Tätigkeitsbericht

2009/2010



Bayerisches Landesamt für Datenschutzaufsicht

Tätigkeitsbericht
der
Datenschutzaufsichtsbehörde
für den
nicht-öffentlichen Bereich
2009/2010

Bayerisches Landesamt für Datenschutzaufsicht

Vorwort

Mit den drei im Jahr 2009 verabschiedeten Novellen zum Bundesdatenschutzgesetz hat der Gesetzgeber den Datenschutz in der Bundesrepublik Deutschland gestärkt. Die Debatten über die neuen oder geänderten Vorschriften des Bundesdatenschutzgesetzes, die laufenden Gesetzgebungsverfahren zum Beschäftigungsdatenschutz sowie zum Schutz des Persönlichkeitsrechts durch unzulässige Veröffentlichungen im Internet (sog. Rote-Linie-Gesetz) bis hin zu den Ankündigungen der Europäischen Kommission zu einer Überarbeitung der EG-Datenschutzrichtlinie („Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010) 609 endg.") zeigen jedoch, dass schon in naher Zukunft noch weitere Rechtsänderungen zu erwarten sind, die weitere Verbesserungen beim Schutz des informationellen Selbstbestimmungsrechts, aber auch neue Fragen für die Datenschutzaufsichtsbehörden mit sich bringen werden. Der stetig wachsende technische Fortschritt der Informations- und Kommunikationstechnologie, das ebenso rasante Anwachsen unvorstellbar großer Datenvolumina in den sog. sozialen Netzwerken und vielen anderen Bereichen des Internets, und die mit der Globalisierung zwangsläufig verbundene Zunahme des internationalen Datenverkehrs zeigen sowohl dem deutschen und europäischen Gesetzgeber als auch den Datenschutzaufsichtsbehörden immer wieder neue Fragestellungen auf, für die datenschutzgerechte Lösungen zu entwickeln sind.

Das Landesamt geht davon aus, dass die Bedeutung des Datenschutzes im nicht-öffentlichen Bereich auch in Zukunft weiter zunehmen wird. Ein Indiz dafür mag die öffentliche Wahrnehmung von Datenschutzthemen in den Medien gerade in den beiden Jahren des Berichtszeitraums dieses Tätigkeitsberichts sein.

Schon in den letzten beiden Jahren kamen die meisten Eingaben aus dem Bereich des Internets. Es ist davon auszugehen, dass die Fortschritte der Informationstechnologie und der Wandel des Nutzerverhaltens einschließlich der Entwicklung zunehmend globalisierter Datenverarbeitungen (Stichwort Cloud Computing) auch in den kommenden Jahren den Datenschutz im Internet zu einer der zentralen Aufgabenstellungen der bayerischen Datenschutzaufsichtsbehörde machen werden.

Rückmeldungen der Bürgerinnen und Bürger und aus Wirtschaft, Politik und Verwaltung zeigen, dass die Datenschutzaufsicht im nicht-öffentlichen Bereich in Bayern bisher den in sie gesetzten Erwartungen nicht nur Rechnung tragen konnte, sondern sich eine hohe Wertschätzung erarbeiten konnte. Dafür gebührt meinem Vorgänger im Amt, Herrn Günther Dorn, der seit der Aufgabenzentralisierung an der Spitze der Datenschutzaufsicht für den nicht-

öffentlichen Bereich in Bayern gestanden ist, und allen Mitarbeiterinnen und Mitarbeitern des Landesamts ganz herzlicher Dank. Ebenso danke ich Herrn Regierungspräsidenten Dr. Bauer, Herrn Regierungsvizepräsidenten Dr. Ehmann und den Mitarbeiterinnen und Mitarbeitern der Regierung von Mittelfranken, die dem Landesamt vor allem in organisatorischer Hinsicht zahlreiche Hilfestellungen geleistet haben und leisten. Möge es gelingen, dass wir unseren Aufgaben zum Wohle der Bürgerinnen und Bürger in Bayern auch in Zukunft erfolgreich gerecht werden.

Ansbach, im März 2011

Thomas Kranig
Leiter des Bayerischen
Landesamtes für Datenschutzaufsicht

Inhaltsverzeichnis

1 Datenschutzaufsicht im nicht-öffentlichen Bereich 10
1.1 Aufgaben einer Datenschutzaufsichtsbehörde 10
1.2 Gesetzliche Grundlage für die Erstellung des Tätigkeitsberichts 10
1.3 Bayerische Datenschutzaufsichtsbehörde 10
1.4 Erste Erfahrungen mit den BDSG Novellen 2009 11
2 Allgemeiner Überblick über die Tätigkeit des Landesamtes 12
2.1 Statistik 12
2.1.1 Bearbeitung von Eingaben (Anfragen und Beschwerden) 12
2.1.2 Beratung der verantwortlichen Stellen und der betrieblichen Datenschutzbeauftragten 14
2.1.3 Kontrolltätigkeit 15
2.1.4 Ordnungswidrigkeitenverfahren und Strafanträge 16
2.1.5 Öffentliches Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen (§ 38 Abs. 2 BDSG) 16
2.2 Zusammenarbeit mit den anderen Datenschutzaufsichtsbehörden 17
2.3 Teilnahme und Mitwirkung bei Veranstaltungen der Wirtschaft und anderer Berufsgruppen 17
2.4 Datenschutzfachtagungen und -kongresse 18
2.5 Öffentlichkeitsarbeit 18
3 Der betriebliche Datenschutzbeauftragte 20
3.1 Unmittelbare und umfassende Unterstellung unter die Unternehmensleitung 20
3.2 Die Datenschutzschulung der Beschäftigten – eine wichtige Aufgabe des Datenschutzbeauftragten 21
4 Rechtsfragen des Datenschutzes im Internet 22
4.1 Veröffentlichung personenbezogener Daten im Internet 22
4.1.1 Allgemeines 22
4.1.2 Fotos von Personen im Internet 23
4.1.3 Straßenansichten im Internet („Google Street View") 24
4.1.4 Bewertung von Personen im Internet 26
4.1.5 Veröffentlichung von Privatinsolvenzdaten im Internet 28
4.2 Erhebung, Verarbeitung und Nutzung von Nutzerdaten 29
4.2.1 Speicherung von IP-Adressen 29
4.2.2 Analyseverfahren zur Webseitennutzung 30
4.2.3 Rechtsfragen der mobilen Internetnutzung 32
4.3 Soziale Netzwerke im Internet 34

5 Übertragung von Aufgaben auf andere Unternehmen (Outsourcing) 35
5.1 Auftragsdatenverarbeitung 35
5.1.1 Gegenstände einer Auftragsdatenverarbeitung 35
5.1.2 Höhere Anforderungen bei der Auswahl und Überwachung von Auftragnehmern ... 36
5.1.3 Praxisfall: Auftragsdatenverarbeiter gibt Daten eigenmächtig weiter 37
5.2 Funktionsübertragung 38
6 Versicherungen 40
6.1 Fahrlässige Veröffentlichung von Gesundheitsdaten eines Kunden im Internet 40
6.2 Unbefugte und zweckwidrige Verwendung von Versicherungsdaten durch eine Beschäftigte eines Lebensversicherungsunternehmens 40
6.3 Erhebung von Gesundheitsdaten durch Versicherer bei Dritten im Rahmen der Risiko- oder Leistungsprüfung 41
7 Banken 43
7.1 Schülerpraktikum bei Banken 43
7.2 Einwilligung in die Auswertung von Kontobewegungen für Kundenbetreuung 43
7.3 Prüfung von Mitarbeiterkonten 44
7.4 Herausgabe von Bankunterlagen an Dritte, deren Empfangsvollmacht vom Kontoinhaber widerrufen worden ist 45
7.5 Bildschirmanzeigen am Geldautomat bzw. Kontoauszugsdrucker 45
7.6 Aufzeichnung von Telefongesprächen mit Banken 46
7.7 Berechtigungskonzepte und Protokollierungen der Kontenzugriffe 47
8 Auskunfteien 48
8.1 Mehr Transparenz im Auskunfteiwesen 48
8.2 Das berechtigte Interesse an einer Auskunfteiabfrage 49
8.2.1 Vor einer Probefahrt 50
8.2.2 Bonitätsauskünfte über Mieter im Rahmen einer Immobilienbewertung 51
8.2.3 Vor einem reinen Beratungsgespräch für einen Küchenkauf 51
8.2.4 Überlegungen bezüglich einer Beendigung der Geschäftsbeziehung wegen häufiger unberechtigter Beschwerden des Kunden 52
8.2.5 Aus privatem Anlass 52
9 Werbung, Adressenhandel 54
9.1 Telefon- und Faxwerbung 54
9.1.1 Wettbewerbsrechtliche Kriterien der Telefon- und Faxwerbung 54
9.1.2 Datenschutzrechtliche Kriterien der Telefon- und Faxwerbung 55
9.2 E-Mail-/SMS-Werbung 55
9.2.1 Wettbewerbsrechtliche Kriterien der E-Mail- und SMS-Werbung 55
9.2.2 Datenschutzrechtliche Kriterien der E-Mail- und SMS-Werbung 56

