Entscheidung des Oberverwaltungsgericht Schleswig-Holstein vom 12. Januar 2011 (Az.: 4 MB 56/10) möglich ist. In diesem im Rahmen des vorläufigen Rechtsschutzes ergangenen Beschluss kam das Gericht zu dem Ergebnis, dass die in den damaligen Verträgen zur hausarztzentrierten Versorgung vorgesehene Datenverarbeitung im Auftrag der Hausärzte durch die Hausärztliche Vertragsgemeinschaft e. G. (HÄVG) und weitere Dienstleister nicht die gesetzlichen Anforderungen des § 295 Abs. 1b Satz 5 bis 8 SGB V (alte Fassung) im Verbindung mit § 80 SGB X erfüllte.

Die Ende Juni 2011 ausgelaufene Bestimmung des § 295 Abs. 1b Satz 5 bis 8 SGB V wurde durch die Neuregelung des § 295a SGB V ersetzt. Auch bei der Anpassung der Vertragsregelungen an die neue Bestimmung des § 295a SGB V waren wir wiederum umfassend beteiligt.

Mit der Neuregelung des § 295a SGB V schaffte der Gesetzgeber eine bereichsspezifische Befugnisnorm für die Datenübermittlung zu Abrechnungszwecken im Rahmen der Verträge u. a. zur hausarztzentrierten Versorgung nach § 73b SGB V. Nach § 295a Abs. 1 SGB V sind die an Verträgen über eine hausarztzentrierte Versorgung (§ 73b SGB V) teilnehmenden Leistungserbringer (Hausärzte) befugt, die für die Abrechnung der erbrachten Leistungen erforderlichen Angaben an den Vertragspartner auf Leistungserbringerseite (Hausärzteverband) als verantwortliche Stelle zu übermitteln, indem diese Angaben entweder an ihn oder an eine nach Absatz 2 beauftragte andere Stelle (z. B. ein Rechenzentrum) weitergegeben werden. Voraussetzung für diese Datenübermittlung ist, dass der Versicherte vor Abgabe seiner Teilnahmeerklärung an der hausarztzentrierten Versorgung umfassend über die vorgesehene Datenübermittlung informiert worden ist und mit der Einwilligung in die Teilnahme zugleich in die damit verbundene Datenübermittlung schriftlich eingewilligt hat. Die übermittelten Daten dürfen dabei von dem Vertragspartner auf Leistungserbringerseite oder der beauftragten anderen Stelle nur zu Abrechnungszwecken verarbeitet und genutzt werden.

Mit der Regelung in Absatz 2 des § 295a SGB V wurde im Wesentlichen die in § 295 Abs. 1b SGB V enthaltene Regelung, wonach der Vertragspartner auf Leistungserbringerseite eine andere Stelle mit der Erhebung, Verarbeitung und Nutzung der für die Abrechnung der ärztlichen Leistungen erforderlichen personenbezogenen Daten beauftragen darf, übernommen. Dabei enthält § 295a Abs. 2 Satz 2 SGB V die ausdrückliche Einschränkung, dass die Einschaltung von Unterauftragnehmern ausgeschlossen ist. Sinn und Zweck dieser Beschränkung ist es, den Kreis der an der Datenverarbeitung beteiligten Stellen zum Schutz der besonders sensiblen Gesundheitsdaten der Versicherten einzugrenzen (vgl. BtDrs 17/6141, Seite 51).

Auch im Zusammenhang mit dieser neuen Regelung wurden (datenschutzrechtliche) Fragestellungen aufgeworfen. U. a. wurde teilweise als rechtlich unzulässig kritisiert, dass der an der hausarztzentrierten Versorgung teilnehmende Hausarzt an den vertraglich vorgegebenen Abrechnungsweg gebunden sei.

Nach § 73b Abs. 4 Satz 1 SGB V haben Krankenkassen zur flächendeckenden Sicherstellung des Angebots einer hausarztzentrierten Versorgung Verträge mit Gemeinschaften zu schließen, die mindestens die Hälfte der an der hausärztlichen Versorgung teilnehmenden Allgemeinärzte eines Bezirks der Kassenärztlichen Vereinigung vertreten. Kommt ein solcher Vertrag zustande, können Verträge auch mit einzelnen hausärztlichen Leistungserbringern abgeschlossen werden (vgl. § 73b Abs. 4 Satz 3 Nr. 1 SGB V). Die Hausärzte haben demnach die Möglichkeit, entweder dem Vertrag zur hausarztzentrierten Versorgung des Hausärzteverbandes mit der Krankenkasse beizutreten oder einen Einzelvertrag mit der Krankenkasse zu schließen und über § 295 Abs. 1b Satz 1 SGB V direkt mit der Krankenkasse abzurechnen.

Nach § 73b Abs. 5 Satz 1 SGB V ist in den Verträgen nach Absatz 4 das Nähere über den Inhalt und die Durchführung der hausarztzentrierten Versorgung, insbesondere die Ausgestaltung der Anforderun-

gen nach Absatz 2, sowie die Vergütung zu regeln. Aus dieser Regelung ergibt sich zwar nicht, dass der Abrechnungsprozess notwendiger Gegenstand von Verträgen zur hausarztzentrierten Versorgung sein muss, allerdings kann den sozialrechtlichen Regelungen auch kein Verbot der Koppelung der materiellen Regelungen zur hausarztzentrierten Versorgung mit dem Abrechnungsweg entnommen werden.

Entscheidet sich ein Hausarzt, einem Vertrag zur hausarztzentrierten Versorgung des Hausärzteverbandes mit der Krankenkasse beizutreten, so entscheidet er sich zugleich für die vertraglich und auch von § 295a SGB V vorgesehene Abrechnungsform. Dies ist in erster Linie Ausfluss des Grundsatzes der Vertragsfreiheit und keine Frage des Datenschutzrechts.

14.3.2 Technische Überprüfung

Beim Vollzug der Einschreibung zur hausarztzentrierten Versorgung und bei der Abrechnung wird eine Software eingesetzt, die von einzelnen anderen Aufsichtsbehörden insbesondere unter dem Gesichtspunkt mangelnder Transparenz stark kritisiert wurde. Wir hatten dies zum Anlass genommen, das eingesetzte serviceorientierte System zur Abrechnung von Leistungen der beteiligten Hausärzte bis zur Überprüfung des Source-Codes insbesondere unter dem Gesichtspunkt zu untersuchen, inwiefern der Datenverarbeitungsvorgang den notwendigen Anforderungen der Transparenz für den Hausarzt genügt.

Gesundheitsdaten unterliegen einem hohen bis sehr hohem Schutzbedarf. Aus diesem Grund wurden bei dem von uns geprüften System sämtliche Abrechnungsdaten mit einem asymmetrischen Verschlüsselungsverfahren (RSA, 2048-Bit) verschlüsselt. Vor einer Verschlüsselung fand automatisch eine Prüfung der Abrechnungsdaten auf Korrektheit statt. Damit konnte sichergestellt werden, dass nur valide erzeugte Abrechnungsdaten als verschlüsselte Datenlieferung an das Rechenzentrum gesendet wurden.

Asymmetrische Verschlüsselungsverfahren besitzen die Eigenschaft, dass mit dem öffentlichen Schlüssel verschlüsselte Daten nur mit dem dazu passenden privaten Schlüssel wieder entschlüsselt werden können. Das Softwaremodul, das als Webservice über das SOAP-Protokoll von dem Arztinformationssystem (AIS) des Hausarztes angesprochen wird, beinhaltet den zur Verschlüsselung verwendeten öffentlichen Schlüssel. Der private Schlüssel befindet sich im beteiligten Rechenzentrum und wird zur Entschlüsselung der Datenlieferung vor der Verarbeitung eingesetzt. Dies führt zu dem Problem, dass ein Arzt über die graphische Oberfläche seines Arztinformationssystems eine Übermittlung seiner Abrechnungsdaten startet, die verschlüsselte Datenlieferung aber selbst nicht mehr entschlüsseln kann (da dieser den privaten Schlüssel nicht besitzt). Da das Prüfmodul als Webservice keine Benutzeroberfläche besitzt, kann auch der Arzt keinen Einblick in den Datenverarbeitungsvorgang nehmen.

Im Rahmen unserer Prüfung stellte sich die Frage, ob ein solches System, das durchaus den aktuellen Stand der Technik widerspiegelt, überhaupt den datenschutzrechtlichen Anforderungen entsprechen kann. Im konkreten System sind die XML-Schnittstellen der Webservices vollständig dokumentiert und bezüglich der Übergabeparameter eindeutig. Angesprochen werden diese Schnittstellen über das AIS. Das Prinzip der Transparenz ist für uns damit auch bei Verwendung von Softwaremodulen über Webservices erfüllt, da der Arzt sein AIS über die Benutzerschnittstelle bedient und das AIS die vom Arzt ausgewählten Daten nur über eine transparente XML-Schnittstelle an den Webservice übergeben kann.

Eine weitere bedeutende Frage war, ob das Prüfmodul die Abrechnungsdaten vor der Verschlüsselung nicht auch verändern könnte, ohne dass der Arzt dies feststellen kann. Damit wäre es theoretisch möglich, dass andere Abrechnungsdaten an das Rechenzentrum gesendet werden als der Arzt über sein AIS an das Servicemodul übertragen hat. Wir sind der Auffassung, dass Softwaresystemen, bzw. deren Erstellern nicht prinzipiell ein rechtwidriges Verhalten unterstellt werden kann, auch wenn diese Systeme nicht quelloffen (Open-Source) sind und mit Verschlüsselungsverfahren arbeiten. Aufgrund des hohen Schutzbedarfs der Gesundheitsdaten haben wir im konkreten Fall dennoch eine Source-Code-Analyse mit dem Hersteller durchgeführt. Ebenfalls wurden Laufzeituntersuchungen in eigenen Laboraufbauten durchgeführt, um festzustellen, ob durch Speicherung invalider Abrechnungsdaten eine spätere Veränderung der Abrechnungen erfolgt. Wir sind zu dem Ergebnis gekommen, dass keine Manipulationen stattfinden.

Obwohl es allein aus praktischen Gründen nicht möglich ist, sämtliche Softwaresysteme durch Source-Code-Analysen beim Hersteller zu untersuchen, wird dieses Vorgehen von uns in begründeten Einzelfällen auch zukünftig durchgeführt.

14.4 Apothekenrechenzentren

Rezeptdaten dürfen gemäß § 300 Abs. 2 Satz 2 SGB V für andere Zwecke als zur Abrechnung verarbeitet und genutzt werden, wenn sie anonymisiert sind. Ausreichend ist dabei eine faktische Anonymisierung.

Innerhalb des Berichtszeitraums waren wir mit der Frage befasst, in welcher Art und Weise Rezeptdaten von Apothekenrechenzentren an Firmen weitergegeben werden dürfen, die diese Daten insbesondere im Auftrag von Pharmaunternehmen auswerten. Nach § 300 Abs. 2 SGB V dürfen Apotheken zur Erfüllung ihrer Abrechnungsverpflichtungen gegenüber den Krankenkassen Rechenzentren in Anspruch nehmen. Die Rechenzentren dürfen die Daten für im Sozialgesetzbuch bestimmte Zwecke verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind; anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden.

In den bei uns anhängigen Verfahren ging es im Wesentlichen um die Frage, welche konkreten Anforderungen für die Nutzung zu anderen Zwecken an die Anonymisierung der Rezeptdaten zu stellen sind. Prüfungsmaßstab war dabei die gesetzliche Definition in § 3 Abs. 6 BDSG, wonach Anonymisieren das Verändern personenbezogener Daten derart ist, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Das Gesetz geht damit von zwei Möglichkeiten der Anonymisierung aus:

- Bei einer absoluten Anonymisierung werden die Merkmale, die eine Person identifizieren können, aus den Datensätzen entfernt. Dieser Informationsverlust hat zur Folge, dass eine Verknüpfung von Datensätzen über einen bestimmten Zeitraum nicht möglich ist.
- Bei einer faktischen Anonymisierung werden die Merkmale, die eine Person identifizieren können, durch kryptographische Verfahren derart verarbeitet, dass diese mit verhältnismäßigen Mitteln nicht mehr hergestellt werden können. Damit ist ein Rückschluss auf die dahinter stehende natürliche Person ausgeschlossen, eine Verknüpfung der Datensätze über einen gewissen Zeitraum jedoch möglich.

Verfahren zur Gewährleistung einer faktischen Anonymisierung müssen derart ausgestaltet sein, dass die eingesetzten kryptographischen Funktionen bezüglich der Algorithmen und Schlüssellängen sowohl dem aktuellen als auch dem absehbar zukünftigen Stand der Technik entsprechen. Die technischen und organisatorischen Maßnahmen nach § 9 BDSG müssen derart ausgestaltet sein, dass die kryptographischen Schlüssel sicher erzeugt, regelmäßig gewechselt sowie derart sicher verwahrt werden, dass ein Kopieren oder Entwenden der Schlüssel nicht möglich ist. Entsprechendes gilt bei dem Einsatz von asymmetrischen Verschlüsselungsverfahren, wenn sich die Identifikationsmerkmale aus wenigen Ziffern zusammensetzen, um die Möglichkeit einer Brute-Force-Entschlüsselung zu verhindern.

Wenn derart anonymisierte Daten zur zusätzlichen Sicherung über eine unabhängige Stelle (Clearingstelle) laufen, die eine zweite Verschlüsselung der bereits verschlüsselten Identifikationsmerkmale vornimmt, so stufen wir dies als sinnvolle, aber auch notwendige Schutzmaßnahme ein. Auch hier gelten die oben beschriebenen Maßstäbe für die Schlüsselerzeugung, -verwendung und -verwahrung.

Bei den von uns im letzten Jahr geprüften Verfahren sind wir zu dem Ergebnis gekommen, dass die praktizierte Verfahrensweise, abgesehen von geringfügigen Punkten, die bereits behoben wurden, den oben dargestellten Vorgaben entspricht.

14.5 Die Rache eines Sanitätshauses

Die zweckwidrige Übermittlung von Daten einer Kundin durch ein Sanitätshaus, die sowohl das Sanitätshaus als auch einen Arzt auf einer Bewertungsplattform im Internet schlecht bewertet hatte, ist datenschutzrechtlich unzulässig und erfüllt den Tatbestand einer Ordnungswidrigkeit.

Eine Petentin wandte sich an uns, weil sie vermutete, dass Angaben zu ihrer Person von einem Sanitätshaus, bei dem sie Kundin gewesen ist, unberechtigt weitergegeben worden seien. Eine Überprüfung des Vorganges durch uns ergab folgendes:

Auf einer Bewertungsplattform im Internet hatte die Petentin sowohl ein Sanitätshaus als auch einen Arzt bewertet. Der Inhaber des Sanitätshauses konnte aufgrund des von der Petentin verwendeten „Nickname“ und der abgegebenen Bewertung den konkreten Bezug zu ihr als Kundin herstellen. Er kontaktierte sie und forderte sie unter Fristsetzung auf, den negativen Eintrag zu löschen oder zu überschreiben. Nach fruchtlosem Verstreichen der Frist erhielt die Petentin auf ihrem Mobiltelefon einen Anruf von dem Arzt, den sie ebenfalls auf dieser Internetseite bewertet hatte. Dieser teilte ihr mit, dass er per Fax von einem Sanitätshaus über die von ihr abgegebene schlechte Bewertung zu seiner Person informiert worden sei. Das Sanitätshaus hatte dem Arzt neben dem Namen und der Anschrift auch die Nummer des Mobiltelefons der Petentin übermittelt, die diese für mögliche Rückfragen bei dem Sanitätshaus hinterlegt hatte.

