Regierung von Mittelfranken

Bayerische Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich

1. Tätigkeitsbericht

2002/2003

Impressum

Herausgeber:

Regierung von Mittelfranken
Bayerische Datenschutzaufsichtsbehörde
für den nicht-öffentlichen Bereich
Promenade 27
91522 Ansbach

Telefon: (0981) 53-0
Telefax: (0981) 53-1206
E-Mail: datenschutz@reg-mfr.bayern.de

Vorwort

Die Regierung von Mittelfranken legt hiermit in ihrer Eigenschaft als Bayerische Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich ihren ersten Tätigkeitsbericht vor. Er umfasst den Zeitraum vom 01.01.2002 bis zum 31.12.2003 und gibt einen Überblick über die wahrgenommenen Aufgaben.

Die in diesem Bericht dargestellten typischen Fallbeispiele und ihre rechtlichen Wertungen zeigen, dass dem Datenschutz heute in Wirtschaft und Gesellschaft ein hoher Stellenwert eingeräumt werden muss. Die elektronische Datenverarbeitung und die Kommunikationstechnik entwickeln sich in rasanter Weise fort und sind nunmehr in nahezu allen Lebensbereichen präsent. Damit muss auch der Datenschutz Schritt halten. Dies gilt sowohl für die Schaffung und die ständige Anpassung der gesetzlichen Grundlagen als auch für die Umsetzung dieser Regelungen in der Praxis.

In erster Linie müssen sich diejenigen vom Datenschutzrecht angesprochen fühlen, die mit personenbezogenen Daten umgehen. Aber auch jeder Einzelne muss noch mehr für den Schutz seiner personenbezogenen Daten sensibilisiert werden. Viele Datenmissbräuche könnten verhindert werden, wenn die Betroffenen selbst nicht zu sorglos Daten über ihre Person preisgeben würden.

Deshalb sehen wir nicht nur in der Überprüfung datenschutzrechtlicher Vorgänge, sondern auch in der Information eine wesentliche Aufgabe der Datenschutzaufsicht. In diesem Sinne soll auch mit diesem Bericht die Öffentlichkeit auf wichtige Fragen des Datenschutzes aufmerksam gemacht werden.

Ansbach, im April 2004

Inhofer
Regierungspräsident

Inhaltsverzeichnis:

1 Die Datenschutzaufsicht im nicht-öffentlichen Bereich

1.1 Aufgaben einer Datenschutzaufsichtsbehörde im nicht-öffentlichen Bereich

Nach § 38 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) kontrolliert die Aufsichtsbehörde die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln.

Die Aufgaben einer Aufsichtsbehörde lassen sich im Wesentlichen wie folgt beschreiben:

- Bearbeitung von Anfragen, Eingaben und Beschwerden
- Beantwortung der Anfragen der betrieblichen Datenschutzbeauftragten
- Kontrollen in den Unternehmen und sonstigen verantwortlichen Stellen
- Beanstandungen bei Datenschutzverstößen
- Anordnungen bei Sicherheitsmängeln
- Führung des öffentlichen Registers der meldepflichtigen Unternehmen vor allem im Hinblick auf Auskunfteien, Adressenhandel, Markt- und Meinungsforschungsinstitute
- Genehmigungen von Datenübermittlungen in Drittstaaten (also außerhalb der Staaten der Europäischen Union und des Europäischen Wirtschaftsraumes) gem. § 4c Abs. 2 BDSG
- Überwachung der Anbieterkennzeichnung bei Tele- und Mediendiensten
- Durchführung von Bußgeldverfahren
- Stellung von Strafanträgen gemäß § 44 BDSG

Die Überprüfungen der Datensicherheit führt in Bayern der TÜV Süd im Auftrag der Datenschutzaufsichtsbehörde durch (vgl. Art. 34 Abs. 1 Satz 1 Bayerisches Datenschutzgesetz - BayDSG).

1.2 Gesetzliche Grundlage für die Erstellung des Tätigkeitsberichts

Die gesetzliche Verpflichtung der Aufsichtsbehörden, spätestens alle zwei Jahre einen Tätigkeitsbericht zu erstellen, ergibt sich aus § 38 Abs. 1 Satz 6 BDSG. Diese Bestimmung ist im Rahmen der am 23.05.2001 in Kraft getretenen Änderung des BDSG neu eingeführt worden. Sie beruht auf Art. 28 Abs. 5 der Richtlinie 95/64/EG des Europäischen Parlaments und des Rates vom 24.10.1995. Nach dieser Vorschrift legt jede Kontrollstelle regelmäßig einen Bericht vor, der veröffentlicht wird.

1.3 Die Regierung von Mittelfranken als Bayerische Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich

Die Regierung von Mittelfranken ist von der Bayerischen Staatsregierung ab 01.06.2002 zur bayernweit zuständigen Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich bestimmt worden. Die durch die Novellierung des BDSG im Jahr 2001 eingetretene wesentliche Ausweitung der Aufgaben der Aufsichtsbehörden und die auf Grund der fortschreitenden Automatisierung ständig steigenden Anforderungen an die Aufsicht waren ausschlaggebend für die Konzentration dieser bisher von den sieben Regierungen wahrgenommenen Aufgabe auf nunmehr eine Behörde.

Für die Aufgaben der Bayerischen Datenschutzaufsichtsbehörde sind bei der Regierung von Mittelfranken derzeit folgende Personen tätig:

Sachgebietsleiter	Ltd. Regierungsdirektor Dorn
Stv. Sachgebietsleiter	Oberregierungsrat Meier (anteilig zur Hälfte)
	Regierungsamtsrat Ilgenfritz
	Regierungsoberinspektor Andörfer (anteilig zur Hälfte)
	Regierungsoberinspektorin Fürst
	Regierungsoberinspektorin Dierauff

* * *

2 Überblick und Statistik

2.1 Bearbeitung von Anfragen, Eingaben und Beschwerden

Den größten Raum in der alltäglichen Arbeit nimmt die Bearbeitung von Anfragen, Eingaben und Beschwerden von Betroffenen ein. Vorwiegend werden Verletzungen von Datenschutzvorschriften geltend gemacht.

Schwerpunktthemen sind dabei seit Jahren die Datenverarbeitungen

- in der Versicherungswirtschaft (Anteil ca. 15 %),
- bei den Banken (Anteil ca. 5 %),
- bei den Auskunfteien (Anteil ca. 5 %),
- im Zusammenhang mit Direktwerbemaßnahmen und der Adressenverarbeitung (Anteil ca. 15 %),
- in Arbeitsverhältnissen (Anteil ca. 10 %),
- im Gesundheitswesen (Anteil ca. 5 %),
- in Vereinen und Verbänden (Anteil ca. 5 %),
- bei der Videoüberwachung (Anteil ca. 5 %) und
- bei der Nutzung der neuen Medien wie Internet und E-Mail (Anteil ca. 10 %).

Grundsätzlich versuchen wir, die vorgebrachten Beschwerden von Betroffenen über den schriftlichen, telefonischen oder elektronischen Kontakt mit den davon berührten Unternehmen zu klären. Gelegentlich erweisen sich aber auch konkrete Prüfungen vor Ort in den Firmen als erforderlich, um Sachverhalte ausreichend zu ermitteln.

Die interessantesten Fälle sind in den nachstehenden Fachabschnitten behandelt. Verstöße gegen Datenschutzvorschriften gibt es, insbesondere aufgrund menschlicher Fehlleistungen, in allen Bereichen der Wirtschaft. Hier ist es Aufgabe aller Datenschutzverantwortlichen in den Unternehmen, durch personelle, technische und organisatorische Maßnahmen den Datenschutz sicherzustellen.

Statistik 2002

Für das Jahr 2002 wurde keine offizielle Statistik erstellt, da sie im Hinblick auf den Beginn unserer bayernweiten Zuständigkeit am 01.06.2002 als wenig aussagekräftig erschien.

Statistik 2003:

- Schriftliche Eingaben insgesamt 502

Überprüfungsergebnisse:	
Keine Verstöße	312
Leichte Verstöße	141
Erhebliche Verstöße	49
Eingeleitete Bußgeldverfahren	31
Erlassene Bußgeldbescheide	2
Eingestellte Bußgeldverfahren	3

- Telefonische Anfragen ca. 350

2.2 Unterstützung der betrieblichen Datenschutzbeauftragten

Die Beantwortung von Anfragen betrieblicher Datenschutzbeauftragter nahm an Bedeutung und Menge zu. Vielfach wurde zur schnellen Beratung der telefonische Kontakt gesucht. Schwierigere Fallgestaltungen wurden schriftlich (einschl. E-Mail) vorgetragen. Hier standen folgende Themen im Vordergrund:

- Anfragen zur Umsetzung des BDSG in der Betriebspraxis, wie Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten (bDSB), Verfahrensverzeichnis des bDSB,

- Arbeitnehmerdatenschutz in seiner ganzen Breite, von der Behandlung der Bewerbungsunterlagen und -daten bis zur innerbetrieblichen Regelung der Internet- und E-Mail-Nutzung am Arbeitsplatz,

- Fragen zu Datenübermittlungen ins Ausland.

Wegen der komplexen Materie wurden manche Sachverhalte auch mit den Unternehmen in Besprechungen erörtert, entweder bei uns oder vor Ort.

2.3 Kontrolltätigkeit

Seit der BDSG-Novellierung 2001 können die Aufsichtsbehörden bei allen dem BDSG unterliegenden Stellen des nicht-öffentlichen Bereiches Prüfungen durchführen. Hinreichende Anhaltspunkte für Verletzungen von Datenschutzvorschriften, wie nach früherem Recht, müssen nicht mehr vorliegen. Der Bundesgesetzgeber hat auf Grund der Vorgabe durch die EG-Datenschutzrichtlinie die sog. Anlassaufsicht abgeschafft. Auch nach Wegfall der Anlassaufsicht wird die Aufsichtsbehörde Schwerpunkte setzen müssen. Sie wird weiterhin die meldepflichtigen Unternehmen kontrollieren und im Übrigen vor allem dann tätig werden, wenn Bürger sich beschweren, sonstige Hinweise auf mögliche Rechtsverletzungen vorliegen oder in einem Bereich Gefahren für das Persönlichkeitsrecht erkennbar werden. Eine solche „Konzentration auf das Wesentliche“ ist schon im Hinblick auf die notwendige Bündelung der Kräfte der Aufsichtsbehörde notwendig.

Unsere Kontrollen bezogen sich vor allem auf die meldepflichtigen Unternehmen (Auskunfteien, Adressenhandel und Marktforschung). Im Übrigen nahmen wir Beschwerden oder sonst bekannt gewordene Datenschutzprobleme zum Anlass, eine Prüfung durchzuführen.

Im Jahr 2002 haben wir 11 Firmen vor Ort geprüft, davon

- 4 Markt-/Meinungs-/Sozialforschungsunternehmen
- 4 Auskunfteien
- 2 DV-Dienstleister
- 1 Versandhandelsunternehmen

Im Jahr 2003 wurden 22 Firmen vor Ort geprüft, davon

- 16 Markt-/Meinungs-/Sozialforschungsunternehmen
- 2 Auskunfteien
- 1 DV-Dienstleister
- 2 Versicherungen
- 1 Versandhandelsunternehmen

Handlungsbedarf aus den Feststellungen der Datenschutzprüfungen hat sich insbesondere ergeben:

- bei der Auswahl und der Tätigkeit der betrieblichen Datenschutzbeauftragten,
- beim öffentlichen Verfahrensverzeichnis des Datenschutzbeauftragten nach § 4g Abs. 2 Satz 2 BDSG,
- im Hinblick auf die schriftlichen Vertragsregelungen bei der Auftragsdatenverarbeitung nach § 11 BDSG,
- bei der Erfüllung der Meldepflicht nach § 4d BDSG,
- für notwendige Sicherheitsmaßnahmen im Sinne von § 9 BDSG und
- bezüglich der Inhalte der Verpflichtungserklärung für die Mitarbeiter nach § 5 BDSG.

Die speziellen Beanstandungen bei Auskunfteien sind unter Kapitel 6 dargestellt.

Prüfungen zur Datensicherheit

In Bayern wird die Prüfung der nach § 9 BDSG erforderlichen Datensicherheitsmaßnahmen nicht von der Datenschutzaufsichtsbehörde, sondern in deren Auftrag vom Technischen Überwachungsverein (TÜV Süd) vorgenommen.

Von den 12 im Berichtszeitraum erteilten Prüfungsaufträgen wurden 8 abgeschlossen. Bei keinem der überprüften Unternehmen wurden wesentliche Sicherheitsmängel festgestellt.

Darüber hinaus haben wir den TÜV Süd in verschiedenen Fällen zur sachverständigen Beratung herangezogen.

2.4 Meldepflicht

Nach § 4d BDSG sind im wesentlichen die folgenden zwei Geschäftsfelder gegenüber den Datenschutzaufsichtsbehörden meldepflichtig:

- Die Datenspeicherung zum Zweck der Übermittlung, also der Handel mit personenbezogenen Daten, wie es bei Wirtschaftsauskunfteien und Adressenhändlern der Fall ist.

- Die Datenspeicherung zum Zweck der anonymisierten Übermittlung, also die Tätigkeit der Markt-, Meinungs- und Sozialforschungsinstitute.

Wir haben für Bayern zur Zeit 90 Anmeldungen vorliegen, die sich regional in den Regierungsbezirken wie folgt verteilen:

45	aus Oberbayern
25	aus Mittelfranken
9	aus Oberfranken
5	aus Unterfranken
5	aus Schwaben
1	aus der Oberpfalz

Aus Niederbayern liegt derzeit keine Anmeldung vor.

Von der Struktur her entfallen von den 90 Meldungen 42 auf Auskunfteien und Adressenhändler sowie 48 auf Markt-, Meinungs- und Sozialforschungsunternehmen.

Das bei uns geführte Register über die meldepflichtigen Unternehmen kann nach § 38 Abs. 2 Satz 2 BDSG von jedem eingesehen bzw. aus ihm Auskunft erteilt werden. Bisher wurde aber von dieser Möglichkeit kaum Gebrauch gemacht. Das Register dient in erster Linie zur Unterstützung der Arbeit der Aufsichtsbehörde.

2.5 Zusammenarbeit der für den Datenschutz Verantwortlichen

2.5.1 Gremien der Datenschutzaufsichtsbehörden

Seit dem erstmaligen Inkrafttreten des BDSG im Jahr 1977 arbeiten die obersten Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich bundesweit zusammen, um Grundsatzfragen und länderübergreifende Problematiken abzustimmen. Wegen des langjährigen Tagungsorts Düsseldorf hat sich für diesen Ausschuss der Begriff „Düsseldorfer Kreis“ eingebürgert, auch wenn der Ort inzwischen jährlich wechselt. In das Gesamtgremium des „Düsseldorfer Kreises“ sind wir vom Bayerischen Staatsministerium des Innern als der obersten bayerischen Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich ebenso eingebunden worden wie auch in die dazu gehörenden fünf Arbeitsgruppen Kreditwirtschaft, Auskunfteien/SCHUFA, Versicherungswirtschaft, Internationaler Datenverkehr und Tele- und Mediendienste.

Seit 1995 besteht ein Workshop der Aufsichtsbehörden der Länder nach § 38 BDSG für die bundesweite Klärung und Abstimmung von Praxisfragen. Dabei geht es vor allem um die auch von der Wirtschaft zu Recht geforderte bundesweit möglichst einheitliche Handhabung der Datenschutzvorschriften. Der Workshop wird jedes Jahr in einem anderen Bundesland veranstaltet. Im September 2003 waren wir in Ansbach Gastgeber.

2.5.2 Arbeitskreise der Wirtschaftsunternehmen

Betriebliche Datenschutzbeauftragte aus den Unternehmen haben sich unter der Federführung der Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) ebenfalls einen Erfahrungsaustausch in sogenannten „Erfa-Kreisen“ organisiert, um von- bzw. miteinander zu lernen und sich fortzubilden. In Nürnberg und München existiert je eine derartige branchenunabhängige Gesprächsrunde, die sich dreimal im Jahr trifft.

Die Datenschutzbeauftragten der bayerischen Versicherungen haben einen auf ihre speziellen Fachfragen ausgerichteten Datenschutz-Arbeitskreis installiert, der zweimal jährlich tagt.

An diesen Veranstaltungen nehmen wir auf Einladung der Veranstalter regelmäßig teil, um aus unserer Sicht zu den diskutierten Problemen Stellung zu nehmen und Anfragen zu beantworten.

2.5.3 Datenschutzfachtagung

Die Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) richtet jährlich in Köln die zweitägige Datenschutzfachtagung (DAFTA) aus. Dort wird über die aktuellen Fragen des Datenschutzes und der Datensicherheit in Deutschland referiert und diskutiert. Unser Sachgebiet ist dort regelmäßig vertreten.

* * *

3 Der betriebliche Datenschutzbeauftragte

Zu diesem Thema gingen zahlreiche Anfragen ein. Man kann daraus entnehmen, dass ein hoher Informationsbedarf in den Unternehmen, bei neu berufenen Datenschutzbeauftragten oder bei Personen, die die Aufgaben eines Datenschutzbeauftragten übernehmen möchten, besteht. Die zahlreichen Anfragen zeigen aber auch, dass man es in der Wirtschaft mit der Umsetzung der sich aus dem BDSG ergebenden Verpflichtungen ernst nimmt.

Am häufigsten wurden folgende Fragen gestellt:

- Wann muss ein betrieblicher Datenschutzbeauftragter bestellt werden?
- Kann auch ein Externer die Funktion übernehmen?
- Welche Aufgaben hat ein betrieblicher Datenschutzbeauftragter?
- Welche Fachliteratur wird benötigt?
- Was versteht man unter Zuverlässigkeit und Fachkunde?
- Wer bietet Fortbildungsveranstaltungen an?
- Gibt es „Externe“, die die Dienstleistung „Datenschutzbeauftragter“ anbieten?
- Wie sieht ein Bestellschreiben aus?
- Ist ein Widerruf der Bestellung möglich?
- Gibt es für den Datenschutzbeauftragten Kündigungsschutz/Abberufungsschutz?
- Welche Personen können nicht zum Datenschutzbeauftragten berufen werden?

Oft konnten wir diese Fragen telefonisch oder durch Versendung von Informationsmaterial beantworten. Soweit dies wegen der Komplexität des Inhaltes nicht möglich war, nahmen wir schriftlich Stellung.

3.1 Auswahl des Datenschutzbeauftragten

3.1.1 Unvereinbarkeit mit anderen Aufgaben

Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Soweit der Datenschutzbeauftragte noch mit anderen Aufgaben befasst ist, gehört zur Zuverlässigkeit auch, dass für ihn keine Interessenkollision entsteht.

Dieser Fall kann insbesondere dann auftreten, wenn der Datenschutzbeauftragte gleichzeitig Aufgaben in den Bereichen Personal oder EDV verantwortlich wahrnimmt. Unter Umständen müssten diese Personen ihre eigene Tätigkeit überwachen. Nach einer Literaturmeinung können auch zwischen einer Betriebsratstätigkeit und der Tätigkeit eines Datenschutzbeauftragten Interessenkonflikte entstehen.

Wir haben bei entsprechenden Anfragen dazu geraten, bei der jeweiligen Entscheidung im Einzelfall eine ggf. bestehende Unvereinbarkeit zu bedenken.

3.1.2 Der Datenschutzbeauftragte im Konzern

In größeren Konzernen wird häufig ein Konzerndatenschutzbeauftragter bestellt, der gleichzeitig für die einzelnen Unternehmen des Konzerns als externer Datenschutzbeauftragter fungiert. In den einzelnen Unternehmen sind dann häufig zu seiner Unterstützung noch „Datenschutzkoordinatoren“ tätig.

Der Konzerndatenschutzbeauftragte entwickelt Leitlinien für den Datenschutz und stellt entsprechende allgemeine Grundsätze auf. Außerdem klärt er datenschutzrechtliche Einzelfragen, ist für die Sachverhaltsaufklärung bei Datenschutzverletzungen zuständig und unterstützt die Datenschutzkoordinatoren.

Die Datenschutzkoordinatoren setzen die Leitlinien in ihrem Unternehmen um und nehmen dem Datenschutzbeauftragten die Routinearbeiten vor Ort ab.

Diese Lösung hat einerseits die Vorteile, dass der konzerninterne Datenaustausch gut überblickt werden kann, die Umsetzung des Datenschutzes konzernweit einheitlich erfolgt und bei gleichartigen Konzernunternehmen Synergieeffekte und zahlreiche Praxiserfahrungen ausgenutzt werden können. Andererseits hat sie aber auch oft den Nachteil, dass der notwendige eigene Einblick in die einzelnen Unternehmen und damit der jeweilige betriebsinterne Bezug vor allem dann fehlt, wenn der Konzern nicht einheitlich strukturiert ist und unterschiedliche Geschäftsfelder aufweist.

Wir raten deshalb in der Regel zur gegenteiligen Lösung, bei der in jedem rechtlich selbständigen Mitgliedsunternehmen ein Datenschutzbeauftragter bestellt wird. Einer davon wird von der Konzernspitze als Koordinator für den gesamten

Konzern eingesetzt. Seine Aufgaben sollten denen eines Konzerndatenschutzbeauftragten angenähert sein, um die oben genannten Vorteile auch hier weitgehend wirksam werden zu lassen.