9.3 Briefwerbung 56
9.3.1 Wettbewerbsrechtliche Kriterien der Briefwerbung....56
9.3.2 Datenschutzrechtliche Kriterien der Briefwerbung....56
10 Handel, Dienstleistung 58
10.1 Elektronisches Lastschriftverfahren als Zahlungsform 58
10.1.1 Problemstellung....58
10.1.2 Interessen des Handels, Rechtsposition des Kunden 59
10.1.3 Sachstand und Zielsetzung der Arbeitsgruppe....60
10.2 Fahrzeugdatenspeicher 61
10.3 Übermittlung von Kundendaten bei Geschäftsveräußerungen u.a. 63
10.3.1 Fitness-Studio verkauft Kundendaten 63
10.3.2 Übernahme eines Online-Shops incl. Kundendaten, die über das Listenprivileg hinausgingen 64
10.3.3 Weitergabe von Abonnentendaten....64
10.4 Versendung von E-Mails mit offenem „Verteiler" 65
10.5 Versendung einer CD-ROM mit Kundendaten durch ein Software-Unternehmen ...67
10.6 Offenlegung von Adressdaten und Beteiligungsquoten innerhalb einer Kommanditgesellschaft....68
11 Internationaler Datenverkehr 70
11.1 Datenübermittlung in die USA für Zwecke eines Gerichtsverfahrens 70
11.2 Neue Standardvertragsklauseln für die Datenübermittlung an Auftragsdatenverarbeiter in Drittstaaten....71
11.3 Auftragsdatenverarbeitung in Drittstaaten....72
12 Beschäftigtendatenschutz 74
12.1 Unternehmensinterne Veröffentlichung von Rankings 74
12.2 Online-Bewerbung....74
12.3 Weiterleitung einer Absage an Mitbewerber....75
12.4 Anzeige von Krankheitstagen im Intranet....76
13 Gesundheitswesen 77
13.1 Übermittlung einer Behandlungsakte durch einen Arzt an seinen Rechtsanwalt im Rahmen einer rechtlichen Auseinandersetzung mit einem Patienten....77
13.2 Überschießende Datenübermittlung durch behandelnden Arzt an ein Versicherungsunternehmen....78
14 Vereine und Verbände 80
14.1 Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen 80
14.2 Übermittlung von Spenderdaten bei Anlassspenden....81

15 Wohnungswirtschaft und Mieterdatenschutz 83
15.1 Mieterselbstauskünfte 83
15.2 Einholen von Auskünften über die Bonität von Mietinteressenten bei Auskunfteien 84
15.3 Benennung einer Wohnung als Vergleichsobjekt im Mieterhöhungsverfahren 86
15.4 Datenschutz bei „intelligenter“ Stromverbrauchsmessung - Smart Metering 87
16 Videoüberwachung 89
16.1 Videoüberwachung der Außenbestuhlung eines Cafes 89
16.2 Videoüberwachung in Aufzugskabine oder Waschküche 89
16.3 Videoüberwachung in einer Gaststätte 90
16.4 Videoüberwachung des Küchenpersonals 91
16.5 Videoüberwachung in einem Fitness-Studio 91
16.6 Videoüberwachung in Lagerräumen 92
16.7 Veröffentlichung des Bildes einer Ladendiebin 92
16.8 Videoüberwachung in Bierzelten 93
17 Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten (§ 42a BDSG, § 93 Abs. 3 TKG, § 15a TMG) 94
17.1 Voraussetzungen für die Informationspflicht 94
17.2 Umsetzung der Informationspflicht 95
17.3 Praxisfälle 96
18 Entsorgung bzw. Rückgabe von Datenträgern 98
18.1 Entsorgung von Geschäftsakten in einem Altpapier- und Bauschuttcontainer 98
18.2 Rückgabe von (defekten) Geräten mit Datenspeicherungen an den Handel oder Abgabe beim Wertstoffhof 99
Stichwortverzeichnis 100

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

1.1 Aufgaben einer Datenschutzaufsichtsbehörde

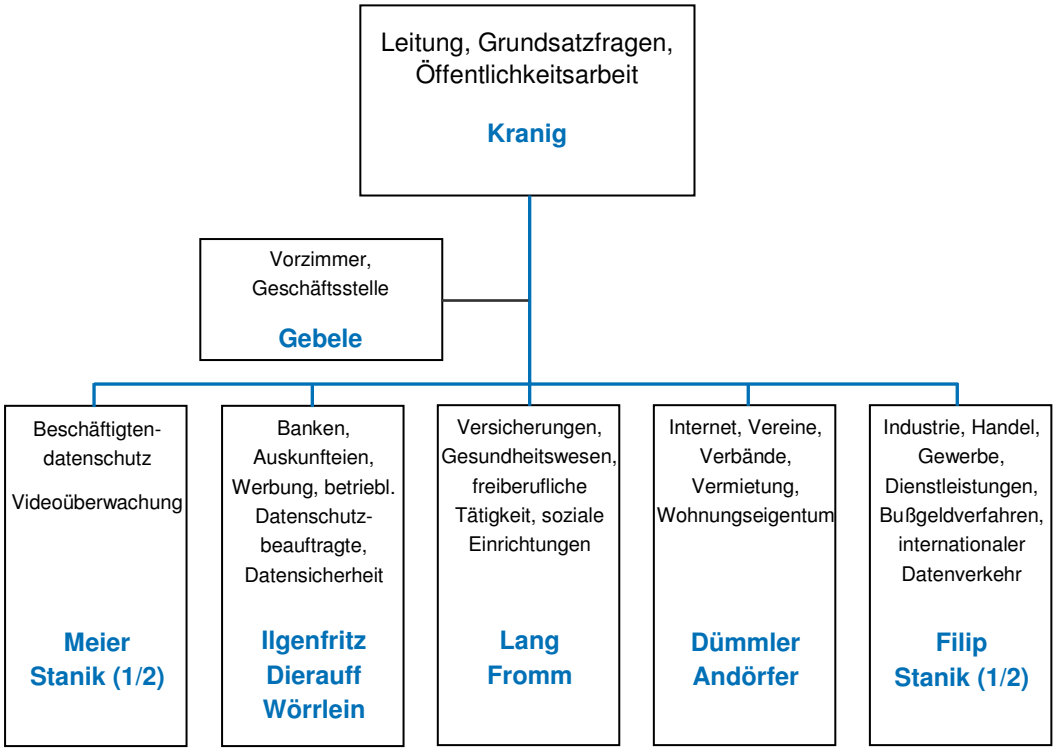
Für die Überprüfung der Einhaltung der datenschutzrechtlichen Vorschriften ist zu unterscheiden zwischen dem öffentlichen und dem nicht-öffentlichen Bereich. Für die Einhaltung der datenschutzrechtlichen Vorschriften im öffentlichen Bereich ist in Bayern der Landesbeauftragte für den Datenschutz und für die Einhaltung der datenschutzrechtlichen Vorschriften im nicht-öffentlichen Bereich das Bayerische Landesamt für Datenschutzaufsicht (im Folgenden: Landesamt) zuständig. Hinsichtlich der Überprüfung der Einhaltung der Vorschriften über die Datensicherheit wird das Landesamt durch den Technischen Überwachungsverein (TÜV Süd) unterstützt.

1.2 Gesetzliche Grundlage für die Erstellung des Tätigkeitsberichts

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

1.3 Bayerische Datenschutzaufsichtsbehörde

Die bis zum Jahr 2002 bei allen sieben Bezirksregierungen in Bayern vorhandene Zuständigkeit für die Datenschutzaufsicht im nicht-öffentlichen Bereich wurde mit einer Änderung der Datenschutzverordnung vom 3. Dezember 2001 für den Freistaat Bayern zentral der Regierung von Mittelfranken übertragen und dort im Sachgebiet 205 vollzogen. Um die Bedeutung dieser Aufgabe hervorzuheben und die zentrale Zuständigkeit für den Freistaat Bayern besser zum Ausdruck zu bringen, hat die Bayerische Staatsregierung mit Beschluss vom 3. Februar 2009 diese Aufgabe dem in der Regierung von Mittelfranken eingerichteten „Landesamt für Datenschutzaufsicht“ übertragen. Gleichzeitig wurde das Personal des Landesamts verstärkt, um dem Stellenwert des Datenschutzes im nicht-öffentlichen Bereich Rechnung zu tragen. Den derzeitigen Stand des Personalverstärkungskonzepts spiegelt folgendes Organigramm wider, das den Ausbau auf 12 Stellen zum Ende des Berichtszeitraums dokumentiert.



Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 9. März 2010 (Az. C-518/07) u.a. entschieden, dass auch die Datenschutzaufsicht im nicht-öffentlichen Bereich in „völliger Unabhängigkeit“ - so wie sie für den öffentlichen Bereich in den Bundesländern durch die jeweiligen Landesbeauftragten für den Datenschutz bzw. im Bund durch den Bundesbeauftragten als gegeben angesehen wird - erfolgen muss. Das Landesamt für Datenschutzaufsicht ist daher angesichts des Anwendungsvorrangs des Europarechts bei seiner Tätigkeit völlig frei von jeglicher Weisung.

1.4 Erste Erfahrungen mit den BDSG Novellen 2009

Selbst wenn im Folgenden eine Reihe von Fällen dargestellt werden, bei denen datenschutzrechtliche Verstöße, zum Teil auch in so erheblichem Umfang festgestellt wurden, dass sie durch Bußgeldfestsetzungen geahndet werden mussten, ist dennoch zu erkennen, dass der weitaus überwiegende Teil der nicht-öffentlichen Stellen, mit denen das Landesamt zu tun hatte, daran interessiert war, zu erfahren, welche Maßnahmen zu ergreifen sind, um die datenschutzrechtlichen Vorschriften einzuhalten. Insbesondere für die Bereiche der Auftragsdatenverarbeitung (§ 11 BDSG), der Datenerhebung und -speicherung für eigene Geschäftszwecke (§ 28 BDSG), der Auskunft an den Betroffenen (§ 34 BDSG) und der erst seit dem 1. September 2009 bestehenden Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten (§ 42a BDSG) war ein hohes Informationsbedürfnis festzustellen.

2 Allgemeiner Überblick über die Tätigkeit des Landesamtes

2.1 Statistik

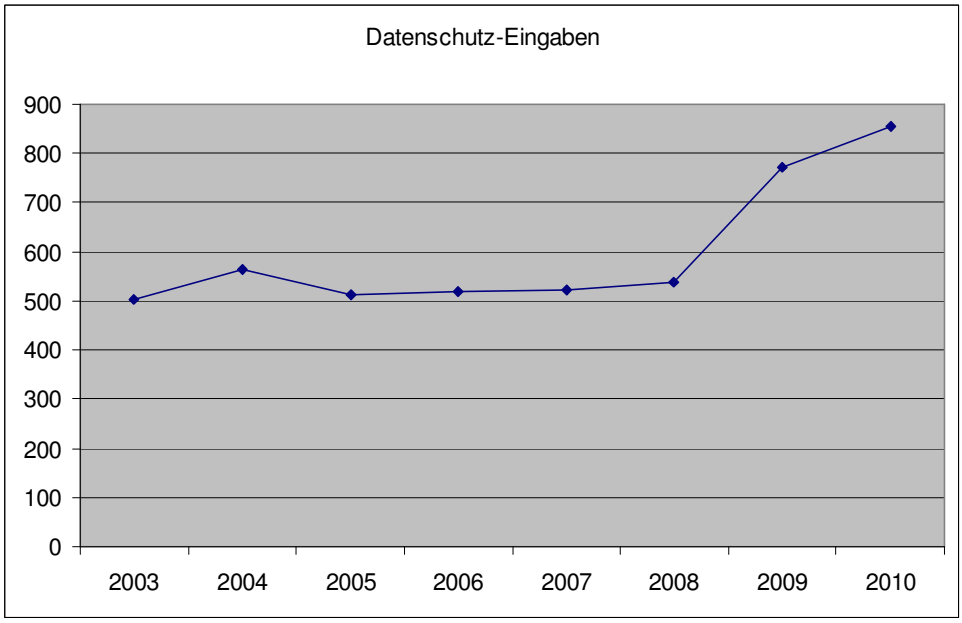
2.1.1 Bearbeitung von Eingaben (Anfragen und Beschwerden)

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

Im Berichtszeitraum 2009/2010 wurden Beschwerden zu folgenden Themen erhoben (Mehrfachnennungen sind möglich):

- Umgang mit Daten im Internet 358
- Erteilung von Eigenauskünften an Betroffene 270
- Werbung und der Adressenhandel 228
- Umgang mit Daten bei Versicherungen 155
- Übermittlung von Daten 149
- Löschung von Daten 134
- Zulässigkeit der Erhebung von Daten 120
- Umgang mit Daten bei Banken 89
- Videoüberwachung 71
- Verwendung von Daten im Gesundheitsbereich 59
- Tätigkeit von Rechtsanwälten 50
- Tätigkeit von Wirtschaftsauskunfteien 44
- Arbeitnehmerdatenschutz 39
- Maßnahmen zur Datensicherheit 35
- Umgang mit Daten in Vereinen und Verbänden 20
- Umgang mit Daten von Mietern 16
- Markt- und Meinungsforschung 11

Mit einem Gesamtanteil von ca. 20 % bildeten Eingaben, die den Umgang mit Daten im Internet betrafen, den Schwerpunkt, gefolgt von Auskunftsfragen mit ca. 15 % und Werbung und Adresshandel mit ca. 13 %. Dies bedeutet, dass die Eingaben aus diesen drei Bereichen etwa die Hälfte aller vom Landesamt bearbeiteten Eingaben betrafen.



Statistik 2009

- Schriftliche Eingaben insgesamt 773
  - Keine Verstöße 371
  - Verstöße 402
    - davon Bußgeldbescheide 11

- Anfragen/Beratungen von Betroffenen per Telefon oder E-Mail: 1255

Statistik 2010

- Schriftliche Eingaben insgesamt 856
  - Keine Verstöße 489
  - Verstöße 367
    - davon Bußgeldbescheide 11

- Anfragen/Beratungen von Betroffenen per Telefon oder E-Mail: 1084

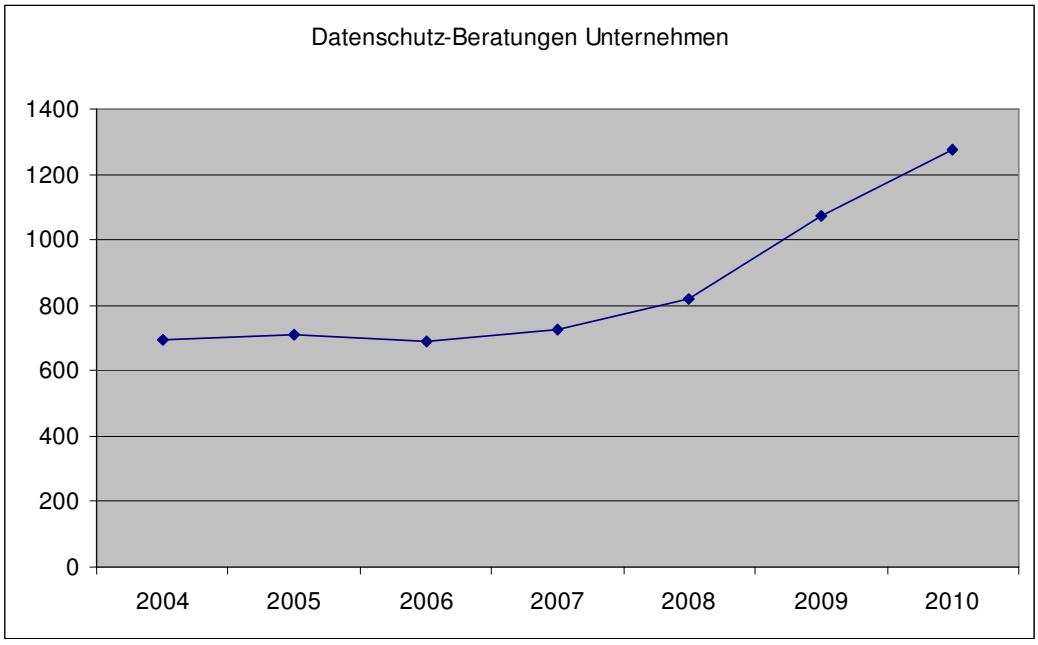
Statistisch betrachtet lag somit durchschnittlich fast jeder zweiten Eingabe ein Verstoß gegen datenschutzrechtliche Bestimmungen zu Grunde, bei denen aber lediglich in ca. 3% der Fälle Anlass zur Ahndung durch Festsetzung eines Bußgeldes bestand.

2.1.2 Beratung der verantwortlichen Stellen und der betrieblichen Datenschutzbeauftragten

Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§ 3 Abs. 7 BDSG). Datenschutzbeauftragte haben insbesondere auf die Einhaltung der datenschutzrechtlichen Vorschriften bei den verantwortlichen Stellen hinzuwirken. Die Beratung der verantwortlichen Stellen und der betrieblichen Datenschutzbeauftragten (siehe dazu auch unten unter Ziff. 4) gemäß § 38 Abs. 1 Satz 2 BDSG stellt daher einen wichtigen Schwerpunkt der Arbeit des Landesamts dar. Zur schnellen Beratung wird meist der telefonische Kontakt gesucht. Schwierigere Fallgestaltungen werden schriftlich vorgetragen oder in Besprechungen bei uns bzw. in den Unternehmen erörtert.