Diese ohne gesetzliche Rechtsgrundlage erfolgte vorsätzliche und unbefugte Datenübermittlung haben wir gegenüber dem Inhaber des Sanitätshauses mit einem Bußgeld geahndet.

14.6 Frauenhaus verweigert Auskunft

Eine Auskunftspflicht nach dem Bundesdatenschutzgesetz besteht nicht, wenn die Daten ihrem Wesen nach geheim zu halten sind.

Innerhalb des Berichtszeitraums wandte sich ein Petent an uns, weil er auf sein Auskunftsersuchen gegenüber einem Frauenhaus nach § 34 BDSG keine Auskunft erhalten hatte. Zur Begründung seiner Beschwerde führte er u. a. aus, dass seine Ehefrau während seiner beruflichen Abwesenheit unter Mitnahme des gemeinsamen Kindes heimlich aus der ehelichen Wohnung verschwunden sei. Erst nach längerer persönlicher Recherche habe er - trotz sofortiger Einschaltung der Polizei - erfahren, dass seine Ehefrau in einem Frauenhaus untergetaucht sei. Dies habe ihn überrascht, weil er gegenüber seiner Frau nie gewalttätig geworden sei.

Die sich aus § 34 Abs. 1 BDSG ergebende Auskunftspflicht der verantwortlichen Stelle - hier des Frauenhauses - besteht nicht, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen (§ 34 Abs. 7 BDSG in Verbindung mit § 33 Abs. 2 Nr. 3 BDSG). Für die Bestimmung, ob die Daten ihrem Wesen nach geheim zu halten sind, ist auf die Art der Daten in Bezug auf ihren Verwendungszusammenhang abzustellen (vgl. Bergmann /Möhrle/Herb, BDSG, § 33 Rn. 90).

Zweck von Frauenhäusern ist es insbesondere, misshandelten oder von Misshandlung bedrohten Frauen und deren Kindern vorübergehend Schutz und Unterkunft zu gewähren. Um diesen Schutzzweck erfüllen zu können und um zu verhindern, dass bekannt wird, wo genau sich die schutzsuchende Frau mit dem Kind aufhält, ist es notwendig, Informationen insbesondere gegenüber der Person, die der Grund für das Aufsuchen des Frauenhauses gewesen ist, geheim zu halten.

Unter Berücksichtigung dieser Gesamtumstände kamen wir im Rahmen unserer Überprüfung zu dem Ergebnis, dass das Frauenhaus berechtigterweise eine Auskunft gegenüber dem Petenten verweigert hat.

15 Vereine und Verbände

15.1 Vorstellung des Vereinslebens mit Fotos auf der vereinseigenen Homepage

Bei einer Veröffentlichung von Fotos auf der vereinseigenen Homepage sind die Regelungen des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturheberrechtsgesetz - KUG) zu beachten

Im Berichtszeitraum haben uns zahlreiche mündliche und schriftliche Anfragen, aber auch Beschwerden zum Thema „Fotos im Internetauftritt eines Vereins“ erreicht. Sehr viele Vereine möchten die vereinseigene Homepage aufwerten und lebendiger gestalten, indem sie Fotos aus dem Vereinsleben veröffentlichen. Gedacht wird dabei an Mannschaftsfotos der Fußballmannschaften aller Altersgruppen, „Schnappschüsse“ von Wettkämpfen, Fotos von Ausflügen oder Vereinsfeiern und dergleichen mehr.

Zwar wurden die rechtlichen Rahmenbedingungen für die Veröffentlichung von Fotos von Personen im Internet bereits im letzten Tätigkeitsbericht 2009/2010 dargestellt, doch haben unsere Erfahrungen im Berichtszeitraum gezeigt, dass diese Thematik nicht an Aktualität verloren hat.

Grundsätzlich beurteilt sich die Zulässigkeit der Veröffentlichung von Fotos, auf denen Personen abgebildet sind, nach den Vorschriften des KUG, das als bereichsspezifische Vorschrift den Regelungen des BDSG vorgeht (§ 1 Abs. 3 Satz 1 BDSG).

Einschlägige Rechtsvorschriften sind dort die §§ 22 und 23 KUG, die die „Verbreitung und öffentliche Zur-Schau-Stellung von Bildnissen“ regeln.

Nach § 22 Satz 1 KUG dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Ausnahmen von diesem Grundsatz ergeben sich aus § 23 KUG, wonach „Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben“, auch ohne Einwilligung veröffentlicht werden dürfen (§ 23 Abs. 1 Nr. 3 KUG).
Trifft die Ausnahmeregelung nicht zu, kommt es für die Rechtmäßigkeit der Bildveröffentlichungen im Internet also darauf an, ob die aufgenommenen Personen vorher wirksam eingewilligt haben. Da die Vorschriften des KUG eine besondere Form für die Einwilligung nicht vorsehen, kann diese sowohl ausdrücklich, als auch durch schlüssiges Handeln („konkludent“) erfolgen. Dafür genügt es allerdings nicht, dass sich die Personen „einfach fotografieren lassen“ oder sogar dafür „posieren“. Sie müssen dies vielmehr auch in dem Bewusstsein tun, dass diese Bilder ins Internet gestellt werden. Dasselbe muss auch für diejenigen gelten, die im Einzelfall gar nicht mitbekommen, dass sie fotografiert werden.

Vor dem Hintergrund dieser gesetzlichen Rahmenbedingungen beurteilen wir die folgenden Sachverhalte beispielhaft wie folgt:

- Mannschaftsfotos von Vereinsmannschaften können im Internetauftritt des Vereins nur veröffentlicht werden, sofern die Einwilligung der abgebildeten Personen bzw., sofern die Person nicht selbst einsichtsfähig ist, deren Eltern vorliegt.
- Bilder von öffentlichen Wettkämpfen können nicht ohne weiteres ohne Einwilligung der abgebildeten Personen veröffentlicht werden. Es kommt hier darauf an, was das Bild konkret zeigt: Kann man das Startfoto einer Laufveranstaltung, auf dem zahlreiche Läufer zu sehen sind, wohl zweifellos unter die oben zitierte Ausnahmevorschrift des § 23 Abs. 1 Nr. 3 KUG fassen, ist dies bei einer Einzelaufnahme einer völlig erschöpften Läuferin dagegen nicht der Fall. Im letzteren Fall wäre für eine Veröffentlichung des Fotos die Einwilligung der Läuferin erforderlich.
- Bei „Schnappschüssen“ aus dem Vereinsleben (Feste, Ausflüge usw.) muss den betroffenen Personen nicht nur die Tatsache bewusst sein, dass sie fotografiert werden, sondern auch, dass die geschossenen Fotos auf der Homepage des Vereins veröffentlicht werden sollen.

Mitunter wird es situationsbedingt nicht immer einfach sein, festzustellen, ob nach den Ausnahmeregelungen des § 23 KUG auf eine Einwilligung der abgebildeten Personen bzw. deren Eltern verzichtet werden kann. Im Vereinsinteresse ist zu empfehlen, im Zweifelsfall eine Einwilligung einzuholen oder von einer Veröffentlichung des Fotos im Internet abzusehen.

15.2 Einladung durch einen Verein zur Mitgliederversammlung

Lädt ein Verein zu einer Mitgliederversammlung ein, hat er darauf zu achten, dass es im Rahmen einer beigefügten Tagesordnung nicht zu einer unzulässigen Übermittlung personenbezogener Daten kommt.

Ein Verein hatte seine Mitglieder per Brief zur jährlichen Mitgliederversammlung eingeladen. Dem Einladungsschreiben beigelegen hat dabei die vorgesehene Tagesordnung, auf der sich unter anderem ein Tagesordnungspunkt „Offene Pacht“ mit der namentlichen Nennung desjenigen befunden hat, der sich daraufhin an uns gewandt hat.

Wie sich bei der weiteren Ermittlung des Sachverhalts ergeben hat, wurde die Mitgliederversammlung auch in der örtlichen Tageszeitung öffentlich bekannt gegeben, allerdings ohne in der Tagesordnung den Namen zu nennen. Ob der Aushang der Tagesordnung im Schaukasten des Vereinsheimes mit oder ohne Namensnennung erfolgt ist, konnte nicht mehr aufgeklärt werden.

Aus datenschutzrechtlicher Sicht handelt es sich bei der namentlichen Nennung einer Person auf der an alle Vereinsmitglieder verschickten Tagesordnung zur Mitgliederversammlung unter dem Tagesordnungspunkt „Offene Pacht“ um eine „Übermittlung personenbezogener Daten“.

Nach den Vorschriften des BDSG ist eine solche Übermittlung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG). Nachdem eine Einwilligung des Genannten offensichtlich nicht vorgelegen hat, kommt als mögliche Rechtsgrundlage nach dem BDSG die Vorschrift des § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Danach ist das Übermitteln personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung überwiegt.

Zwar muss die Tagesordnung einer Mitgliederversammlung erkennen lassen, worüber beraten und ggf. ein Beschluss gefasst werden soll, d. h. sie muss die einzelnen Vereinsmitglieder in die Lage versetzen, sich zu informieren und vorzubereiten. Nach unserer Beurteilung war eine Namensnennung im konkret vorliegenden Fall dafür aber nicht erforderlich. Fehlt es aber an der Erforderlichkeit der Übermittlung personenbezogener Daten an Dritte, lässt sich hierfür auch keine datenschutzrechtliche Rechtsgrundlage finden und führt dies zu einer unzulässigen Übermittlung personenbezogener Daten.

16 Wohnungswirtschaft und Mieterdatenschutz

16.1 Übermittlung von Kontaktdaten der Wohnungseigentümer durch die Hausverwaltung an Handwerker zum Zweck der Terminabsprache

Eine Herausgabe der Handynummer und E-Mail-Adresse an Handwerker durch die Hausverwaltung ist nur mit Einwilligung des Wohnungseigentümers zulässig.

Ein Wohnungseigentümer hatte sich an uns gewandt, da die Hausverwaltung seine Festnetz-Telefonnummer, Handynummer und E-Mail-Adresse, die keinem öffentlich zugänglichen Verzeichnis zu entnehmen sind, an Dritte, nämlich Handwerker zur Terminabsprache eines Reparaturauftrags weitergegeben hatte.

Nach den datenschutzrechtlichen Vorschriften ist eine derartige Übermittlung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG).

Da für die angesprochene Übermittlung der Kontaktdaten des Wohnungseigentümers weder dessen Einwilligung vorgelegen hat, noch sich eine Rechtsgrundlage aus anderen Rechtsvorschriften, insbesondere dem Wohnungseigentumsgesetz (WEG), entnehmen lässt, kommen als mögliche Rechtsgrundlagen nach dem BDSG allein die Vorschriften des § 28 Abs. 1 Satz 1 Nrn. 1 und 2 BDSG in Betracht.

Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) oder soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG).

Nach § 27 Abs. 1 Nr. 1 WEG ist der Verwalter u. a. dazu berechtigt und verpflichtet, „die für die ordnungsgemäße Instandhaltung und Instandsetzung des gemeinschaftlichen Eigentums erforderlichen Maßnahmen zu treffen“. Hierunter fällt sicherlich auch eine notwendige Beauftragung von Handwerkern. Eine Übermittlung von Vorname, Familienname und Adresse der einzelnen Eigentümer an beauftragte Handwerker ist dabei nachvollziehbar und kann unseres Erachtens auf die obige Rechtsgrundlage gestützt werden. Anders sehen wir dies in Bezug auf anderweitige Kontaktdaten der Eigentümer (Telefonnummern, E-Mail-Adresse). Eine Erforderlichkeit der Übermittlung dieser personenbezogenen Daten von Seiten der Hausverwaltung an Handwerker sehen wir nicht, da eine Terminabsprache grundsätzlich zwischen Verwalter und Handwerker einerseits und Verwalter und Eigentümer andererseits erfolgen kann.

Zwar mag ein berechtigtes Interesse des Verwalters an einer direkten Kontaktaufnahme zwischen Handwerker und Eigentümer (oder auch Mieter) existieren, da dies die Terminkoordination für ihn einfacher gestaltet, doch erkennen wir hier ein entgegenstehendes schutzwürdiges Interesse betroffener Eigentümer (oder Mieter), insbesondere in den Fällen, in denen Telefonnummern und E-Mail-Adresse keinen öffentlich zugänglichen Quellen entnommen werden können.

Infolgedessen haben wir im vorliegenden Fall einen datenschutzrechtlichen Verstoß erkannt.

16.2 Übermittlung einer Liste mit personenbezogenen Daten von Eigentümern und Mietern eines Wohnobjekts durch die Hausverwaltung an alle Wohnungseigentümer

Die Herausgabe einer Liste aller Wohnungseigentümer und Mieter mit deren Handynummern und dienstlichen Telefonnummern durch die Hausverwaltung an alle Wohnungseigentümer ist ohne entsprechende Einwilligungserklärungen unzulässig.

Durch einen Wohnungseigentümer wurden wir darauf aufmerksam gemacht, dass eine Hausverwaltung zusammen mit dem Beschluss-Protokoll einer Eigentümerversammlung eine Liste mit Name, Adresse, Handy- und dienstlicher Rufnummern

aller Eigentümer und Mieter und diese betreffende personenbezogene Daten an alle Wohnungseigentümer versandt hat.

Die für eine derartige Übermittlung personenbezogener Daten in Frage kommenden datenschutzrechtlichen Regelungen aus § 28 BDSG wurden bereits unter Kapitel 16.1 erläutert.

Bei diesem Sachverhalt haben wir keine Erforderlichkeit dafür gesehen, dass an alle Wohnungseigentümer beispielsweise die Handynummern aller Mieter übermittelt werden. Weder aus einem bestehenden Hausverwaltervertrag lässt sich üblicherweise eine solche Übermittlung personenbezogener Daten herleiten, noch konnten von der Hausverwaltung berechtigte Interessen vorgetragen werden, die dies rechtfertigen könnten und denen nicht zumindest schutzwürdige Interessen der betroffenen Personen entgegenstehen.

Im Ergebnis halten wir eine Übermittlung derartiger Listen durch die Hausverwaltung an die jeweiligen Wohnungseigentümer nur mit der ausdrücklichen Einwilligung aller betroffenen Personen (d. h. auch der betroffenen Mieter) für zulässig. Da im gegebenen Fall keine Einwilligungen vorgelegen haben, ist es zu einer datenschutzrechtlich unzulässigen Übermittlung personenbezogener Daten gekommen.

16.3 „Saldenliste“ als Anlage zur Einladung einer Eigentümerversammlung

Die Versendung einer „Saldenliste“ an alle Wohnungseigentümer ohne ausdrückliche Regelung im Hausverwaltervertrag ist unzulässig.

Eine Hausverwaltung hatte Wohnungseigentümer zur jährlich stattfindenden Eigentümerversammlung eingeladen und dem Einladungsschreiben dabei jeweils die betreffende Einzelabrechnung des vergangenen Jahres mit der Heizkostenabrechnung und den Wirtschaftsplan für das bevorstehende Jahr beigefügt. Darüber hinaus beinhaltete die Einladung die Gesamtabrechnung des vergangenen Jahres und eine „Saldenliste“. Dieser Saldenliste konnten die Hausgeldzahlungen der einzelnen Eigentümer entnommen werden („Sollwerte“ und „Bezahlt“). Damit konnte von jedem einzelnen Wohnungseigentümer nachvollzogen werden, wer aus dem Kreis der anderen Wohnungseigentümer seiner Zahlungsverpflichtung nachkommt und wer nicht.