Dieses Modell entspricht mehr der Intention des BDSG, das davon ausgeht, dass der Datenschutzbeauftragte mit den betrieblichen Zusammenhängen und Abläufen gut vertraut sein muss, um seine gesetzlichen Aufgaben erfüllen zu können. Dazu gehören auch eine gewisse Ortsnähe und ein guter Einblick in den jeweiligen Betrieb.

3.1.3 Datenschutzbeauftragter mit Sitz im Ausland

Es wurde angefragt, ob der niederländische Angehörige eines zum Konzern gehörenden niederländischen Unternehmens, der seinen Arbeitsplatz in den Niederlanden hat, zum Datenschutzbeauftragten eines in Bayern ansässigen Unternehmens bestellt werden kann.

§ 4f Abs. 2 Satz 2 BDSG sieht ausdrücklich vor, dass mit der Aufgabe des Datenschutzbeauftragten auch eine Person außerhalb der verantwortlichen Stelle betraut werden kann. Einschränkende Maßgaben sind im Gesetz dazu nicht vorgesehen. Somit kann auch ein Ausländer, der bei einem zum Konzern gehörenden, im Ausland angesiedelten Unternehmen beschäftigt ist, grundsätzlich zum externen Datenschutzbeauftragten eines Inlandsunternehmens bestellt werden.

Allerdings muss auch der externe Datenschutzbeauftragte die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. Eine Person, die in einem ausländischen Rechtskreis beruflich tätig ist, muss mit den einschlägigen deutschen Rechtsvorschriften im Allgemeinen und mit dem deutschen Datenschutzrecht im Besonderen so vertraut sein, dass sie die Aufgaben eines Datenschutzbeauftragten zuverlässig und fachkundig wahrnehmen kann. Auch in tatsächlicher Hinsicht muss sichergestellt werden können, dass dieser Datenschutzbeauftragte das Unternehmen, die betrieblichen Zusammenhänge und die Informationswege im Unternehmen über eine so große Entfernung und noch dazu über eine Staatsgrenze hinweg genau genug im Auge behalten kann.

Wir haben das Unternehmen gebeten, diese Gesichtspunkte bei der Entscheidung zu beachten.

3.2 Verhältnis Datenschutzbeauftragter - Betriebsrat

Die an uns herangetragene Frage, ob eine gegenseitige Kontrolle dieser beiden Institutionen stattfindet, haben wir im Grundsatz aus folgenden Gründen verneint:

- Der Betriebsrat hat gemäß § 80 Abs. 1 Nr. 1 Betriebsverfassungsgesetz (BetrVG) darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze eingehalten werden. Dies gilt auch für die Beachtung des Datenschutzrechts. Ansprechpartner für den Betriebsrat ist dabei in erster Linie der Arbeitgeber.

  Der Betriebsrat kann den Datenschutzbeauftragten nicht unmittelbar kontrollieren. Soweit er der Auffassung ist, dass dieser seine Aufgaben nicht ordnungsgemäß wahrnimmt, hat er allerdings die Möglichkeit, beim Arbeitgeber bzw. bei der Aufsichtsbehörde die Abberufung des Datenschutzbeauftragten nach § 4f Abs. 3 BDSG anzuregen.

- Da der Betriebsrat aus datenschutzrechtlicher Sicht Teil der verantwortlichen Stelle (= des Unternehmens) ist, ist der Datenschutzbeauftragte auch für die Datenverarbeitung des Betriebsrats zuständig. Auch hier wird mit personenbezogenen Daten umgegangen.

  Bei der Wahrnehmung seiner Aufgaben kann es für den Datenschutzbeauftragten zu einem Konflikt mit Rechtspositionen des Betriebsrats kommen. Es wird sich nicht vermeiden lassen, dass er auch vom Inhalt der vom Betriebsrat gespeicherten Daten Kenntnis erlangt. Darin kann man eine Gefährdung der nach dem Betriebsverfassungsgesetz geforderten Unabhängigkeit des Betriebrats sehen, da einem Vertreter der Arbeitgeberseite Zugang zu allen Dateien des Betriebsrats eröffnet wird, ohne Rücksicht darauf, ob sie personenbezogene Daten enthalten oder nicht. Damit hätte der Datenschutzbeauftragte Kontrollbefugnisse, die dem Arbeitgeber im Verhältnis zum Betriebsrat nicht zustehen (vgl. Beschluss des Bundesarbeitsgerichts vom 11.11.1997, 1 ABR 21/97; NJW 1998, S. 2466 ff.).

In der Praxis bietet es sich an, diese vom Gesetzgeber bisher nicht geregelte Problematik einvernehmlich in einer Betriebsvereinbarung zu regeln, in der die Befugnisse des Datenschutzbeauftragten bezüglich der Kontrolle des Betriebsrats und ihre Art und Weise festgelegt werden.

* * *

4 Versicherungen

In der Versicherungswirtschaft spielt der Datenschutz naturgemäß eine besondere Rolle. Werden doch schon bei der Antragstellung zahlreiche personenbezogene Daten abgefragt. Dies setzt sich dann bei den einzelnen Erstattungsanträgen der Versicherungsnehmer fort. Es geht dabei auch immer wieder um besondere Arten von personenbezogenen Daten (§ 3 Abs. 9 BDSG), vor allem um Gesundheitsdaten. Es kann deshalb nicht überraschen, dass sich zahlreiche Anfragen und Beschwerden auf die Datenverwendungen bei Versicherungen beziehen.

Allgemein kann man feststellen, dass der Datenschutz von den Versicherungsgesellschaften sehr ernst genommen wird. Die Versicherungsnehmer vertrauen darauf, dass die gesetzlichen und vertraglichen Datenschutzbestimmungen strikt eingehalten werden. Eine Versicherungsgesellschaft würde diesen Vertrauensvorschuss verspielen und sich damit einen großen Schaden zufügen, wenn sie sich in dieser Beziehung nicht korrekt verhalten würde. Es ist deshalb in der Versicherungsbranche allgemein anerkannt, dass eine auch nach außen sichtbare Beachtung des Datenschutzes heutzutage zum Markenzeichen einer Versicherung gehört.

4.1 Umfang der Datenerhebung bei Reiserücktrittsversicherungen

Eine Reihe von Eingaben bezieht sich auf die Datenerhebung durch die Reiserücktrittsversicherungen im Rahmen von Erstattungsanträgen. Es wird vor allem Klage darüber geführt, dass zu viele personenbezogene Daten, speziell Gesundheitsdaten, abgefragt werden. Darüber hinaus werden oft weitergehende Auskünfte des behandelnden Arztes zum Teil auch über Vorerkrankungen nachgefordert, obwohl dem Erstattungsantrag bereits eine ärztliche Bescheinigung beilag.

Rechtsgrundlage der Erhebung stellt § 28 Abs. 1 Satz 1 Nr. 1 BDSG dar, demzufolge das Erheben personenbezogener Daten zur Erfüllung eigener Geschäftszwecke zulässig ist, wenn es der Zweckbestimmung eines Vertragsverhältnisses dient.

Beim Vollzug der oben genannten Versicherungsverträge ist die Erhebung der Daten dann erforderlich, wenn die geforderten Angaben aus vertraglicher oder aus versicherungsrechtlicher Sicht für die Prüfung eines Erstattungsantrages notwendig sind. Dabei ist ein objektiver Maßstab anzulegen. Soweit danach die Versicherung berechtigt ist, die Angaben zu verlangen, steht auch das Datenschutzrecht einer Erhebung der Daten nicht entgegen.

Bei der Beurteilung der versicherungsrechtlichen Vorfrage, ob die verlangten Angaben für die Versicherung erforderlich sind, orientieren wir uns unter anderem an einer Entscheidung des Bundesgerichtshofes (BGHZ 47, 101 ff.). Nach ihr kann einem Versicherer nicht verwehrt werden, in Vordrucken alle Angaben zu verlangen, die er, abgestellt auf die Masse der Versicherungsfälle, nach seinen Erfahrungen für sachdienlich halten darf, um sich ein möglichst zuverlässiges Bild von dem für seine Leistung maßgeblichen Sachverhalt zu verschaffen. Fragebogen und Antragsvordrucke, die für Massenverfahren vorgehalten werden, tragen in der Regel das Problem in sich, dass nicht jeder Punkt für jeden Fall relevant ist.

Wir diskutieren derzeit mit einer Versicherungsgesellschaft die Frage, ob sie es ggf. unter Inkaufnahme eines höheren Verwaltungsaufwandes dem Versicherungsnehmer freistellen könnte, nur die Angaben in dem Fragebogen zu machen, die er aus seiner Sicht bei dem gegebenen Sachverhalt für notwendig ansieht.

Oft verweisen wir die Eingabeführer an die Bundesanstalt für Finanzdienstleistungsaufsicht oder an den Ombudsmann für die Versicherungswirtschaft. Soweit die Betroffenen auf diesen Wegen keine Lösung ihrer Probleme erreichen können, müssten sie den Zivilrechtsweg beschreiten.

4.2 Übermittlung von Daten der Versicherungsnehmer

4.2.1 Übermittlung an eine Wirtschaftsberatungsgesellschaft

Eine Versicherungsgesellschaft übermittelte Adressdaten von Versicherungsnehmern, deren Lebensversicherungsvertrag auslief, an eine Wirtschaftsberatungsgesellschaft zu Werbezwecken („Wiederanlageberatung“).

Als gesetzliche Grundlage für diese Datenübermittlung könnte das in § 28 Abs. 3 Satz 1 Nr. 3 BDSG verankerte Listenprivileg in Betracht kommen. Nach dieser

Bestimmung ist unter bestimmten Voraussetzungen eine Übermittlung für Zwecke der Werbung zulässig. Allerdings darf kein Grund zu der Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

In dem vorgetragenen Fall hatten die Versicherungsnehmer nach unserer Auffassung ein derartiges schutzwürdiges Interesse daran, dass die Tatsache ihrer frei werdenden Lebensversicherung nicht an Dritte weitergegeben wird. Mit der Offenbarung, dass die Betroffenen einen Lebensversicherungsvertrag bei dieser Versicherungsgesellschaft unterhalten, hat die Versicherungsgesellschaft einen besonderen Vertrauenstatbestand verletzt, der sogar in § 203 Abs. 1 Nr. 6 Strafgesetzbuch (StGB) strafbewehrt ist. Es kommt hinzu, dass ein Lebensversicherungsvertrag, der meist über hohe Summen abgeschlossen wird, indirekt auch Aufschluss über die finanziellen Verhältnisse geben kann.

Da somit § 28 Abs. 3 Satz 1 Nr. 3 BDSG als Rechtsgrundlage nicht in Frage kam und auch keine Einwilligung der Versicherungsnehmer zu dieser Datenübermittlung vorlag, haben wir das Vorgehen der Versicherungsgesellschaft beanstandet. Die Versicherung hat mitgeteilt, dass sie derartige Datenübermittlungen künftig unterlassen wird.

4.2.2 Übermittlung an den geschiedenen Ehemann

Ein Versicherungsvertreter erteilte nach der Scheidung eines Ehepaares dem Ex-Ehemann Auskunft über die neue Wohnanschrift der Ex-Ehefrau, die sie ihm zum Zwecke der weiteren Betreuung der bestehenden Versicherungsverträge mitgeteilt hatte.

Indem er die auf einem Datenträger gespeicherte Adresse der Betroffenen abgerufen und an ihren früheren Ehemann weitergegeben hat, hat der Versicherungsvertreter ein personenbezogenes Datum an einen Dritten übermittelt.

Für diese Datenübermittlung lag weder eine Einwilligung der Betroffenen vor noch kann sie durch eine Rechtsvorschrift gerechtfertigt werden.

Wir haben deshalb die Weitergabe der Adresse durch den Versicherungsvertreter als datenschutzrechtlich unzulässig beanstandet.

4.3 Hinweisdateien und Vorversichererabfrage

Bevor eine Versicherungsgesellschaft mit einem Neukunden einen Vertrag abschließt, prüft sie üblicherweise das für sie mit diesem Vertrag verbundene Risiko. Der Kunde muss deshalb nach § 16 Abs. 1 des Versicherungsvertragsgesetzes (VVG) in diesem Stadium alle ihm bekannten Umstände, die für die Übernahme der Gefahr erheblich sind, dem Versicherer anzeigen. Erheblich sind danach die Gefahrumstände, die geeignet sind, auf den Entschluss des Versicherers, den Vertrag überhaupt oder zu dem vereinbarten Inhalt abzuschließen, einen Einfluss auszuüben. Ein Umstand, nach welchem der Versicherer ausdrücklich und schriftlich gefragt hat, gilt nach dem VVG im Zweifel als erheblich.

In den Antragsformularen sind u. a. Angaben über frühere gleichartige Versicherungen verlangt. Die neue Versicherung möchte sich bei ihrer Risikoprüfung von dem Verhalten des Neukunden im Rahmen von früheren Versicherungsverträgen ein Bild machen. Sie möchte sich aber auch davon überzeugen, ob die Angaben des Neukunden zutreffen und vollständig sind.

Zu diesem Zweck haben die verschiedenen Versicherungssparten jeweils gemeinsame Hinweissysteme installiert. Es handelt sich dabei um Dateien, die nur Hinweise auf andere Versicherungsgesellschaften enthalten, die im Hinblick auf den Betroffenen eine Dateneinmeldung über bestimmte Sachverhalte bei bestehenden oder bei zwischenzeitlich beendeten Verträgen vorgenommen haben. Erhält die neue Versicherung von dort eine positive Auskunft, so kann sie die Umstände, die seinerzeit zur Vertragsbeendigung führten, erst durch eine weitere Nachfrage bei der Vorversicherung erfahren.

Die Zulässigkeit der Einmeldung der Versicherungen in eine derartige gemeinsame Auflistung sowie der folgenden Datenübermittlungen aus der Auflistung und von den Vorversicherungen beruht auf einer datenschutzrechtlichen Einwilligung der Versicherungsnehmer, die diese im Rahmen der Versicherungsverträge abgeben bzw. abgegeben haben.

4.4 Löschung von Daten bei Nichtzustandekommen eines Versicherungsvertrages

Im Falle der Ablehnung eines Versicherungsantrages durch ein Versicherungsunternehmen ist es häufig ein Anliegen der Antragsteller, dass alle eingereichten Unterlagen und bekannt gegebenen persönlichen Daten vernichtet bzw. gelöscht werden. Dies ist insbesondere im Bereich der Krankenversicherung der Fall, wenn ausführliche Angaben über den Gesundheitszustand gemacht wurden. Die Betroffenen fürchten dann eine zweckwidrige Verwendung der Gesundheitsdaten für die Beurteilung weiterer Versicherungen, z. B. Lebensversicherungen.

Der Anspruch des Betroffenen auf Löschung dieser gespeicherten Daten richtet sich nach § 35 BDSG. Nach dieser Bestimmung sind Daten, die für eigene Zwecke verarbeitet werden, zu löschen, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist.

Die Versicherungsgesellschaften unterliegen dem Handelsrecht. Nach dem Handelsgesetzbuch (§ 257 HGB) und nach den Vorschriften des Steuerrechts (vgl. § 147 Abs. 3 Abgabenordnung - AO) besteht für Handelsbriefe eine Aufbewahrungsfrist von sechs bzw. zehn Jahren. Wenn einer Löschung diese gesetzlichen Aufbewahrungsfristen entgegenstehen, tritt nach § 35 Abs. 3 Nr. 1 BDSG an die Stelle der Löschung eine Sperrung. Die Daten dürfen in gesperrtem Zustand ohne Einwilligung des Betroffenen nur unter den besonderen Voraussetzungen des § 35 Abs. 8 BDSG übermittelt oder genutzt werden. Falls der Betroffene in den Antragsformularen eine besondere Einwilligungserklärung zur Verarbeitung und Nutzung der Antragsdaten abgegeben hat, ist diese Einwilligung Rechtsgrundlage für eine weitere Verarbeitung oder Nutzung.

4.5 Die Allfinanzklausel

4.5.1 Einwilligung der Kunden

Die wirtschaftliche Entwicklung in den vergangenen Jahren hat verbreitet zur Bildung sog. Allfinanz-Gruppen geführt. In ihnen sind Banken, Versicherungen und Bausparkassen unter einem Konzerndach zusammengefasst. Man ist auf diese Weise in der Lage, die Kundenstämme der Konzernunternehmen in gezielte Werbemaßnahmen mit einzubeziehen. Den Kunden kann eine ganze Palette

von Finanz- und Versicherungsdienstleistungen rationell und kostengünstig angeboten werden.

Datenschutzrechtliche Voraussetzung für die Zulässigkeit einer derartigen über die Vertragsabwicklung hinausgehenden Verarbeitung und Nutzung bestimmter Kundendaten ist jedoch die gemäß § 4a BDSG formgerecht erteilte Einwilligung der Kunden.

Eine derartige Einwilligungserklärung lautet dann beispielsweise wie folgt:

„Ohne Einfluss auf den Vertrag und jederzeit widerrufbar willige ich weiter ein, dass personenbezogene Daten im Rahmen der regelmäßigen Kundenbetreuung, auch zu Finanzdienstleistungen, beim Vermittler oder der Gesellschaft gespeichert und den Vermittlern und anderen deutschen Gesellschaften der …….-Gruppe übermittelt werden können."

Allfinanzklauseln sind inzwischen in vielen Versicherungsverträgen enthalten, können aber entsprechend dem Wortlaut gestrichen bzw. nachträglich widerrufen werden, ohne dass dadurch das Zustandekommen bzw. Bestehen des Versicherungsvertrages berührt wird.

4.5.2 Streichung der Einwilligungserklärung

Ein Beschwerdeführer teilte uns mit, dass eine Versicherungsgesellschaft einen Vertragsabschluss über das Internet anbietet, bei dem alle Versicherungsbedingungen - einschließlich Allfinanzklausel - nur als Ganzes akzeptiert werden können. Er monierte, dass ihm dadurch die Möglichkeit genommen werde, der Nutzung seiner persönlichen Daten zu Werbezwecken für Finanzdienstleistungen zu widersprechen.

Bei unserer Überprüfung stellte sich heraus, dass der Versicherungsantrag online tatsächlich nur dann an das Versicherungsunternehmen gesendet werden kann, wenn allen Vertragsbestandteilen einschließlich der Allfinanzklausel durch Betätigen eines Buttons zugestimmt wurde. Allerdings weist die Versicherung darauf hin, dass diese Einwilligung jederzeit widerrufbar ist und auch bereits bei Vertragsschluss gestrichen werden kann. Die Streichung müsste in diesem Fall online in einem „für Anmerkungen" vorgesehenen Feld erklärt werden.

Wir baten die Versicherung, im Online-Antragsformular auf diese Möglichkeit ausdrücklich hinzuweisen.

4.6 Versicherungsdaten der Unternehmensangehörigen

Der Betriebsrat eines Versicherungsunternehmens wandte sich an uns, weil in dem Unternehmen die Mitarbeiter die Versicherungsdaten ihrer Kollegen, die mit ihrem Unternehmen Versicherungsverträge abgeschlossen haben, uneingeschränkt einsehen konnten.

Wir konnten in einem gemeinsamen Gespräch mit dem Betriebsrat und dem Datenschutzbeauftragten erreichen, dass die Versicherungsangelegenheiten der Unternehmensangehörigen in den einzelnen Abteilungen nur von wenigen ausgewählten Sachbearbeitern bearbeitet und dass enge Zugriffsbeschränkungen angeordnet werden. Auf diese Weise erhalten die Versicherungsdaten der Mitarbeiter den angemessenen Schutz, der in etwa mit dem Schutz der Personaldaten vergleichbar ist.

4.7 Zugriff zu online eingereichten Versicherungsanträgen

Wir wurden darauf hingewiesen, dass per Internet auf Kundendaten einer Versicherung zugegriffen werden konnte, und zwar auf online eingereichte Versicherungsanträge. Wir haben sofort mit dem Versicherungsunternehmen Kontakt aufgenommen, auf diese Sicherheitslücke hingewiesen und um Abhilfe gebeten.

Umgehend wurde von der Versicherung eine Reihe von Maßnahmen getroffen, um die Sicherheit der DV-Systeme zu verbessern. Unter anderem wurde ein externes Fachunternehmen mit der Verbesserung der Datensicherheit beauftragt.
Der TÜV Süd, der uns in Datensicherheitsfragen gemäß Art. 34 BayDSG unterstützt, stellte bei einer anschließenden Prüfung fest, dass unzulässige Internet-Zugriffe nicht mehr möglich waren.

* * *

5 Banken

Weil viele Bürger und Unternehmen ausschließlich oder überwiegend mit ihrer Hausbank zusammenarbeiten, besteht dort regelmäßig eine gute Kenntnis der wirtschaftlichen Verhältnisse und der finanziellen Leistungsfähigkeit der Kunden. Auf Grund des weit verbreiteten bargeldlosen Zahlungsverkehrs verfügen die Banken zusätzlich über vielfältige Informationen über ihre Kunden und deren Lebensgestaltung.

Trotz dieser umfangreichen, sensiblen Datenbestände halten sich die Datenschutzeingaben und -beschwerden in diesem Bereich in Grenzen. Das liegt wohl daran, dass die allgemeinen Datenschutzgesetze durch das von den Banken vertraglich den Kunden zugesicherte Bankgeheimnis ergänzt werden und dass das Personal eine vertrauliche Behandlung der sensiblen Kundendaten gewohnt ist.

Die bei uns im Berichtszeitraum eingegangenen Eingaben und Beschwerden über Banken richteten sich z. B. gegen Werbeschreiben, beanstandeten den fehlenden Hinweis auf das Werbewiderspruchsrecht oder die nicht erteilte Auskunft nach § 34 BDSG.