Folgende Themen standen im Berichtszeitraum im Vordergrund:

- Fragen des Arbeitnehmerdatenschutzes
- die neuen gesetzlichen Regelungen zu Werbedaten
- Fragen zur externen Datenverarbeitung durch Dienstleister
- Videoüberwachung
- Gestaltung von Einwilligungserklärungen
- Umgang mit personenbezogenen Daten bei Versicherungen und Banken



Statistik 2009

- Anfragen/Beratungen per Telefon, Brief, Fax oder E-Mail: 1073
- Besprechungen 28

Statistik 2010

- Anfragen/Beratungen per Telefon, Brief, Fax oder E-Mail: 1278
- Besprechungen 38

2.1.3 Kontrolltätigkeit

Es handelt sich hier sowohl um umfassende als auch um nur Einzelfragen betreffende Kontrollen, bei denen die Beachtung der datenschutzrechtlichen Vorschriften und der Datensicherheit auf den Prüfstand gestellt werden (§ 38 Abs. 1 Satz 1 BDSG). Wir haben im Berichtszeitraum sowohl schriftlich als auch vor Ort in folgendem Umfang Prüfungen durchgeführt:

- 2009: 12
- 2010 12

Es ging dabei insbesondere um folgende Themen:

- Internet-Angebote 6
- Industrieunternehmen 3
- Finanzdienstleister/Banken 3
- Dienstleistungsunternehmen verschiedener Art 4
- Videoüberwachung 2
- Wirtschaftsauskunfteien 2
- Datenschutzorganisation 2
- Medienunternehmen 1
- Callcenter 1

Handlungsbedarf aus den Feststellungen der Datenschutzprüfungen hat sich insbesondere ergeben

- zur organisatorischen Umsetzung des Datenschutzes in Unternehmen (Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten, Verfahrensverzeichnis, Verarbeitungsübersicht, Verpflichtung auf das Datengeheimnis usw.),
- im Hinblick auf die schriftlichen Vertragsregelungen bei der Auftragsdatenverarbeitung nach § 11 BDSG,
- zur Verbesserung der Transparenz für die betroffenen Personen über den Umgang mit ihren Daten,
- für notwendige Sicherheitsmaßnahmen im Sinne von § 9 BDSG,
- bei der Videoüberwachung und
- beim Umgang mit Arbeitnehmerdaten.

Im Einzelnen werden die Beanstandungen aus der Kontrolltätigkeit des Landesamts in den folgenden Fachkapiteln dargestellt.

2.1.4 Ordnungswidrigkeitenverfahren und Strafanträge

Im Berichtszeitraum hat das Landesamt insgesamt 22 Ordnungswidrigkeitenverfahren durchgeführt (je 11 in den Jahren 2009 und 2010) sowie zwei Strafanträge wegen datenschutzrechtlicher Verstöße gestellt (je eine in den Jahren 2009 und 2010).

2.1.5 Öffentliches Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen (§ 38 Abs. 2 BDSG)

Nach § 38 Abs. 2 BDSG führt die Aufsichtsbehörde ein Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen. Danach sind im Wesentlichen die folgenden zwei Geschäftsfelder gegenüber den Datenschutzaufsichtsbehörden meldepflichtig:

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

Uns liegen derzeit 138 Anmeldungen vor.

Etwa die Hälfte dieser Anmeldungen entfällt auf Auskunfteien und Adresshändler, die andere Hälfte auf Markt-, Meinungs- und Sozialforschungsunternehmen.

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

2.2 Zusammenarbeit mit den anderen Datenschutzaufsichtsbehörden

Die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich arbeiten bundesweit in dem zwei Mal jährlich tagenden sog. „Düsseldorfer Kreis“ zusammen, um grundsätzliche Rechtsfragen und die Entscheidungen in länderübergreifenden Sachverhalten abzustimmen. In das Gesamtgremium des „Düsseldorfer Kreises“ sind wir ebenso eingebunden wie auch in die dazu gehörenden Arbeitsgruppen Kreditwirtschaft, Auskunfteien/SCHUFA, Versicherungswirtschaft, Internationaler Datenverkehr, Telekommunikation/Tele- bzw. Mediendienste und Beschäftigtendatenschutz.

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

Die Ergebnisse der Beratungen werden, wenn ein Einvernehmen erreicht werden konnte, in Beschlüssen festgehalten. Eine Übersicht über die vom Düsseldorfer Kreis seit 2006 gefassten Beschlüsse finden Sie auf der Homepage des Bundesbeauftragten für Datenschutz und Informationsfreiheit unter: www.datenschutz.bund.de.

Einmal im Jahr treffen sich die Vertreter der Datenschutzaufsichtsbehörden bei einem Workshop zur Klärung und Abstimmung von Praxisfragen.

2.3 Teilnahme und Mitwirkung bei Veranstaltungen der Wirtschaft und anderer Berufsgruppen

Betriebliche Datenschutzbeauftragte treffen sich unter der Federführung der Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) zum Erfahrungsaustausch in

sogenannten „Erfa-Kreisen“ (**Erfa**hrungsaustausch-**Kreis**), um von- bzw. miteinander zu lernen und sich fortzubilden. Diese Arbeitskreise bestehen in München, Nürnberg, Würzburg und Coburg. Ihre Sitzungen finden jeweils zwei- bis dreimal im Jahr statt.

Darüber hinaus haben die Datenschutzbeauftragten der bayerischen Versicherungen einen auf Versicherungsfachfragen ausgerichteten Datenschutz-Arbeitskreis installiert, der sich zweimal im Jahr trifft.

An diesen Veranstaltungen nehmen wir auf Einladung der Veranstalter regelmäßig teil, halten Fachvorträge, nehmen zu den diskutierten Problemen Stellung und beantworten Anfragen.

2.4 Datenschutzfachtagungen und -kongresse

Mehrmals im Jahr besuchen wir Datenschutz-Kongresse, bei denen über die aktuellen Fragen des Datenschutzes und der Datensicherheit in Deutschland referiert und diskutiert wird.

Auf Wunsch und im Zusammenwirken mit Unternehmensverbänden und Datenschutzorganisationen haben wir bei Fortbildungsveranstaltungen, Kongressen und Seminaren Vorträge zu datenschutzrechtlichen Themen gehalten, um auch auf diesem Weg eine Breitenwirkung in der Datenschutzinformation zu erreichen:

- 2009: 22 Vorträge
- 2010: 31 Vorträge

2.5 Öffentlichkeitsarbeit

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

Zahlreiche Besuche von Abgeordneten des Bayerischen Landtags wie auch des Bundestages sowie Gespräche und Anfragen unterstreichen das politische Interesse an einem Informationsaustausch über konkrete Erfahrungen der datenschutzaufsichtlichen Praxis.

Der Leiter des Landesamtes nahm am 18. Mai 2009 an einem Spitzengespräch über Fragen des Beschäftigtendatenschutzes beim Bayerischen Staatsminister des Innern, Joachim Herrmann, mit Vertretern des Verbandes der Bayerischen Wirtschaft und der Gewerkschaften teil.

Er stellte bei der Dialogveranstaltung „Perspektiven Deutscher Netzpolitik“ des Bundesministers des Innern, Dr. Thomas de Maiziere, am 18. Januar 2010 in Berlin die Sichtweise einer Datenschutzaufsichtsbehörde zu Datenverwendungen im Internet vor.

Am 25. Februar 2010 erstattete er dem Ausschuss für Verfassung, Recht, Parlamentsfragen und Verbraucherschutz im Bayerischen Landtag einen Bericht über die Arbeitsschwerpunkte des Landesamtes im Jahr 2009.

In der Sitzung dieses Ausschusses vom 21. Oktober 2010 beantwortete er Fragen zu den Erfahrungen des Landesamtes zu sozialen Netzwerken.

3 Der betriebliche Datenschutzbeauftragte

3.1 Unmittelbare und umfassende Unterstellung unter die Unternehmensleitung

Nach dem Bundesdatenschutzgesetz ist der Beauftragte für den Datenschutz dem Leiter der nicht-öffentlichen Stelle - ohne Zwischenebenen- unmittelbar zu unterstellen.

Auf die häufiger gestellte Frage, wie die in § 4f Abs. 3 BDSG vorgesehene unmittelbare Unterstellung des Datenschutzbeauftragten unter den Leiter der verantwortlichen nicht-öffentlichen Stelle umzusetzen ist, geben wir vor allem folgende Hinweise:

- Der Leiter muss die Vorgesetztenfunktion in vollem Umfang wahrnehmen, so zum Beispiel die Personalaufsicht und die disziplinarische Zuständigkeit ebenso wie die Zuteilung des erforderlichen Budgets. Der Datenschutzbeauftragte darf nicht mehreren Personen unterstellt sein.