Im Rahmen eines Beschwerdeverfahrens, das durch einen Wohnungseigentümer angestoßen wurde, der die Versendung einer derartigen Saldenliste befremdlich fand, wurde von der Hausverwaltung als Begründung vorgetragen, dass - gerichtlich geklärt - jeder Eigentümer berechtigt sei, in die Jahresabrechnungen der anderen Eigentümer Einsicht zu nehmen und es keinen Unterschied mache, „ob die Eigentümer im Büro der Hausverwaltung Einsicht in die „fremden“ Abrechnungen nähmen oder ob gleich die Saldenlisten verschickt würden.“

Aus datenschutzrechtlicher Sicht handelt es sich bei der Versendung der „Saldenliste“ um eine „Übermittlung personenbezogener Daten“ in der Form, dass die Daten an den Dritten weitergegeben werden (§ 3 Abs. 4 Satz 2 Nr. 3 a BDSG).

Eine mögliche Rechtsgrundlage hierfür würde in der konkreten Fallgestaltung § 28 Abs. 1 Satz 1 Nr. 2 BDSG darstellen, der eine Übermittlung personenbezogener Daten für zulässig erachtet, 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. Als berechtigtes Interesse der Hausverwaltung kann anerkannt werden, dass diese bestrebt ist, ihren Verpflichtungen aus dem Hausverwaltervertrag nachzukommen. Ebenso scheint unstreitig, dass ein Wohnungseigentümer gegenüber dem Hausverwalter ein Einsichtsrecht in sämtliche Verwaltungsunterlagen geltend machen kann. Dies hat zuletzt der Bundesgerichtshof in einem Urteil vom 11. Februar 2011 bestätigt (Az.: V ZR 66/10). Danach hat ein Wohnungseigentümer nach §§ 675, 666 BGB i.V.m. dem Verwaltervertrag einen Anspruch auf Einsicht in sämtliche Verwaltungsunterlagen, die grundsätzlich in den Geschäftsräumen des Verwalters zu gewähren ist. Von diesem Einsichtsrecht unterscheidet der BGH in seiner Entscheidung einen Anspruch auf Auskunft zu der Jahresabrechnung und zu dem Wirtschaftsplan, der zwar auch seine Grundlage in §§ 675, 666 BGB i.V.m. dem Verwaltervertrag hat. Allerdings handelt es sich dabei nicht um einen individuellen Anspruch des einzelnen Wohnungseigentümers, sondern um einen allen Wohnungseigentümern als unteilbare Leistung zustehenden Anspruch, weshalb der einzelne Wohnungseigentümer die Auskunft grundsätzlich nur in der Wohnungseigentümerversammlung verlangen kann. Machen die

Wohnungseigentümer von ihrem Auskunftsrecht keinen Gebrauch, steht der Auskunftsanspruch allerdings jedem einzelnen Wohnungseigentümer zu. Außerdem besteht ein Individualanspruch des einzelnen Wohnungseigentümers dann, wenn sich das Auskunftsverlangen auf Angelegenheiten bezieht, die ausschließlich ihn betreffen.

Im Ergebnis sehen wir einen grundlegenden Unterschied darin, ob einem Wohnungseigentümer auf Antrag Einsicht in Unterlagen zu gewähren ist oder Unterlagen durch die Hausverwaltung im Vorgriff an alle in Frage kommenden Wohnungseigentümer übermittelt werden. Weder nach dem Gesetz, noch aufgrund der bekannten Rechtsprechung gehört die Versendung von Saldenlisten zu den Pflichten des Hausverwalters. Es fehlt damit an der Erforderlichkeit, den Wohnungseigentümern bereits zu einem Zeitpunkt, zu dem sie einen Auskunftsanspruch noch nicht geltend gemacht haben, die personenbezogenen Daten Dritter zu übermitteln.

Eine andere datenschutzrechtliche Beurteilung ist dann möglich, wenn eine gesonderte vertragliche Regelung im Hausverwaltervertrag die Hausverwaltung zur Versendung von Saldenlisten verpflichtet. Im Laufe des konkreten Beschwerdeverfahrens legte die Hausverwaltung tatsächlich einen Hausverwaltervertrag vor, der unter den von Seiten der Hausverwaltung zu erbringenden Grundleistungen ausdrücklich die Versendung der Saldenliste über den Saldo aus der Jahresrechnung der übrigen Wohnungseigentümer an den einzelnen Wohnungseigentümer vorsieht. Im konkreten Fall war damit die Übersendung der Saldenliste vertraglich vereinbart, so dass dem keine datenschutzrechtlichen Hinderungsgründe entgegenstanden.

17 Videoüberwachung

17.1 Webcam Liveview einer Großbaustelle

Die Übertragung von Live-Bildern von einer Großbaustelle mittels Webcam ins Internet, bei der mit Hilfe von Zusatzwissen eine Identifizierung der Bauarbeiter möglich ist, ist nur zulässig, wenn die Bilder in entsprechend großem zeitlichen Abstand erneuert werden (hier alle vier Stunden eine neue Aufnahme).

Wir wurden auf den Betrieb einer Webcam aufmerksam gemacht, die im Minutenabstand den Baufortschritt auf einer Großbaustelle in das Internet übertrug. Die Kamera wurde von einer Arztpraxis betrieben, die aufgrund der Lage und des Ausblickes aus dem dritten Stock einen Überblick über die Baustelle liefern konnte. Wegen der niedrigen Auflösung der Aufnahmen konnten Person zunächst nicht identifiziert werden. Allerdings konnten Einzelne mit Hintergrundwissen, z. B. wer welche Baumaschine steuert oder welches Fahrzeug fährt (Kranführer, Baggerfahrer, usw.), ein Bewegungsprofil dieser Bauarbeiter erstellen. Somit war ein relativer Personenbezug gegeben und der Sachverhalt nach den Vorschriften des Bundesdatenschutzgesetzes zu beurteilen.

Die datenschutzrechtlichen Voraussetzungen für die Zulässigkeit einer Videoüberwachung von öffentlich zugänglichem Raum ist in § 6b Abs. 1 BDSG geregelt. Nach dieser Bestimmung ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) für private Stellen insbesondere nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Ein berechtigtes Interesse am Betrieb der Webcam kann darin gesehen werden, für den Besuch der Homepage zu werben. Darüber hinaus könnte ein berechtigtes Interesse darin liegen, die Öffentlichkeit aufgrund der Lage und der Aussicht von den Praxisräumen über den Baufortschritt auf der Großbaustelle zu informieren.

Allerdings überwog hier das Interesse der dort beschäftigten Personen, dass ihre Tätigkeit nicht ständig unbemerkt beobachtet werden kann. Der Fokus der Kamera war zwar nicht direkt auf die Personen gerichtet, allerdings wurde das Arbeitsumfeld eines von Dritten bestimmbaren Personenkreises direkt und im Minutentakt über das Internet veröffentlicht. Anders als bei den meisten Webcams, die bestimmte Landschaftsteile oder öffentliche Plätze abbilden, bestand für die auf der Baustelle Beschäftigten nicht die Möglichkeit, den Aufnahmebereich nach einem kurzen Zeitraum wieder zu verlassen. Die Bauarbeiter waren während ihrer Tätigkeit gezwungen, sich ständig im Fokus der Kamera zu bewegen, so dass sie im vorliegenden Fall nicht als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit gem. § 23 Abs. 1 Nr. 2 Kunsturhebergesetz (KUG) gesehen werden konnten. Dieser Gesichtspunkt musste bei der Interessenabwägung nach § 6b Abs. 1 BDSG berücksichtigt werden.

Wir haben die Übertragung der mit der Webcam aufgenommenen Bilder im öffentlich zugänglichen Internet in der bisher durchgeführten Form aus datenschutzrechtlicher Sicht für unzulässig erachtet und den Betreiber aufgefordert, die schutzwürdigen Interessen der Arbeiter stärker zu beachten.

Um das Persönlichkeitsrecht der betroffenen Personen einerseits zu schützen, andererseits das Informationsbedürfnis der Öffentlichkeit an der Bautätigkeit zu befriedigen, haben wir gefordert, die Bilder nur in einem wesentlich längeren Abstand zu „erneuern“. Wir haben deshalb eine Übertragung von Bildern der Großbaustelle in einem Abstand von vier Stunden für angemessen erachtet. Da es sich bei diesen Bildern nur um Einzelbilder ohne Serienfunktion handelt, kann aus datenschutzrechtlicher Sicht kein „Beobachten“ mehr erfolgen. Außerdem ist damit aus Sicht der Betroffenen sichergestellt, dass während eines neunstündigen Arbeitstages maximal drei Aufnahmen übertragen werden.

17.2 Flugdrohnen

Werden von einer an einer Drohne angebrachten Kamera Live-Bilder auf das Handy des Besitzers übertragen, gelten für die Zulässigkeit von Aufnahmen öffentlich zugänglicher Bereiche die gleichen Vorgaben wie beim Einsatz sonstiger mobiler Kameras. Bei Aufnahmen von nicht öffentlich zugänglichen Bereichen sind die Erlaubnisvorschriften des § 6b BDSG nicht anwendbar.

Von verschiedenen Seiten wurden wir um datenschutzrechtliche Bewertung von sog. Flugdrohnen gebeten, da diese mittlerweile auch für Privatpersonen günstig auf dem freien Markt erhältlich sind.

Nach unserer Auffassung greift § 6b BDSG nur, wenn zumindest auch öffentlich zugängliche Bereiche erfasst werden. Wenn sich das Filmen auf kurzzeitige Übersichtsaufnahmen öffentlicher Bereiche beschränkt, halten wir das für vertretbar. Es unterscheidet sich dann von einem Schwenk mit einer mobilen Videokamera oder einem Foto - beides ist datenschutzrechtlich akzeptabel - kaum. Die gezielte Aufnahme von Personen stellt allerdings einen erheblichen Eingriff in deren Persönlichkeitsrecht dar und ist - ohne Einwilligung - unzulässig.

Soweit jemand (ohne gewerblichen Hintergrund) eine Flugdrohne ausschließlich über nicht öffentlich zugängliche Bereiche fliegen und Aufnahmen machen lässt, handelt es sich um eine persönliche Tätigkeit, für die die datenschutzrechtlichen Erlaubnisvorschriften nicht einschlägig sind. Derartige Aufnahmen sind in der Regel unzulässig, weil sie eine strafbare Handlung darstellen (§ 201a StGB - Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen) oder zivilrechtliche Ansprüche wegen Beeinträchtigung des Persönlichkeitsrechts nach sich ziehen können (Unterlassungsanspruch, u. U. Schadensersatzanspruch). Falls der Besitzer der Flugdrohne Bilder des Bewohners veröffentlichen sollte, könnten Ansprüche im Zusammenhang mit einer Verletzung des Rechts am eigenen Bild nach dem Kunsturhebergesetz geltend gemacht werden.

17.3 Videoüberwachung in Gastwirtschaft

Eine Videoüberwachung des Kassen- und Thekenbereiches einer Gastwirtschaft kann unter bestimmten Bedingungen zulässig sein, wenn es bereits im Vorfeld zu massiven Eigentumsstraftaten gekommen ist.

Ein Besucher einer Gastwirtschaft, die sich in einem Bahnhof befindet, teilte uns mit, dass er im Gastraum eine Videokamera entdeckt habe. Er bat uns um datenschutzrechtliche Prüfung der Angelegenheit.

Da der Gastbereich im datenschutzrechtlichen Sinn als öffentlich zugänglicher Raum gilt, sind auch hier die Vorschriften nach § 6b BDSG zu Grunde zu legen. Demnach ist eine Videoüberwachung erlaubt, wenn sie zur Wahrnehmung berechtigter Interessen des Kamerabetreibers erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Gerade in Bereichen, in denen sich Personen zurückziehen, um ungestört kommunizieren, essen, trinken oder sich erholen zu können - wie u. a. in Gasträumen - überwiegt in aller Regel das schutzwürdige Interesse dieser Gäste gegenüber den Interessen des Kamerabetreibers.

Wir hatten deshalb den Inhaber der Gaststätte aufgefordert, uns darzulegen, weshalb er eine Videoüberwachung dort für notwendig erachtet und wie die schutzwürdigen Interessen der Betroffenen berücksichtigt werden. Dabei stellte sich heraus, dass mehrere Kameras zur Überwachung des Lokals eingesetzt wurden.

Im konkreten Fall hatte sich ergeben, dass in dem Lokal über 150 Mitarbeiter beschäftigt und in den letzten Jahren zum Teil bandenmäßig organisierte Unterschlagungen von Kassenbeständen und Waren durch Mitarbeiter erfolgt waren. Gegen 19 Beschuldigte waren Ermittlungs- sowie zahlreiche Strafverfahren anhängig. Die Betreiber der Gaststätte hatten sich deshalb entschlossen, Kameras zur Überwachung der Angestellten an den Schank- und Kassenplätzen zu installieren. Aufgrund der geschilderten Vorfälle haben wir eine Überwachung der genannten Bereiche mittels Videokameras unter folgenden Auflagen für vertretbar angesehen:

Die gefertigten Aufnahmen dürfen nur zum Abgleich etwaiger größerer Inventurdifferenzen durch die Geschäftsleitung ausgewertet werden. Die Mitarbeiter sind entsprechend über die Videoüberwachung zu informieren. Eine Auswertung zur Leistungs- und Verhaltenskontrolle ist unzulässig. Ferner sind die Löschfristen nach § 6b Abs. 5 BDSG zu beachten. Die Kameras sind so auszurichten, dass keine Tische des Gästebereiches erfasst werden.

17.4 Hinweis auf Videoüberwachung

Der Hinweis auf die Videoüberwachung nach § 6b Abs. 2 BDSG muss für die Kunden ohne Schwierigkeiten vor Betreten des Geschäftes erkennbar sein. Ein Monitor, der Bilder der Videokameras zeigt, reicht dazu nicht aus. Dieser darf auch nicht das unbemerkte Beobachten durch Kunden ermöglichen.

Ein Bekleidungsgeschäft hatte fünf Videokameras zur Überwachung des Verkaufsraumes installiert. An der Eingangstüre wurde mit einem Kamerasymbol auf die Überwachung hingewiesen. Dieser Hinweis befindet sich in etwa 2,50 Meter Höhe auf einem Türflügel. Innen im Eingangsbereich ist ein Monitor angebracht, der in kurzen Sequenzen gleichzeitig Bilder aus vier Ladenbereichen zeigt und damit auch auf die im Gebäude eingerichtete Videoüberwachung hinweisen und Ladendieben zur Abschreckung dienen soll.

Gemäß § 6b Abs. 2 BDSG ist der Umstand der Videoüberwachung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Die Kunden sollen dabei vor Betreten des Geschäfts ohne größere Schwierigkeiten erkennen können, dass sie einen videoüberwachten Bereich betreten.

Wir hielten deshalb die Kennzeichnung am Eingang über Augenhöhe für unzureichend, woraufhin das Unternehmen die Hinweise mit den Angaben zur verantwortlichen Stelle jeweils auf die Türflügel in 1,60 Meter Höhe angebracht hat.