5.1 Kauf von Kundendaten einer insolventen Bank

Eine Bank kaufte Kundendaten von ehemaligen Kunden einer insolventen anderen Bank und sandte diesen Personen Werbung für ihre eigenen Angebote zu.

Wir haben dieses Vorgehen datenschutzrechtlich beanstandet, weil für die Datenübermittlung aus dem Bereich der insolventen Bank an die Empfängerbank keine Rechtsgrundlage nach dem BDSG gegeben war. Insbesondere stand einer Übermittlung gemäß § 28 Abs. 3 Satz 1 Nr. 3 BDSG das schutzwürdige Interesse der Betroffenen entgegen, weil in deren Bankverträgen das sog. Bankgeheimnis und daraus folgend eine Garantie, dass Daten nicht übermittelt werden, zugesichert war.

Wir baten deshalb die Bank, die Adressdaten zu löschen, soweit keine entsprechende Einwilligungserklärung der betroffenen Kunden vorlag.

5.2 Offene Übergabe von Kontoauszügen an Boten

Eine Bank händigte die Kontoauszüge einem Dritten aus, ohne sich vorher eine Empfangsvollmacht vorlegen zu lassen.

Der Datenschutzbeauftragte der Bank teilte mit, dass es sich wohl um ein Versehen im Einzelfall gehandelt hat. Das Personal wurde von ihm nochmals ausdrücklich darauf hingewiesen, dass neben der Übergabe von Kontoauszügen im verschlossenen Kuvert vom Abholer dann eine Vollmacht verlangt wird, wenn der Abholer nicht als Kontoinhaber oder sonst Berechtigter persönlich bekannt ist.

Damit wurden von Seiten der Bank geeignete Sicherheitsmaßnahmen dahingehend getroffen, dass nur berechtigte Personen Kontoauszüge erhalten.

* * *

6 Auskunfteien

Den Auskunfteien gilt das besondere Interesse des Datenschutzes. Schließlich bezieht sich ihre Haupttätigkeit auf die Erhebung, Speicherung und Übermittlung personenbezogener Daten. Handels- und Wirtschaftsauskunfteien sammeln Informationen über die wirtschaftliche Betätigung, die Kreditwürdigkeit und die Zahlungsfähigkeit von Unternehmen und von Privatpersonen.

Neben den großen, bundesweit tätigen Auskunftsdiensten gibt es auch kleinere Auskunfteien im regionalen Bereich. Auch im Internet werden diese Dienste angeboten.

Wirtschaftsauskunfteien dienen dem Schutz der Wirtschaft und der Allgemeinheit vor Kreditbetrug und vor Zahlungsausfällen. Das BDSG enthält in den §§ 29 ff. die rechtlichen Rahmenbedingungen für den Umgang dieser Branche mit personenbezogenen Daten. Danach ist eine Übermittlung von Daten dann zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zur Annahme besteht, dass der Betroffene ein berechtigtes Interesse an dem Ausschluss der Übermittlung hat.

Den Interessen der Betroffenen dienen vor allem ihre Auskunftsrechte (§ 34 BDSG) sowie ihre Rechte auf Berichtigung, Löschung und Sperrung von Daten (§ 35 BDSG) und die Verpflichtung der Auskunfteien, die Betroffenen von der ersten Übermittlung zu benachrichtigen (§ 33 BDSG).

Die automatisierten Datenverarbeitungen der Auskunfteien sind gemäß § 4d BDSG gegenüber der Datenschutzaufsicht meldepflichtig.

Um zu überprüfen, ob bei den Auskunfteien ein datenschutzgerechter Umgang mit den personenbezogenen Daten stattfindet, führen wir in regelmäßigen Abständen Kontrollen durch.

6.1 Datenerhebung

6.1.1 Nachbarschaftsbefragungen

Auskunfteien bedienen sich zur Beschaffung von Daten unterschiedlicher Informationsquellen. Im Rahmen einer Eingabe wurde vorgetragen, dass ein Mitarbeiter einer Auskunftei bei einer Nachbarin des Betroffenen telefonisch Informationen einholen wollte, ob und unter welcher Anschrift dieser einer Geschäftstätigkeit nachgeht. Auf Nachfrage der Nachbarin, warum er nicht gleich bei dem Betroffenen anrufe, teilte er mit, dass er dort niemanden erreichen konnte. Dies entsprach jedoch nicht der Wahrheit, denn die Nachbarin klingelte bei dem Betroffenen und übergab den Telefonhörer.

Nach dem in § 4 Abs. 2 Satz 1 BDSG verankerten Grundsatz der Direkterhebung sind personenbezogene Daten beim Betroffenen zu erheben. Das Vorliegen eines Ausnahmetatbestands nach § 4 Abs. 2 Satz 2 BDSG wurde von der Auskunftei nicht geltend gemacht.

Da eine sich auf Privatpersonen beziehende Nachbarschaftsbefragung allein zur Feststellung des Wohnsitzes als zulässig erachtet werden kann, nicht jedoch die o. g. Befragung, haben wir das Verhalten der Auskunftei beanstandet.

6.1.2 Weitergabe von Daten aus einem Inkassoverfahren an eine Auskunftei

Die Weitergabe von Daten aus einem Inkassoverfahren an Auskunfteien ist unter bestimmten Voraussetzungen zulässig. Zum einen muss unter Berücksichtigung des allgemeinen berechtigten Interesses der Wirtschaftsunternehmen, vor einem Forderungsausfall geschützt zu werden, festgestellt werden, dass kein schutzwürdiges Interesse des Betroffenen entgegen steht (§ 28 Abs. 3 Satz 1 Nr. 1 BDSG). Dies ist vor allem dann der Fall, wenn das Inkassounternehmen auf die Zahlungsunfähigkeit oder Zahlungsunwilligkeit des Betroffenen schließen kann. Eine derartige Situation kann z. B. bei insgesamt vier erfolglosen Mahnungen (zweimal durch den Gläubiger, zweimal durch das Inkassounternehmen) angenommen werden.

Darüber hinaus darf eine Datenweitergabe nur bei unbestrittenen Forderungen erfolgen. Bestreitet der Schuldner zu einem späteren Zeitpunkt die Forderung, ist

an die Auskunftei unverzüglich eine entsprechende Meldung zu übermitteln, die zur Sperrung der Daten führt. Erfolgt nach der Übermittlung ein Forderungsausgleich, ist dies der Auskunftei unverzüglich zu melden.

Ein Betroffener hatte die Zahlungsaufforderungen eines Inkassounternehmens nicht beachtet. Daraufhin wurde ihm vor Einleitung des gerichtlichen Mahnverfahrens eine letzte Gelegenheit zum Forderungsausgleich gegeben. In diesem Schreiben war ein Hinweis angebracht, dass die zu seiner Person gespeicherten Daten an die namentlich genannte Auskunftei zur Weitergabe an Dritte gemeldet werden, falls er bis zu einem bestimmten Zeitpunkt weder die Forderung bezahlt noch einen begründeten Einwand vorbringt. Der Betroffene erkundigte sich bei der Aufsichtsbehörde, ob eine derartige „Drohung“ rechtmäßig ist.

Wir teilten ihm mit, dass die Datenweitergabe an die Auskunftei korrekt wäre, da die oben beschriebenen Voraussetzungen in seinem Fall gegeben waren.

6.2 Unrichtige Daten

6.2.1 Personenverwechslungen

Personenverwechslungen sind bei Auskunfteien immer wieder anzutreffen. Auslöser ist meistens eine Namensgleichheit, z. B. Vater und Sohn wohnen im gleichen Haus, oder eine Namensähnlichkeit. Wird einer Auskunftei bekannt, dass namensgleiche oder sonst verwechslungsgefährdete Personen in ihrer Datei gespeichert sind, muss sie entsprechende Vorkehrungen treffen, um eine Verwechslung zu vermeiden.

Ein Beschwerdeführer bekam von einem Unternehmen, mit dem er bereits in längerer Geschäftsverbindung stand, eines Tages die Mitteilung, dass er künftig nur noch per Nachnahme beliefert werden könne. Da er sich nicht vorstellen konnte, warum sich seine Bonität verschlechtert haben könnte, wandte er sich an die Aufsichtsbehörde.

Im Rahmen unserer Überprüfungen stellte sich heraus, dass das Unternehmen bei einer Auskunftei nachgefragt hatte, ob dort Negativdaten des Kunden vorliegen. Die Auskunftei hat dies bestätigt, hat aber dabei auf Grund des fast identischen Namens und der gleichen Wohnanschrift den Vater mit dem Sohn ver-

wechselt. So war es zu einer unrichtigen Zuordnung und damit unzulässigen Speicherung von Negativdaten gekommen.

Auf Grund unseres Einschreitens wurde die unrichtige Datenspeicherung bei der Auskunftei und bei der Vertragspartnerin des Beschwerdeführers berichtigt (§ 35 Abs. 1 BDSG). Die Geschäftsbeziehung konnte wie bisher auf der Basis „Lieferung gegen Rechnung“ fortgeführt werden.

Die Auskunftei haben wir aufgefordert, künftig Identitätsprüfungen sorgfältiger vorzunehmen. Dabei haben wir auch auf das Risiko von Schadensersatzverpflichtungen hingewiesen (§ 7 BDSG).

In einem anderen Fall beschwerte sich eine Betroffene, dass es trotz einer bereits vor mehreren Jahren erfolgten Personenverwechslung und der Zusicherung, einen entsprechenden Bearbeitungsvermerk anzubringen, wieder zu einer Personenverwechslung gekommen ist. Die beiden verwechselten Personen besitzen denselben Namen und das gleiche Geburtsdatum.

Bei der Überprüfung stellte sich heraus, dass der damals eingetragene Bearbeitungsvermerk, der eine weitere Verwechslung vermeiden sollte, irrtümlich bei einer Prüf- und Löschroutine gelöscht wurde. Deshalb lag zum Zeitpunkt der Erteilung der Auskunft kein Hinweis auf die fehlende Identität der betroffenen Person mit der namensgleichen Person mehr vor, was wieder zur Verwechslung führte. Der Bearbeitungshinweis wurde nunmehr erneut gesetzt. Der Auskunftsempfänger wurde über die Berichtigung der Daten informiert.

Zu beachten ist in diesem Fall auch, dass die Auskunftsempfänger gegenüber der Auskunftei i. d. R. vertraglich verpflichtet sind, die Identität der betroffenen Person zu überprüfen. Soweit dabei die Identität nicht eindeutig festgestellt werden kann, unterliegt die Auskunft einem absoluten Nutzungsverbot, bis die Sache geklärt ist (z. B. durch Rückfrage beim Betroffenen).

Wir haben die Auskunftei gebeten, in Zukunft dafür Sorge zu tragen, dass die entsprechenden Bearbeitungshinweise bei den notwendigen Prüf- und Löschroutinen zuverlässig bestehen bleiben. Sofern wir feststellen sollten, dass diese Verpflichtung nicht eingehalten wird, würden wir weitere aufsichtliche Maßnahmen gegen die Auskunftei ergreifen.

6.2.2 Auf Vermutungen beruhende Daten

Eine Auskunftei hat in den Datensatz einer Betroffenen ein unrichtiges Bankkonto aufgenommen. Sie hatte vermutet, die Betroffene würde ihr Konto bei einer ortsansässigen Bank unterhalten, was jedoch nicht den Tatsachen entsprach.

Die Speicherung unrichtiger Daten beeinträchtigt ebenso wie die spätere Übermittlung schutzwürdige Interessen der Betroffenen. Da somit die tatbestandlichen Voraussetzungen der Absätze 1 und 2 des § 29 BDSG für die genannten Datenverwendungen nicht vorliegen, sind diese unzulässig.

Die Auskunftei hat auf den entsprechenden Hinweis der Betroffenen das unrichtige Datum gelöscht und durch die richtige Angabe „Eine Bankverbindung ist nicht bekannt“ ersetzt. Diese Korrektur wurde dem Auskunftsempfänger unverzüglich nachgemeldet.

Wir haben die Auskunftei aufgefordert, Daten, die nur auf Vermutungen basieren, künftig nicht mehr zu speichern.

6.2.3 Schätzdaten

Von den Auskunfteien werden zuweilen auch Schätzdaten verwendet. So werden in den Fällen, in denen nicht alle für die Bonität relevanten Daten erhoben werden können, geschätzte Zahlenwerte in die Datensätze aufgenommen. Dabei zieht man z. B. für die Umsatzzahlen den Branchendurchschnitt heran.

Die Übermittlung von Schätzdaten ist nur dann zulässig, wenn diese als Schätzdaten gekennzeichnet sind. Bei Schätzdaten handelt es sich in den meisten Fällen zwangsläufig um unrichtige Daten. Bei der Übermittlung solcher Daten sind ohne eine entsprechende Angabe schutzwürdige Interessen des Betroffenen beeinträchtigt, da der Eindruck erweckt wird, es handle sich um gesicherte Erkenntnisse. Die sich daraus gemäß § 29 Abs. 2 Satz 1 Nr. 2 BDSG ergebende Unzulässigkeit der Übermittlung kann nur durch eine entsprechende Kennzeichnung vermieden werden.

Der Verband der Handelsauskunfteien teilt diese Rechtsauffassung allerdings nicht. Nach seiner Meinung reicht es aus, wenn jede Auskunft einen Hinweis enthält, dass ein Teil der Angaben auf Schätzungen beruhen kann. Die Verhandlungen der Arbeitsgruppe Auskunfteien mit dem Verband dauern an.

6.3 Berechtigtes Interesse des Auskunftsempfängers

Derjenige, der von einer Auskunftei Daten übermittelt bekommt, muss nach § 29 Abs. 2 Satz 1 Nr. 1 BDSG ein berechtigtes Interesse dargelegt haben.

Zur Verhinderung von Missbrauchsfällen wird das Vorliegen des berechtigten Interesses sowohl durch die Auskunfteien selbst als auch durch die Datenschutzaufsichtsbehörden in Einzelfällen stichprobenartig dahingehend nachgeprüft, ob zu dem bei der Auskunftseinholung geltend gemachten Interesse auch ein realer Hintergrund besteht.

Zuweilen stellen wir bei Datenschutzkontrollen fest, dass das vom Anfragenden für eine Wirtschaftsauskunft dargelegte berechtigte Interesse für die Auskunft bei der stichprobenmäßigen Nachprüfung nicht zweifelsfrei belegt wird, ohne dass von seiten der Auskunftei nachgehakt wird. Hier fordern wir für die Zukunft, dass die Auskunftei nur schlüssige Erläuterungen der anfragenden Stelle anerkennt.

Ein Unternehmer hatte sich über eine Kundenreklamation geärgert und wollte in diesem Zusammenhang wissen: „Was ist das für ein Mensch?“. Er holte über den Betroffenen eine Wirtschaftsauskunft ein und machte dabei ein in Wahrheit nicht vorliegendes kreditorisches Risiko geltend.

Auf Grund der Benachrichtigung gemäß § 33 Abs. 1 BDSG erfuhr dieser von der Auskunftei, dass über ihn eine Wirtschaftsauskunft erteilt worden ist und wandte sich an die Aufsichtsbehörde. Wir konnten den Sachverhalt aufklären und haben den Unternehmer beanstandet.

In einem anderen Fall hatte ein ausgeschiedener Mitarbeiter eines Unternehmens die üblichen geschäftlichen Kontakte zu einer Auskunftei genutzt, um für private Zwecke eine Wirtschaftsauskunft einzuholen. Für die Auskunftei war dies nicht erkennbar, weil der Anfragende ihr gegenüber in der üblichen geschäftli-

chen Art und Weise aufgetreten ist und ein berechtigtes Interesse geltend gemacht hat.

Wir haben uns in diesem Fall mit dem Unternehmen und der Auskunftei in Verbindung gesetzt und darum gebeten, Maßnahmen zu ergreifen, die ein derartiges unberechtigtes Einholen von Wirtschaftsauskünften künftig verhindern oder zumindest wesentlich erschweren können.

6.4 Benachrichtigung des Betroffenen

Werden personenbezogene Daten von einer Auskunftei ohne Kenntnis des Betroffenen gespeichert, ist dieser gemäß § 33 Abs. 1 Satz 2 BDSG von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Ausnahmen ergeben sich aus dem Abs. 2 dieser Bestimmung.

Bei unseren Kontrollen fällt uns immer wieder auf, dass Auskunfteien den Zeitpunkt der Benachrichtigung zu weit hinausschieben. So sehen wir eine Benachrichtigung erst vier Wochen nach einer Datenübermittlung als nicht dem Gesetzeszweck entsprechend an. Eine Benachrichtigung muss vielmehr innerhalb von zwei Wochen erfolgen.

6.5 Auskunftsanspruch des Betroffenen

Betroffene können von Auskunfteien gemäß § 34 Abs. 2 BDSG Auskunft über ihre personenbezogenen Daten verlangen unabhängig davon, ob die Daten in einer Datei gespeichert sind. Einen Anspruch auf Auskunft über Herkunft und Empfänger haben sie nur, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt.

Viele Eingabeführer beschwerten sich darüber, dass die betroffenen Unternehmen die erforderlichen Auskünfte auf Herkunft und Empfänger ihrer Daten (§ 34 BDSG) nicht oder nur unzureichend erteilen würden. Oft wurde dies auf unsere Aufforderung hin unverzüglich nachgeholt.

In einigen anderen Fällen blieben die Auskunfteien bei ihrer Weigerung und begründeten dies damit, dass ihr Interesse an der Wahrung des Geschäftsgeheim-

nisses überwiege. Bei einigen Beschwerden hatte der Kunde der Auskunftei größten Wert darauf gelegt, gegenüber dem Betroffenen nicht genannt zu werden. Bei anderen Beschwerden haben die Betroffenen gegenüber den Auskunfteien nicht substantiiert begründet, weshalb Sie die Auskunft verlangen.

Bei der Prüfung der Frage, ob die Auskunftsverweigerung rechtmäßig ist, ist zwischen den Interessen der Auskunftei und des Betroffenen abzuwägen. Unsere Verhandlungen mit den Auskunfteien in Einzelfällen haben vielfach dazu geführt, dass die Betroffenen schließlich doch erfahren konnten, wer über sie eine Wirtschaftsauskunft eingeholt hatte. In den wenigen übrigen Fällen, in denen eine Auskunftei zu Recht die Information über den Datenempfänger verweigern durfte, konnte dem Betroffenen zumindest mitgeteilt werden, dass nach neutraler Prüfung durch die Aufsichtsbehörde keine Anhaltspunkte für einen Missbrauchsfall vorliegen.

In letzter Zeit wurde zwischen dem Verband der Handelsauskunfteien und den obersten Datenschutzaufsichtsbehörden eine Absprache dahin gehend erzielt, dass einem Betroffenen künftig dann der konkrete Datenempfänger mitzuteilen ist, wenn er entweder ein begründetes Interesse an der Kenntnis des Datenempfängers geltend machen kann oder der Datenempfänger einer Branche angehört, bei der die Zusammenarbeit mit Auskunfteien allgemein bekannt ist. Hierzu zählen z. B. Versandhandel, Telekommunikationsunternehmen und Banken. In den übrigen Fällen erfolgt eine Einzelfallprüfung durch die Auskunftei.

6.6 Anspruch des Betroffenen auf Löschung seiner Daten

Auskunfteien lehnen es immer wieder ab, personenbezogene Daten zu löschen. Die Betroffenen waren von der erstmaligen Übermittlung ihrer Daten benachrichtigt worden und wollten daraufhin ihre Daten aus dem Bestand der Auskunfteien gelöscht haben. Häufig handelt es sich dabei um negative Informationen über den Betroffenen.

Ein Anspruch auf Löschung von Daten besteht nach § 35 Abs. 2 Satz 2 Nr. 1 BDSG gegenüber Auskunfteien dann, wenn die Speicherung der Daten unzulässig ist. Die Speicherung ist aber - und zwar ohne Einwilligung des Betroffenen - zulässig nach § 29 Abs. 1 Satz 1 Nr. 1 BDSG, wenn kein Grund zu der Annahme

besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat. Ein schutzwürdiges Interesse würde der Speicherung z. B. dann entgegenstehen, wenn unrichtige Daten oder Daten, die für die Beurteilung der Bonität nicht relevant sind, gespeichert würden. In allen anderen Fällen wird anerkannt, dass auch bei negativen Daten kein Grund zu der Annahme besteht, dass schutzwürdige Interessen des Betroffenen der Speicherung entgegenstehen könnten. Das Interesse, trotz schlechter Bonität weitere Bestellungen tätigen oder neue Kredite eingehen zu können, ist nicht schutzwürdig.

Personenbezogene Daten sind von Auskunfteien auch dann zu löschen, wenn es sich um Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann (§ 35 Abs. 2 Satz 2 Nr. 2 BDSG).

Ein weiterer Anspruch gegenüber Auskunfteien auf Löschung der Daten besteht, wenn eine Prüfung jeweils am Ende des vierten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, dass eine länger währende Speicherung nicht erforderlich ist (§ 35 Abs. 2 Satz 2 Nr. 4 BDSG). Die Auskunfteien müssen danach regelmäßig ihre Datenbestände durchforsten und nicht mehr benötigte Informationen entfernen.