- Zwischen dem Datenschutzbeauftragten und der Unternehmensleitung dürfen sich keine Zwischenebenen befinden. Sinn der gesetzlich vorgeschriebenen unmittelbaren Unterstellung des Datenschutzbeauftragten unter den Leiter der nicht-öffentlichen Stelle ist, dass der Datenschutzbeauftragte seine Aufgaben unbeeinflusst, unabhängig und weisungsfrei wahrnehmen kann und einen „ungefilterten" Zugang zum Leiter hat. Damit wäre nicht vereinbar, wenn er in seiner Funktion in eine weitere Organisationseinheit eingegliedert ist. Denn bei dieser vorgesetzten Stelle können leicht Interessenkonflikte zwischen dem Datenschutz und den weiteren Aufgaben auftreten, die das Gesetz mit der unmittelbaren Unterstellung des Datenschutzbeauftragten unter den Leiter der nicht-öffentlichen Stelle vermeiden wollte.

- Die Zuordnung des Datenschutzbeauftragten zur Unternehmensleitung muss im Organigramm klar erkennbar sein.

3.2 Die Datenschutzschulung der Beschäftigten – eine wichtige Aufgabe des Datenschutzbeauftragten

Der Datenschutzbeauftragte muss die Personen, die im Unternehmen mit personenbezogenen Daten umgehen, tätigkeitsbezogen mit den einschlägigen Vorschriften über den Datenschutz vertraut machen.

Bei unseren Prüfungen wie auch bei der Aufarbeitung von Datenschutzverstößen stellen wir oft fest, dass die Beschäftigten und andere im Unternehmen tätige Personen, z.B. Leiharbeiter, mit den Datenschutz- und Datensicherheitsbestimmungen nicht genügend vertraut sind. Wir führen dies unter anderem auf nicht genügende Schulungen zurück.

Die Verpflichtung, die Beschäftigten mit den einschlägigen Vorschriften vertraut zu machen, obliegt sowohl der Unternehmensleitung als auch dem Datenschutzbeauftragten (§ 4g Abs. 1 Satz 4 Nr. 2 BDSG). Sie beginnt bei der Aufnahme der Tätigkeit eines Beschäftigten im Rahmen der Verpflichtung auf das Datengeheimnis gemäß § 5 BDSG. Wir haben hierzu in unserem 3. Tätigkeitsbericht (2008) unter der Nr. 2 nähere Hinweise zum Inhalt und zur Durchführung der Verpflichtung gegeben.

Nach dieser ersten Belehrung, bei der nur die allgemeinen Grundsätze angesprochen werden können, müssen in der Folgezeit je nach der Art der Tätigkeit weitere Schulungen im Datenschutz folgen. Dabei kommt es für die Intensität der Schulungen darauf an, ob die Beschäftigten z.B. in der Personalverwaltung, der Werbeabteilung, beim Forderungseinzug oder im IT-Bereich tätig sind.

Für die Schulungen können auch E-Learning-Tools eingesetzt werden, die abzuarbeiten und mit der erfolgreichen Beantwortung von Prüfungsfragen abzuschließen sind.

Neben regelmäßigen allgemeinen Schulungen zum Datenschutz empfehlen sich auch Beiträge in den Personalversammlungen ebenso wie tätigkeitsbezogene spezielle Informationen für die Fachabteilungen mit Hinweisen auf aktuelle Themen und Entwicklungen.

4 Rechtsfragen des Datenschutzes im Internet

Bei der Behandlung von Rechtsfragen des Datenschutzes im Internet ist zu unterscheiden zwischen der Rechtmäßigkeit der Veröffentlichung von personenbezogenen Daten über Dritte (siehe dazu 4.1), und der Erhebung, Verarbeitung und Nutzung von Nutzerdaten (siehe dazu 4.2).

4.1 Veröffentlichung personenbezogener Daten im Internet

4.1.1 Allgemeines

Die Veröffentlichung personenbezogener Daten im Internet hat das Bayerische Landesamt für Datenschutzaufsicht auch im aktuellen Berichtszeitraum in erheblichem und zunehmendem Umfang beschäftigt. Die Erscheinungsformen sind vielgestaltig. Sie reichen von Beiträgen auf Bewertungsplattformen über Online-Datenbanken zu Privatinsolvenzen bis hin zu Bildern und Videos von Personen im Internet.

Der Anwendungsbereich des BDSG ist eröffnet, wenn die veröffentlichten Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person darstellen, § 3 Abs. 1 BDSG. Hierzu gehören nicht nur die „klassischen" Angaben über eine Person wie Name, Adresse, Geburtsdatum und Geburtsort. Vielmehr umfasst der Begriff des personenbezogenen Datums alle Informationen, die über eine Bezugsperson etwas aussagen oder mit ihr in Verbindung zu bringen sind (so auch der Bundesgerichtshof im „spickmich.de"-Urteil vom 23.06.2009, Az.: VI ZR 196/08, siehe unten unter 4.1.4.). Personenbezogene Daten sind daher insbesondere auch

- Meinungsäußerungen, Beurteilungen und Werturteile, die sich auf eine bestimmte oder bestimmbare Person beziehen,
- die Wiedergabe von mündlichen und schriftlichen Aussagen einer Person und
- die Darstellung des privaten oder dienstlichen Verhaltens einer Person.

Die Veröffentlichung dieser Daten im Internet stellt datenschutzrechtlich eine Übermittlung personenbezogener Daten in der Form dar, dass Dritte die zur Einsicht oder zum Abruf bereitgehaltenen Daten einsehen oder abrufen, § 3 Abs. 1 und Abs. 4 Nr.

3b BDSG. Die Zulässigkeit der Veröffentlichung richtet sich nach den Vorschriften des BDSG, bei Bildern von Personen nach dem Kunsturhebergesetz (KUG).

4.1.2 Fotos von Personen im Internet

Das Veröffentlichen von Fotos von Personen im Internet bedarf grundsätzlich der Einwilligung der abgebildeten Personen gemäß § 22 KUG.

Bei vielen Gelegenheiten, insbesondere Veranstaltungen, werden Einzelpersonen, Paare oder Gruppen fotografiert und diese Bilder dann ins Internet gestellt. Dem Zweck, die Fotos auf möglichst einfache Weise zu verbreiten, steht das Recht der Fotografierten am eigenen Bild gegenüber, denn die Fotos sind nicht nur weltweit zugänglich, sondern können kopiert, bearbeitet und für vielfältige Zwecke verwendet werden.

Die Zulässigkeit der Veröffentlichung von Fotos, die Personen zeigen, beurteilt sich nach den Vorschriften des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KUG). Diese gehen als bereichsspezifische Vorschriften i. S. v. § 1 Absatz 3 Satz 1 BDSG den Regelungen des BDSG vor. Das Veröffentlichen der Fotos im Internet bedarf danach grundsätzlich der Einwilligung der fotografierten Personen, § 22 KUG. Die Einwilligung nach § 22 KUG kann ausdrücklich oder konkludent abgegeben werden. Bei einer Einwilligung durch schlüssiges Handeln ist Folgendes zu beachten:

- Die freiwillige Teilnahme an einer Veranstaltung, auf der Fotos gemacht werden, reicht als Einwilligung durch schlüssiges Handeln für die Veröffentlichung der Bilder im Internet nur aus, wenn für den Teilnehmer vor dem Betreten des Veranstaltungsortes klar ist, dass dort Fotos gemacht werden **und** diese nach der Veranstaltung online veröffentlicht werden. Daher muss im Eingangsbereich entsprechend auffällig auf diese Umstände hingewiesen werden.

- Posieren für den Fotografen (ohne entsprechende Hinweisschilder im Eingangsbereich) reicht als konkludente Einwilligung für eine Internetveröffentlichung der Bilder nicht aus. Die fotografierten Personen erklären sich nur mit dem Fotografiertwerden konkludent einverstanden, ein Erklärungswert hinsichtlich einer Internetveröffentlichung der Bilder kann daraus nicht abgeleitet werden.

Jeder hat das Recht, seine Einwilligung nach § 22 KUG für die Veröffentlichung seiner Bilder im Internet zu widerrufen. Die Bilder sind dann unverzüglich zu entfernen.

Ohne Einwilligung der Betroffenen ist eine Veröffentlichung der Fotos nur unter den Voraussetzungen von § 23 KUG zulässig. Danach können

- Bildnisse aus dem Bereich der Zeitgeschichte,
- Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen,
- Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben und
- Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient,

verbreitet und zur Schau gestellt werden, sofern hierdurch kein berechtigtes Interesse des Abgebildeten verletzt wird.