Die Anzeige von Aufnahmen aus anderen Bereichen des Ladens auf dem Monitor im Eingangsbereich ist aus datenschutzrechtlicher Sicht bedenklich. Jeder eintretende Kunde kann damit Kunden in anderen Abteilungen unbemerkt beobachten. Wir haben deshalb das Unternehmen aufgefordert, die Einstellungen der Videoanlage dahingehend zu ändern, dass nur noch die Live-Aufnahmen des Eingangsbereiches auf dem Bildschirm gezeigt werden. Dies wurde von der Geschäftsführung umgehend umgesetzt.

17.5 Einsatz von Wildkameras

Aufnahmen von Wildkameras sind in „öffentlich zugänglichen“ Bereichen des Waldes in der Regel unzulässig, weil die schutzwürdigen Interessen der Erholungssuchenden überwiegen.

Insbesondere nachdem von einem großen Discounter sog. Wildkameras, die gesteuert von einem Bewegungsmelder auch in der Dunkelheit relativ gute Bilder machen, zu einem Preis von ca. 100 EUR angeboten wurden, erreichten uns zahlreiche Anfragen von Privatpersonen und der Presse, die sich nach der datenschutzrechtlichen Zulässigkeit des Betriebs dieser Kameras erkundigten. Auch der Bayerische Landtag hat diese Fragestellung in seinem Beschluss vom 25. Oktober 2012 (Drs. 16/1431) aufgegriffen. Wildkameras können jedoch nicht nur zur reinen Wildbeobachtung eingesetzt werden, sondern auch für alle anderen Zwecke.

Bei frei zugänglichen Privat-Waldflächen handelt es sich um öffentlich zugängliche Bereiche, so dass sich die Zulässigkeit einer Videoüberwachung nach § 6b BDSG richtet. Diese ist insbesondere dann zulässig, wenn sie zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen überwiegen.

Jedermann hat nach Art. 141 Abs. 3 Satz 1 der Bayerischen Verfassung das Recht auf Naturgenuss, wozu auch das freie Betretungsrecht des Waldes gehört. Ein Erholungssuchender braucht dann auch nicht damit zu rechnen, dass er im Wald gefilmt wird, so dass seine schutzwürdigen Interessen überwiegen. Im Bereich von Waldwegen dürften Kameras deshalb regelmäßig unzulässig sein. In Bereichen, die wegen des Bewuchses von normalen Spaziergängern nicht betreten werden, kann eine derartige Kamera angebracht werden, wenn es ein plausibles Interesse für eine tatsächliche Wildbeobachtung gibt. Auch dann, wenn eine Kamera z. B. zur Beobachtung einer Dachshöhle so niedrig angebracht ist, dass ein Personenbezug nicht herstellbar ist, d. h. dass allenfalls nur die Beine erfasst werden, halten wir die Nutzung dieser Kamera für zulässig. Sollte dennoch eine Person versehentlich aufgenommen werden, müsste die Aufnahme unverzüglich nach ihrer Entdeckung gelöscht werden.

Im Wege der Abwägung kann man gegebenenfalls eine Zulässigkeit der Videoüberwachung annehmen, wenn nachweislich eine Gefährdung vorliegt und sich der Erfassungsbereich der Kamera auf den unmittelbaren Umgriff des gefährdeten Bereichs beschränkt (Diebstahlgefahr bei Holzstapel; Gefahr des Ansägens eines Hochsitzes).

17.6 Videoüberwachung in Tiefgarage

Eine Videoüberwachung im Einfahrtsbereich sowie im Inneren einer Tiefgarage einer Eigentumswohnanlage ist datenschutzrechtlich zulässig, wenn mehrmals Unbefugte in die Garage gelangt sind und Fahrzeuge aufgebrochen haben. Im Interesse einer möglichst schonenden Vorgehensweise dürfen die Aufzeichnungen nur nach Vorfällen und nur von einem ausgewählten Personenkreis angesehen werden.

Die Hausverwaltung einer großen Eigentumswohnanlage brachte, nachdem ein entsprechender Beschluss der Eigentümerversammlung mit großer Mehrheit gefasst worden war, im Einfahrtsbereich sowie im Inneren der zur Anlage gehörenden Tiefgarage mehrere Videokameras an. Anlass dafür waren einige Fälle von Diebstählen und Sachbeschädigungen an Fahrzeugen. Wohnungseigentümer hatten in der Vergangenheit wiederholt fremde Personen mit Aufbruchswerkzeugen im Bereich der Tiefgarage angetroffen. Diese waren in die Garage geschlüpft, wenn ein Fahrzeug hinein fuhr oder diese verließ, weil das Tor eine gewisse Zeit geöffnet blieb. Die Eigentümergemeinschaft ließ daraufhin eine Kamera im Einfahrtsbereich und drei weitere im Inneren der Tiefgarage zur Überwachung der Einfahrtsrampe, des Notausgangs und der Türen, über die man in die Wohnhäuser gelangt, anbringen. Die Kameras zeichneten auf. Die Aufzeichnungen wurden nach 72 Stunden gelöscht, wenn sich kein Vorfall ereignet hat.

Eine Wohnungseigentümerin, deren Stellplatz von einer Kamera aufgenommen wird, wandte sich bei der Hausverwaltung gegen die Videoüberwachung. Die Hausverwaltung bat uns um datenschutzrechtliche Beurteilung des Sachverhalts.

Da es sich bei der Tiefgarage um einen nicht öffentlich zugänglichen Bereich handelt, ist maßgebliche Rechtsgrundlage § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist ein Datenumgang zulässig, wenn er zur Wahrung berechtigter Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegen. Das berechtigte Interesse der Hausverwaltung bzw. der durch sie vertretenen großen Mehrheit der Wohnungseigentümer am Einsatz der Kameras liegt aufgrund der geschilderten Vorfälle in der Tiefgarage vor. Andererseits ist durch die Kameraaufnahmen das Persönlichkeitsrecht der Betroffenen beeinträchtigt. Bei der Abwägung der widerstreitenden Interessen sind die näheren Umstände des Falles zu berücksichtigen.

Zunächst waren keine geeigneten Alternativen zur Kameraüberwachung erkennbar. Die örtlichen Verhältnisse machten es den aus der Garage herausfahrenden Autofahrern unzumutbar, unmittelbar nach Passieren des Tores solange stehen zu bleiben, bis dieses wieder geschlossen ist, um auf diese Weise ein Eindringen Unbefugter zu unterbinden. Die Autofahrer müssen auf Passanten am Gehweg achten und sich dann zügig in den fließenden Verkehr einfädeln, um nicht ein Hindernis zu bilden und dadurch Gefahrensituationen zu verursachen. Da Unbefugte in erster Linie durch das geöffnete Tor in die Garage gelangten, war gerade diese Kamera für die Wohnungseigentümer besonders wichtig. Ein Wachdienst als Alternative schied aus Kostengründen aus. Angesichts der Tatsache, dass die Aufzeichnungen nur nach Vorfällen und auch nur durch einen eng begrenzten Personenkreis (i. d. R. die Hausverwaltung) angesehen werden, haben auch wir das Interesse an der Überwachung der Zufahrt als überwiegend bewertet.

Auch die Kameras im Inneren der Tiefgarage betrafen markante Bereiche, über die Unbefugte in die Garage gelangen konnten. Die Beeinträchtigungen des Persönlichkeitsrechts halten sich wegen der kurzen Aufenthaltszeit der Betroffenen im Erfassungsbereich der Kameras sowie wegen der strengen Zugriffsregelung (siehe oben) in Grenzen. Bezüglich der Person, die sich beschwerte, war festzustellen, dass ihr Stellplatz zwar erfasst wurde, aber kaum erkennbar war. Wir forderten die Hausverwaltung auf, eine leichte Kameradrehung vorzunehmen, weil er dadurch fast ganz aus dem Aufnahmewinkel herausfallen könnte, ohne dass damit das Sicherheitsinteresse geschmälert wurde. Somit wurde diese Person nur noch beim Zutritt zur Tiefgarage sowie beim An- und Abfahren gefilmt, was sie angesichts des gewichtigen Sicherheitsinteresses hinzunehmen hat.

Auch im nicht öffentlich zugänglichen Raum halten wir einen Hinweis auf die Videoüberwachung für nötig, auch wenn sich diese Verpflichtung nicht unmittelbar aus § 28 BDSG ergibt. Der Hinweis hat aus Transparenzgründen, der auch der Regelung des § 6b Abs. 2 BDSG zugrunde liegt, zu erfolgen, damit sich Betroffene auf die Videoüberwachung einstellen können. Ein entsprechendes Hinweisschild war durch die Hausverwaltung angebracht worden.

Insgesamt gesehen haben wir die Videoüberwachung in diesem Fall datenschutzrechtlich für zulässig erachtet.

17.7 Veröffentlichung von Bild- und Videoaufnahmen von Personen, die einer Straftat verdächtig sind

Die Veröffentlichung von Bild- oder Videoaufnahmen von Personen, die des Ladendiebstahls verdächtig sind, durch betroffene Unternehmen zur Identifizierung der Verdächtigen ist nicht zulässig.

Ein Ladeninhaber hatte Videoaufnahmen und Bilder vermeintlicher Ladendiebe, die durch Überwachungskameras in seinem Ladengeschäft erstellt worden waren, auf der Internet-Seite seines Geschäfts veröffentlicht. Zusätzlich hatte er einige der Bilder in seinem Schaufenster veröffentlicht. In entsprechenden Begleittexten erklärte er, dass es sich hierbei um Ladendiebe handle, und stellte die Frage, ob jemand die abgebildeten Personen kenne. Als uns der Sachverhalt zur Kenntnis gebracht wurde, hatte der Ladeninhaber die Aufnahmen von seiner Homepage und aus seinem Schaufenster bereits entfernt. Seiner Homepage ließ sich jedoch entnehmen, dass er plante, weitere Aufnahmen zu veröffentlichen, sobald er eine technische Möglichkeit gefunden habe, auf den Aufnahmen die Gesichter von Nichtbeteiligten - also von Personen, die aus seiner Sicht nicht des Diebstahls verdächtig waren - unkenntlich zu machen.

Wir haben den Ladeninhaber nachdrücklich darauf hingewiesen, dass derartige Veröffentlichungen rechtswidrig sind, und zwar nicht nur im Hinblick auf die abgebildeten „Unverdächtigen“, sondern auch bezüglich solcher Abgebildeter, die nach seiner Ansicht des Ladendiebstahls verdächtig sind. Zwar dürfen gemäß § 6b Abs. 3 BDSG personenbezogene Daten, die durch Videoüberwachung erhoben wurden, zur Aufklärung von Straftaten verwendet werden. Solche Datenverwendungen sind jedoch den Strafverfolgungsbehörden vorbehalten. Wie bereits in unserem Tätigkeitsbericht 2009/2010 festgehalten, kann daher eine Veröffentlichung von Video- oder Bildaufnahmen zur Identifizierung des Verdächtigen nicht als berechtigtes Interesse einer privaten Stelle anerkannt werden. Der Ladeninhaber hat zugesichert, auf weitere Veröffentlichungen zu verzichten.

18 Informationspflichten bei Datenpannen (§ 42a BDSG, § 15a TMG)

Bei bestimmten Datenschutzverstößen und Datenschutzpannen müssen die verantwortlichen Stellen die Datenschutzaufsichtsbehörden und die betroffenen Personen informieren, wenn schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Personen drohen.

Aus Anlass des Inkrafttretens der Regelungen zu den Informationspflichten bei Datenpannen in § 42a BDSG und § 15a TMG hatten wir im letzten Tätigkeitsbericht die neue Rechtslage dargestellt. Die unrechtmäßige Kenntniserlangung von Daten durch Dritte kann auf einer unrechtmäßigen Übermittlung von Daten beruhen (z. B. Fehlversendungen, illegale Datenweitergaben oder Datenabrufe). Die Daten können aber auch auf sonstige Weise dritten Personen unrechtmäßig zur Kenntnis gelangen, insbesondere beim Verlust von Datenträgern, durch Einbrüche, Diebstähle und Fundunterschlagungen oder beim Hacking von Websites.

Eine vollständige Übersicht über die bei uns gemeldeten Datenpannen ist im Anhang enthalten. Im Folgenden stellen wir einige dieser Datenpannen vor, die entweder wiederholt vorgekommen sind oder aufgrund ihrer Besonderheit eine Veröffentlichung rechtfertigen.

18.1 Hacking-Angriffe

Folgende Hacking-Angriffe haben wir als Datenpannen bewertet (siehe auch Kapitel 19.1):

- Entwendung von Kunden- und Kreditkartendaten: Der Webserver eines Unternehmens wurde gehackt. Die erlangten Kunden- und Kreditkartendaten wurden in ausländischen Hackerforen zum Verkauf angeboten.
- Hacking eines Host-Providers: Bei einem Web-Hoster war es Externen gelungen, über eine offensichtlich schon länger bestehende Sicherheitslücke einen Zugriff auf Datenbanken zu erreichen. Betroffen waren Datensätze von Kunden mit ihren Zugangsdaten einschließlich Passwort sowie deren Kontodaten. Des Weiteren konnte auf internen Schriftverkehr des Host-Providers zugegriffen werden, u. a. auf Auskunftsanfragen von Sicherheitsbehörden bezüglich der Zuordnung von IP-Adressen auf Personen.
- Hacking von IT-System: Ein Unbekannter hackte sich in das IT-System eines Unternehmens ein und erlangte Zugriff auf Kundendaten einschließlich Kreditkartendaten.

18.2 Skimming an Geldautomaten

Fälle von Skimming (engl.: abschöpfen), bei denen illegal Daten am Geldautomaten ausgelesen werden, betrachten wir - im Gegensatz zu manchen Banken - nach wie vor als meldepflichtige Datenpannen nach § 42a BDSG.

Im Berichtszeitraum haben zehn Banken Manipulationen durch Straftäter an Geldausgabeautomaten (Anbringung von Lesegerät und Mini-Kamera) mitgeteilt, die Kartendaten und die PIN von Kunden unbemerkt aufzeichnen und mittels danach erstellter Kartendoubletten Geld von fremden Konten abheben wollten. Die eingetretenen Schäden - meist Geld-Abheben im nord- bzw. südamerikanischen Raum - bewegten sich insgesamt durchwegs im fünfstelligen Bereich; den Kunden ersetzen die Banken bei einer Reklamation jeweils den Schaden.

18.3 Einbrüche, Diebstähle, Erschleichen von Daten

Folgende Straftaten oder strafloses Fehlverhalten haben wir „zusätzlich“ als Datenpannen bewertet:

- Verlust von Datensicherungsmedien durch einen Einbruch: Bei einem Einbruch wurde u. a. ein Tresor entwendet. In dem Tresor wurden auch Sicherungskopien der EDV aufbewahrt (mit Kontoverbindungs- und den sich aus dem Arbeitsverhältnis ergebenen besonderen Arten personenbezogener Daten der Mitarbeiter), wobei die Daten auf den Sicherungsmedien nicht besonders geschützt waren.
- Transportkoffer mit Zahlungsverkehrsbelegen einer Bank abhandengekommen: Ein Kurier hatte bei Beendigung seiner Fahrt den Verlust eines Transportkoffers, der Zahlungsverkehrsbelege einer bestimmten Bankfiliale beinhaltete, festgestellt. Er hatte den Koffer zwar bei der Fi-

liale abgeholt, dann aber wohl versehentlich beim Wegfahren stehen gelassen. Der Koffer konnte nicht mehr aufgefunden werden.