Für Daten, die aus dem Schuldnerverzeichnis eines Vollstreckungsgerichts übernommen sind, haben die Auskunfteien spezielle Löschungsfristen, die in der Zivilprozessordnung (ZPO) und der Schuldnerverzeichnisverordnung (SchuVVO) geregelt sind, vorrangig anzuwenden. Nach § 15 Abs. 1 SchuVVO haben die Auskunfteien die Löschung der Eintragungen aus dem Schuldnerverzeichnis nach der ZPO eigenverantwortlich durchzuführen. Gemäß § 915g i. V. m. § 915a ZPO sind Eintragungen im Schuldnerverzeichnis nach Ablauf von drei Jahren seit dem Ende des Jahres zu löschen, in dem die eidesstattliche Versicherung abgegeben, die Haft angeordnet oder die sechsmonatige Haftvollstreckung beendet worden ist. Eine Information aus dem Schuldnerverzeichnis wird u. a. vorzeitig gelöscht, wenn die Befriedigung des Gläubigers nachgewiesen ist.

* * *

7 Handel, Dienstleistung

7.1 Kundenbindungsprogramme

Nach der Aufhebung des Rabattgesetzes und der Zugabeverordnung hat sich für den Einzelhandel der Spielraum für die Einräumung von Rabatten und für Sonderaktionen erweitert. Viele Unternehmen versuchen deshalb, mit den sogenannten Rabatt- oder Kundenkarten die Kunden an sich zu binden. Marktführende Unternehmen verschiedenster Branchen haben sich zu Kundenbindungsprogrammen zusammengeschlossen und bieten in diesem Rahmen gemeinsam eine Kundenkarte an. Nach den Veröffentlichungen der letzten Zeit schwanken die Schätzungen der Zahl der derzeit in Deutschland ausgegebenen Karten zwischen 22 und 70 Millionen.

Neben der Kundenbindung durch Rabatt- oder Prämiengewährung geht es den Unternehmen auch darum, Informationen über ihre Kunden zu bekommen und damit die Anonymität aufzuheben. Dies beginnt bei der Auswertung der auf den Antragsformularen eingetragenen Stammdaten und geht hin bis zur Nutzung der Bewegungsdaten, aus denen sich das Einkaufsverhalten der einzelnen Personen ergibt. Die gewonnenen Daten eignen sich für Zwecke der Werbung und Marktforschung ebenso wie für die Erstellung von weit gehenden Kundenprofilen (Stichwort „Gläserner Verbraucher“).

Aus der Sicht des Datenschutzes sind diese Kundenbindungssysteme dahin gehend zu kontrollieren, ob sie mehr Daten über ihre Kunden sammeln und auswerten als für die Durchführung der jeweiligen Rabatt- und Bonusprogramme erforderlich ist (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Soweit dies der Fall ist oder wenn die Daten auch für Zwecke der Werbung oder der Marktforschung verarbeitet oder genutzt werden, ist dies nur zulässig, wenn die Kunden rechtwirksam eingewilligt haben (§§ 4, 4a BDSG).

Die Datenschutzaufsicht in Bayern befasst sich ebenso wie die anderen Aufsichtsbehörden von Anfang an, d. h. seit dem Jahr 2000, mit den bei den einzelnen Systemen auftretenden datenschutzrechtlichen Fragen. Es fanden auch immer wieder Abstimmungen zwischen einzelnen Behörden und im gemeinsamen Gremium der obersten Aufsichtsbehörden, dem „Düsseldorfer Kreis“, statt.

In unserem Zuständigkeitsbereich haben wir bisher keine schwer wiegenden Verstöße gegen datenschutzrechtliche Vorschriften festgestellt. Auch die Zahl der Eingaben und Beschwerden zu den Kundenbindungssystemen ist mit 21 seit dem Jahr 2000 verschwindend gering im Verhältnis zu der im zweistelligen Millionenbereich liegenden Zahl der ausgegebenen Karten.

Allerdings muss bei einigen Systemen die Verwendung der Daten für den Kunden wesentlich transparenter dargestellt werden. Dies gilt insbesondere für die inhaltliche und textliche Gestaltung der Antragsformulare und der Hinweise zum Datenschutz. Die Kunden müssen über die Datenverwendung besser informiert und aufgeklärt werden, damit sie sich darüber im Klaren sein können, was mit ihren Daten geschieht.

Darüber hinaus entsprechen die in den Antragsformularen vorformulierten Einwilligungserklärungen im Bezug auf schriftliche Werbung und Marktforschung oft noch nicht den strengen Anforderungen des § 4a Abs. 1 BDSG. Unter anderem ist nach dieser Bestimmung die Einwilligung, wenn sie zusammen mit anderen Erklärungen schriftlich erteilt werden soll, besonders hervorzuheben. Soweit in der Einwilligungsklausel die Möglichkeit einer Streichung vorgesehen ist, ist deutlich darauf hinzuweisen.

Bezüglich der inhaltlichen und formalen Anforderungen an diese Erklärungen besteht seit November 2003 Übereinstimmung unter der überwiegenden Mehrheit der obersten Datenschutzaufsichtsbehörden. Einige der in Bayern ansässigen Kundenbindungsprogramme modifizieren derzeit ihre Formulare in diesem Sinne.

7.2 Besucherregistrierung auf offenen Messen

Bei einer offenen Messe wurden personenbezogene Daten aller Besucher registriert, d. h. erhoben und gespeichert. Ohne diese Angaben konnte man die Messe nicht besuchen. Man wollte mit Hilfe dieser Daten die einzelnen Besucher an den Messeständen interessengerecht ansprechen und betreuen. Darüber hinaus verfolgte man den Zweck, ihnen auch im Nachhinein zielgruppengerechtes Werbe- und Informationsmaterial zusenden zu können.

Für offene Messen lässt sich eine zwangsweise Besucherregistrierung aus dem BDSG nicht rechtfertigen. Eine derartige Datenerhebung ist nicht erforderlich. Sie dient nicht der Zweckbestimmung des Vertragsverhältnisses zwischen Messeveranstalter und Besucher (vgl. § 28 Abs. 1 Satz 1 Nr. 1 BDSG).

Eine Registrierung eines Messebesuchers auf Grund einer wirksamen freiwilligen Einwilligung (§ 4 Abs. 1, § 4a BDSG) ist jedoch denkbar. Bei der Erhebung der Messebesucherdaten im Rahmen der freiwilligen Registrierung sind allerdings die Informationspflichten gegenüber den Betroffenen aus § 4 Abs. 3 BDSG zu berücksichtigen (informierte Einwilligung). Wir haben noch während der Messe, nachdem wir von der Registrierung erfahren hatten, von den betroffenen Messeorganisatoren gefordert, die Registrierung deutlich auf eine freiwillige Basis zu stellen. Die Messebetreiber haben daraufhin unverzüglich das Verfahren geändert.

Werden Vergünstigungen, wie Vorverkaufsrabatt, Freikarte usw., von einer Registrierung abhängig gemacht, bestehen dagegen keine datenschutzrechtlichen Bedenken.

7.3 Registrierung vor der kostenlosen Nutzung einer CD-ROM

Einer Computerzeitschrift war, wie so oft, eine CD-ROM mit Computerprogrammen beigelegen. Nach einer entsprechenden Registrierung des Interessenten gab ihm der Vertreiber dieses Computerprogramms die Möglichkeit, das Programm kostenlos zu nutzen.

Gegen das Registrierungsverfahren und die dabei von ihm angeforderten personenbezogenen Daten wandte sich ein Beschwerdeführer. Er war der Meinung, dass ihm eine Nutzung der Software auch ohne Registrierung möglich sein müsse.

Hier konnten wir dem Betroffenen nicht weiterhelfen. Im Rahmen der allgemeinen Vertragsfreiheit kann jedes Unternehmen die Bedingungen für die kostenlose Nutzung seines Produkts im Rahmen der Gesetze selbst festlegen. Auf der anderen Seite steht es jedem Interessenten frei, auf bestimmte Bedingungen einzugehen oder nicht.

7.4 Verkauf einer ungelöschten Festplatte

Der Käufer einer Festplatte teilte uns mit, dass er statt einer neuen Festplatte nur eine reparierte gebrauchte Festplatte erhalten habe und dass auf der Festplatte noch die privaten Dateien des früheren Eigentümers enthalten sind, z. B. Online-Banking-Aktivitäten, private Urlaubsfotos, der gesamte E-Mail-Verkehr usw.

Wir haben uns unverzüglich mit dem betreffenden Unternehmen in Verbindung gesetzt und auch polizeiliche Ermittlungen angestoßen. Von Seiten des Unternehmens wurde uns berichtet, dass dort zwar eine Anordnung zur vollständigen Löschung von übernommenen gebrauchten Festplatten bestehe. In dem Einzelfall sei jedoch wohl durch ein Versehen eines Mitarbeiters eine ungelöschte Festplatte in die Reparatur und den Wiederverkauf gelangt.

Wir haben den Sachverhalt bei dem Unternehmen beanstandet.

Der Verkauf einer gebrauchten ungelöschten Festplatte mit personenbezogenen Daten stellt eine Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG dar. Es handelt sich um eine fahrlässige unbefugte Übermittlung personenbezogener Daten. Weil sich nicht mehr aufklären ließ, wer von den Mitarbeitern des Unternehmens für die Löschung der Festplatte verantwortlich war, musste das Bußgeldverfahren eingestellt werden.

* * *

8 Werbung, Adressenhandel

Die unterschiedlichen Werbeformen werden von der Rechtsprechung zum Verbraucherschutz je nach „Belästigungsgrad“ verschieden behandelt. Während die klassische personalisierte Briefwerbung grundsätzlich als zulässig angesehen wird, solange der Betroffene dem nicht widersprochen hat, muss für andere Mittel wie Telefonwerbung, Faxwerbung und E-Mail-Werbung wegen des stärkeren Eindringens in den privaten Lebensbereich (Telefonwerbung) oder wegen des beim Empfänger notwendigen Aufwandes für den Empfang und die Auswertung (Faxwerbung, E-Mail-Werbung) das vorherige Einverständnis des Betroffenen hierzu vorliegen.

Der Gesetzgeber hat mit § 28 Abs. 3 Satz 1 Nr. 3 BDSG die Übermittlung oder Nutzung von bestimmten Daten zu Werbezwecken zwar ausdrücklich zugelassen, jedoch den Betroffenen gleichzeitig mit Rechten ausgestattet, um sich gegen die Zusendung von unerwünschter Werbung zur Wehr zu setzen. Hierzu gehören das Recht auf Auskunft über gespeicherte Daten sowie deren Herkunft (§ 34 Abs. 1 BDSG) und das Recht auf Widerspruch gegen die Verwendung der Daten zu Werbezwecken (§ 28 Abs. 4 BDSG). Der Werbende ist verpflichtet, auf persönlich adressierter Werbung einen Hinweis auf das Widerspruchsrecht anzubringen.

Durch unerwünschte Direktwerbung in ihren unterschiedlichen Ausgestaltungen fühlen sich viele Bürger belästigt. In den Fällen der „klassischen“ Briefwerbung kommt es immer wieder vor, dass die Betroffenen trotz der ihnen nach dem BDSG zustehenden Rechte bei dem Versuch, Auskunft über die Herkunft der Daten zu erhalten bzw. die Zusendung persönlich adressierter Werbeschreiben einstellen zu lassen, nicht weiterkommen und daher die Datenschutzaufsichtsbehörde einschalten. Jährlich wenden sich ca. 50 Personen mit solchen Anliegen an uns. Auf unsere Intervention hin reagieren die Unternehmen in aller Regel.

8.1 Telefon-, Fax- und E-Mail-Werbung

Nahezu täglich erreichen uns Beschwerden und Anfragen zu diesem Thema, wobei gerade in den letzten beiden Jahren die unverlangten E-Mails, sog. Spams, geradezu sintflutartig auf die Bevölkerung hereinzubrechen scheinen. So traten viele Betroffene an uns mit der Bitte heran, diesem Treiben ein Ende zu

setzen bzw. ihnen bei der Durchsetzung ihres Auskunftsanspruches nach dem BDSG gegenüber dem Urheber der E-Mail-Zusendung behilflich zu sein. Verständlicherweise wollten die Betroffenen, die in der überwiegenden Mehrheit der Fälle bislang in keiner geschäftlichen Beziehung mit dem Werbenden standen, in Erfahrung bringen, welche personenbezogenen Daten der Absender der E-Mail über sie gespeichert hat bzw. woher dieser die personenbezogenen Daten erhalten hat.

Hierzu ist zunächst festzustellen, dass es sich hier nur nachrangig um ein datenschutzrechtliches Problem handelt. Nach der herrschenden Rechtsprechung verstößt die unverlangte Telefon-, Fax- und E-Mail-Werbung gegenüber Privaten gegen das Gesetz gegen den unlauteren Wettbewerb (UWG) und ist bereits aus diesem Grund unzulässig. Eine derartige Werbung darf somit nur mit ausdrücklicher vorheriger (!) Einwilligung des Empfängers erfolgen. Wir verweisen die Beschwerdeführer deshalb auch an die Verbraucherschutzverbände und auf die Möglichkeit, gegen die Werbenden einen Unterlassungs- bzw. einen Schadensersatzanspruch geltend zu machen.

Von Seiten des Datenschutzes können wir die betroffenen Bürger nur insoweit unterstützen, als es um die Verwendung ihrer Daten durch den Werbetreibenden geht. Wenn uns der für die Werbung Verantwortliche bekannt ist und seinen Sitz in Bayern hat können wir in solchen Fällen prüfen, ob die Daten beim Versender zulässigerweise gespeichert sind und ob der Auskunftsanspruch des Betroffenen zu den gespeicherten Daten und deren Herkunft gemäß § 34 BDSG ordnungsgemäß erfüllt worden ist. Darüber hinaus kontrollieren wir, ob bei der Werbeansprache auf das Widerspruchsrecht hingewiesen wurde und ob der von einem Betroffenen gemäß § 28 Abs. 4 Satz 1 BDSG erhobene Werbewiderspruch von der verantwortlichen Stelle beachtet wird.

Auf diesem Wege konnten wir dafür sorgen, dass vielen Beschwerden abgeholfen wurde. Die Absender haben die betreffende E-Mail-Adresse in eine entsprechende Sperrdatei aufgenommen und dem Betroffenen versichert, dass er künftig keine unerwünschte E-Mail mehr erhalten wird. Entsprechendes gilt für den Bereich der Telefon- und Faxwerbung.

Befindet sich der für die Werbung Verantwortliche außerhalb Bayerns, wird von uns die örtlich zuständige Aufsichtsbehörde eingeschaltet.

8.2 Adressmittlungsverfahren

Ein Versicherungsunternehmen, mit dem der Eingabeführer bisher keine Geschäftskontakte unterhalten hatte, war mittels persönlich adressierter Werbung für ein Versicherungsprodukt an ihn herangetreten. Dabei entstand beim Beworbenen der Eindruck, dass das Unternehmen seine Adressdaten einschließlich seines Geburtsdatums kennt, denn in dem Werbeschreiben wurde auf den in nächster Zeit bevorstehenden Geburtstag Bezug genommen. Die von ihm angenommene Datenweitergabe hat jedoch nicht stattgefunden. Vielmehr wurde hier ein sogenanntes Adressmittlungsverfahren durchgeführt.

Da nach den Regelungen des BDSG die Übermittlung von Kundendaten für Werbezwecke eingeschränkt ist (vgl. § 28 Abs. 3 Satz 1 Nr. 3 BDSG), wählen die Unternehmen statt einer Datenübermittlung oft das umgekehrte Verfahren. Dabei gibt das werbende Unternehmen das zu versendende Werbematerial einem anderen Unternehmen, an dessen Adressenbestand die Werbeschreiben gehen sollen. In diesem Zusammenhang kann der Adressenbestand entsprechend den Vorgaben des Auftraggebers nach bestimmten Merkmalen selektiert werden. Das adressenbesitzende Unternehmen setzt die ausgewählten Adressdaten auftragsgemäß in das fremde Werbematerial ein und gibt die Werbesendungen direkt zur Post. Das werbende Unternehmen erfährt - für Abrechnungszwecke - nur die Gesamtzahl der Personen, an die sein Werbematerial geschickt worden ist, nicht jedoch die einzelnen Daten der Betroffenen. Erst wenn der Betroffene auf die Werbesendung hin reagiert und z. B. mit Hilfe der übersandten Antwortkarte Informationsmaterial anfordert, erfährt das werbende Unternehmen die personenbezogenen Daten von dem Betroffenen selbst.

Eine Übermittlung von Daten des adressbesitzenden Unternehmens an das werbende Unternehmen findet bei dem Adressmittlungsverfahren nicht statt. Aus datenschutzrechtlicher Sicht ist eine derartige Werbeaktion somit nicht zu beanstanden.

In dem hier geschilderten Fall ist die Werbeaussendung nach diesem Schema abgelaufen. Dabei hat der Adresseneigner im Auftrag des Versicherungsunternehmens dessen Werbematerial beschriften und an seine eigenen Kundenadressen, selektiert nach den in nächster Zeit bevorstehenden Geburtstagen, versenden lassen. Dem adressbesitzenden Unternehmen hatten die Betroffenen ihr Geburtsdatum im Rahmen einer Geschäftsbeziehung freiwillig mitgeteilt.

8.3 Information des Betroffenen über Herkunft der Adressdaten

Eine Versicherungsagentur konnte einem Bürger die Frage nach der Herkunft seiner für eine Werbemaßnahme verwendeten Adresse nicht beantworten.

Aufgrund der Nennung der möglichen Adressenquellen für den bestimmten Sachverhalt konnten wir zwar feststellen, dass die Werbeadressen auf datenschutzrechtlich zulässige Weise bei großen Adressenhändlern beschafft wurden. Für den konkreten Fall war es jedoch nicht möglich, den bestimmten Adressenhändler festzustellen. Die Versicherungsagentur hatte die Adressen nach der Bearbeitung sofort gelöscht und konnte somit deren Herkunft nicht mehr nachvollziehen.

Nach § 28 Abs. 4 Satz 2 Halbsatz 2 BDSG hätte die Versicherungsagentur, da sie personenbezogene Daten nutzt, die bei einer dem Betroffenen nicht bekannten Stelle gespeichert sind, auch sicherstellen müssen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. In der Praxis geschieht dies durch eine Kennzeichnung der Werbeschreiben mit einer Ziffern-/Buchstabenkombination, mit der der Werbetreibende die konkrete Werbemaßnahme sowie die Herkunft der dafür verwendeten Adressdaten feststellen kann.

Da die Versicherungsagentur die genannte Rechtsvorschrift nicht beachtet hat, haben wir ihr gegenüber eine Beanstandung ausgesprochen.

* * *

9 Internationaler Datenverkehr

Wenn ein deutsches Unternehmen personenbezogene Daten an ein außerhalb des EU- und EWR-Raumes (also in einem Drittland) gelegenes Unternehmen übermitteln will, z. B. weil dieses die Personalverwaltung zentral für alle zu einem Konzern gehörenden Unternehmen erledigt (Übermittlung von Mitarbeiterdaten) oder weil es für das deutsche Unternehmen Marketingmaßnahmen durchführt (Übermittlung von Kundendaten), stellt sich die Frage, unter welchen Voraussetzungen die Übermittlung zulässig ist.

Zunächst müssen bei Datenübermittlungen in Drittländer immer die Voraussetzungen, die auch bei Datenübermittlungen im Inland gegeben sein müssen, also die §§ 4, 4a bzw. 28 ff. BDSG vorliegen. Fehlt es daran, so scheidet eine Datenübermittlung in ein Drittland bereits aus diesem Grunde aus.

Liegen die Voraussetzungen der §§ 4, 4a bzw. 28 ff. BDSG vor, sind die besonderen Vorschriften für die Datenübermittlung an Stellen außerhalb des EU- und EWR-Raums zu beachten (§ 4b Abs. 2 bis 6, § 4c BDSG). Es gilt der Grundsatz, dass Datenübermittlungen in Drittländer nur zulässig sind, wenn bei den empfangenden Stellen ein angemessenes Datenschutzniveau gewährleistet ist. Hiervon ist dann stets auszugehen, wenn die Europäische Kommission gemäß Art. 25 Abs. 6 EG-Datenschutzrichtlinie eine positive Entscheidung für ein bestimmtes Land getroffen hat. Bisher ist dies geschehen für die Schweiz, für Ungarn, Argentinien, Guernsey und in begrenztem Umfang für Kanada.

Liegt eine solche Entscheidung der Kommission nicht vor, empfiehlt es sich, zu klären, ob einer der in § 4c Abs. 1 BDSG genannten Tatbestände gegeben ist, z. B. das Vorliegen einer Einwilligung des Betroffenen für die Datenübermittlung in das Drittland oder der Fall, dass die Datenübermittlung für die Erfüllung eines Vertrages erforderlich ist, den das datenübermittelnde Unternehmen mit dem Betroffenen oder mit einem Dritten im Interesse des Betroffenen abgeschlossen hat. Liegt einer dieser Fälle vor, so ist die Datenübermittlung in das Drittland zulässig.

Greift keiner der Tatbestände des § 4c Abs. 1 BDSG ein, hat das übermittelnde Unternehmen im Hinblick auf die geplante Datenübermittlung zu prüfen, ob bei der empfangenden Stelle ein angemessenes Datenschutzniveau gewährleistet ist. Dabei sind z. B. die Art der Daten (je sensibler, desto strenger die Anforde-

rungen), die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland oder die für das empfangende Unternehmen geltenden Rechtsnormen (Gibt es im Zielland ein Datenschutzgesetz, das einen gewissen Schutz bietet oder fehlen jegliche Datenschutznormen?) zu berücksichtigen. Bei einem in den USA gelegenen Unternehmen liegt ein angemessenes Datenschutzniveau vor, wenn es sich den „Safe Harbor"-Prinzipien unterwirft, einem Regelwerk, das zwischen der US-Regierung und der Europäischen Kommission ausgehandelt wurde; es steht jedem US-amerikanischen Unternehmen frei, sich diesen Regelungen anzuschließen (siehe www.europa.eu.int/com/privacy).