4.1.3 Straßenansichten im Internet („Google Street View")

Bei den vom Internetdienst „Google Street View" gezeigten Straßenansichten sind die Gesichter der zufällig erfassten Personen, aber auch Kfz-Kennzeichen aus Datenschutzgründen zu verpixeln.

In „Google Street View" sind Panoramabilder von Straßenzügen zu sehen, die mit Kameras, die in einer Höhe von ca. 2,90 m auf speziellen Fahrzeugen montiert sind, aufgenommen wurden.

Die Gesichter der zufällig erfassten Personen und Kfz-Kennzeichen, die als personenbezogene Daten anzusehen sind, sind aus Datenschutzgründen vor einer Veröffentlichung im Internet zu verpixeln. Darüber hinaus hat der Hamburgische Datenschutzbeauftragte, der aufgrund der deutschen Niederlassung von Google in Hamburg federführend für die Aufsichtsbehörden in Deutschland mit Google verhandelt hat, mit Google vereinbart, dass die Betroffenen Widerspruch gegen die Abbildung ihrer (ganzen) Person, ihres Kfzs und des ihnen gehörenden oder von ihnen bewohnten Anwesens einlegen können.

Nachdem im Zuge der Befahrungen bekannt geworden war, dass nicht nur Panoramabilder, sondern auch WLAN-Daten einschließlich - sofern die Netze nicht gesichert waren - Kommunikationsdaten aufgenommen worden waren, hat der Bayerische Staatsminister des Innern im Mai 2010 Google aufgefordert, die Befahrungen einzustellen, bis alle Sachverhalte im Zusammenhang mit der Erfassung privater WLAN-Daten durch die zuständigen Datenschutzaufsichtsbehörden geklärt sind und die Wiederherstellung rechtmäßiger Aufnahmebedingungen bestätigt ist. Google hat daraufhin verbindlich mitgeteilt, dass die Aufnahmefahrten von Street View erst dann wieder aufgenommen würden, wenn die Street View Fahrzeuge so umgerüstet seien, dass WLAN-Daten von diesen Aufnahmefahrzeugen nicht mehr erfasst werden könnten.

Der Internetdienst „Street View" von Google ist seit dem 18. November 2010 für die 20 größten deutschen Städte, darunter München und Nürnberg, online verfügbar. Bereits am 2. November 2010 gingen die Street-View-Ansichten der Gemeinde Oberstaufen im Allgäu auf deren besonderen Wunsch online. Vor der Veröffentlichung hatte sich die Gemeinde Oberstaufen mit dem Landesamt in Verbindung gesetzt, um ihre Bewohner über die Widerspruchsmöglichkeiten zu informieren. Nach Mitteilung der Gemeinde haben 16 Personen um die Verpixelung von Gebäuden gebeten.

Das Thema „Google Street View" war eines unserer Schwerpunktthemen am Tag der offenen Tür am 12. September 2010. Daneben informierten wir regelmäßig die Landratsämter und kreisfreien Städte in Bayern über geplante Befahrungen in ihrem Gebiet verbunden mit der Bitte, die Informationen an die örtliche Presse und an die Gemeinden weiterzugeben. Trotz der lebhaften Debatte in den Medien haben sich die bei uns eingereichten Beschwerden und Nachfragen zu „Google Street View" aber in Grenzen gehalten.

Das Landesamt wird vor der für das Jahr 2011 geplanten Wiederaufnahme der Befahrungen im Freistaat Bayern eine Überprüfung der Fahrzeuge vornehmen und sich davon überzeugen, dass die zur WLAN-Datenerfassung benutzten Geräte aus den Fahrzeugen entfernt worden sind. Im Übrigen wird das Landesamt darauf hinwirken, dass die von Google zu erfüllenden Auflagen zur Gewährleistung des Datenschutzes eingehalten werden, insbesondere die Möglichkeit eines zeitlich angemessenen Vorabwiderspruchs, d.h. eines Widerspruchs gerichtet auf die der Verpixelung der Fassadenansicht vor Veröffentlichung im Internet, weiterhin bestehen bleibt. Nähere

Hinweise zum Widerspruchsverfahren einschließlich Muster-Widerspruchsschreiben bieten wir nach wie vor auf unserer Homepage zum Download an (www.datenschutz aufsicht.bayern.de). Außerdem bieten wir weiterhin an, dass Widerspruchsschreiben auch bei uns zur Weiterleitung an Google eingereicht werden können.

Parallel zu diesen Fragen des Vollzugs des geltenden Datenschutzrechts im Zusammenhang mit der Veröffentlichung von Panoramaansichten unserer Städte im Internet konnte auch die rechtspolitische Diskussion hierzu im Berichtszeitraum noch nicht abgeschlossen werden:

Der Bundesrat hat im Juli 2010 einen Gesetzentwurf beschlossen, der besondere datenschutzrechtliche Regelungen für den Umgang mit personenbezogenen Daten im Zusammenhang mit der georeferenzierten großräumigen Erfassung von Gebäuden, Straßen, Plätzen sowie vergleichbaren Geodaten vorsieht (BR-Drs. 259/10). Die Beratungen des Deutschen Bundestages über diese Initiative standen zum Abschluss des Berichtszeitraums noch aus. Als Gegenentwurf zu den Vorschlägen des Bundesrates legte das Bundesinnenministerium ein Konzept aus begrenzten gesetzlichen Regelungen zum Datenschutz im Internet und ergänzend dazu der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) seinen Kodex zur Selbstverpflichtung im Umgang mit Panorama-Bilderdiensten für Anbieter von Geodatendiensten vor. Dieser vom BITKOM am 1. Dezember 2010 vorgestellte Kodex wird in Gesprächen mit den Datenschutzaufsichtsbehörden sowohl bezüglich seines Inhalts als auch bezüglich seiner möglichen Verbindlichkeit (§ 38a BDSG) noch intensive Beratung erfordern.

4.1.4 Bewertung von Personen im Internet

Die Bewertung von Personen im Internet ist mit deren Einwilligung oder in den Fällen zulässig, in denen eine Interessenabwägung ergibt, dass das schutzwürdige Interesse des Betroffenen nicht überwiegt. Ob dies der Fall ist, muss in jedem Einzelfall gesondert geprüft werden.

Wesentlich einschneidender für das Persönlichkeitsrecht des Einzelnen als die Abbildung der Fassade seines Hauses ist die Bewertung seiner Person im Internet.

Der Bundesgerichtshof (BGH) hatte im sogenannten „spickmich.de"-Urteil vom 23. Juni 2009 (Az. VI ZR 196/08) über die Klage einer Lehrerin zu entscheiden, die

sich mit dem Ziel der Löschung bzw. Unterlassung der Veröffentlichung ihres Namens, der Schule und der unterrichteten Fächer auf der Domain www.spickmich.de an die Gerichte gewandt hatte. Der BGH lehnte den Unterlassungsanspruch der Lehrerin mit der Feststellung ab, dass sie nicht in ihrem allgemeinen Persönlichkeitsrecht verletzt sei. Zur Begründung wies er darauf hin, dass hier eine Abwägung zwischen dem Schutz des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG und dem Recht auf Kommunikationsfreiheit nach Art. 5 Abs. 1 GG erfolgen müsse. Der Name, die berufliche Tätigkeit und die unterrichteten Fächer der Lehrerin seien (zutreffende) Tatsachenbehauptungen, so dass schon deshalb ein Unterlassungsanspruch ausscheide. Die (in diesem Fall vorhandenen) Bewertungen stellten weder eine unsachliche Schmähkritik noch eine formale Beleidigung oder einen Angriff auf die Menschenwürde der Lehrerin dar, die eine Abwägung der Rechte der Beteiligten entbehrlich gemacht hätte. Ein schutzwürdiges Interesse der Klägerin gegen die Erhebung und Nutzung der Daten durch die Beklagte, die Betreiberin der Domain, sei nicht gegeben, so dass die Speicherung und Veröffentlichung der Daten nach § 29 Abs. 1 Satz 1 und Abs. 2 Nr. 1a und 2 BDSG zulässig sei. Ferner umfasse die Meinungsfreiheit das Recht des Äußernden, die Modalitäten seiner Äußerung und damit das Verbreitungsmedium (hier das Internet) frei zu bestimmen. Grundsätzlich könnten Form und Umstände einer Meinungskundgabe so gewählt werden, dass damit die größte Verbreitung oder die stärkste Wirkung erzielt werde. Bewertungsportale bewegten sich naturgemäß in einem Spannungsfeld, in dem der Betroffene bei negativen Bewertungen ein Interesse am Ausschluss der Verwendung seiner Daten habe. Beschränkungen der grundrechtlich geschützten Meinungs- und Informationsfreiheit seien aber nur dann rechtmäßig, wenn sie verhältnismäßig seien. Die Befürchtung einer generellen Prangerwirkung könne kein schutzwürdiges Interesse für die von den Schülern benotete Lehrerin begründen, solange Anhaltspunkte für eine solche Wirkung im Hinblick auf ihre Person nicht gegeben seien.