- Gefälschte Überweisung im Briefkasten einer Bank: Aus dem technisch unsicheren Briefkasten einer Bank wurden Überweisungsvordrucke mit langen Zangen herausgefischt und die Zahlungsempfängerdaten in Richtung der Täter abgeändert.
- Erschleichen von Kreditkartendaten über Internetplattform: Der Täter hatte sich bei einer Vermittlungsplattform als Hotel ausgegeben und darüber Buchungsdaten von Hotelgästen, einschließlich Kreditkartendaten, erschlichen. Anschließend meldete er sich bei den Buchenden und bat um Herausgabe des Sicherheitscodes zu der Kreditkarte, was bei einigen Personen auch erfolgreich war. Die fremden Kreditkartendaten wurden für Einkäufe im Internet eingesetzt.

18.4 Fehlerhafte und versehentliche Datenübermittlungen

Folgendes Fehlverhalten haben wir als Datenpannen bewertet:

- Abrufbarkeit von Bank-Depotdaten: Auf die öffentliche Website einer Bank wurde im Rahmen eines Softwaretests versehentlich ein reales Kundendepot (einschließlich Depot-Einzelwerte und Gesamtwert des Depots) gestellt.
- Fehl-Versendung von Gehaltsmitteilungen: Infolge eines Fehlers beim DV-Dienstleister wurden fremde Gehaltsmitteilungen an andere Bedienstete mitgeschickt (mit Konfession, Bankdaten usw.).
- Sammel-E-Mail-Versendung über MS-Patienten: Eine medizinische Fachkraft hatte ihre neue Mail-Adresse in einem offenen Verteiler an alle ihre Kontaktpersonen verschickt, worunter auch - erkennbar - MS-Patienten waren, die von der Fachkraft freiberuflich medizinisch betreut wurden.

19 Technischer Datenschutz

19.1 Hacking

Selbst wenn es trotz aller Sicherheitsmaßnahmen im Bereich der IT-Sicherheit keinen 100%-igen Schutz vor Angriffen gibt, können verantwortliche Stellen mit überschaubarem Aufwand an Zeit und Ressourcen viele Angriffe von vorne herein verhindern.

Wir bekommen regelmäßig Eingaben zu Szenarien, in denen Benutzerkonten wie zum Beispiel E-Mail-Konten von unberechtigten Personen „gekapert" wurden. Aufgefallen ist dies den Betroffenen meist erst dadurch, dass in deren Namen Spam-Mail versandt oder Informationen in Form von Phishing-Angriffen verwendet wurden. Obwohl die Datenschutzaufsicht nicht die zuständige Behörde zur Verfolgung der Hacker ist (dies übernimmt die Polizei auf Basis des sogenannten „Hackerparagraphen" § 202c StGB) überwachen wir die Umsetzung der notwendigen Maßnahmen zur Minimierung der Wahrscheinlichkeit, dass ein Unternehmen Opfer eines Angriffs wird.

Häufig werden viele E-Mail-Konten einem automatisierten Angriff unterzogen. Ziel der Angreifer ist es, irgendwelche E-Mail-Konten zu übernehmen, nicht unbedingt das Konto einer konkreten Person. Dazu werden meist sogenannte Wörterbuchangriffe durchgeführt, die häufig verwendete unsichere Passwörter ausprobieren. Selbst wenn nur ein Konto von zehntausend mit dieser Methode übernommen werden kann, scheint es für die Angreifer eine lohnende Methode zu sein. Der Aufwand an Zeit und Ressourcen ist wegen der Verwendung bestehender Angriffswerkzeuge minimal. Schützen kann sich ein Nutzer vor dieser Art von Angriffen sehr leicht, indem ein komplexes Passwort, das nicht aus einem gängigen Wort besteht, verwendet wird (siehe Kapitel 19.2.). Dies wird leider in der Praxis noch immer nicht zwingend umgesetzt, obwohl viele Diensteanbieter den Benutzer meist bei der Verwendung eines unsicheren Passwortes warnen.

Eine weitere Möglichkeit, an personenbezogene Daten von registrierten Webseitenbesuchern zu kommen, besteht in sogenannten Injection-Angriffen. Bei dieser Angriffsvariante werden Schwachstellen in der Anwendungssoftware ausgenutzt, um an vertrauliche Informationen wie Namen, E-Mail-Adressen oder Kreditkartendaten zu gelangen. Wurde ein Hacking-Angriff erfolgreich durchgeführt, besteht für das betroffene Unternehmen u. U. im Rahmen der sogenannten § 42a Fälle die Verpflichtung, dies bei der zuständigen Aufsichtsbehörde zu melden. Im Rahmen dieser Meldungen werden Angriffe auch von unserer Seiten in Kooperation mit dem betroffenen Unternehmen aufgearbeitet. Zielsetzung von uns ist in diesem Zusammenhang auch, konkrete Beratung zur Verringerung des Risikos zukünftiger Angriffe zu leisten. Dazu bieten wir grundsätzlich, auch ohne erfolgten Hacking-Angriff im Rahmen unsere Beratungen für Unternehmen an, bestehende Sicherheitskonzepte mit in eine Datenschutzbewertung einfließen zu lassen.

Trotz aller Sicherheitsmaßnahmen gibt es im Bereich der IT-Sicherheit keinen 100%-igen Schutz vor Angriffen. Gelangt eine unberechtigte Person durch einen Hacking-Angriff auf die gespeicherten Daten von Nutzern, ist ein Unternehmen evtl. vor einem umfassenden Datenverlust geschützt, wenn zum Beispiel Passwörter durch kryptographische Funktionen zusätzlich geschützt wurden (siehe Kapitel 19.2).

Wir erwarten, dass auch zukünftig Unternehmen Opfer von Hacking-Angriffen und damit personenbezogene Daten von Unbefugten entwendet werden. Auch stellt sich uns die Frage, wie hoch die Dunkelziffer sowohl in Bezug auf nicht erkannte Angriffe als auch in Bezug auf nicht gemeldete Angriffe im Sinne der § 42a Fälle ist. Durch automatisierte, teilweise frei zugängliche Werkzeuge können manche Angriffe auch von technisch wenig versierten Personen durchgeführt werden. Neben Webapplikationen sehen wir mittlerweile auch mobile Endgeräte im Fokus von Angreifern.

19.2 Passwortsicherheit

Durch Verwendung eines geeigneten Passwortes kann man mit einfachen Mitteln ein hohes Maß an Sicherheit gewinnen.

Die sichere Verwendung von Zugangsdaten gehört schon seit den frühen Zeiten des Computereinsatzes zu den grundlegenden Sicherheitsmechanismen. Auf Hardwareebene, im Betriebssystem oder auf Seiten eines Anwendungsprogramms wird ein Benutzer durch seinen Benutzernamen und sein Passwort authentifiziert. Im Rahmen unserer Prüfungstätigkeit oder auch bei Beratungen stellen wir immer wieder fest, dass Unternehmen beim Umgang mit Passwörtern und der damit verbundenen Zuteilung von Berechtigungen locker umgehen.

Zum einen geschieht es, dass Passwörter nicht personen-, sondern gruppenbezogen vergeben und zum Teil an die Ausgestaltung der Passwörter keinerlei Anforderungen gestellt werden.

Während in den früheren Jahren die Zugangskennungen noch lokal am Computer oder Serverterminal abgefragt wurden, hat sich deren Verwendung auf das Internet oder auch auf mobile Endgeräte wie Smartphones ausgedehnt. Ein Passwort soll sicher gewählt werden, wobei die Sicherheit im Kontext des Anwendungsfalles betrachtet werden muss. Die Verwendung einer 4-stelligen Ziffernfolge bei einer Bankkarte ist zumindest noch einsetzbar, da eine Sperrung des Kontos nach drei ungültigen Eingaben erfolgt. Die Verschlüsselung einer PDF-Datei mit einem Passwort, das ebenfalls nur aus Ziffern besteht (fand im Rahmen unserer Prüftätigkeit Anwendung bei der Kommunikation mit einem Land, das kyrillische Zeichensätze verwendet), benötigt je nach Verfahren ein 20-stelliges Passwort. Die im Datenschutz gängige Empfehlung für ein sicheres Passwortes ist, mindestens acht Zeichen zu verwenden - bestehend aus einem Alphabet mit Buchstaben, Ziffern und Sonderzeichen. Ferner sollte jedes Passwort nur für einen zu schützenden Bereich verwendet werden.

Die Bewertung der Passwortkomplexität als Sicherheitsmaßnahme geht von der Annahme aus, dass ein Angreifer viele, mitunter alle Passwortkombinationen an einem System ausprobiert, um das Passwort im Falle eines erfolgreichen Zugangs zum System zu erlangen. Ist es möglich, beliebig viele Passwörter automatisch auszuprobieren (zum Beispiel durch ein Skript), dann misst sich die Sicherheit eines Passworts an der statistischen Dauer eines durchschnittlichen Zeitrahmens, bis das Passwort erraten wird. Besteht das dem Passwort zugrundeliegende Alphabet aus Ziffern und ist das Passwort zum Beispiel 6-stellig, ist die durchschnittliche Anzahl aller Kombinationen (ein sogenannter Brute-Force-Angriff) bis zum Erraten eines Passwortes $10^6/2$, also 500.000 Versuche. Ist ein System so konzipiert, dass zwischen ungültigen Anfragen kurze Zeiträume, zum Beispiel drei Sekunden, erzwungen werden, dann kann eine praktische Realisierung eines solchen Angriffes selbst bei kürzeren Passwörtern mit hoher Wahrscheinlichkeit ausgeschlossen werden. Bei einem 8-stelligen Passwort aus dem kompletten Zeichenraum von Klein- und Großbuchstaben, Ziffern und Sonderzeichen braucht man im Mittel (je nach zulässigen Sonderzeichen) zum Beispiel $62^8/2$, ca. 109 Billionen viele Kombinationen zum Erraten eines Passwortes. Neben dem Ausprobieren aller Kombinationen werden auch sogenannte Wörterbuchangriffe durchgeführt. Diese Technik geht von der Annahme aus, dass sich der durchschnittliche Nutzer keine zufälligen Passwortkombinationen ausdenkt, da diese sich schlecht merken lassen. Stattdessen werden einfach zu merkende Wörter, meist mit einer Ziffer versehen, als Passwort verwendet. Hier liegt es in der Verantwortung der Unternehmen, geeignete Passwortrichtlinien zu erstellen und die Mitarbeiter bzw. Kunden über eine richtige Passwortvergabe zu informieren.

Bei der Prüfung, ob ein Passwort richtig ist, findet ein Vergleich mit einem bereits vorhandenen Passwort statt. Dieses vorhandene Passwort muss in einem System so gespeichert sein, dass Unbefugte nicht an das Passwort gelangen können. Zum Schutz der gespeicherten Passwörter empfehlen wir im Rahmen unserer Beratungen den Einsatz von kryptographischen Verfahren, die sogenannten Hash-Funktionen. Durch Anwendung einer geeigneten Hash-Funktion auf ein Passwort entsteht ein Passwort-Hash. Mit diesem ist es möglich, den berechtigten Zugang zu einem System abprüfen zu können. Ebenso kann selbst bei Kenntnis des Passwort-Hashes nicht auf das ursprüngliche Passwort geschlossen werden, wenn das ursprüngliche Passwort ausreichend komplex ist. Zugang zu den Passwort-Hashes finden Unbefugte in der Praxis meist durch Hacking-Angriffe, besonders durch SQL-Injection-Methoden, indem eine Datenbank über die Webseite des angegriffenen Unternehmens ausgelesen wurde (siehe Kapitel 19.1).

Im Rahmen unserer aufsichtlichen Prüftätigkeit finden wir das ganze Spektrum der Passwortsicherheit vor: Passwortrichtlinien samt Schulungen, erzwungene komplexe Passwörter mit Speicherung des Hash-Wert samt SALT-Wert, sowie die Speicherung von (einfachen) Passwörtern als Klartext. Da eine sichere Passwortvergabe ein sehr wichtiger Baustein der IT-Sicherheit darstellt, fordern wir auf Basis von Nr. 2 der Anlage zu § 9 BDSG (Zugangskontrolle) eine verschlüsselte Speicherung von Passwörtern sowie eine dem Anwendungszweck entsprechend ausreichende Passwortkomplexität.

19.3 Anonymisierung von Sensordaten

Bewegungsdaten dürfen ohne ausdrückliche Einwilligung des Nutzers nur erhoben und verarbeitet werden, wenn eine Rückführungsmöglichkeit auf die natürliche Person ausgeschlossen ist.

Viele drahtlose Geräte senden Signalinformationen aus, die von beliebigen Stellen empfangen und ausgewertet werden können. So sendet zum Beispiel ein Smartphone mit aktiviertem Bluetooth die weltweit eindeutige MAC-Adresse des Netzwerkchips, die von potentiellen Partnergeräten (zum Beispiel einer Freisprecheinrichtung des Pkws) zum Aufbau einer Verbindung verwendet werden, aus. Wir waren im Rahmen unserer Beratungstätigkeit mit der Frage beschäftigt, inwiefern eindeutige Geräteinformationen verwendet werden dürfen, um - ohne ausdrückliche Einwilligung des Nutzers - ein Bewegungsprofil zu erstellen. Auf Basis eines solchen Profils soll zum Beispiel festgestellt werden, wie lange ein bestimmter Pkw (falls ein Insasse ein Bluetooth-Smartphone besitzt oder ein Infotainment-System vorhanden ist) für eine bestimmte Strecke braucht und wo es zu Verzögerungen wie zum Beispiel Verkehrsstaus gekommen ist. Welche Person in diesem Pkw saß oder welches Kennzeichen dieser Pkw hatte, war nicht von Interesse. Das eindeutig identifizierbare Signal wird als Pseudonym angesehen, durch welches zwar der Besitzer nicht unmittelbar erkannt werden kann, eine Zuordnung allerdings dann möglich wäre, wenn sogenanntes Zusatzwissen über das Gerät vorhanden wäre. Dies könnten eine Datenbank mit Kunden eines Fahrzeugs sowie eine Datenbank mit verbauten Infotainment-Geräten samt enthaltenen MAC-Adressen der Signalgeber sein. Obwohl uns eine solche Möglichkeit der Zusammenführung von Einzeldaten im Rahmen unserer Beratungstätigkeit nicht bekannt war, haben wir die Ansicht vertreten, dass eine zusätzliche kryptographische Verarbeitung mit dem Ziel der Datenanonymisierung notwendig ist. Dies begründet sich einerseits aus der Sensibilität der Daten, die sich aus einer möglichen zukünftigen Verknüpfung der Pseudonymdaten ergibt. Zum anderen kann der Zweck der Sensordatenauswertung mit den gleich guten Resultaten anhand anonymisierter Daten erfolgen. Zur Anonymisierung von Sensordaten können Hash-Verfahren verwendet werden, die eine sogenannte Einwegfunktion realisieren. Damit kann sehr einfach aus einer Netzwerkadresse ein Hashwert erzeugt werden. Aus dem Hashwert könnte nur durch Ausprobieren aller Kombinationen die zugrundeliegende MAC-Adresse bestimmt werden. Zur Erhöhung der Sicherheit hielten wir es für erforderlich, zusätzlich einen kryptographischen Schlüssel bei der Berechnung des anonymisierten Sensorwertes zu verwenden. Wir hielten es des Weiteren für erforderlich, den geheimen Schlüssel einmal pro Tag zu wechseln, um das Risiko einer Reidentifikation eines anonymisierten Sensorwertes anhand von Sekundärinformationen zu minimieren als auch eine sichere Schlüsselerzeugung und -speicherung zu gewährleisten.