Ist ein angemessenes Datenschutzniveau nicht feststellbar, ist die Datenübermittlung dennoch gemäß Art. 26 Abs. 4 EG-Datenschutzrichtlinie möglich, wenn sie auf der Grundlage der von der EG-Kommission herausgegebenen Standardvertragsklauseln erfolgt. Diese müssten zwischen datenübermittelndem und datenempfangendem Unternehmen vereinbart werden. Es gibt Standardvertragsklauseln für die Übermittlung in Drittländer und Standardvertragsklauseln für die Übermittlung an Auftragsdatenverarbeiter in Drittländern (www.europa.eu.int/com/privacy). Verträge zwischen übermittelndem und empfangendem Unternehmen, die nicht den Standardvertragsklauseln entsprechen, bedürfen einer Genehmigung durch die zuständige Aufsichtsbehörde (§ 4c Abs. 2 BDSG). Die Genehmigung wird unter Widerrufsvorbehalt erteilt, da für die anderen EU-Mitgliedsstaaten die Möglichkeit besteht, Widerspruch einzulegen. Für die Genehmigungsfähigkeit ist entscheidend, ob der Vertrag ein Datenschutzniveau gewährleistet, das mit dem der Standardvertragsklauseln vergleichbar ist. Es stellt eine wesentliche Vereinfachung dar, wenn von vornherein die Standardvertragsklauseln verwendet werden. Damit entfällt jegliche Genehmigungspflicht.

Verbindliche Unternehmensregelungen international tätiger Konzerne, die die Übermittlungen personenbezogener Daten innerhalb eines Konzerns regeln, können für die Beurteilung des angemessenen Datenschutzniveaus beim Empfänger von Bedeutung sein. Damit sollen auch für in Drittländern gelegenen Konzerngesellschaften einheitliche Datenschutz- und Datensicherheitsstandards im Sinne der europäischen Datenschutzrichtlinie festgelegt werden, um sicherzustellen, dass auch bei diesen ein angemessenes Datenschutzniveau hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte gewährleistet wird. Maßstab für die inhaltliche Gestaltung ist das Da-

tenschutzniveau, das durch die von der Europäischen Kommission herausgegebenen Standardvertragsklauseln vorgegeben ist.

Im Berichtszeitraum wurden auch viele - vor allem telefonisch gestellte - Fragen zum internationalen Datenverkehr beantwortet. Sie bezogen sich meist darauf, welche Möglichkeiten es für Datenübermittlungen ins Ausland überhaupt gibt und an welche Voraussetzungen diese geknüpft sind.

9.1 Datenübermittlung an den Mutterkonzern in den USA zur Verwendung vor Gericht

In einem Fall sollten personenbezogene Daten, die bei einem in Deutschland ansässigen Tochterunternehmen gespeichert sind, an den in den USA befindlichen Mutterkonzern übermittelt werden, weil dieser im Rahmen eines Rechtsstreits vom Gericht aufgefordert worden war, personenbezogene Daten des Konzerns offen zu legen.

Im Rahmen einer Zulässigkeitsprüfung ist hier zunächst zu klären, ob die Voraussetzungen der §§ 4, 28 ff. BDSG erfüllt sind. Sind sie gegeben, könnte der Ausnahmetatbestand des § 4c Abs. 1 Satz 1 Nr. 4 BDSG in Betracht kommen, da die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich sein könnte. Trifft dies nicht zu, ist zu fragen, ob der amerikanische Konzern sich den „Safe Harbor“-Regelungen unterworfen hat. Wenn dies der Fall ist, liegt ein angemessenes Datenschutzniveau vor und die besonderen Anforderungen an die Datenübermittlung in Drittländer sind erfüllt. Kommt auch diese Möglichkeit nicht in Betracht, so muss die Geltung der von der Europäischen Kommission erarbeiteten Standardvertragsklauseln vereinbart werden.

9.2 Datenübermittlung von einer deutschen Zweigstelle in die USA

Personenbezogene Daten sollten von einem in Deutschland gelegenen, rechtlich unselbständigen, Büro einer international tätigen Anwaltskanzlei an die sich in den USA befindende Hauptstelle übermittelt werden. Es stellte sich die Frage, ob

die Hauptstelle im Verhältnis zum deutschen Büro als Dritte (§ 3 Abs. 8 Satz 2 BDSG) anzusehen ist, ob also eine Datenübermittlung vorliegt oder eine interne Weitergabe.

In Übereinstimmung mit den anderen Aufsichtsbehörden sehen wir die unselbständige Zweigstelle in Drittländern (außerhalb von EU und EWR) als Dritte im Verhältnis zur deutschen Hauptstelle. Gleiches muss dann auch für den vorliegenden Fall gelten, bei dem sich die unselbständige Stelle im Inland befindet. Es mussten folglich die verschiedenen Zulässigkeitsvoraussetzungen für Datenübermittlungen ins Ausland durchgeprüft werden.

9.3 Übermittlung von Mitarbeiterdaten bei Baustellen im Ausland

Im Zusammenhang mit der Auszahlung von Löhnen für Mitarbeiter eines deutschen Unternehmens, die auf Baustellen im Ausland tätig waren, sollten deren Daten dorthin übermittelt werden. Die Baustellen befanden sich in den Niederlanden und in Rumänien.

Spezifische Vorgaben im Hinblick auf die Übermittlung ins Ausland gibt es bezüglich der Niederlande nicht, da es sich um einen Mitgliedsstaat der EU handelt. Der EU- und der EWR-Raum werden insoweit wie Inland behandelt, so dass nur die Voraussetzungen der §§ 4, 28 ff. BDSG zu beachten sind, die bei jeder Datenübermittlung erfüllt sein müssen.

Bei Rumänien, das nicht der EU angehört, handelt es sich um ein sogenanntes Drittland. Neben den §§ 4 und 28 ff. BDSG sind auch die Vorschriften des § 4b Abs. 2 bis 6 und des § 4c BDSG zu beachten. Hier ist § 4c Abs. 1 Satz 1 Nr. 2 BDSG einschlägig, da die Datenübermittlung zur Erfüllung des Arbeitsvertrages erforderlich war, also die Lohnzahlung an die betreffenden Mitarbeiter sonst nicht möglich gewesen wäre.

* * *

10 Arbeitnehmerdatenschutz

Aus der beträchtlichen Anzahl von Eingaben, Anfragen und Beschwerden ersehen wir, dass sich Arbeitgeber, Arbeitnehmer, Betriebsratsmitglieder und die betrieblichen Datenschutzbeauftragten immer häufiger mit der Zulässigkeit der Verarbeitung von personenbezogenen Daten der Arbeitnehmer befassen. Der Datenschutz findet also auch in der Arbeitswelt sowohl auf Seiten der Betroffenen als auch bei den verantwortlichen Stellen immer mehr Beachtung. Es fällt auf, dass zahlreiche Anfragen von Arbeitnehmern mit der Bitte verbunden werden, ihr Unternehmen nicht einzuschalten.

Da ein spezielles Arbeitnehmerdatenschutzgesetz noch nicht erlassen ist, sind Prüfungsmaßstäbe für die Rechtmäßigkeit der Datenverarbeitungen das BDSG, die diesem vorgehenden bereichsspezifischen Vorschriften und andere Vorschriften, zu denen unter anderem auch Betriebsvereinbarungen gehören.

Soweit eine Einwilligung des Arbeitnehmers in eine Datenverwendung oder eine andere Rechtsvorschrift nicht vorliegt, kommt es nach dem in vielen Fällen einschlägigen § 28 Abs. 1 Satz 1 Nr. 1 BDSG auf die entscheidende Frage an, ob die Datenverarbeitung der „Zweckbestimmung des Arbeitsverhältnisses dient“.

10.1 Überwachung der Internet- und E-Mail-Nutzung am Arbeitsplatz

Viele Eingaben befassen sich mit der Frage, inwieweit eine Kontrolle der ein- und ausgehenden E-Mails oder der Internetnutzung am Arbeitsplatz durch den Arbeitgeber datenschutzrechtlich zulässig ist. Für die Beantwortung kommt es entscheidend darauf an, ob der Arbeitgeber die private Nutzung von Internetdiensten am Arbeitsplatz einschließlich der Versendung und des Empfangs von E-Mails gestattet oder nicht.

In den folgenden Unterabschnitten werden unsere Antworten auf die wichtigsten Fragestellungen nach den Kontrollmöglichkeiten des Arbeitgebers in einem pauschalierenden Überblick wiedergegeben. Dabei ist darauf hinzuweisen, dass in diesem Bereich viele Rechtsunsicherheiten bestehen und dass viele Rechtsfragen umstritten sind. Die hier dargestellten Rechtsauffassungen orientieren sich

weitgehend an dem derzeit herrschenden Meinungsstand bei den Aufsichtsbehörden und in der Literatur.

Für alle Kontrollen gilt, dass auch die einschlägigen Vorschriften des Betriebsverfassungsgesetzes zur Mitbestimmung des Betriebsrats, insbes. § 87 Abs. 1 Nr. 6 BetrVG, beachtet werden müssen. Die Arbeitnehmer sind über die zulässigen Kontrollmöglichkeiten zu informieren. Die Kontrollen sollten auch mit dem Datenschutzbeauftragten abgesprochen sein.

10.1.1 Kontrollen durch den Arbeitgeber, wenn er die private Internet- und E-Mail-Nutzung nicht erlaubt hat

Eine derartige Situation ist nicht nur anzunehmen, wenn der Arbeitgeber die private Nutzung ausdrücklich verboten hat, sondern auch dann, wenn keine Äußerung des Arbeitgebers zu dieser Frage vorliegt. Schließlich muss man davon ausgehen, dass eine private Nutzung der vom Arbeitgeber zur Verfügung gestellten Arbeitsmittel zunächst einmal nicht erlaubt ist.

Der Arbeitgeber muss allerdings konsequent zu erkennen geben, dass er die private Nutzung nicht duldet und dass er Verstöße nicht hinnimmt, sondern ihnen - z. B. durch Abmahnungen - entgegentritt. Tut er dies nicht, besteht die Gefahr, dass daraus auf eine bewusste Duldung und damit auf eine Gestattung geschlossen werden kann (vgl. unter 10.1.2).

Für die Beantwortung der Frage, welche Kontrollen des Arbeitgebers zulässig sind und wie weit sie gehen dürfen, ist bei dieser Fallgestaltung vor allem das BDSG einschlägig. Danach ist im Einzelfall zwischen dem Persönlichkeitsrecht des Arbeitnehmers und dem Interesse des Unternehmens abzuwägen.

Soweit nicht eine konkrete Einwilligung des Arbeitnehmers oder eine Betriebsvereinbarung/Richtlinie gesonderte Regelungen vorsieht, sind die im Folgenden genannten Kontrollen nur unter den genannten Voraussetzungen zulässig:

Inhaltliche Stichprobenkontrolle	Zulässig zur Überprüfung, ob Missbrauch für private Zwecke vorliegt
Inhaltliche Vollkontrolle	Zulässig bei konkretem Missbrauchsverdacht
Einsichtnahme in das elektronische Postfach des Arbeitnehmers	Zulässig aus dringenden betrieblichen Gründen, insbes. bei Abwesenheit des Arbeitnehmers
Verfügung des Arbeitgebers, dass ihm bzw. einem Vorgesetzten alle ein- und ausgehenden dienstlichen Mails zuzuleiten sind	Zulässig
Auswertung der Protokolle über Verbindungs- und Inhaltsdaten	Zulässig bei überwiegendem Interesse des Arbeitgebers für folgende Zwecke: • Datensicherheit • Datenschutz • Sicherung des ordnungsgemäßen Betriebes § 31 BDSG ist zu beachten!
Darüber hinausgehende Verhaltens- und Leistungskontrolle	Unzulässig

10.1.2 Kontrollen durch den Arbeitgeber, wenn er die private Internet- und E-Mail-Nutzung gestattet hat

Die Entscheidung, ob und in welchem Umfang er den Arbeitnehmern die private Nutzung von Internet und E-Mail erlaubt, liegt allein beim Arbeitgeber. Eine Mitwirkung des Betriebsrates ist bei dieser Entscheidung vom Gesetzgeber nicht vorgesehen.

Die Erlaubnis bedarf keiner besonderen Form. Sie kann ausdrücklich im Arbeitsvertrag oder in einer Betriebsvereinbarung ebenso enthalten sein wie in einer Bekanntmachung des Arbeitgebers durch Rundschreiben oder am schwarzen Brett. Darüber hinaus ist eine private Nutzung auch dann als gestattet anzusehen, wenn eine betriebliche Übung durch den Arbeitgeber bewusst geduldet wird.

Bei dieser Fallgestaltung ist der Arbeitgeber Anbieter von Telekommunikations- bzw. Telediensten. Bezüglich der Kontrollen muss er die Vorschriften des Telekommunikations- und des Teledienstrechtes beachten. Dabei unterliegt er insbesondere den entsprechenden Regeln des Fernmeldegeheimnisses und des Teledienstedatenschutzrechts.

Die folgende Übersicht geht davon aus, dass eine Unterscheidung von dienstlicher und privater Nutzung auf technischem Weg nicht erfolgt, spezielle Regelungen in einer Betriebsvereinbarung oder Richtlinie nicht vorliegen und eine Einwilligung des Arbeitnehmers nicht erteilt ist. Die aufgeführten Kontrollen sind nur unter den genannten Voraussetzungen zulässig:

Inhaltliche Kontrolle	Unzulässig
Verfügung des Arbeitgebers, dass ihm bzw. einem Vorgesetzten alle ein- und ausgehenden dienstlichen Mails zuzuleiten sind	Zulässig
Auswertung der Protokolle über Verbindungs- und Inhaltsdaten	Zulässig bei überwiegendem Interesse des Arbeitgebers ggf. unter Hinzuziehung des Betriebsrates, des Datenschutzbeauftragten und des Betroffenen für folgende Zwecke: • Datensicherheit • Datenschutz • Sicherung des ordnungsgemäßen Betriebes • Abrechnung § 31 BDSG ist zu beachten!
Darüber hinausgehende Verhaltens- und Leistungskontrolle	Unzulässig

Die Kontrollmöglichkeiten des Arbeitgebers sind hier auf Grund der o. g. Rechtsgrundlagen äußerst beschränkt. So ist er nicht befugt, Missbrauch oder strafbare Handlungen festzustellen und zu unterbinden oder im Krankheitsfall des Arbeitnehmers dessen elektronisches Postfach einzusehen. In diesen Fällen ist eine Kontrolle nur mit der Einwilligung des Arbeitnehmers zulässig.

Da dem Arbeitgeber ein berechtigtes Interesse zuzugestehen ist, gewisse Kontrollen vorzunehmen, bestehen keine rechtlichen Bedenken, wenn er die Erlaubnis der privaten Nutzung nur denjenigen erteilt, die die Einwilligung in angemessene Kontrollmöglichkeiten geben.

Diese Einwilligung des Arbeitnehmers kann Bestandteil des einzelnen Arbeitsvertrages sein oder kann gesondert erklärt werden. Als Alternative kann aber auch eine Betriebsvereinbarung vorsehen, dass der Arbeitnehmer seine Einwilligung mit der privaten Nutzung konkludent erklärt. Er muss über den Inhalt einer derartigen Regelung jedoch ausreichend informiert werden und sollte die Kenntnisnahme der Regelung schriftlich bestätigen.

Eine derartige „Einwilligungskonstruktion“ ist in einer vom Bundesbeauftragten für den Datenschutz veröffentlichten Musterdienstvereinbarung vorgesehen (http://www.bfd.bund.de/information/Leitfaden.pdf), die auch für den privaten Bereich herangezogen werden kann. In der Literatur sind weitere Muster für derartige Regelungen in Dienst- bzw. Betriebsvereinbarungen zu finden.

Im Hinblick auf ihre sehr eingeschränkten Kontrollmöglichkeiten bei der Gestattung und ebenso bei der wohl häufig vorkommenden bewussten Duldung der privaten Nutzung ist den Arbeitgebern in jedem Falle zu empfehlen, mit dem Betriebsrat eine entsprechende Betriebsvereinbarung abzuschließen oder ggf. eine Richtlinie zu erlassen. Dort können dann auch noch weitere Maßgaben für die private Nutzung, z. B. der Zeitrahmen, die zugelassenen Bereiche usw., mit aufgenommen werden.

10.2 Einsichtsrecht in Arbeitszeitaufteilungssystem

In einem neuen Arbeitszeitaufteilungssystem eines Unternehmens hat jeder Mitarbeiter seine geleisteten Stunden aufgeteilt auf verschiedene Projekte und Tätigkeiten einzugeben. Gespeichert werden dort auch die Fehlzeiten (Urlaub, Krankheit usw.), nicht aber der Arbeitsbeginn und das Arbeitsende. Die Leiter der Projekte haben dabei die Möglichkeit, die Arbeitszeiten aller Firmenangehörigen einzusehen. Eine Einwilligung der Arbeitnehmer in dieses System wurde nicht eingeholt.

Bei der Beurteilung, ob das System in dieser Form datenschutzrechtlich zulässig ist, kommt es darauf an, ob auch die Zugriffsmöglichkeit aller Projektleiter auf die gespeicherten Daten aller Arbeitnehmer der Zweckbestimmung des Arbeitsverhältnisses dient. Arbeitszeiten sind Personaldaten. Sie besitzen nach allgemeiner Auffassung vertraulichen Charakter. Nach der Rechtsprechung des Bundesarbeitsgerichtes ist der Kreis der mit Personaldaten befassten Mitarbeiter möglichst eng zu halten. Ohne die Einwilligung des Betroffenen dürfen nur diejenigen Einblick nehmen, die nach der internen Kompetenzordnung mit diesen Daten befasst sind. Im vorliegenden Fall wäre dies u. a. der vorgesetzte Projektleiter, nicht aber die Leiter der anderen Projekte.

Soweit das System allen Projektleitern die Nutzung dieser Personaldaten aller Betriebsangehörigen ermöglicht, muss es beanstandet werden. Wir haben dem lediglich anfragenden Firmenangehörigen empfohlen, sich an den betrieblichen Datenschutzbeauftragten und/oder an den Betriebsrat zu wenden.

10.3 Datenübermittlung im Vorfeld einer Fusion

Es wurde angefragt, ob es datenschutzrechtlich zulässig ist, dass ein Tochterunternehmen im Vorfeld einer Fusion genaue Angaben über seine Arbeitnehmer (Eintrittsdatum, Geburtsdatum, Tätigkeit, Betriebszugehörigkeit, Ausbildung) an die Muttergesellschaft übermittelt. Die beiden Unternehmen sind in diesem Stadium der Prüfung noch völlig selbständig. In den Arbeitsverträgen sind keine Einwilligungen der Arbeitnehmer zur Übermittlung von Daten enthalten.

Die Zulässigkeit der Datenübermittlung richtet sich hier nach den allgemeinen Bestimmungen. Das BDSG kennt keine „Konzernklausel“, die den Datenverkehr zwischen konzernangehörigen, aber rechtlich selbständigen Unternehmen erleichtern oder begünstigen würde. Das Gleiche gilt für Datenübermittlungen zwischen zwei noch selbständigen Unternehmen, die sich in Fusionsverhandlungen befinden. Auch bei derartigen Datenflüssen handelt es sich um den Tatbestand der Übermittlung, deren Rechtmäßigkeit, soweit nicht andere Erlaubnistatbestände vorliegen, an § 28 BDSG zu messen ist.

Wir teilten dem Unternehmen mit, dass § 28 Abs. 1 Satz 1 Nr. 1 BDSG die Übermittlung von Personaldaten zwischen zwei in Fusionsverhandlungen ste-

henden Unternehmen nicht rechtfertigen kann. Im Übrigen müsste eine anonymisierte Übermittlung der Arbeitnehmerdaten, bei der die Identifizierungsangaben weggelassen werden, für den angestrebten Zweck ausreichen.

10.4 Die Speicherung der privaten Telefonnummer des Arbeitnehmers durch den Arbeitgeber

Eine Arbeitnehmerin beschwerte sich darüber, dass ihr Arbeitgeber ihre private Telefonnummer erhoben und abgespeichert hat. Wir teilten ihr mit, dass dies zulässig ist, wenn der Arbeitgeber die private Telefonnummer der Arbeitnehmerin im Rahmen des konkreten Arbeitsverhältnisses benötigt. Dies wird häufig der Fall sein. Die Rechtsgrundlage für die Zulässigkeit ergibt sich hier aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Ansonsten müsste eine auf einer freien Entscheidung beruhende Einwilligung der Arbeitnehmerin gemäß § 4a BDSG vorliegen.

* * *

11 Gesundheitswesen

In diesem Spektrum sind wir in vielfältiger Weise mit Unternehmen und Berufsgruppen befasst, die mit zum Teil sehr sensiblen personenbezogenen Daten umgehen, von den niedergelassenen Ärzten über die Apotheker, Verrechnungs-/ Abrechnungsstellen, Forschungseinrichtungen bis hin zu Pflegediensten und privaten Kliniken. Neben dem BDSG sind hier auch die speziellen Rechtsnormen für die verschiedenen Fachbereiche des Gesundheitswesens zu beachten, z. B. bei privaten Kliniken das Bayerische Krankenhausgesetz oder bei den Pflegediensten das Sozialgesetzbuch.