Die dagegen eingelegte Verfassungsbeschwerde wurde vom Bundesverfassungsgericht nicht zur Entscheidung angenommen (Beschluss vom 16.08.2010, 1 BvR 1750/09).

Wir haben bislang regelmäßig ein der Bewertung entgegenstehendes, schutzwürdiges Interesse des Betroffenen angenommen. Aus unserer Sicht wohnt dem Kommunikationsmedium „Internet" ein derart hoher Verbreitungsgrad inne, dass eine Prangerwirkung von Bewertungen im Internet nicht von vornherein verneint werden kann. Hierin liegt die besondere Intensität der Beeinträchtigung des informationellen

Selbstbestimmungsrechts des Betroffenen, selbst wenn die Bewertung nur seine Sozialsphäre betrifft, also den Lebensbereich, der sich naturgemäß in Kontakt und Auseinandersetzung mit seiner Umwelt vollzieht. Der BGH hat sich dieser Auffassung im o.g. „spickmich.de"-Urteil nicht angeschlossen und in dieser Entscheidung die Interessenabwägung zugunsten des Rechts auf freie Meinungsäußerung und auf Information und zu Lasten des informationellen Selbstbestimmungsrechts der Betroffenen ausfallen lassen. Nachdem der BGH in seiner Entscheidung aber betont hat, dass es sich um eine Einzelfallentscheidung handelt, werden wir in gleichgelagerten Fallgestaltungen das BGH-Urteil beachten, in anderen Fällen aber eine Zulässigkeit von Bewertungen im Internet weiterhin eher zurückhaltend annehmen.

4.1.5 Veröffentlichung von Privatinsolvenzdaten im Internet

Die Veröffentlichung von Privatinsolvenzdaten im Internet ist ohne Einwilligung der Betroffenen unzulässig. Etwas anderes gilt nur innerhalb der ersten zwei Wochen der öffentlichen Bekanntmachung der Privatinsolvenz, da innerhalb dieses Zeitraums die Privatinsolvenzdaten ungehindert unter der Internetadresse www.insolvenzbekanntmachungen.de **abrufbar sind.**

Onlinedatenbanken haben in größerem Umfang Informationen über Privatinsolvenzen im Internet veröffentlicht. Betroffene haben sich dagegen bei uns beschwert.

Die in diesem Rahmen vorzunehmende Interessenabwägung fällt aus unserer Sicht stets eindeutig zugunsten der schutzwürdigen Interessen des Betroffenen aus. Die Angabe, dass sich jemand in Privatinsolvenz befindet, hat Relevanz für sämtliche Lebensbereiche. So wird sich neben dem Vermieter auch der (potentielle) Arbeitgeber für diese Information interessieren. Gleiches gilt für den Bankberater oder jeglichen Geschäftspartner des Betroffenen. Auch das private Umfeld lässt diese Information nicht „kalt". Gerade diese Konsequenz wird in vielen Eingaben befürchtet.

Bei Angaben über die finanziellen Verhältnisse einer Person handelt es sich um hochsensible personenbezogene Daten, die für einen breiten Kreis eine interessante Information darstellen. Die Veröffentlichung über das Internet bedeutet, dass diese Information weltweit und einer unbegrenzten Vielzahl von Dritten zugänglich ist. Dies macht die Beeinträchtigung besonders intensiv. Damit besteht Grund zu der Annahme, dass die Betroffenen ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben.

Etwas anderes gilt nur innerhalb der ersten zwei Wochen der öffentlichen Bekanntmachung der Privatinsolvenz, da innerhalb dieses Zeitraums die Privatinsolvenzdaten ungehindert unter der oben genannten Internetadresse abrufbar sind (§ 2 Abs. 1 Nr. 3 Insolvenzbekanntmachungsverordnung - InsoBekV). Die Privatinsolvenzdaten sind insoweit allgemein zugänglich. In diesem Fall ist eine Internetveröffentlichung nur dann unzulässig, wenn das entgegenstehende Interesse des Betroffenen offensichtlich überwiegt, was in aller Regel jedoch nicht der Fall ist.

In letzter Zeit haben sich diesbezügliche Eingaben stark gehäuft. Durch unser aufsichtliches Einschreiten konnte eine umgehende Löschung und die Entfernung der Privatinsolvenzdaten von den Internetseiten einer der größten Online-Datenbanken erreicht werden.

4.2 Erhebung, Verarbeitung und Nutzung von Nutzerdaten

4.2.1 Speicherung von IP-Adressen

IP-Adressen können personenbezogene Daten sein. Ihre kurzfristige Speicherung zum Zweck der Gewährleistung der Integrität der technischen Systeme ist nach dem BDSG zulässig. Im Übrigen richtet sich die Zulässigkeit ihrer Erhebung, Verarbeitung und Nutzung nach dem Telemediengesetz (TMG). Dort findet sich keine Erlaubnis, IP-Adressen vorsorglich zu Strafverfolgungszwecken zu speichern.

Immer wieder wird uns bekannt, dass Webseiten-Betreiber die IP-Adressen von Nutzern, die ihre Webseite besuchen, längerfristig speichern. Die IP-Adresse ist eine eindeutige Nummer, die einem Gerät, das sich mit dem Internet verbinden will, durch den sogenannten Access-Provider, der den Zugang zum Internet vermittelt, zugewiesen wird.

Die IP-Adresse ist häufig nicht nur für den jeweiligen Access-Provider, der die IP-Adressen vergibt, einem bestimmten Nutzer zuordenbar. Insbesondere in den Fällen, in denen sich der Nutzer auf der besuchten Webseite registriert hat, ist auch für den jeweiligen Webseitenbetreiber eine Verbindung zwischen der empfangenen IP-Adresse und der Person des Nutzers herstellbar. Wir gehen daher im Regelfall von der Personenbezogenheit der IP-Adresse aus. Allerdings ist die Frage, ob IP-

Nummern personenbezogene Daten sind, in der Rechtsprechung nicht unumstritten (zustimmend AG Berlin-Mitte vom 27.03.2007, Az. 5 C 314/06, ablehnend AG München vom 30.09. 2008, Az. 133 C 5677/08 und Hanseatisches OLG vom 03.11.2010, Az. 5 W 126/10). Eine höchstrichterliche Entscheidung steht noch aus. Das Landesamt wird die Debatte weiter verfolgen.

Als Grund für die Speicherung der IP-Adresse wird seitens der Webseiten-Betreiber häufig angeführt, diese im Bedarfsfall den Ermittlungsbehörden zur Verfügung stellen zu können. Gerade dieses Argument belegt noch einmal den Personenbezug der IP-Adresse. Denn den Ermittlungsbehörden geht es ja darum, einen Täter zu finden, also letztendlich eine Person zu identifizieren.

Eine gesetzliche Erlaubnis, die IP-Adresse vorsorglich zu Strafverfolgungszwecken zu speichern, besteht nicht. Nach dem BDSG kommt allenfalls eine kurzfristige Speicherung, die nach unserer Auffassung sieben Tage nicht überschreiten sollte, zum Zweck der Gewährleistung der Integrität der technischen Systeme in Betracht (§ 9 Satz 1 BDSG i. V. m. der Anlage zu § 9 Satz 1 BDSG). Das im Übrigen einschlägige Telemediengesetz erlaubt die Erhebung und Verwendung von IP-Adressen ohne Einwilligung des Betroffenen nur, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen oder unter Einschränkungen für Zwecke der Werbung, Marktforschung oder der bedarfsgerechten Gestaltung der Webseite.

Wird von Ermittlungsbehörden die Herausgabe rechtmäßig (z.B. zu Zwecken der Abrechnung) gespeicherter IP-Adressen zum Zweck der Strafverfolgung verlangt, steht das Datenschutzrecht dem nicht entgegen. Die Zulässigkeit des Herausgabeverlangens hängt allein von den jeweiligen Befugnisnormen der Ermittlungsbehörden ab.

4.2.2 Analyseverfahren zur Webseitennutzung

Zahlreiche Betreiber von Internetseiten nutzen Analyse-Verfahren zur sog. Reichweitenmessung, also einer statistischen Auswertung des Nutzerverhaltens. Sie wollen damit erfahren, wer sich auf ihren Internetseiten wann und wie lange aufhält.

Die gängigen Analyseverfahren setzen hierzu sogenannte Cookies ein. Dies sind Textdateien, die auf dem Computer des Internetnutzers gespeichert werden und eine

Analyse der Benutzung der Webseite ermöglichen. In diesem Zusammenhang wird auch die IP-Adresse des genutzten Computers gespeichert.