Durch den Einsatz von Hashfunktionen mit kryptographischen Schlüsseln ist es möglich, Forschungsvorhaben wie zum Beispiel eine Verkehrsflussoptimierung durchzuführen. Verhindert werden kann damit, dass einer Person zuordenbare Bewegungsprofile mit realistischen Mitteln erstellt werden können.

19.4 Smartphone

Datenschutzfreundliche Aspekte im Umgang mit Benutzerdaten werden bei Smartphones meist noch vernachlässigt.

Im Allgemeinen versteht man unter Smartphones Mobiltelefone, die neben der zentralen Einbindung des Internets über deutlich mehr Funktionalitäten und Kommunikationsmöglichkeiten verfügen als herkömmliche Mobiltelefone. Smartphones begleiten mittlerweile einen großen Teil der Bevölkerung permanent im Alltag. Da im Rahmen der Nutzung dieser Geräte auf verschiedenste Weise persönliche Daten erhoben, verarbeitet und genutzt werden, die detaillierte Rückschlüsse auf Gewohnheiten, Verhaltensweisen oder gar Aufenthaltsorte des Nutzers zulassen, wurden wir im Berichtszeitraum von einigen Bürgern mit Anfragen und Beschwerden kontaktiert.

Eine beratende Funktion haben wir meist dann eingenommen, wenn es um Einstellungen im Bereich der Sicherheit und Privatsphäre eines Smartphones ging. Hier halfen wir den Bürgern, durch gezielte Auswahl von Parametern innerhalb des Betriebssystems eines Geräts ungewollte Datenübermittlungen abhängig vom Betriebssystem auf ein Minimum zu reduzieren.

Auch erreichten uns Beschwerden über automatische Datenübermittlungen vom Smartphone des jeweiligen Besitzers, die ohne Zutun der Nutzer an unbekannte Empfänger stattfanden. Hier haben wir versucht, herauszufinden, welche Daten an

welche Stellen übermittelt wurden. In unseren Untersuchungen zeigte sich zudem, dass in einigen Fällen durch Apps und die Betriebssysteme selbst personenbezogene Daten wie Gerätekennungen, Standortdaten bis hin zu Kontakten ohne Unterrichtung der Nutzer an Unternehmen übermittelt wurden. Die Nutzer wurden lediglich beim Herunterladen der App aus einem offiziellen App-Download-Store einmalig auf die Berechtigungen der App hingewiesen. Zu welchem Zweck, in welchem Umfang und zu welchem Zeitpunkt die App persönliche Daten des Nutzers übermittelt, blieb jedoch offen. Eine einmalig durch Download und Installation erteilte Berechtigung für eine App ließ sich in der Regel nicht deaktivieren, ohne die Anwendung vollständig zu löschen.

Es gilt deshalb festzuhalten, dass bei den Anbietern von Smartphones und mobilen Betriebssystemen sowie insbesondere auch bei den App-Entwicklern noch sehr großer Handlungsspielraum bezüglich einer datenschutzfreundlicheren Gestaltung besteht. Aus diesem Grund nimmt dieser Themenbereich für uns künftig eine wichtige Rolle ein (siehe auch Kapitel 19.7)

19.5 Bring your own device (BYOD)

Die Einbindung privater Geräte von Mitarbeitern in die IT-Infrastruktur eines Unternehmens birgt datenschutzrechtliche Herausforderungen.

Bring your own device, kurz BYOD, ist ein in unserem Berichtszeitraum aufgekommener neuer Themenkomplex der IT, der sich mit der Integration von in der Regel privaten mobilen Geräten von Mitarbeitern in das Umfeld eines Unternehmens beschäftigt. Eine tiefgreifende Verbindung des Arbeits- und Privatlebens der Mitarbeiter wird damit ermöglicht, die durch die Vermischung persönlicher Daten mit dienstlichen Interessen aus datenschutzrechtlicher Perspektive mehrere Herausforderungen mit sich bringt.

Uns tangierte die Fragestellung, welche Besonderheiten dabei im Unternehmen zu berücksichtigen sind, mehrfach im Rahmen von Veranstaltungen und teilweise auch bei von uns selbst gehaltenen Vorträgen. Wir haben dabei registriert, dass es eine größere Zahl von Fragestellungen gibt, auf die in der Praxis noch keine datenschutzrechtlich ausreichenden Antworten gefunden oder gar umgesetzt worden sind.

Während beispielsweise der Geräteeigentümer stets der Mitarbeiter bleibt, hat das Unternehmen die Sicherheit der Geschäftsdaten auf dem Gerät zu gewährleisten. Dies muss in der Regel durch eine strikte Datentrennung mittels technischer Maßnahmen auf dem Gerät erfolgen. Ebenso sollte eine kontrollierte Geräteverwaltung, ein sogenanntes Mobile Device Management, umgesetzt werden, weshalb umfangreiche Veränderungen der IT-Infrastruktur des betroffenen Unternehmens meist zwingend notwendig sind. Da die Mitarbeitergeräte sehr verschieden sind (z. B. unterschiedliche Hersteller, abweichende Betriebssysteme, verschiedene Systemversionen), besteht die Schwierigkeit, eine Vielzahl an Ausnahmen administrieren zu müssen, d. h. es existiert kein Standardgerät.

Es gilt zu betonen, dass neben technischen und organisatorischen Anforderungen an eine datenschutzgerechte Einbindung von Mitarbeitergeräte ins Unternehmensnetzwerk auch rechtliche Aspekte beachtet werden müssen. Auch ein nicht zu vernachlässigender Aufwand an Kosten und Zeit macht dieses Thema zu einer strategischen Entscheidung der Geschäftsleitung.

19.6 Einsatz einer Diagnosesoftware beim Betrieb von Smartphones und Tablets

Der von den Medien mit viel Aufmerksamkeit bedachte Einsatz einer Diagnosesoftware durch einen Anbieter von Smartphones und Tablets erwies sich nach intensiver Prüfung als datenschutzrechtlich nicht unzulässig.

Eine amerikanische Firma bietet ein Produkt an, welches Herstellern von mobilen Geräten und Netzbetreibern Diagnosedaten zu den Mobilfunknetzen und den darin eingewählten Geräten liefern kann. Diese Daten können zum Beispiel Informationen über Verbindungsabbrüche wegen mangelnder Netzabdeckung oder die automatische Erkennung eines Kunden bei Anruf einer Servicenummer über dessen Geräte-ID sein.

Bei Verwendung dieses Softwareprodukts in den Betriebssystemen vieler Smartphone-Anbieter kam die Frage auf, ob eine bekanntgewordene Sicherheitslücke in diesem Modul, die Fragmente von SMS-Nachrichten an die Betreiber übermittelte, auch bei Produkten eines Anbieters von Smartphones, dessen Deutschlandniederlassung in unserem Zuständigkeitsbereich liegt, auftrat. Zur Klä-

rung dieses Sachverhalts besuchten wir das Unternehmen, um im Rahmen eines Fachgespräches diese Fragestellungen aufzuarbeiten.

Die Diagnosesoftware stellte eine Middleware dar, die entweder von den Herstellern von Geräten oder Netzbetreibern in die von ihnen hergestellten oder angebotenen Geräte integriert werden müssen. Dabei gibt es vielfältige Konfigurationsmöglichkeiten, was dazu führt, dass sich der Einsatz dieser Software von einem Hersteller oder Netzbetreiber zu einem anderen erheblich unterscheiden kann. Die lauffähige Instanz dieser Software sammelte je nach Konfiguration Daten über das jeweilige Gerät, führt ggf. eine Vorverarbeitung durch und übermittelt die Diagnosedaten an den Empfänger, welcher die Herstellerfirma der Diagnosesoftware, der Gerätehersteller oder der Netzbetreiber sein kann. Unter einem Profil wird die Menge der im jeweiligen Einsatz von der Diagnosesoftware gesammelten Daten verstanden. Ein konkretes Datenfeld (z. B. Signalstärke) wird als Metrik bezeichnet. Dies bedeutet, dass es mehrere Profile mit unterschiedlichen Metriken für einen Anwender der Diagnosesoftware geben kann. Eine komplette Liste der möglichen Metriken, welche die Software sammeln kann, wurde von der Herstellerfirma veröffentlicht.

Die Anbieterfirma setzte die Diagnosesoftware in früheren Versionen ihres Betriebssystems ein, um Diagnosedaten zu erheben und an eigene Server zu übermitteln. Ab einer späteren, jetzt gängigen, Version wird die Diagnosesoftware durch eine von dem Anbieter selbst entwickelte Diagnosesoftware ersetzt. Dabei kam in allen Einsatzszenarien nur ein einziges Profil zum Einsatz. Die Diagnosesoftware übermittelt die Diagnosedaten, welche sich aus dem Hot-Ship-Profil zusammensetzen, einmal im Monat an die Server des Anbieters. Der Zeitpunkt der Übertragung wird zufällig bestimmt. Der Server des Anbieters befindet sich in den USA. Die Diagnosedaten werden nur bei Vorhandensein eines WLAN-Netzes übertragen. Ist dieses über einen längeren Zeitraum nicht verfügbar, werden reduzierte Informationen über das GSM-Netz übertragen, deren Größenordnung sich laut Angaben des Anbieters im Kilobyte Bereich bewegt.

Bei dem Einsatz der Diagnosesoftware wurde eine Technik verwendet, die Identitäten für den Einsatz der Diagnosesoftware zufällig erstellt. Diese Anonymisierungstechnik wurde durch Anforderungen des Anbieters an die Herstellerfirma in das Diagnosesoftware-Produkt aufgenommen. Laut Aussage des Anbieters wurde die Diagnosesoftware-Version, die durch einen Softwarefehler Teile von SMS-Nachrichten aufgezeichnet und übertragen hat, in keiner Geräteversion des Anbieters eingesetzt.

Bei dem Gespräch mit der Anbieterfirma waren Vertreter aus den USA anwesend, die uns einen Einblick in die verwendete Diagnosesoftware und die damit übertragenen Daten ermöglicht hat. Wir haben uns dabei davon überzeugt, dass beim Übertragungsvorgang der Diagnosedaten weder Hardware-Seriennummern, IMEI/ISMI Nummern noch weitere personenbeziehbare Diagnosedaten übertragen wurden. Inhalte wie Tastenbedienungen, HTTP-Aufrufe oder SMS wurden nicht erfasst. Die verwendeten Metriken dienten dem Erfassen der Netzqualität, die zur Verbesserung der Netzabdeckung eingesetzt wird. Keine der erfassten Metriken sind dafür geeignet, ein Gerät oder eine Person zu identifizieren. Die Aufzeichnung von einzelnen Funkzellen wurde laut Aussage des Anbieters in Deutschland niemals durchgeführt.

Anhand der gewonnenen Informationen haben wir keine unzulässige Erhebung oder Verarbeitung personenbezogener Daten festgestellt.

19.7 App-Analyse

Die steigende Verbreitung von Smartphones bringt eine ebenfalls stark ansteigende Verbreitung von Anwendungen auf mobilen Endgeräten (Apps) mit sich, die von Nutzern Einwilligungen zur Berechtigungen erfordern, die nicht auf Anhieb nachvollziehbar sind.

In den Medien wird zunehmend von den Gefahren der Anwendungen auf mobilen Endgeräten, den sogenannten Apps, gewarnt. Diese haben gegebenenfalls die Möglichkeit, die Kontakte auszulesen, den Standort des Benutzers zu erkennen oder zum Beispiel auf weitere persönliche Daten wie Fotos zuzugreifen.

Zur Bewertung der Frage, ob eine App den datenschutzrechtlichen Anforderungen genügt, müssen zuerst Informationen zu dem Verhalten der App ermittelt werden. Dazu gehören Informationen wie die übermittelten Netzwerkdaten, die beteiligten Datenempfänger, die sichere Verschlüsselung oder auch der Einsatz von Methoden zur Reichweitenmessung. Dazu bauen wir im Augenblick ein Prüflabor bei uns auf, um die von uns entwickelten Ideen, die aus dem Bereich der IT-Forensik und aktuellen Forschungsprojekten zu Mobile Security abgeleitet wurden, zu realisieren.

Wir werden damit gezielt Datenschutzprüfungen von Apps bayerischer Anbieter durchführen, was im Jahr 2013 einen Schwerpunkt in unserem technischen Referat ausmachen wird. Diese Vorgehensweise ist eine Fortführung des von uns bereits bei der Webanalyse gegangenen Wegs, durch möglichst computergestützte Verfahren technische Prüfungen mit einem angemessenen Personalaufwand durchzuführen.

20 Bußgeldverfahren

Neben unserer Tätigkeit als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich besitzen wir auch eine Zuständigkeit als Bußgeldbehörde. Für Bußgeldverfahren gelten spezielle gesetzliche Regeln. Daher sind die Tätigkeiten der Aufsichtsbehörde einerseits und der Bußgeldbehörde andererseits streng voneinander zu unterscheiden.

Das Bayerische Landesamt für Datenschutzaufsicht ist nicht nur Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich, sondern daneben gemäß § 11a der Bayerischen Verordnung über Zuständigkeiten im Ordnungswidrigkeitenrecht (ZuVOWiG) auch zuständige Verwaltungsbehörde für die Verfolgung und Ahndung von (datenschutzrechtlichen) Ordnungswidrigkeiten im Sinne von § 43 BDSG und von § 16 Abs. 2 Nrn. 2 bis 5 TMG.

Selbst wenn § 38 Abs. 1 Satz 7 BDSG uns, soweit wir Bußgeldbehörde sind, nicht verpflichtet, einen Tätigkeitsbericht abzugeben, erachten wir es als sinnvoll, auch über unsere Tätigkeit als Bußgeldbehörde zu berichten, um den Lesern ein Gesamtbild unserer Arbeit zu ermöglichen.

Die Tätigkeit einer Bußgeldbehörde unterscheidet sich in mehrerlei Hinsicht von derjenigen der Datenschutzaufsichtsbehörde, da unterschiedliche Verfahrensvorschriften gelten und die Verfahren unterschiedliche Zwecke verfolgen: Während das aufsichtliche Verfahren gemäß § 38 Abs. 1 Sätze 1 und 2 BDSG der Kontrolle der Einhaltung der datenschutzrechtliche Vorschriften dient, ist primärer Zweck des Bußgeldverfahrens die Verfolgung und Ahndung von Rechtsverstößen, was freilich mittelbar ebenfalls der Durchsetzung der Rechtsordnung dient. Im Bußgeldverfahren gelten die spezifischen Verfahrensvorschriften des Ordnungswidrigkeitengesetzes (OWiG). Zusätzlich kommen gemäß § 46 Abs. 1 OWiG in erheblichem Umfang Vorschriften der Strafprozessordnung sinngemäß zur Anwendung, etwa die Vorschriften über die Vernehmung von Zeugen und Sachverständigen (§§ 48 ff. StPO). Das Bußgeldverfahren ist wesentlich stärker formalisiert als das Verfahren der Datenschutzaufsichtsbehörde. So sind im Bußgeldverfahren zahlreiche Maßnahmen, die in Grundrechte eingreifen, nur mit richterlicher Genehmigung zulässig, so etwa die Durchsuchung oder die Beschlagnahme.