11.1 Recht auf Auskunft aus Krankenunterlagen

Eltern von Kindern mit Behinderungen hatten Fragen zum Recht auf Einsichtnahme in die Krankenunterlagen ihrer Kinder sowie zur Dauer der Aufbewahrung der Unterlagen. Dabei wurden oft Stigmatisierungen der Betroffenen befürchtet.

Patienten, die einen Aufenthalt in privaten Rehakliniken hinter sich hatten, wandten sich an uns mit der Frage, ob und inwieweit sie Anspruch auf Einsichtnahme in die Klinikentlassberichte hätten.

Einer Patientin wollten die sie behandelnden Ärzte ihre Krankenunterlagen und Röntgenaufnahmen nicht überlassen. Sie bat um Mitteilung, auf welchem Wege sie diese Unterlagen mit Erklärung der Vollständigkeit und Richtigkeit einfordern könnte.

Ein Einsichts- oder Auskunftsanspruch von Patienten gegenüber Ärzten und privaten Krankenhäusern/Kliniken kann sich aus § 34 BDSG, aus Art. 27 Abs. 3 Bayerisches Krankenhausgesetz (BayKrG) sowie aus dem Behandlungsvertrag ergeben. Nach der Rechtsprechung erstreckt sich der Anspruch auf Einsichtnahme des Patienten auf alle Aufzeichnungen über medizinisch-naturwissenschaftliche objektivierbare Befunde und Berichte über Behandlungsmaßnahmen (vgl. dazu Beschluss des Bundesverfassungsgerichtes vom 16.09.1998 - 1 BvR 1130/98). Die Einsicht kann lediglich aus medizinischen Gründen eingeschränkt werden, die sich aus der Art der Erkrankung und dem Zustand des Patienten ergeben können.

Auch steht einem Patienten nach der Rechtsprechung statt des Anspruches auf Einsicht in seine Krankenunterlagen ggf. auch ein Anspruch auf zeitweise Herausgabe von Originalunterlagen zu, wenn er diese durch einen Sachverständigen seines Vertrauens zwecks Feststellung von Behandlungsfehlern begutachten lassen will und diese Begutachtung durch bloße Einsichtnahme oder anhand von Kopien nicht korrekt erfolgen kann.

11.2 Anspruch auf Löschung der Daten

Eine Datenlöschung muss nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG erfolgen, sobald die Kenntnis der Daten für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist. Dabei ist zu beachten, dass die fehlende Erforderlichkeit der weiteren Datenspeicherung sich nicht schon nach Abschluss einer Behandlung bzw. Untersuchung ergibt.

Ärztliche Unterlagen müssen nach der ärztlichen Berufsordnung aus Dokumentationsgründen in jedem Fall 10 Jahre lange aufbewahrt werden. Darüber hinaus gibt es weitergehende Regelungen zur Aufbewahrung medizinischer Unterlagen, z. B. für die Dauer von 30 Jahren bei Röntgenaufnahmen. Die Erforderlichkeit für eine über 10 oder gar 30 Jahre hinaus gehende Speicherung von medizinischen Daten kann sich z. B. aus Behandlungsgründen ergeben. Dies gilt generell für alle Krankheiten, die über Jahrzehnte hinaus fortdauern, etwa bei Erbkrankheiten, manchen psychischen Störungen und Transplantationen.

Wir haben uns in den Streit zwischen den Patienten und der datenspeichernden Stelle jeweils vermittelnd eingeschalten und haben über die Rechtslage informiert. In der Regel konnte eine für beide Seiten zufriedenstellende Lösung erreicht werden.

11.3 Unzulässige Weitergabe von Patientendaten

Bedauerlicherweise mussten wir während des Berichtszeitraumes auch feststellen, dass von Ärzten vorsätzlich unzulässigerweise Patientendaten weitergegeben wurden, obwohl die Verpflichtung zur Wahrung des ärztlichen Geheimnisses als älteste Datenschutzvorschrift überhaupt gilt.

So hatte eine Reihe von Ärzten im Rahmen einer Protestaktion die Arbeitsunfähigkeitsbescheinigungen ihrer Patienten statt an die zuständige Krankenkasse gezielt zentral an eine andere gesetzliche Krankenkasse weitergeleitet. Auf diese Weise erhielt ein nicht zuständiger Krankenversicherungsträger für die jeweiligen Versicherten Informationen, auch über Gesundheitsdaten, die zu den besonderen Arten personenbezogener Daten i. S. d. § 3 Abs. 9 BDSG gehören (z. B. Dauer der Arbeitsunfähigkeit, Diagnose).

Die Arbeitsunfähigkeitsbescheinigungen sind gemäß § 295 Sozialgesetzbuch V (SGB V) allein an die zuständige Krankenkasse, nicht jedoch an eine unzuständige Krankenkasse zu senden. Für diese Datenübermittlung lag weder eine Einwilligung der Betroffenen noch eine rechtliche Grundlage in Form eines Gesetzes oder einer anderen Rechtsvorschrift vor.

Hierbei wurden unbefugt personenbezogene Daten im Sinne der Bußgeldvorschriften des § 43 Abs. 2 Nr. 1 BDSG an Dritte übermittelt. Gegen die beteiligten Ärzte haben wir Ordnungswidrigkeitenverfahren eingeleitet. Diese Verfahren sind derzeit noch nicht abgeschlossen.

11.4 Datensicherheit in Arzt- und Therapeutenpraxen

- Einwohner einer größeren Wohnanlage fanden Physiotherapeutenrezepte in der Papiertonne. Sie stammten aus einer in der Wohnanlage untergebrachten Physiotherapeutenpraxis.

  Hier haben wir festgestellt, dass unzulässigerweise personenbezogene Patientendaten über die normale Hausmüllanlage entsorgt wurden. Solche Unterlagen sind, sofern sie nicht mehr der Dokumentationspflicht unterliegen, sachgerecht unter Datensicherheitsaspekten zu entsorgen, z. B. über einen geeigneten Schredder oder über ein auf solche Arbeiten spezialisiertes Datenträ-

gerentsorgungsunternehmen. Derzeit wird geprüft, ob gegen die Physiotherapeutenpraxis ein Ordnungswidrigkeitverfahren eingeleitet wird und ob weitere Datensicherungsmaßnahmen angeordnet werden müssen.

- Eine Eingabeführerin teilte uns mit, dass in der Tiefgarage eines Mehrfamilienhauses, in der sich auch eine Arztpraxis befindet, für jedermann zugänglich Patientenunterlagen gelagert werden.

  Unsere Recherchen ergaben, dass sich in der Tiefgarage tatsächliche Kisten befanden, die ausgesonderte Patientenunterlagen enthielten. Wir wiesen den betreffenden Arzt darauf hin, dass Patientenunterlagen nach Ablauf der jeweils geltenden Aufbewahrungsfristen datenschutzgerecht zu entsorgen sind. Die Aufbewahrung der Unterlagen auf einem Parkplatz in der Tiefgarage war unzulässig, da die gelagerten Unterlagen jederzeit von unbefugten Dritten eingesehen werden konnten. Neben den anderen Mitbewohnern hätten auch noch weitere Personen, wie z. B. Besucher, Einsicht in die Patientenunterlagen nehmen können.

  Da der Inhalt der Kisten nach unserer Intervention unverzüglich in die Praxisräume verbracht wurde, haben wir von weiteren aufsichtsbehördlichen Maßnahmen abgesehen.

- In gleicher Weise unzulässig war die Aufbewahrung von Patientenunterlagen im Kelleraufgang eines Mehrfamilienhauses, in dem auch die Praxis untergebracht war. Die offenen Schubfächer enthielten die Patientenkarteien. Eine aufmerksame Mitbewohnerin informierte die Polizei.

  Patientenunterlagen sind ordnungsgemäß und sicher zu verwahren und vor dem unbefugten Zugriff Dritter zu schützen. Durch die Intervention von Polizei und Datenschutzaufsichtsbehörde konnte sichergestellt werden, dass die Schubladen mit den Patientenunterlagen ordnungsgemäß weggeschlossen wurden.

11.5 Sicherheit des Arzt-PCs

Ein Problem kann sich bei der Doppelnutzung eines Arzt-PCs ergeben, wenn dieser sowohl zur Patientendatenverwaltung als auch zur Internetnutzung einschließlich E-Mail eingesetzt wird. Trotz eines aktuellen Virenscanners und einer Firewall kann nicht ausgeschlossenen werden, dass mittels neuer, noch unbekannter Viren, Spyware usw. nicht doch Schaden auf dem Arzt-PC angerichtet wird oder Informationen ausgespäht werden können.

Eine Datenverschlüsselung kann zwar möglicherweise das Ausspähen verhindern oder erschweren, aber nicht Schäden durch virenverseuchte Programme vermeiden.

Die Berufsordnungen für Ärzte fordern für Aufzeichnungen auf elektronischen Datenträgern besondere Sicherungs- und Schutzmaßnahmen, um deren Veränderung, vorzeitige Vernichtung oder unrechtmäßige Verwendung zu verhindern.

Die beste Sicherungs- und Schutzmaßnahme in diesem Sinne besteht jedenfalls darin, für die Internetnutzung und die Patientendatenverwaltung jeweils gesonderte, nicht miteinander vernetzte PCs einzusetzen. Allein dazu haben wir anfragenden Ärzten geraten.

11.6 Zusammenarbeit zwischen Ärzten

Zwei Anfragen befassten sich mit dem datenschutzgerechten Umgang mit Patientendaten in Gemeinschaftspraxen bzw. Praxisgemeinschaften. Dabei ging es jeweils um das Ausscheiden eines Arztes aus der Gemeinschaftspraxis bzw. der Praxisgemeinschaft und es ergaben sich die Fragen, wie mit den betreffenden Patientendaten umgegangen werden muss und ob der ausscheidende Arzt die Daten „seiner“ Patienten mitnehmen kann.

11.6.1 Gemeinschaftspraxis

Unter einer Gemeinschaftspraxis versteht man die gemeinschaftliche Führung der Praxis durch mehrere Ärzte, die gemeinsame Karteiführung und die Abrechnung aller Fälle unter einem Namen bzw. einer Arztnummer. Dies bedeutet: Wer

sich einem bestimmten Arzt in einer Gemeinschaftspraxis anvertraut, muss davon ausgehen, dass die anderen Ärzte in der Gemeinschaftspraxis seine persönlichen und medizinischen Daten auch erfahren können, z. B. im Rahmen der gegenseitigen Vertretung und Beratung der Praxispartner. Hier kann in der Regel von einer konkludenten Einwilligung der Patienten zu einem gemeinsamen Umgang mit den Daten in der Praxis ausgegangen werden.

Wenn nun ein Vertragsarzt als bisher gleichberechtigter Partner die Gemeinschaftspraxis verlässt und eine eigene Praxis eröffnet, hat er ein Interesse, die Daten „seiner“ bisherigen Patienten mitzunehmen.

Datenschutzrechtlich hat er aber nur einen Anspruch auf die Daten derjenigen Patienten, die ihm aus der bisherigen Gemeinschaftspraxis in seine neue Vertragsarztpraxis folgen. Folglich ist in der Regel erst dann eine Herausgabe der Patientenunterlagen bzw. Datenträger aus der Gemeinschaftspraxis-EDV vertretbar, wenn der Patient bei dem ausgeschiedenen Arzt wieder vorspricht. Dies sieht auch die Kassenärztliche Vereinigung in der Publikation „Ärztliche Schweigepflicht, Datenschutz in der Arztpraxis, Sicherheit der Praxis-EDV“ so.

11.6.2 Praxisgemeinschaft

Bei der Praxisgemeinschaft handelt es sich um selbständige Einzelärzte, die sich nur zu dem Zweck der gemeinsamen Nutzung von Praxisräumen, Arbeitsmitteln und gemeinsamen Mitarbeitern zusammengefunden haben. Von Bedeutung hierbei ist, dass die Ärzte im Verhältnis zum Patienten einzeln auftreten. Dabei ist zu berücksichtigen, dass jeder Arzt seine eigene Dokumentation zu führen hat und damit auch seinen eigenen Datenbestand innehat, für den er selbst verantwortlich ist. Zugang zu diesen Daten dürfen neben dem jeweiligen Arzt nur die von ihm angestellten Assistenten usw. sowie das gemeinsame nichtärztliche Personal der Praxisgemeinschaft haben. Dabei ist sicherzustellen, dass der Zugriff auf die Patientendaten durch Assistenten und nichtärztliche Hilfskräfte (z. B. Arzthelferinnen, Verwaltungskräfte) nur auf die Daten erfolgen darf, für die diese unter Berücksichtigung des Arbeitsvertrages und der innerdienstlichen Anweisungen eine entsprechende Berechtigung haben. Es sind Berechtigungskonzepte zu erstellen und durch geeignete organisatorische Maßnahmen (Vergabe von Passwörtern etc.) ist sicherzustellen, dass nur berechtigtes Personal auf die jeweiligen Datenbestände Zugriff hat.

Ist ein Patient mit einer Vertretung durch einen an der Praxisgemeinschaft beteiligter Arzt einverstanden, so willigt er damit auch konkludent in den Zugriff auf seine Patientendaten durch den Vertreter ein.

Bei der Auflösung einer Praxisgemeinschaft bereitet die Trennung der Partner datenschutzrechtlich keine Probleme, wenn die Zuordnung der Patienten zu dem jeweils behandelnden Arzt konsequent durchgeführt wurde. Jeder Arzt verfügt dann über die Unterlagen „seiner“ Patienten; er ist insoweit auch für die weitere Dokumentation verantwortlich.

Bei einer gemeinsamen Praxis-EDV ist dem Arzt, der die Praxisgemeinschaft verlässt, ein Ausdruck oder ein Datenträger mit den Daten „seiner“ Patienten mitzugeben.

* * *

12 Verbände, Vereine, Parteien

Die zahlreichen Anfragen zeigen, dass sich Vereinsmitglieder zunehmend mit der Verwendung ihrer Daten durch die Vereine und Verbände befassen. Andererseits machen sich viele Verbandsfunktionäre und Vereinsvorstände Gedanken über die Verwirklichung des Schutzes der personenbezogenen Daten.

12.1 Veröffentlichungen von Landes-, Bezirks- und Kreisverbänden im Internet

Verbände, z. B. Sportverbände, denen die örtlichen Vereine auf den verschiedenen Ebenen angeschlossen sind, geben zunehmend über das Internet Informationen an die Öffentlichkeit. Dabei stellen sie sich, ihre Verantwortlichen und die Funktionäre ihrer Vereine ebenso vor wie die unter ihrer Obhut stattfindenden Aktivitäten. Im Bereich des Sports werden u. a. auch mit der Veröffentlichung von Mannschaftsaufstellungen, Spielergebnissen sowie Rang- und Bestenlisten im Internet personenbezogene Daten „übermittelt".

In den folgenden Unterabschnitten werden einige Fallgruppen von Datenveröffentlichungen datenschutzrechtlich beurteilt.

12.1.1 Kontaktadressen der Vereine und der Verbandsfunktionäre

Veröffentlicht ein Landesverband Kontaktadressen der Vereine und der Verbandsfunktionäre im Internet, so ist § 28 Abs. 1 Satz 1 Nr. 2 BDSG einschlägig. Nach dieser Bestimmung ist eine allgemeine Veröffentlichung von personenbezogenen Daten, u. a. im Internet, zulässig, soweit es zur Wahrung berechtigter Interessen des Landesverbandes erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des jeweils Betroffenen an dem Ausschluss dieser Veröffentlichung überwiegt.

Für den Landesverband ist ein berechtigtes Interesse, eine Liste der Anschriften der Vereine und Verbandsfunktionäre auch im Internet zu veröffentlichen, anzuerkennen. Es entspricht gerade in der heutigen Zeit allgemeinen Gepflogenheiten, dass sich große, in der Öffentlichkeit wirkende Organisationen im Internet präsentieren und für ihre Ziele werben. Bei einem landesweit tätigen sportlichen

Dachverband gehört es dann dazu, dass er nicht nur sich selbst und seine Funktionsträger, sondern auch seine Mitgliedsvereine mit ihren Ansprechpartnern auf diese Weise öffentlich vorstellt. Schließlich ist das Internet heute das Medium, das besser als jedes andere geeignet ist, eine breite Öffentlichkeit über eine bestimmte Sportart in Bayern zu informieren.

Überwiegende schutzwürdige Belange derjenigen, deren Adresse im Internet veröffentlicht wird, sind nicht ersichtlich. Die in der Liste angegebenen Ansprechpartner vertreten entweder einen Verein oder nehmen Aufgaben für den Verband wahr. Ihnen muss bekannt sein, dass sich Verbände an die Öffentlichkeit wenden und dass sie aufgrund ihrer Funktion als Ansprechpartner allgemein zur Verfügung stehen müssen und dementsprechend auch öffentlich bekannt gemacht werden dürfen. Im Übrigen entspricht es auch ihrem Eigeninteresse als Verantwortliche ihres Vereins, sich für diesen „werbend“ in der Öffentlichkeit zu präsentieren.

Dem Schutz der Betroffenen dient es, dass an Stelle der eigenen Adresse eine Kontaktadresse angegeben werden kann und dass die Angabe der Telefon-, Telefax- und Mobilfunknummer sowie der E-Mail-Adresse freiwillig ist. Ihrer Veröffentlichung muss auch in Zukunft jederzeit widersprochen werden können.

Der Landesverband muss in seiner Verbandszeitung und in Rundschreiben immer wieder auf diese Modalitäten der Internetveröffentlichungen hinweisen, damit alle Personen, die Funktionen übernehmen, darüber informiert sind.

12.1.2 Ranglisten, Bestenlisten, Spielergebnisse

Werden auf Vereins- oder Verbandsebene Ranglisten, Bestenlisten oder Spielergebnisse mit den Namen von Sportlern im Internet veröffentlicht, so ergibt sich die Zulässigkeit derartiger Datenübermittlungen aus § 28 Abs. 1 Satz 1 Nr. 3 Alt. 1 BDSG. Nach dieser Bestimmung ist eine Veröffentlichung von allgemein zugänglichen Daten zulässig, wenn nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Veröffentlichung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Die von einem Sportverband ausgerichteten Sportveranstaltungen (z. B. “Verbandsspiele“) sind öffentlich. Die Namen und die Ergebnisse der Spieler werden dort öffentlich bekannt gegeben. Es handelt sich somit um allgemein zugängliche Daten. Die Daten der Ranglisten sind zwar nicht direkt allgemein zugänglich, stammen jedoch aus allgemein zugänglichen Quellen und stellen nur eine Zusammenfassung und Auswertung dieser Daten dar.

Es liegen keine Anhaltspunkte vor, dass hier das schutzwürdige Interesse der Sportler an einem Ausschluss der Veröffentlichung das berechtigte Interesse des Landesverbandes offensichtlich überwiegt (§ 28 Abs. 1 Satz 1 Nr. 3 BDSG). Zwar hat die Veröffentlichung der Ergebnisse im weltweiten (!) Internet eine weitaus größere Dimension als die Veröffentlichung in den anderen Medien. Die Daten werden im Internet im Gegensatz zur Tagespresse für einen längeren Zeitraum veröffentlicht. Durch die einfache und schnelle Zugänglichkeit besteht auch eine größere Missbrauchsgefahr (z. B. Datenabgleich durch die Werbewirtschaft, „Profilerstellung“).

Andererseits sind alle Sportler darüber informiert, dass offiziellen Sportwettkämpfen Öffentlichkeit immanent ist, die Ergebnisse meist veröffentlicht werden und dies nun auch mit dem „Medium der heutigen Zeit“, nämlich dem Internet, geschieht. Es ist nicht anzunehmen, dass eine Internetveröffentlichung die Persönlichkeit eines Sportlers mehr beeinträchtigt als die Veröffentlichung in einer Tageszeitung, in deren Verbreitungsgebiet er bekannt ist.

Um eine Missbrauchsgefahr im Internet weitgehend auszuschließen, dürfen bei derartigen Veröffentlichungen auf der Rechtsgrundlage des § 28 Abs. 1 Satz 1 Nr. 3 BDSG in der Regel nur die Namen, Vornamen, die Vereinszugehörigkeit, die Nationalität und in berechtigten Ausnahmefällen der Geburtsjahrgang genannt werden. Einer Veröffentlichung des Geburtsdatums oder der Adresse stehen in der Regel die schutzwürdigen Interessen der Sportler entgegen. Sie wäre nur mit der ausdrücklichen Einwilligung der Betroffenen zulässig.

Wichtig ist auch, dass die Veröffentlichungen im Internet, soweit sie nicht mehr der aktuellen oder ständigen Information dienen, zeitlich begrenzt werden.

12.2 Weitergabe der Adressen von Delegierten vom Unterbezirk an den Kreisverband einer Partei

Der Beisitzer im Vorstand eines Kreisverbandes einer politischen Partei bat die Geschäftsstelle des Unterbezirks um Übermittlung der Adressen der von den Ortsvereinen gewählten Delegierten. Nachdem er erfahren hatte, dass bei einem Wahlvorgang im Unterbezirk seiner Partei von seinem Kreisverband nur 60 % der Delegierten erschienen waren, wollte er allen Delegierten die Bedeutung ihres Amtes noch einmal schriftlich darstellen. Die Geschäftsstelle des Unterbezirks verweigerte jedoch die Herausgabe der Adressen mit dem Hinweis auf den Datenschutz.