Zwischen der Tätigkeit im Rahmen von Bußgeldverfahren und der Tätigkeit der Datenschutzaufsichtsbehörde ist daher stets sorgfältig zu unterscheiden. Jedes Verfahren unterliegt nur den für den jeweiligen Verfahrenstyp geltenden Rechtsvorschriften. „Mischverfahren“ irgendwelcher Art gibt es nicht. Wir unterscheiden deshalb auch bei der Aktenführung streng zwischen Bußgeldverfahren und Verfahren der Datenschutzaufsichtsbehörde.

Vor diesem Hintergrund müssen wir bei Eingaben, die uns erreichen, bereits zu Beginn der Bearbeitung klären, ob die Eingabe als Ordnungswidrigkeitenanzeige verstanden werden muss oder aber als „normale“ Eingabe bzw. Beschwerde bei der Datenschutzaufsichtsbehörde. Von einer Ordnungswidrigkeitenanzeige gehen wir grundsätzlich (nur) dann aus, wenn es dem Eingabeführer ersichtlich gerade auf die Verfolgung und Ahndung eines von ihm behaupteten oder für möglich gehaltenen Verstoßes ankommt.

Die Entscheidung, ob ein Bußgeldverfahren eingeleitet wird, wird nicht immer durch uns selbst getroffen, sondern bisweilen bereits durch die Polizei: Sofern die Polizei aufgrund eines ihr bekannt gewordenen Sachverhalts, z. B. einer Anzeige, Ermittlungshandlungen wegen Verdachts einer Ordnungswidrigkeit vornimmt, etwa indem sie den (im bußgeldrechtlichen Sinne) Betroffenen - d. h. den aus ihrer Sicht einer Ordnungswidrigkeit Verdächtigen - anhört und/oder einen Zeugen vernimmt, leitet sie dadurch bereits selbst ein Bußgeldverfahren ein. Gibt die Polizei die Akte anschließend an uns ab, ist ein „stillschweigender Übergang“ in das datenschutzaufsichtliche Verfahren nicht möglich. Vielmehr haben wir hier als Bußgeldbehörde zunächst über den weiteren Fortgang des Bußgeldverfahrens zu entscheiden. Dabei sind folgende Handlungsmöglichkeiten denkbar:

- Soweit die Sache noch nicht entscheidungsreif ist: Vornahme weiterer Ermittlungen im Bußgeldverfahren (u. a. etwa: Anhörung des Betroffenen)
- Soweit die Sache entscheidungsreif ist: Verfahrensabschluss durch Einstellung des Bußgeldverfahrens oder Ahndung mit Geldbuße oder Verwarnung
- Bei Verdacht auf eine Straftat: Abgabe an die Staatsanwaltschaft (§ 41 OWiG), ggf. zusätzlich mit Stellung eines Strafantrags (§ 44 Abs. 2 Satz 2 BDSG)

Daneben erhalten wir regelmäßig Vorgänge im Wege der Abgabe durch die Staatsanwaltschaft an die Bußgeldbehörde gemäß § 43 OWiG. In solchen Fällen hat die Staatsanwaltschaft ein von ihr geführtes Ermittlungsverfahren eingestellt, hält aber eine datenschutzrechtliche Ordnungswidrigkeit für

möglich und gibt daher den Vorgang an uns als Bußgeldbehörde ab. In diesen Fällen müssen wir entscheiden, ob ein Bußgeldverfahren eingeleitet bzw. in den Fällen des § 43 Abs. 2 OWiG, ob ein von der Staatsanwaltschaft bereits - im Rechtssinne - eingeleitetes Bußgeldverfahren fortgeführt oder eingestellt wird.

Zudem haben wir im Rahmen unserer täglichen Arbeit als Datenschutzaufsichtsbehörde - wie jede andere Behörde auch - laufend zu beurteilen, ob sich im konkreten Fall Anhaltspunkte für (datenschutzrechtliche) Ordnungswidrigkeiten ergeben, die unserer Zuständigkeit als Bußgeldbehörde unterfallen. Anders als dies für die Staatsanwaltschaft gemäß § 152 Abs. 2 StPO im Falle eines Straftatverdachts gilt, besteht jedoch beim Anfangsverdacht auf eine Ordnungswidrigkeit keine Pflicht, diese in jedem Falle zu verfolgen. Die Bußgeldbehörden haben gemäß § 47 Abs. 1 Satz 1 OWiG im Wege des pflichtgemäßen Ermessens darüber zu entscheiden, ob sie die Einleitung eines Bußgeldverfahrens für angezeigt halten. Bei dieser Entscheidung sind insbesondere die Bedeutung des Verstoßes - etwa dessen Auswirkungen, z. B. bereits eingetretene oder potentielle Schäden - und die Schwere des Tatvorwurfs zu berücksichtigen. Darüber hinaus ist auch die Frage relevant, ob die Ahndung mit einer Geldbuße zur Durchsetzung der Rechtsordnung im konkreten Fall erforderlich ist. Ist dies zu bejahen, leiten wir von Amts wegen in Fällen, die von uns zunächst als Aufsichtsbehörde behandelt wurden, Bußgeldverfahren ein.

Die Geldbußen wurden z. T. gegen natürliche Personen, z. T. aber auch gemäß § 30 Abs. 1, Abs. 4 OWiG gegen juristische Personen oder Personenvereinigungen verhängt (sog. Verbandsgeldbuße). Eine Verbandsgeldbuße kann verhängt werden, wenn eine Person mit Leitungsverantwortung in der entsprechenden juristischen Person bzw. Personenvereinigung - der Kreis der hierfür in Frage kommenden Personen ist in § 30 Abs. 1 Nr. 1 bis Nr. 4 OWiG definiert - eine Ordnungswidrigkeit begangen hat und dadurch eine sog. betriebsbezogene Pflicht der juristischen Person bzw. Personenvereinigung verletzt wurde. Ein recht häufiger Anwendungsfall hiervon ist die Verletzung der Aufsichtspflicht, die vom Betriebs- und Unternehmensinhaber - und für diesen gemäß § 9 OWiG durch ein Organ, eine sonstige vertretungsberechtigte Person, einen sog. Betriebsleiter oder einen besonderen Beauftragten - wahrzunehmen ist, wenn es infolge der Aufsichtspflichtverletzung zu einem datenschutzrechtlichen Verstoß durch einen Mitarbeiter des Unternehmens kommt, der bei gehöriger Aufsicht verhindert oder wesentlich erschwert worden wäre (Ordnungswidrigkeit gemäß § 130 OWiG). Als Aufsichtspflichtverletzung im Sinne von § 130 OWiG kommen auch unzureichende organisatorische Vorkehrungen in Betracht, mithin auch fehlende oder unzureichende Maßnahmen zur Sicherstellung der Einhaltung datenschutzrechtlicher Vorschriften im Unternehmen. Liegen die gesetzlichen Voraussetzungen vor, machen wir i. d. R. von der Möglichkeit der Verbandsgeldbuße Gebrauch.

Entsprechend den hier dargestellten Fallgestaltungen gibt es verschiedentliche Anlässe, in denen wir Entscheidungen in unserer Eigenschaft als Bußgeldbehörde zu treffen haben. Im Berichtszeitraum haben wir insgesamt 38 Bußgeldbescheide (davon sechs wegen Ordnungswidrigkeiten durch datenschutzrechtswidrigen Einsatz von Google Analytics) und eine Verwarnung erlassen. In 135 Fällen (davon die meisten im Zusammenhang mit Google Analytics) haben wir Bußgeldverfahren eingestellt oder bei uns eingegangenen Ordnungswidrigkeitenanzeigen keine Folge gegeben. Nur in drei Fällen wurde gegen die verhängten Geldbußen Einspruch eingelegt. Davon wurde in einem Fall der Einspruch vor Durchführung der Hauptverhandlung wieder zurückgenommen.

Zwar sind „Mischformen“ aus Bußgeldverfahren und datenschutzaufsichtlicher Tätigkeit nicht zulässig. Jedoch besteht bisweilen das Bedürfnis und im Ergebnis rechtlich häufig auch die Möglichkeit, Informationen bzw. Erkenntnisse, die im Rahmen eines Bußgeldverfahrens angefallen sind, in einem vom Bußgeldverfahren zu trennenden aufsichtlichen Verfahren zu verwenden. Die Vorschrift des § 49a Abs. 4 Nr. 1 OWiG ermöglicht durch Verweisung auf 17 Nr. 3 EGGVG die Übermittlung personenbezogener Daten aus einem Bußgeldverfahren, sofern dies zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist. Da zur „öffentlichen Sicherheit“ anerkanntermaßen auch der Schutz der Rechtsordnung zählt, ist in entsprechender Anwendung dieser Vorschriften die Verwendung von - auch personenbezogenen - Daten aus einem Bußgeldverfahren für die Führung einer aufsichtlichen Prüfung zulässig, sofern möglich erscheint, dass datenschutzrechtliche Verstöße noch stattfinden oder bevorstehen.

Generell zeigt sich, dass es trotz der Vielfalt der Lebenssachverhalte, in denen es zu datenschutzrechtlichen Verstößen kommt, bei denen eine Ahndung mit einer Geldbuße angezeigt ist, doch einige Fallgestaltungen gibt, die uns besonders häufig bzw. in jüngerer Zeit gehäuft bekannt werden, die im Folgenden dargestellt werden.

Die detaillierte Übersicht der Bußgeldverfahren befindet sich im Anhang 2.

20.1 Bußgeldverfahren wegen unzulässiger Nutzung von Google Analytics

Zahlreiche bayerische Webseiten-Betreiber setzten „Google Analytics" ein, ohne die durch dieses Verfahren erfassten IP-Adressen der Webseiten-Besucher zu anonymisieren, und übermittelten damit ungekürzte IP-Adressen an Google in die USA (siehe auch Kapitel 4.1.3).

Bußgeldverfahren haben wir in 105 Fällen eingeleitet, in denen die Betreiber („Diensteanbieter" im Sinne des TMG) nicht bereits im aufsichtlichen Verfahren zur Vornahme von Änderungen, insbesondere Einbau der Anonymisierungsfunktion zu bewegen waren. Wir sahen hierin eine Verwendung von Nutzungsdaten entgegen § 15 Abs. 1 Satz 1 TMG (Ordnungswidrigkeit nach § 16 Abs. 2 Nr. 4 TMG), da durch die Übermittlung ungekürzter IP-Adressen mittels „Google Analytics" Nutzungsdaten von Nutzern verwendet werden, obwohl dies weder zur Inanspruchnahme der entsprechenden Internetseiten erforderlich ist noch Abrechnungszwecken dient, sondern lediglich der sog. Reichweitenanalyse der Website. Im Rahmen der eingeleiteten Bußgeldverfahren hat der bei weitem größte Teil der betreffenden Stellen die datenschutzrechtlichen Anforderungen doch noch erfüllt. In diesen Fällen haben wir unter Ausübung pflichtgemäßen Ermessens die Bußgeldverfahren eingestellt. In sechs Fällen haben wir Geldbußen verhängt, da die Anbieter den Verstoß nicht abgestellt haben. Gegen einen der Bußgeldbescheide wurde Einspruch eingelegt, vor der Hauptverhandlung aber wieder zurückgenommen.

20.2 Heimliche Ortung von Fahrzeugen

Die heimliche Fahrzeugortung ist ein erheblicher Eingriff in das Recht des Betroffenen auf informationelle Selbstbestimmung und dürfte in vielen Fällen datenschutzrechtliche Bußgeldtatbestände erfüllen. Nur für sehr wenige, besondere Fallgestaltungen ist überhaupt vorstellbar, dass eine solche Überwachung datenschutzrechtlich zulässig sein kann.

Mehrfach wurden wir im Berichtszeitraum mit Fällen befasst, in denen Betroffene beim Besuch einer Kfz-Werkstatt entdeckten, dass an ihrem Fahrzeug ein Ortungsgerät angebracht worden war. Bei den Ortungsgeräten handelte es sich meist um Systeme zur GPS-Ortung mit einer eingebauten SIM-Karte. Die Geräte ermittelten per GPS laufend die Fahrzeugpositionsdaten und übermittelten diese an eine IP-Adresse. Dort wurden die Daten von den Personen, die die Überwachung in Auftrag gegeben hatten, oder von beauftragten Detekteien mit entsprechender Zugangskennung eingesehen oder online abgerufen. In den von uns bearbeiteten Fällen haben die Auftraggeber auf diese Weise über mehrere Wochen die Fahrtrouten der überwachten Fahrzeuge verfolgt. Die Ortungsgeräte waren z. T. von Detekteien auf entsprechendes Verlangen der Auftraggeber beschafft und an den Fahrzeugen angebracht worden. Die Überwachungsaufträge hatten unterschiedliche Motivation: In einem Fall wollte der Auftraggeber überprüfen, ob seine Bekannte, mit der er eine Beziehung einzugehen erhoffte, andere Männerbekanntschaften unterhielt. In einem anderen Fall fühlte sich der Auftraggeber von einem Bekannten, der ihm die Rückzahlung eines Darlehens schuldete, hintergangen und wollte durch die Überwachung Beweismaterial dafür sammeln, dass der Schuldner entgegen seinen Beteuerungen über finanzielle Mittel verfügte.

Gemeinsam war den Fällen, dass die Überwachung jeweils eindeutig unzulässig war. Die Positionsdaten waren als personenbezogene Daten im Sinne von § 3 Abs. 1 BDSG anzusehen, da die Auftraggeber jeweils davon ausgehen konnten, dass das überwachte Fahrzeug lediglich von einer bestimmten Person verwendet wird. Die Erhebung und Speicherung der Daten war jeweils unzulässig, weil gegenüber den o. g. Interessen der Auftraggeber das schutzwürdige Interesse der Betroffenen am Unterbleiben der Überwachung ganz eindeutig überwog. Die heimliche Überwachung des Aufenthaltsorts stellt einen massiven Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung dar. Gemessen an der Tiefe des Eingriffs sind nur sehr wenige Fallgestaltungen denkbar, in denen eine derartige Überwachung überhaupt datenschutzrechtlich zulässig sein könnte. Die vorliegenden Fälle gehörten jedenfalls eindeutig nicht dazu, da weder das o. g. Interesse an einer Darlehensrückzahlung noch - erst recht - das Motiv, die Männerkontakte einer Bekannten zu überprüfen, als hinreichend gewichtig angesehen werden können, um einen derart erheblichen Eingriff in das informationelle Selbstbestimmungsrecht rechtfertigen zu können.

Wir haben die Verstöße mit Geldbußen gegen die jeweiligen Auftraggeber geahndet. Gegen die beteiligten Detekteien wurde z. T. strafrechtlich ermittelt. Es wird zu beobachten sein, ob die Anzahl derartiger Fälle zunimmt. In diesem Zusammenhang könnte auch Anlass bestehen, die Rolle von Detekteien in solchen Fällen datenschutzrechtlich näher zu beleuchten.

Sofern derartige Überwachungen ohne Einschaltung gewerblich tätiger Dritter erfolgen, betrachten wir dies als eine ausschließlich persönliche Tätigkeit im Sinne des § 1 Abs. 2 Nr. 3 BDSG, so dass der Anwendungsbereich des BDSG nicht eröffnet und damit auch die Bußgeldvorschrift des § 43 BDSG nicht einschlägig ist. Bei entsprechenden Eingaben verweisen wir die Eingabeführer auf den Zivilrechtsweg.

20.3 Entsorgung von Unterlagen der Lohnbuchhaltung im Papiermüll

Unterlagen mit personenbezogenen Daten, für die die gesetzlichen Aufbewahrungspflichten abgelaufen und die zu entsorgen sind, müssen so vernichtet werden, dass eine Kenntnisnahme Dritter von den darin enthaltenen Daten ausgeschlossen ist - etwa mittels eines geeigneten Schredders oder unter Einschaltung eines spezialisierten (Datenträger-) Entsorgungsunternehmens.

Immer wieder werden wir in Fällen eingeschaltet, in denen Unterlagen mit personenbezogenen Daten an öffentlich zugänglichen Stellen aufgefunden werden. In einem besonders gravierenden Fall wurden über 20 Ordner mit Unterlagen, die aus einem Lohnbuchhaltungsbüro stammten, in einem öffentlich zugänglichen Altpapiercontainer aufgefunden. Zu den Unterlagen, die personenbezogene Daten enthielten, gehörten u. a. Jahreslohnkonten, Lohnsteueranmeldungen, Sozialversicherungsbeitragsnachweise und -anmeldungen zu Beschäftigten, sonstiger Schriftverkehr unterschiedlichster Art mit Behörden, Berufsgenossenschaften, Versicherungen u. ä., Kontoauszüge, Umsatzsteuer- und Einkommensteuerbescheide und Rechnungen. Die Ermittlungen ergaben, dass das Lohnbuchhaltungsbüro aufgelöst worden war, ohne für alle Unterlagen eine ordnungsgemäße Entsorgung bzw. Rückgabe der Unterlagen an die betreffenden Kundenunternehmen sicherzustellen. Das Lohnbuchhaltungsbüro hatte die aufgefundenen Unterlagen an eine externe Person zur Entsorgung abgegeben, ohne hinreichend zu überprüfen, ob letztere zu einer ordnungsgemäßen Entsorgung in der Lage war. Für einen Teil der Unterlagen waren die handels- und steuerrechtlichen Aufbewahrungsfristen von sechs bzw. zehn Jahren (§§ 147 AO, 257 HGB) noch nicht abgelaufen, so dass die Unterlagen insoweit nicht vernichtet werden durften.

Wir haben den Tatbestand einer Ordnungswidrigkeit gemäß § 43 Abs. 2 Nr. 1 BDSG bejaht. Zu einer unbefugten Übermittlung personenbezogener Daten war es spätestens dadurch gekommen, dass die Unterlagen im Altpapiercontainer durch Unbeteiligte aufgefunden und somit die personenbezogenen Daten gemäß § 3 Abs. 4 Satz 2 Nr. 3a BDSG an Dritte durch Bekanntgabe weitergegeben worden waren. Die Verantwortlichkeit für den Verstoß konnte einer leitenden Mitarbeiterin des Lohnbuchhaltungsbüros zugeordnet werden, der nach unserer Bewertung Fahrlässigkeit vorzuwerfen war. Wir haben den Verstoß mit einer Geldbuße geahndet und die Unterlagen nach Abschluss des Verfahrens den betroffenen Kunden gemäß den bußgeldrechtlichen Regelungen zur Herausgabe sichergestellter Beweisgegenstände zurückgegeben.

20.4 Unzulässige Bonitätsabfrage

Wer durch unrichtige Angaben ohne berechtigtes Interesse eine Bonitätsabfrage unternimmt, handelt ordnungswidrig.

Mehrere Geldbußen wurden wegen unzulässiger - d. h. ohne Vorliegen eines berechtigten Interesses vorgenommener - Bonitätsabfragen verhängt. Sofern bei der Abfrage bewusst falsche Angaben gemacht wurden, lag ein Erschleichen der Übermittlung von nicht allgemein zugänglichen personenbezogenen Daten durch unrichtige Angaben vor (§ 43 Abs. 2 Nr. 4 BDSG).

20.5 Sonstige Einzelfälle

Weitere Geldbußen haben wir z. B. wegen Verarbeitung oder Nutzung personenbezogener Daten für Werbezwecke trotz vorherigen Werbewiderspruchs (§ 43 Abs. 2 Nr. 5b BDSG), wegen nicht erteilter Auskunft an die Aufsichtsbehörde (§ 43 Abs. 1 Nr. 1 Nr. 10 BDSG) oder fehlender bzw. nicht ordnungsgemäßer Auskunft an den Betroffenen (§ 43 Abs. 1 Nr. 8a BDSG) in jeweils mehreren - voneinander unabhängigen - Fällen verhängt.

Anhang 1:
Übersicht der Meldungen von Datenpannen nach § 42a BDSG

Seit Inkrafttreten der Meldepflicht zu Datenpannen am 1. September 2009 wurden uns bisher insgesamt 54 Mitteilungen nach § 42a BDSG (einschließlich § 15a TMG) zugeleitet, wobei wir nach unserer Prüfung davon 33 Fälle im Ergebnis als meldepflichtige Sachverhalte gemäß § 42a BDSG eingestuft haben. Skimming-Fälle erscheinen in dieser Statistik erst ab 2011, weil erst dann unsere Auffassung im Bankenbereich durchgesickert ist, dass Skimming-Fälle nach § 42a BDSG meldepflichtig sind. Das Jahr 2009 sehen wir als „Anlaufzeit" an, in dem wir zwar erste Meldungen erhalten hatten (sechs Fälle), die aber allesamt nach unserer Bewertung nicht den Tatbestand von § 42a BDSG erfüllt haben.

Sachverhalt	2009	2010	2011	2012	Gesamt
Hacking von Internet-Diensteanbietern		6	2	2	10
Kopieren von EC-Kartendaten an Geldautomaten (Skimming)			4	6	10
Diebstahl bzw. Einbruch-Diebstahl von Datenträgern/DV-Geräten		3	1	2	6
Verlust von Datenträgern auf dem Transportweg (Post, Botendienst)		1		1	2
Erschleichen von Kreditkartendaten durch ein auf einer Internetplattform vorgetäuschtes Hotelangebot			1		1
Versehentliches Veröffentlichen von Bankdepotdaten im Internet			1		1
Fehl-Versendung von Gehaltsmitteilungen infolge eines Softwarefehlers			1		1
Versehentlichen Sammel-E-Mail-Versendung mit sensiblen Gesundheitsdaten				1	1
Abfotografieren von Bildschirmseiten mit Kreditvertragsdaten in einer Bank				1	1
Summe		**10**	**10**	**13**	**33**

Anhang 2:
Übersicht der Ordnungswidrigkeitenverfahren 2011 und 2012

Die Durchführung von Ordnungswidrigkeitenverfahren ist mit einem erheblichen Aufwand verbunden. Sie erfordern in der Regel die Einvernehmung von Zeugen - schriftlich und gelegentlich auch persönlich -, die Anhörung des Beschuldigten und darüber hinaus unter Umständen auch weitere Maßnahmen wie etwa Beschlagnahmen.

In den früheren Tätigkeitsberichten haben wir lediglich die Zahl der verhängten Bußgeldbescheide angegeben. Die Arbeit in den Verfahren, die zu einer Einstellung geführt haben - weil sich der Vorwurf des Begehens einer Ordnungswidrigkeit nicht bestätigt hat oder nicht nachgewiesen werden konnte - wurde dadurch nicht transparent. Wir haben uns deshalb dafür entschieden, ab diesem Tätigkeitsbericht auch die Verfahren aufzunehmen, die nicht mit dem Erlass eines Bußgeldbescheides geendet haben.

Übersicht der Verfahren im Jahr 2011:

Eingeleitete Verfahren mit Tatvorwurf	Anzahl	davon eingestellt	davon Bußgeld-bescheid	bestandskräftig ohne Rechtsmittel	Entscheidung AG
Unbefugte Bonitätsabfrage	2		2	2	
Herausgabe von Kontoauszügen an Unbefugten bzw. bei fehlender Kontovollmacht	1		1	1	
Übermittlung von Abonnentendaten an einen anderen Verlag nach Einstellung einer Zeitschrift	1		1	1	
Werbung trotz Werbewiderspruchs	2		2	2	
Weitergabe von Stellenbewerberdaten an eine andere Stelle als das inserierende Unternehmen	1		1	1	
Unsachgemäße Entsorgung von Unterlagen mit personenbezogenen Daten (insb. im Papiermüll)	5	1	4	4	
Abrufbarkeit von Daten im Internet	1	1			
Übermittlung überschießender Patientendaten durch Arzt an Berufsunfähigkeitsversicherung	1		1	1	
Unterlassene Meldung einer meldepflichtigen Datenverarbeitung	1		1	1	
Beschaffung von Beschäftigtendaten bei einem Dritten zwecks Nachweis eines Arbeitszeitbetrugs	1	1			
Beschaffung von Patientendaten für eine medizinische Studie ohne ausreichende Einwilligung	2	1	1	1	
Fahrzeugortung mit GPS	2	2			

Eingeleitete Verfahren mit Tatvorwurf	Anzahl	davon eingestellt	davon Bußgeld-bescheid	bestandskräftig ohne Rechtsmittel	Entschei-dung AG
Unzulässiger Abruf von Daten durch einen IT-Systemadministrator	1		1	1	
Einbau einer Videokamera im „Türspion“ in einem Wohnhaus	1	1			
Bereithalten von Bankkundendaten zum Abruf durch externen Unternehmens-berater	1		1	1	
Unbefugtes Abrufen von Patienten-daten aus einem Krankenhaus-informationssystem für private Zwecke	1		1	1	
Anfertigung von Nahaufnahmen (Fotos) von Demonstrationsteilnehmern	1		1		Aufhebung durch AG
Mitteilung von Daten über Einkommen von Arbeitskollegen und Vorgesetzten	1		1		Aufhebung durch AG
Übermittlung von Arztabrechnungen durch Einschaltung unternehmens-fremder Mitarbeiter	1	1			
Speicherung von Leistungsdaten zu Arbeitskollegen	1		1	1	
Ungeklärte Beschaffung von Daten über Fahrzeugzulassungen	1	1			
Unbefugte Übermittlung von Kontoda-ten durch einen Betreuer	1		1	1	
Summe	**30**	**9**	**21**	**19**	

Übersicht der Verfahren im Jahr 2012:

Eingeleitete Verfahren mit Tatvorwurf	Anzahl	davon eingestellt	davon Bußgeld-bescheid	bestandskräftig ohne Rechtsmittel	Entschei-dung AG
Fahrzeugortung mit GPS	2		2	2	
Unsachgemäße Entsorgung von Unterlagen mit personenbezogenen Daten (insb. Papiermüll)	1	1			
Google Analytics: Übermittlung ungekürzter IP-Adressen an Google	105	99	6	5	Einspruch Rücknahme
Anfertigung von Nahaufnahmen (Fotos) von Demonstrationsteilnehmern	2	2			
Unternehmen, das in einem Internet-portal negativ bewertet wurde, teilt den Namen des Bewertenden einem ande-ren Unternehmen mit, das von derselben Person bewertet wurde	1		1	1	
Unternehmen verrät private E-Mail-Adresse eines ausgeschiedenen Mitar-beiters durch Nennung im „Abwesen-heitsassistenten" des E-Mail-Programms (vereinbart war, dass Un-ternehmen eingehende E-Mails an den Mitarbeiter nachsendet)	1	1			
Weitergabe einer Vermögens- und Einkünfteübersicht zu einem Kunden durch Bank an ein verbundenes Unter-nehmen zwecks Verteidigung in einem Schadensersatzprozess	1		1	1	
Ungeklärte Beschaffung einer Telefon-nummer	3	3			
Werbender stellt nicht sicher, dass Beworbene Kenntnis über die Herkunft ihrer Daten erhalten können	2	2			
Weitergabe von Daten eines früheren Bankkunden an Dienstleister zwecks Beobachtung von Insolvenzbekanntma-chungen	1		1	1	
Unzulässige Speicherung, obwohl rechtskräftig gerichtlich geklärt ist, dass keine Geschäftsbeziehung besteht	1		1	1	
Abruf von Daten zu Zahlungsvorgängen durch Mitarbeiter einer Zahlungsver-kehrsdienstleistungfirma aus privater Neugier	1	1			
Hinzuspeicherung einer Telefonnummer (Hinzuspeicherung war zulässig)	1	1			

Eingeleitete Verfahren mit Tatvorwurf	Anzahl	davon eingestellt	davon Bußgeld-bescheid	bestandskräftig ohne Rechtsmittel	Entschei-dung AG
Infolge fehlender Systemabsicherung sind Kundendaten im offenen Internet abrufbar	1		1		Entschei-dung AG noch offen
Werbung trotz Werbewiderspruchs	1		1	1	
Videokamera im Pkw filmt Verkehrsge-schehen auf der Straße (vorliegend keine Personen identifizierbar)	1	1			
Fehlender Hinweis auf Werbewider-spruchsrecht	1	1			
Fehlende bzw. unzureichende Aus-kunftserteilung an die Datenschutzauf-sichtsbehörde	1		1	1	
Energieversorger speichert falsche Adressdaten zu einem Kunden	1	1			
Weitergabe von Inhalten einer polizeili-chen Vernehmung und Durchsuchung am Telefon (im Ergebnis kein Bußgeld-tatbestand erfüllt)	1	1			
Missbräuchliche Eingabe von Daten eines Dritten auf einer Internetseite (unaufklärbar)	1	1			
Weitergabe personenbezogener Daten an einen Rechtsanwalt als Prozessver-treter (im Ergebnis zulässig)	1	1			
E-Mail-Serienbrief wird so versandt, dass jeder Empfänger die Adressen aller anderen Empfänger erhält	1	1			
Fehlende bzw. unzureichende daten-schutzrechtliche Auskunft an Betroffe-nen	1	1			
Videokamera (z.T.) im öffentlichen Straßenraum	4	4			
Unbestätigter Verdacht auf Übermitt-lung von Daten durch eine Zeitarbeits-firma an einen Vermieter	1	1			
Unbefugte Bonitätsabfrage (unbestätig-ter Verdacht)	1	1			
Wiederholte Fehlversendung von Arzt-briefen per Fax	1		1	1	
Unzulässige Speicherung von Daten durch einen Volkszählungs-Erhebungsbeauftragten für eigene ge-werbliche Zwecke	1		1	1	

Eingeleitete Verfahren mit Tatvorwurf	Anzahl	davon eingestellt	davon Bußgeld-bescheid	bestandskräftig ohne Rechtsmittel	Entschei-dung AG
Veröffentlichung eines baurechtlichen Vorbescheids mit Namen und Adressda-ten von Nachbarn im Rahmen einer Immobilienanzeige im Internet	1	1			
Abruf von Kontobewegungsdaten durch Bankmitarbeiter für private Zwecke	2	1	1	1	
Summe	**144**	**126**	**18**	**16**	**2**

Stichwortverzeichnis

K

L

M

N

O

P

R

S

T

U

V

W

Z

Bayerisches Landesamt für DatenschutzAufsicht
Promenade 27
91522 Ansbach

Telefon: 0981 / 53 - 1300
Telefax: 0981 / 53 - 5300
E-Mail: poststelle@lda.bayern.de
Webseite: www.lda.bayern.de