Der Beisitzer im Vorstand fragte deshalb bei der Aufsichtsbehörde nach. Da er jedoch die Einschaltung der Unterbezirksgeschäftsstelle im Rahmen der datenschutzrechtlichen Überprüfung ausdrücklich ablehnte, konnte nur folgende allgemeine Beurteilung abgegeben werden:

Rechtsgrundlage für die Herausgabe der für den genannten Zweck erbetenen Adressdaten der Delegierten könnte ggf. der gesetzliche Zulässigkeitstatbestand des § 28 Abs. 1 Satz 1 Nr. 1 BDSG sein. Danach ist die Übermittlung von personenbezogenen Daten dann zulässig, wenn sie der Zweckbestimmung eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnis dient. Zwischen einer Partei und ihren Mitgliedern besteht ein „vertragsähnliches Vertrauensverhältnis“ im Sinne dieser Vorschrift. Dessen Zweckbestimmung dient eine Datenweitergabe an eine andere - berechtigte - Stelle innerhalb der Partei dann, wenn sie sich im Rahmen der satzungsgemäßen Parteiarbeit hält.

Dies wird man im vorgetragenen Fall dann bejahen können, wenn der Beisitzer die Delegierten im Rahmen seiner satzungsgemäßen Aufgaben oder der ihm vom Vorstand übertragenen Aufgaben anschreiben wollte. Die Unterbezirksgeschäftsstelle hätte die Adressen der Delegierten auf Grund der o. g. gesetzlichen Bestimmung an ihn herausgeben dürfen.

Eine andere datenschutzrechtliche Beurteilung wäre jedoch dann geboten, wenn der Beisitzer diese Aktion ohne eine derartige Legitimation, sozusagen im Alleingang, hätte durchführen wollen. Da in diesem Fall kein vertragsähnliches Vertrauensverhältnis zwischen dem Beisitzer im Vorstand und den betroffenen De-

legierten besteht, könnte § 28 Abs. 1 Satz 1 Nr. 1 BDSG als gesetzliche Grundlage für die Datenübermittlung nicht herangezogen werden. Die Weigerung der Geschäftsstelle wäre rechtmäßig gewesen.

12.3 Weitergabe oder Nutzung von Mitgliederdaten zur Wahlwerbung

Ein Eingabeführer beschwerte sich darüber, dass im Vorfeld der Neuwahl des Bürgermeisters die Mitglieder eines Sportvereins - darunter auch der erst 9-jährige Sohn des Eingabeführers - ein Wahlempfehlungsschreiben des Ehrenvorsitzenden erhielten. In einem anderen Fall nutzte ein Vorstandsmitglied eines Vereins die Mitgliederdaten, auf die er kraft Amtes Zugriff hatte, für die Zusendung von Wahlwerbung.

Mitgliederdaten eines Vereins können gemäß § 28 Abs. 3 Satz 1 Nr. 3 BDSG nur dann für Werbezwecke übermittelt oder genutzt werden, wenn zum einen der Datenkatalog dieser Bestimmung eingehalten ist und darüber hinaus kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.

Bei der Bewertung des schutzwürdigen Interesses der Mitglieder im Hinblick auf die Übermittlung oder Nutzung ihrer Daten für Zwecke der Wahlwerbung ist vor allem zu berücksichtigen, dass es sich bei der Mitgliedschaft in einem Verein um ein personenrechtliches Rechtsverhältnis handelt, aus dem sich für den Verein besondere Schutzpflichten gegenüber seinen Mitglieder ergeben. Ihre Gewichtung kann je nach der Art des Vereins unterschiedlich stark sein.

In den vorliegenden Fällen wird man annehmen müssen, dass die Mitglieder ein schutzwürdiges Interesse am Ausschluss der Nutzung oder der Übermittlung zu Zwecken der Wahlwerbung haben. Zum einen ist die Wahlwerbung, von Ausnahmen abgesehen, nicht vom satzungsgemäßen Vereinszweck gedeckt. Zum anderen vertrauen die Mitglieder regelmäßig darauf, dass der Verein ihre Daten nicht an Dritte zum Zwecke der Wahlwerbung übermittelt. Dieses schutzwürdige Interesse ist insbesondere auch bei den minderjährigen Vereinsmitgliedern anzuerkennen. Somit war die Übermittlung bzw. Nutzung der Mitgliederdaten für Zwecke der Wahlwerbung in beiden Fällen unzulässig.

12.4 Veröffentlichung von Urteilen der Vereinsgerichtsbarkeit im Internet

Ein Verein veröffentlichte im Internet Urteile, die in Vereinsordnungsverfahren ergangen sind und deren Veröffentlichung im Urteil ausdrücklich angeordnet worden ist.

Eine datenschutzrechtliche Überprüfung ergab, dass weder die Nr. 1 noch die Nr. 2 des § 28 Abs. 1 Satz 1 BDSG als Rechtsgrundlage für eine derartige Übermittlung personenbezogener Daten im Internet herangezogen werden kann. Die weltweite Veröffentlichung von Entscheidungen einer Vereinsgerichtsbarkeit dient nicht der Zweckbestimmung eines Mitgliedsverhältnisses (Nr. 1). Sie ergibt sich weder aus der Vereinssatzung, die allein eine Veröffentlichung in den amtlichen Mitteilungen des Vereins vorsieht, noch ist sie aus sonstigen Umständen heraus zur Erfüllung der satzungsmäßigen Zwecke des Vereins erforderlich.

Auch die Voraussetzungen der Nr. 2 liegen hier nicht vor. Es fehlt auch hier an der Erforderlichkeit der Veröffentlichung im Internet. Darüber hinaus überwiegt das schutzwürdige Interesse der Mitglieder daran, dass ihre personenbezogenen Daten, wie Name, Gerichtsbeschluss etc., nicht weltweit bekannt gegeben werden.

Auf Grund der Beanstandung der Datenschutzaufsichtsbehörde hat der Verein diese Veröffentlichungspraxis eingestellt.

* * *

13 Videoüberwachung öffentlich zugänglicher Räume

Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) hat in den vergangenen Jahren immer mehr zugenommen. Auf der einen Seite dient sie vielfältigen Sicherheitsinteressen der Allgemeinheit oder von Einzelnen. Auf der anderen Seite berührt sie das Persönlichkeitsrecht all derjenigen, deren Verhalten beobachtet und ggf. auch aufgezeichnet wird. Mit der Novelle vom 18. Mai 2001 wurde der § 6b neu in das BDSG aufgenommen. Er enthält Regelungen für die Videoüberwachung in öffentlich zugänglichen Räumen.

Die neue Bestimmung versucht, einen Ausgleich zwischen den Interessen an der Durchführung einer Videoüberwachung einerseits und dem Persönlichkeitsschutz der Betroffenen andererseits zu schaffen. Dabei werden als schützenswerte Beobachtungszwecke die Wahrnehmung des Hausrechts, der Eigentumsschutz und Sicherheitsinteressen anerkannt (§ 6b Abs. 1 BDSG). Insgesamt wird jedoch das Ziel verfolgt, eine restriktive Verwendung der neuen Technik herbeizuführen. Schließlich beeinträchtigt die ohne Einwilligung erfolgende Videobeobachtung das Recht auf informationelle Selbstbestimmung. Es besteht auch die Gefahr, dass durch verstärkte Überwachungstätigkeit Bewegungsprofile erstellt werden. Eine Videoüberwachung ist demnach nur dann zulässig, wenn die genannten berechtigten Interessen des Verantwortlichen sie erfordern und keine Anhaltspunkte dafür bestehen, dass die schutzwürdigen Interessen der Betroffenen demgegenüber überwiegen.

Im Berichtszeitraum zeigte sich zur Frage der Rechtmäßigkeit von Videoüberwachungsanlagen ein großer Beratungsbedarf. Zum einen bestehen noch viele Unsicherheiten bei der Anwendung der neuen Regelung. Zum anderen ist wohl im Hinblick auf die hier auftretenden Fragen des Persönlichkeitsschutzes sowohl in den Wirtschaftsunternehmen als auch in der Bevölkerung durchaus ein entsprechendes Problembewusstsein vorhanden.

Zahlreiche Privatpersonen, z. B. Hauseigentümer, die die kostengünstige und einfach zu handhabende Überwachungstechnik zu Kontrollzwecken einsetzen möchten, wandten sich an uns. Wir teilten ihnen mit, unter welchen rechtlichen Voraussetzungen eine Videoüberwachung überhaupt zulässig ist und welche Regelungen dabei zu beachten sind.

Gelegentlich wurden wir von Bürgern, die im Umfeld ihrer Wohnung von einer Videoüberwachung betroffen werden, um Rat gefragt. In diesen Fällen wird die Privatsphäre und damit das Persönlichkeitsrecht besonders stark berührt. Insgesamt hielten sich die konkreten Beschwerden über eine Kameraüberwachung jedoch in Grenzen.

13.1 Kameraüberwachung eines Taxistandes

Eine Taxigenossenschaft hatte an ihrem Taxistand am Bahnhof eine Überwachungskamera installiert, die sowohl den Taxistand als auch einen Teil des öffentlichen Bahnhofsvorplatzes erfasste. Die von der Kamera aufgenommenen Bilder wurden in den Aufenthaltsraum übertragen, um von dort aus sehen zu können, ob die Taxen am Standplatz nachrücken müssen. Eine Aufzeichnung der Bilder erfolgte nicht. Gegen diese Videoüberwachung wurde Beschwerde eingelegt.

Die Zulässigkeit dieser Videoüberwachung beurteilt sich nach § 6b Abs. 1 BDSG. Bei der überwachten Fläche handelte es sich um einen öffentlich zugänglichen Raum. Als Zulässigkeitstatbestand könnte nur die Nr. 3 in Betracht kommen. Nach dieser Bestimmung müsste die Videoüberwachung zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Wir haben in diesem Fall die Auffassung vertreten, dass angesichts der weiträumigen Überwachung die Voraussetzungen dieser restriktiv auszulegenden Ausnahmevorschrift nicht gegeben waren. Zunächst war zweifelhaft, ob zur Verfolgung des Zwecks, am Taxistand einen reibungslosen Betriebsablauf zu gewährleisten, eine derart weiträumige Videobeobachtung erforderlich war. Dieser Zweck konnte eine Videoüberwachung des öffentlichen Straßenraumes am Bahnhofsvorplatz im Hinblick auf die überwiegenden schutzwürdigen Interessen der Passanten nicht rechtfertigen.

Aus diesen Gründen haben wir die weiträumige Videoüberwachung als rechtswidrig beanstandet. Die Taxigenossenschaft hat unserer Bitte, sie einzustellen, entsprochen.

13.2 Überwachung des öffentlichen Straßenraumes

Ein Hausbewohner beobachtete mit einer am Fenster installierten Videokamera sowohl den davor befindlichen gesamten öffentlichen Straßenraum als auch den gesamten Parkplatz des Anwesens und damit dessen Bewohner. Er wollte auf diese Weise seinen vor einiger Zeit auf diesem Platz beschädigten PKW überwachen.

Diese Videoüberwachung ging weit über die in § 6b Abs. 1 BDSG festgelegten Zulässigkeitsvoraussetzungen hinaus und wurde deshalb beanstandet.

13.3 Videoüberwachung eines Biergartens

Der Eigentümer einer Mühle verpachtete den im Bereich des Anwesens befindlichen Garten als Biergarten. Das von ihm bewohnte Mühlenanwesen grenzt unmittelbar an den Biergarten. Um sein Gebäude vor unbefugtem Zutritt der Gäste des Biergartens zu schützen, richtete er eine Videokamera auf den Bereich vor der Eingangstür des Gebäudes. Dagegen wendet sich der Pächter mit der Begründung, die Videoüberwachung halte Gäste vom Besuch seines Biergartens ab.

Der § 6b BDSG ist als Maßstab für die Zulässigkeit dieser Videoüberwachung nur dann einschlägig, wenn der von der Kamera bestrichene Hofbereich öffentlich zugänglich ist. Im vorliegenden Fall ist wohl davon auszugehen, dass im Hofraum eine Abgrenzung zwischen dem Zugang zum Biergarten und zu den Toiletten einerseits und dem privaten Eingangsbereich andererseits in der Natur nicht eindeutig zu bestimmen ist. Im Zweifel wird man den vor der Haustür befindlichen Teil noch als öffentlich zugänglich ansehen müssen. Folglich sind wir von einer Anwendbarkeit des § 6b BDSG ausgegangen.

Wir haben dem Hauseigentümer und dem Beschwerdeführer mitgeteilt, dass nach dieser Bestimmung eine Videoüberwachung zur Wahrnehmung seines Hausrechts mit folgenden Maßgaben zulässig ist:

- Der von der Videokamera bestrichene Teil der öffentlich zugänglichen Hoffläche muss unter Berücksichtigung des Beobachtungszweckes so klein wie möglich sein.

- Es muss im Hofraum noch so viel Platz zur Verfügung stehen, dass der Pächter und die Gäste den beobachteten Bereich meiden können.

- Die Videobeobachtung und ihr etwaiger Umgriff müssen für die Besucher erkennbar gemacht werden.

Unter diesen Umständen sahen wir keine Anhaltspunkte dafür, dass schutzwürdige Belange der Betroffenen das Interesse des Verpächters an der Wahrnehmung seines Hausrechtes überwiegen.

13.4 Videoüberwachung im Kassenbereich und Aufzeichnung der PIN-Eingabe

In den Filialen einer Einzelhandelskette werden die Kassenbereiche videoüberwacht. Ein Eingabeführer befürchtete, dass mit den über den Kassen installierten Kameras u. a. auch die Eingabe der PIN der Kreditkarte aufgezeichnet werden kann.

Der Datenschutzbeauftragte der Unternehmenszentrale begründete in seiner Stellungnahme die Erforderlichkeit der Videoüberwachung der Kassen zu Recht mit den besonderen kriminellen Risiken dieser Bereiche. Um einen datenschutzgerechten Umgang mit der Videoüberwachung zu gewährleisten, seien ausführliche Anweisungen an die Filialen herausgegeben worden. Aus ihnen ergebe sich, dass die Überwachung der PIN-Eingabegeräte verboten ist. Der Datenschutzbeauftragte versicherte, dass die in den Filialen eingebauten Kameras ein Erkennen der PIN nicht zuließen.

Damit konnte, soweit in den Filialen entsprechende Hinweise auf die Videoüberwachung vorhanden sind, kein Verstoß gegen den § 6b BDSG festgestellt werden.

13.5 Webcamübertragung in das Internet

13.5.1 Liveübertragung aus einem Cafe, einer Disko usw.

Wir wurden wiederholt mit der Frage konfrontiert, unter welchen Voraussetzungen es zulässig ist, das Geschehen in Cafes oder Diskos mit einer Webcam live ins Internet zu übertragen. Eine Webcam ist eine Kamera, mit der bewegte Bilder und Standbilder über einen Webserver ins Internet eingestellt werden können.

In datenschutzrechtlicher Hinsicht ist beim Einsatz einer Webcam neben der Zulässigkeit der Beobachtung per Videokamera gemäß § 6b Abs. 1 BDSG auch die Rechtmäßigkeit der Übermittlung der aufgenommenen Bilder an die weltweite Allgemeinheit per Internet gemäß § 6b Abs. 3 bzw. § 4a BDSG zu prüfen.

Im Regelfall wird man davon ausgehen müssen, dass die Betreiber einen Zulässigkeitstatbestand gemäß § 6b Abs. 1 BDSG für die Erhebung der Bilder ebenso wenig nachweisen können wie für ihre Übertragung ins Internet. In den uns bisher bekannten Sachverhalten wurden die Webcams überwiegend zu Werbezwecken eingerichtet. Potenzielle Kunden sollten von zu Hause aus sehen können, ob sich ein Besuch „lohnt“ oder ob Bekannte bereits anwesend sind. Insoweit kann ein berechtigtes Interesse i. S. d. § 6b Abs. 1 Nr. 3 BDSG an einer Kameraüberwachung nicht festgestellt werden. Der restriktiv auszulegende § 6b BDSG verfolgt den Zweck, eine Überwachung per Videokamera nur dann zuzulassen, wenn besondere Interessen, insbesondere Sicherheitsbelange, eine solche Maßnahme erfordern. In diesem Sinne muss das Interesse objektiv begründbar sein. Bei einer Werbemaßnahme ist dies nicht möglich.

Die Aufnahme und die Übertragung der Live-Bilder sind deshalb nur dann zulässig, wenn eine Einwilligung der Betroffenen gemäß § 4 Abs. 1 und § 4a BDSG vorliegt.

Der Besucher ist auf den vorgesehen Zweck der Erhebung, Verarbeitung oder Nutzung seiner Daten hinzuweisen (§ 4a Abs. 1 Satz 2 BDSG). Die Lokalbesucher müssen schon vor Betreten des von der Kamera erfassten Bereiches deutlich und unmissverständlich auf die Beobachtung und die Live-Übertragung der Bilder ins Internet hingewiesen werden.

Unter diesen Umständen kann davon ausgegangen werden, dass sich die Gäste der Tatsache bewusst sind, dass die Webcamaufnahmen ins Internet übertragen werden. Mit dem Betreten des Lokals und ihrem dortigen Aufenthalt erteilen sie dazu konkludent ihre Einwilligung. Diese beruht auf ihrer freien Entscheidung. Schließlich steht es jedermann frei, ein bestimmtes Lokal zu betreten oder nicht.

Nach § 4a Abs. 1 Satz 3 BDSG bedarf zwar die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Ein solcher Ausnahmefall ist hier gegeben. Es wäre kaum umsetzbar, vor Betreten des Restaurants von jedem Gast eine schriftliche Einwilligungserklärung einzuholen.

13.5.2 Liveübertragung aus Fun-Arenen

Eine ähnliche datenschutzrechtliche Situation wie bei den unter Abschnitt 13.5.1 dargestellten Übertragungen ergibt sich bei den in vielen Städten und Gemeinden aufgestellten Fun-Arenen.

Bei einer Fun-Arena handelt es sich um ein durch Bande abgegrenztes rechteckiges Spielfeld (Kleinfeld). Auf dem mit einem Kunststoffbelag versehenen Hartplatz können die verschiedensten Sportarten vom Fußball über Tennis bis zum Schlittschuhlaufen ausgeübt werden. An den vier Ecken des Spielfeldes sind jeweils auf einer Stange Webcams angebracht, deren Bilder ins Internet übertragen werden. In der Produktbeschreibung wird dazu folgendes ausgeführt: „Für den Schutz der Fun-Arena und zur Sicherheit der Benutzer sind vier Web-Cams installiert. Dies ermöglicht eine permanente Videoüberwachung“. Darüber hinaus soll mit der Übertragung ins Internet ein Werbeeffekt für die Anlage erzielt werden.

Wenn auch die übertragenen Bilder nicht besonders scharf sind und auch keine Teleobjektive installiert sind, so ist § 6b BDSG für die datenschutzrechtliche Beurteilung gleichwohl anwendbar. Entscheidend ist, dass die aufgenommenen Personen für Bekannte, Schul- und Sportkameraden ohne weiteres erkennbar sind.

Gemäß § 6b Abs. 1 Nrn. 1 und 2 BDSG ist die reine Videoüberwachung, soweit die Bilder einer überwachenden Stelle zugeleitet werden, zur Wahrnehmung des Hausrechts und aus Sicherheitsgründen zulässig.

Etwas Anderes gilt für die Übertragung der Bilder ins weltweite Internet. Sie geht über die genannten Zwecke hinaus. Die Werbung für die Fun-Arena kann auch nicht als berechtigtes Interesse im Sinne der eng auszulegenden Nr. 3 des § 6b Abs. 1 BDSG anerkannt werden.

Somit ist eine Übertragung der Bilder aus der Fun-Arena in das Internet nur dann zulässig, wenn zumindest eine konkludente Einwilligung der Benutzer vorliegt. Es müssen deshalb dem Benutzer vor dem Betreten des überwachten Bereichs deutliche Hinweise auf die Kameraüberwachung, die verantwortliche Stelle sowie die Liveübertragung im Internet gegeben werden. Nur so kann sicher gestellt werden, dass sich die Besucher dorthin in voller Kenntnis und Billigung der Umstände begeben. Die Kameras sind so einzustellen, dass nur die Fun-Arena selbst, nicht jedoch noch ein weiterer Umgriff abgebildet wird.

* * *

14 Medien- und Teledienste, Internet

Für die neuen Medien wie Internet-Angebote, E-Mail-Verkehr, Online-Chat usw. kommen je nach dem, auf welcher Ebene im Rahmen einer elektronischen Verbindung ein Sachverhalt zu beurteilen ist, folgende Rechtsgrundlagen in Betracht:

- Das Telekommunikationsrecht (in erster Linie Telekommunikationsgesetz (TKG), Telekommunikations-Datenschutzverordnung (TDSV) gilt für den Datentransport per Leitung und die dazugehörende Technik (erste Ebene).

- Das Tele-/Mediendiensterecht (Teledienstegesetz (TDG), Teledienstedatenschutzgesetz (TDDSG), Mediendienstestaatsvertrag (MDStV) ist anwendbar, wenn es um die zweite Ebene, d. h. um das Angebot eines elektronischen Informations- oder Kommunikationsdienstes geht.

- Das allgemeine Datenschutzrecht (z. B. das BDSG) kommt auf der dritten Ebene zur Anwendung. Auf dieser sog. Inhaltsebene geht es um die konkreten Geschäftsbeziehungen im Rahmen von Kauf- oder Versicherungsverträgen. Somit besteht insoweit kein Unterschied zwischen den online- und den offline-Geschäftsbeziehungen.

14.1 Prangerseiten im Internet

Im Berichtszeitraum wurden wir vermehrt auf Veröffentlichungen im offenen Internet in der Form von „Schuldnerlisten“, „Warnlisten“ oder anderen diskriminierenden Darstellungen aufmerksam gemacht, in denen das Verhalten von Personen bzw. ihre Kreditwürdigkeit kritisch dargestellt und damit regelrecht angeprangert wurde.

Soweit dabei personenbezogene Daten in das Internet gestellt werden, handelt es sich um Datenübermittlungen im Sinne des § 3 Abs. 4 Satz 2 Nr. 3 BDSG. Auf einem Datenträger gespeicherte personenbezogene Daten werden an eine unbegrenzte Anzahl von Dritten im weltweiten Internet bekannt gegeben. Die Rechtmäßigkeit derartiger Übermittlungen ist deshalb anhand der datenschutzrechtlichen Vorschriften zu beurteilen.

Generell kann man sagen, dass derartige anprangernde Veröffentlichungen im Internet unabhängig von ihrem Wahrheitsgehalt unzulässig sind. Dies ergibt sich vor allem daraus, dass dabei in unzumutbarem Maße in das Persönlichkeitsrecht der Betroffenen eingegriffen wird.

14.1.1 Schuldnerlisten

Ein Internetversandhaus veröffentlichte im Rahmen seines Internetauftrittes die Namen von Kunden, die eine Rechnung noch nicht bezahlt hatten. Auf diese Weise sollten die säumigen Zahler zur Begleichung der offenen Beträge angehalten werden.

Bei einer derartigen Fallgestaltung werden personenbezogene Daten übermittelt. Die vorgetragene Tatsache, dass eine namentlich genannte Person bei einem Unternehmen Schulden hat, ist unabhängig von ihrem Wahrheitsgehalt eine Einzelangabe über ihre sachlichen Verhältnisse (§ 3 Abs. 1 BDSG).

Es ist davon auszugehen, dass eine Einwilligung der betroffenen Schuldner in eine derartige Veröffentlichung nicht vorliegt. Aber auch ein Zulässigkeitstatbestand in Form einer Rechtsvorschrift ist für die Veröffentlichung einer Schuldnerliste im Internet nicht vorhanden.

Der § 28 Abs. 1 Satz 1 Nr. 1 BDSG kann deshalb nicht als Rechtsgrundlage für die Datenübermittlung herangezogen werden, weil es der Zweckbestimmung des abgeschlossenen Vertrages nicht entspricht, den säumigen Vertragspartner einer weltweiten Öffentlichkeit zu präsentieren. Zwar geht es hier darum, den Schuldner zur Vertragserfüllung anzuhalten. Es widerspricht jedoch in hohem Maße dem in diesem Zusammenhang zu beachtenden Grundsatz der Verhältnismäßigkeit und grenzt schon fast an die nach unserer Rechtsordnung grundsätzlich verbotene Selbstjustiz, wenn ein Gläubiger seinen Schuldner namentlich im Internet bekannt gibt. Ein Gläubiger muss in einem derartigen Fall vielmehr die ihm insbesondere von der Zivilprozessordnung gesetzlich eingeräumten Möglichkeiten zur Durchsetzung seines Zahlungsanspruches wahrnehmen.

Auch die tatbestandlichen Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG sind nicht erfüllt. Nach dieser Bestimmung ist die Veröffentlichung zur Wahrung berechtigter Interessen der verantwortlichen Stelle zulässig, soweit kein Grund

zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Der Erhalt der Vergütung für eine erbrachte Leistung stellt zwar ein berechtigtes wirtschaftliches Interesse eines jeden Unternehmers dar und die entstehende Prangerwirkung mag diesem Zweck dienen. Jedoch überwiegen die schutzwürdigen Belange der Betroffenen an einem Ausschluss der Veröffentlichung ihres Namens auf einer Schuldnerliste im Internet. Mit ihrer öffentlichen Vorführung im Medium Internet wird in unzumutbarem Maß in ihr Persönlichkeitsrecht eingegriffen. Die negativ besetzte Information über den Betroffenen steht im Internet weltweit zur Verfügung, kann von allen möglichen Interessierten über Suchmaschinen schnell abgerufen werden und mit anderen Informationen kombiniert werden. Dies kann weder durch die Wahrheit der veröffentlichten Tatsachen noch durch die Meinungsäußerungsfreiheit gerechtfertigt werden.

Wenn der Gesetzgeber bereits für die Aufnahme in gerichtliche Schuldnerverzeichnisse besondere Voraussetzungen festlegt und enge Grenzen für die öffentliche Zugänglichkeit setzt, spricht dies ebenfalls gegen die Zulässigkeit privater Schuldnerlisten, die lediglich aufgrund von Angaben der Gläubiger geführt und der allgemeinen Öffentlichkeit im Internet zugänglich gemacht werden sollen (OLG Rostock, Urteil vom 21.3.2001 - Az 2 U 55/00).

Es kommt noch hinzu, dass der Eingriff in das Persönlichkeitsrecht dann umso schwerer zu gewichten ist, wenn ein betroffener Schuldner berechtigte Gründe für ein Zurückhalten der Vergütung hat, z. B. weil die Forderung nicht besteht.

Zusammenfassend ist festzustellen, dass die Veröffentlichung einer Schuldnerliste im offenen Internet ohne Einwilligung der Betroffenen in jedem Falle rechtswidrig ist. Da somit in dem angesprochenen Fall eine unbefugte Verarbeitung personenbezogener Daten vorlag (§ 43 Abs. 2 Nr. 1 BDSG), haben wir gegen den Betreiber ein Bußgeldverfahren eingeleitet. Die Schwarze Liste wurde zwischenzeitlich aus dem Internet entfernt.

14.1.2 Warnlisten

Im offenen Internet wurde eine Liste veröffentlicht, die - angeblich - unzuverlässige oder zahlungsunfähige Geschäftspartner enthielt. Auf diese Weise sollten die Unternehmen einer Branche vor risikobehafteten Geschäftsbeziehungen gewarnt und vor finanziellen Verlusten geschützt werden.

Für die Beurteilung der Rechtmäßigkeit dieser Datenübermittlung im Internet ist § 29 BDSG einschlägig. Die Anwendbarkeit dieser Bestimmung ergibt sich aus der geschäftsmäßigen, d. h. auf eine gewisse Dauer hin angelegten Tätigkeit. Dabei kommt es nicht darauf an, ob Einnahmen erzielt werden sollen. Es wird der Zweck verfolgt, Informationen über die angeblich unzuverlässigen Geschäftspartner zu übermitteln.

Eine derartige Übermittlung ist nach § 29 Abs. 2 BDSG nur dann zulässig, wenn der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Durch die Veröffentlichung im offenen Internet werden die Daten ohne weiteres weltweit der gesamten Allgemeinheit zur Verfügung gestellt. Dadurch kann nicht überprüft werden, ob derjenige, der die Einträge über das Internet einsieht, ein berechtigtes Interesse an der Kenntnis dieser Daten hat, z. B. um sich vor finanziellen Verlusten zu schützen. Aufgrund der fehlenden Überprüfung des berechtigten Interesses vor der Übermittlung der Daten ist die Veröffentlichung der Liste im Internet schon aus diesem Grund unzulässig. Die Abwägung mit den schutzwürdigen Belangen der Betroffenen erübrigt sich, wobei aufgrund der eintretenden Prangerwirkung regelmäßig schutzwürdige Interessen der Betroffenen einer allgemeinen Veröffentlichung entgegenstehen (vgl. 14.1.1).

Wir haben gegen den Betreiber der Schwarzen Liste ein Bußgeldverfahren eingeleitet. Gleichzeitig haben wir ihn darauf hingewiesen, dass der von ihm mit dem Warnsystem verfolgte Zweck auch mit einem Auskunfteisystem erreicht werden kann, das den datenschutzrechtlichen Anforderungen des § 29 BDSG gerecht wird. Die Schwarze Liste ist zwischenzeitlich aus dem Netz entfernt worden.

14.1.3 Andere diskriminierende Veröffentlichungen

Immer wieder machen Mitbürger ihrem Unmut über das Verhalten von Unternehmen, Behörden oder anderen Leuten dadurch Luft, dass sie deren Verhalten unter Nennung der Namen der handelnden natürlichen Personen und mit eigenen kritischen Wertungen versehen auf ihren Homepages veröffentlichen. Dabei werden auch Äußerungen von Personen wiedergegeben, Schreiben mit Angaben der Verfasser zitiert usw.

Auch derartige Veröffentlichungen im Internet verstoßen in zahlreichen Fällen gegen das Datenschutzrecht.

Bei den mitgeteilten Inhalten handelt es sich um personenbezogene Daten, d. h. um Einzelangaben über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren natürlichen Personen. Der Begriff des personenbezogenen Datums ist sehr weit auszulegen. Der Gesetzgeber wollte alle Informationen, die über eine Bezugsperson etwas aussagen, erfassen. Deshalb gehören zu den personenbezogenen Daten auch Angaben, die sich auf das berufliche Verhalten einer Person beziehen, wie z. B. Zitate aus dienstlichen Briefen und Äußerungen, Wertungen oder Sachverhaltsdarstellungen mit persönlichen Bezugnahmen.

Die Datenübermittlung an eine unbestimmte Vielzahl von Personen mittels Internet lässt sich häufig nicht mit der Rechtsordnung vereinbaren. Im Rahmen der nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG vorzunehmenden Interessenabwägung (vgl. unter 14.1.1), die auch das Recht auf freie Meinungsäußerung miteinbezieht, kommt man in den genannten Fällen regelmäßig zu dem Ergebnis, dass das schutzwürdige Interesse der von der Veröffentlichung betroffenen Personen an einer Unterlassung einer Anprangerung im Internet das Interesse desjenigen, der der Öffentlichkeit seine Probleme mitteilen möchte, überwiegt. Durch die Veröffentlichung wird, auch wenn es sich hier um den beruflichen Bereich handelt, das Persönlichkeitsrecht der genannten Personen auf Namensanonymität verletzt. Diese müssen nicht damit rechnen, dass privates oder berufliches Verhalten und ihre dienstlichen Äußerungen mit Namensnennung weltweit über eine Homepage veröffentlicht werden. Dies gilt nach unserer Auffassung z. B. in den Fällen, in denen das Verhalten von Nachbarn in einem Nachbarschaftsstreit oder das angeblich unbefriedigende Agieren eines Vertragspartners (z. B. eines Rechtsanwaltes oder eines Arztes) in das Internet eingestellt werden.

Da für derartige Datenübermittlungen auch keine Einwilligungen der Betroffenen vorlagen, haben wir sie als unzulässig beanstandet. Die Seiten wurden daraufhin aus den Homepages genommen.

14.2 Fehlende bzw. mangelhafte Anbieterkennzeichnung bei Tele- und Mediendiensten

Im Berichtszeitraum sind etwa 30 Beschwerden bei uns eingegangen, mit denen die fehlende oder mangelhafte Anbieterkennzeichnung von Tele- oder Mediendiensten angezeigt worden ist. Neben diesen anlassbezogenen Überprüfungen von Anbieterkennzeichnungen haben wir auch anlassunabhängig ca. 200 Internetangebote hinsichtlich ihrer Anbieterkennzeichnung überprüft.

Nach § 6 TDG bzw. § 10 Abs. 2 MDStV haben Diensteanbieter für geschäftsmäßige Tele- oder Mediendienste bestimmte Mindestinformationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten, vor allem den Namen und die Anschrift, den Vertretungsberechtigten, Angaben zur schnellen elektronischen Kontaktaufnahme, zur Handels- oder Vereinsregistereintragung usw. Diese Informationen aus der Anbieterkennzeichnung sollen die Wahrnehmung von Rechtsansprüchen, unter anderem aus dem Datenschutzrecht, erleichtern.

Ein Verstoß gegen die Anbieterkennzeichnungspflicht stellt eine Ordnungswidrigkeit dar, die mit einer Geldbuße geahndet werden kann.

Aufgrund der relativ kurzen Existenz dieser gesetzlichen Vorschriften konzentrierten wir im Berichtszeitraum unser Interesse vor allem auf die Beratung und die entsprechende Unterstützung von Diensteanbietern und haben bisher im allgemeinen auf eine Ahndung einer fehlenden Anbieterkennzeichnung verzichtet. Nahezu in allen Fällen konnte festgestellt werden, dass das Fehlen bzw. die Unvollständigkeit der Anbieterkennzeichnung auf die Unkenntnis der Diensteanbieter bezüglich der gesetzlichen Regelungen zurückzuführen war. Nach entsprechender sachlicher Aufklärung haben sich die Anbieter durchwegs sehr kooperativ gezeigt und auch die Anbieterkennzeichnung im jeweiligen Einzelfall zeitnah angebracht.

14.3 Unterrichtungspflichten von Telediensteanbietern nach dem TDDSG

Aufgrund von Eingaben, aber auch im Rahmen von eigenen Internetrecherchen, wurden wir vielfach mit dem Thema der Unterrichtungspflichten von Telediensteanbietern über Datenverwendungen nach den Regelungen des TDDSG konfrontiert. Nach § 4 Abs. 1 TDDSG hat der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb der EU zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

Bei unseren Überprüfungen stellten wir oft fest, dass derartige Unterrichtungen gänzlich fehlten, nur unvollständig in den Allgemeinen Geschäftsbedingungen „versteckt“ oder aufgrund von Unkenntnis der Diensteanbieter missverständlich formuliert waren.

In der Regel konnte durch entsprechende Aufklärung und der Bereitstellung von geeignetem Informationsmaterial eine Einstellung bzw. Überarbeitung von datenschutzrechtlichen Unterrichtungen im Internetangebot erreicht werden.

14.4 Erhebung von personenbezogenen Daten im Rahmen des Registrierungsverfahrens eines Telediensteanbieters

Von dritter Seite wurden wir auf das Registrierungsverfahren eines E-Mail-Dienstes und den damit verbundenen Umfang der dabei erhobenen personenbezogenen Daten aufmerksam gemacht.

Bei der Überprüfung des besagten Registrierungsverfahrens wurde festgestellt, dass bei dem mehrstufigen Verfahren in einem Schritt noch „zusätzliche persönliche Angaben“ erfragt wurden. In Pflichtfeldern musste unter anderem Auskunft gegeben werden über „Muttersprache“, „Familienstand“, „Personen im Haushalt“, „beruflicher Status“ oder auch die Frage beantwortet werden: „Wie bzw. wo werden/wollen Sie ... den Dienst ... in der Regel nutzen?“.

Nach § 3 Abs. 1 TDDSG dürfen personenbezogene Daten vom Diensteanbieter zur Durchführung von Telediensten nur erhoben verarbeitet und genutzt werden, soweit das TDDSG oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

Aus den Vorschriften des TDDSG ergibt sich keine gesetzliche Rechtfertigung für die Erhebung der oben genannten Daten, da diese nicht für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit dem Nutzer erforderlich sind.

Auf unsere Intervention hin hat der Teledienstеanbieter sein Registrierungsverfahren entsprechend umgestellt und die fragliche Datenerhebung als „freiwillig“ gekennzeichnet. Somit konnten die Nutzer wirksam in die Datenerhebung einwilligen.

14.5 Abfrage von Nutzerdaten auf unverschlüsseltem Wege

Eine Einrichtung, die Kurse zur Weiterbildung anbietet, hatte neben Informationen zum aktuellen Kursangebot auch eine Anmeldemöglichkeit per Internet zur Verfügung gestellt. Allerdings wurden die Daten, darunter auch die Bankverbindung, auf unverschlüsseltem Wege übertragen.

In einem weiteren Fall hatte eine Zeitschrift bei ihrem Abo-Service, der ebenfalls online bereitgestellt wurde, von künftigen Kunden die zur Bestellung eines Abonnement notwendigen Daten, wie z. B. auch die Bankverbindung bei der Angabe der gewünschten Zahlungsweise usw., ebenfalls unverschlüsselt erhoben.

Werden über das Internet personenbezogene Daten erhoben, ist darauf zu achten, dass die erforderlichen technischen und organisatorischen Maßnahmen für deren Schutz auf dem Übermittlungsweg getroffen werden (vgl. Nr. 4 der Anlage zu § 9 BDSG).

In den beiden genannten Fällen haben wir wegen des umfangreichen Datenkatalogs, der für eine Anmeldung zu einem angebotenen Kurs bzw. zur Bestellung eines Abos erforderlich war, darunter auch Kontakt- und Bankverbindungsdaten, eine Verschlüsselung der Daten für notwendig erachtet. Andernfalls müssten die Nutzer deutlich auf die unverschlüsselte Übertragung hingewiesen werden, damit

sie die Risiken für sich abwägen können. Die Betroffenen können dann entscheiden, ob sie die Internetverbindung trotzdem für die Datenübertragung nutzen wollen oder den Postweg wählen.

Beide Teledienstеanbieter haben uns mitgeteilt, dass geplant sei, den Teledienst insoweit in einen ausreichenden SSL-verschlüsselten Bereich zu stellen.

14.6 Unverschlüsselte E-Mails

Unverschlüsselte E-Mails sind eine unsichere Form der elektronischen Kommunikation. Ist man sich bei der Postkarte noch bewusst, dass deren Inhalt für jedermann lesbar ist, sind die Risiken bei E-Mails noch höher. E-Mails werden auf ihrem Weg durch das weltweite Internet auf verschiedenen Servern zwischengespeichert und passieren Stationen, an denen man sie abfangen, mitlesen oder auch verändern kann. In zwei Beispielsfällen war Internetanbietern diese Problematik offensichtlich nicht bewusst.

Ein Sportverband stellte fest, dass sich jemand bei seinem Online-Angebot zwar hat registrieren lassen, dieses aber auch nach geraumer Zeit noch nicht nutzte. Er wies ihn auf diesen Umstand hin und teilte ihm per unverschlüsselter E-Mail sein bei der Registrierung vergebenes Passwort mit. Darüber hinaus erklärte er ihm nochmals den Weg zum erfolgreichen „Einloggen“ in den geschlossenen Benutzerkreis des Online-Angebots.

In einem weiteren Fall hatte ein Teledienstеanbieter per Internet eine Plattform für die Suche nach Freunden und Bekannten aus früheren Zeiten angeboten. Zu diesem Zweck werden von den Betroffenen als Suchende zahlreiche personenbezogene Daten erfasst und in einem nur den Betroffenen zugänglichen Profil abgespeichert. Eine unverschlüsselte E-Mail des Anbieters an die Betroffenen enthielt einen Direktlink auf die abgespeicherten Profildaten, ohne jeden Passwortabfrageschutz. Durch diese Zugriffsmöglichkeit konnten sowohl Daten zur Kenntnis genommen wie auch geändert werden.

In beiden Fällen haben die Anbieter des Internetangebotes, nachdem wir sie über die Sicherheitsrisiken informiert hatten, ihre Praxis geändert

* * *

15 Schlussbetrachtung

Der in diesem Bericht dargestellte Überblick über die Schwerpunkte unserer Tätigkeit in den Jahren 2002 und 2003 zeigt, dass wir mit nahezu allen aktuellen Fragen des Datenschutzrechts im nicht-öffentlichen Bereich befasst worden sind. Dies kann nicht überraschen. Haben wir es doch in Bayern mit den Hauptsitzen von vielen Unternehmen aus Wirtschaftszweigen zu tun, die dem Datenschutz in besonderer Weise verpflichtet sind. Hier streckt sich der Bogen von den vielen großen Versicherungsunternehmen, Banken und Versandhäusern über die Anbieter von Kundenkarten bis hin zu den Marktforschungsinstituten und den großen Dienstleistungsunternehmen im EDV-Bereich.

Wir können mit Befriedigung feststellen, dass sich gerade die genannten Branchen im Allgemeinen sehr um eine Beachtung des Datenschutzrechtes in ihren Betriebsabläufen bemühen. Sie tun dies weniger zur Erfüllung „lästiger“ rechtlicher Verpflichtungen als vielmehr in der Erkenntnis, dass der Datenschutz für ihre Unternehmen ein nicht zu unterschätzendes Qualitätsmerkmal und damit auch einen wesentlichen Faktor im Wettbewerb darstellt. Immer mehr Kunden, Versicherungsnehmer und Teilnehmer an Umfragen achten auf den sorgsamen Umgang mit ihren Daten. Die Unternehmen tun deshalb gut daran, wenn sie nach dem Motto „Datenschutz kommt an“ einen funktionierenden Datenschutz als Wettbewerbsvorteil in ihre Marketingkonzepte mit einbauen.

Wir von der Datenschutzaufsicht binden uns in die laufenden Prozesse mit ein, in denen es darum geht, den Datenschutz in den Unternehmen weiterzuentwickeln und an die sich immer wieder verändernden technischen Vorgaben der elektronischen Datenverarbeitung anzupassen. In dem gemeinsamen Bemühen mit den Unternehmen um eine zeitgerechte und effektive Umsetzung des Datenschutzrechts sehen wir eine wichtige Aufgabe.

Auf der anderen Seite stehen wir der Bevölkerung in Fragen des nicht-öffentlichen Datenschutzes zur Verfügung. Durch unsere Aufsicht und die Verbreitung vielfältiger Informationen, auch über die Medien, möchten wir dazu beitragen, dass der Datenschutz im Bewusstsein unserer Gesellschaft einen angemessenen Stellenwert erhält. Ein Bestandteil dieses Bemühens ist auch die Veröffentlichung dieses ersten Tätigkeitsberichtes.