Der Düsseldorfer Kreis, das Gremium der obersten Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich in Deutschland, hat sich auf seiner Sitzung am 26. November 2009 mit den rechtlichen Anforderungen, die an solche Analyseverfahren zu stellen sind, befasst und diese mit Zustimmung des Bayerischen Landesamtes für Datenschutzaufsicht im folgenden Beschluss unter dem Thema: „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ wie folgt veröffentlicht:

> Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden.
>
> Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes.
>
> Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:
>
> - Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.
>
> - Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.

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

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

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

- Werden pseudonyme Nutzungsprofile durch einen Auftragnehmer erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten.

4.2.3 Rechtsfragen der mobilen Internetnutzung

Mit Hilfe der von WLAN-Zugangspunkten ausgesendeten Daten lassen sich Geräte GPS-unabhängig orten. Nach der Überprüfung eines Anbieters halten wir die damit verbundene Erhebung und Verwendung von MAC-Adresse und SSID eines WLAN-Zugangspunktes in aller Regel für zulässig, sofern hierbei der Grundsatz der Datensparsamkeit beachtet wird. Ein Mitschnitt von unverschlüsselten Kommunikationsinhalten ist jedoch rechtswidrig.

Verschiedene Anbieter von Ortungssystemen nutzen die Verbreitung von WLAN-Zugangspunkten, um ihren Nutzern eine GPS-unabhängige Ortungsfunktion zur Verfügung stellen zu können. Aufgrund ihres hohen Verbreitungsgrades eignen sich nach Angaben eines Anbieters besonders drahtlose Funknetzwerke aus der Familie der IEEE 802.11 WLAN-Standards (Standardisierung eines drahtlosen Netzwerkes nach dem Institute of Electrical and Electronics Engineers). Hierbei werden Signalstärke, MAC-Adresse (Bezeichnung zur eindeutigen Identifizierung eines Geräts) und SSID (Service Set Identifier - [frei wählbarer] Name eines Funknetzes) erhoben, ver-

arbeitet und genutzt. Das Gerät des Nutzers kann mit Hilfe dieser Technologie bis auf wenige Meter genau und auch innerhalb von Gebäuden lokalisiert werden.

Sofern der Inhaber des WLAN-Zugangspunktes bei der Vergabe der SSID seinen Klarnamen verwendet hat, liegt ein personenbezogenes Datum vor. Auch für die MAC-Adresse kann ein Personenbezug nach derzeitigen Erkenntnissen nicht ausgeschlossen werden. Eine gerichtliche Klärung hierüber steht noch aus.

Personenbezug und damit Anwendbarkeit des BDSG vorausgesetzt, halten wir die Erhebung und Verwendung der SSID und MAC-Adresse zum Zweck der Lokalisierung in aller Regel für zulässig.

Sowohl SSID als auch MAC-Adresse werden von dem jeweiligen WLAN-Zugangspunkt für jedermann frei empfangbar ausgesendet. Es handelt sich insofern um allgemein zugängliche Daten. Aus unserer Sicht kommt es nicht auf ein subjektives Element dergestalt an, dass der Dateninhaber die Daten bewusst und gewollt der Öffentlichkeit zugänglich macht. Die Einstufung als allgemein zugängliche Daten hat zur Folge, dass nur im Fall eines **offensichtlichen** Überwiegens der schutzwürdigen Interessen der Betroffenen im Rahmen der Abwägung mit den berechtigten Interessen der verantwortlichen Stelle (§ 28 Abs. 1 S. 1 Nr. 3 BDSG) ein Datenschutzverstoß vorliegt. Ein offensichtliches Überwiegen der schutzwürdigen Interessen der betroffenen WLAN-Anschlussinhaber an dem Ausschluss der Datenerhebung und -verwendung sehen wir weder im Hinblick auf die MAC-Adresse noch auf die SSID, jedenfalls wenn letztere nur für einen sehr kurzen Zeitraum in einem flüchtigen Speicher erfasst wird. Zu berücksichtigen ist, dass es dem jeweiligen Anschlussinhaber freisteht, bei der SSID seinen Klarnamen bzw. andere identifizierende Merkmale zu verwenden oder nicht. SSID und MAC-Adresse werden von ihm aktiv nach außen - für einen unbestimmten Personenkreis empfangbar - ausgesendet. Die Aussagekraft der ausgesendeten Daten im Hinblick auf die Persönlichkeit des Einzelnen ist zudem gering.

Anders beurteilen wir den Einsatz der Technologie, wenn (zusätzlich) unverschlüsselte Kommunikationsinhalte abgefangen werden. Dies ist bereits für die Ortungsfunktion nicht erforderlich und stellt einen intensiven Eingriff in die Privatsphäre dar. Hierüber sind sich die Datenschutzaufsichtsbehörden in Deutschland einig. In der Frage der datenschutzrechtlichen Beurteilung der Erhebung und Verwendung von MAC-Adressen und SSIDs besteht unter den Aufsichtsbehörden derzeit eine intensive Diskussion mit unterschiedlichen Lösungsansätzen.

4.3 Soziale Netzwerke im Internet

Der Begriff "Soziale Netzwerke" ist im Zeitalter von facebook, lokalisten, stayfriends, wer-kennt-wen, schülerVZ und studiVZ, um nur einige Anbieter zu nennen, in aller Munde. Er steht für die Möglichkeiten des Einzelnen, sich über das Internet mit anderen zu vernetzen und auszutauschen. Es geht gerade darum, auch Persönliches von sich preiszugeben, um gemeinsame Interessen herauszufinden oder sich einfach nur gut zu unterhalten.

Vielfach werden aber nicht nur die eigenen Daten preisgegeben, sondern auch die Daten Dritter, was datenschutzrechtlich problematisch sein kann.

Die Rechtsdurchsetzung des Einzelnen, aber auch das aufsichtliche Einschreiten wird durch die Tatsache erschwert, dass viele Anbieter, darunter auch das derzeit größte weltweite Netzwerk im Internet, facebook, nicht in Deutschland ansässig sind. Für das Unternehmen facebook, das in Hamburg eine deutsche Niederlassung besitzt, hat der Hamburgische Beauftragte für den Datenschutz und die Informationsfreiheit in Abstimmung mit den anderen Datenschutzaufsichtsbehörden in Deutschland die Federführung übernommen. Dadurch ist aber nicht ausgeschlossen, dass das Landesamt aufgrund seiner im bayerischen Verwaltungsverfahrensgesetz geregelten örtlichen und in den Datenschutzgesetzen geregelten sachlichen Zuständigkeit ebenfalls tätig wird, wenn datenschutzrechtlich relevante Vorgänge im Freistaat Bayern auftreten.

Die Zahl der Eingaben im Sinne von Beschwerden beim Landesamt im Zusammenhang mit sozialen Netzwerken ist eher gering. Das Bedürfnis an Information über den Datenschutz in sozialen Netzwerken ist jedoch deutlich spürbar. Das Landesamt hat es sich deshalb zur Aufgabe gemacht, im Rahmen seiner Öffentlichkeitsarbeit über die Möglichkeiten des Selbstschutzes in diesen Netzwerken aufzuklären. Das Landesamt hat dazu einen Flyer mit dem Thema **„Internet - bist du dabei?"** für die Zielgruppe der 10- bis 16-jährigen Jugendlichen entwickelt, in dem Chancen und Gefahren aufgezeigt werden sowie mittels weiterführender Links auf Informationsquellen für die Privatsphäreeinstellung in sozialen Netzwerken verwiesen wird. Auf Wunsch senden wir den Flyer gerne interessierten Schulen oder jugendnahen Vereinigungen kostenlos zu. Der Flyer ist außerdem auf Homepage des Landesamtes als PDF-Datei abrufbar (www.datenschutzaufsicht.bayern.de).

5 Übertragung von Aufgaben auf andere Unternehmen (Outsourcing)

5.1 Auftragsdatenverarbeitung

Um es Unternehmen und freiberuflich Tätigen zu ermöglichen, spezielle externe Datenerhebungen und -verwendungen, z.B. elektronische Buchhaltung oder Lohnabrechnung, in praktikabler Weise durchführen zu lassen, ist in § 11 BDSG eine rechtliche Erleichterung (gegenüber den normalen Regelungen für die Übermittlung von Daten u.a. in den §§ 28 ff. BDSG) in Form der „Datenverarbeitung im Auftrag" vorgesehen. Diese Bestimmung privilegiert die verantwortliche Stelle insoweit, als sie die Weitergabe der Daten an das durchführende Unternehmen in diesem Fall nicht als Datenübermittlung qualifiziert, die durch eine Einwilligung oder eine Rechtsvorschrift gerechtfertigt werden müsste. Das Gesetz ordnet vielmehr an, dass die Auftrag gebende Stelle auch für die Tätigkeit des Dienstleisters verantwortlich bleibt und dies durch eine entsprechende Auftragsgestaltung und durch Einzelanweisungen sichergestellt werden kann, aber auch muss.

5.1.1 Gegenstände einer Auftragsdatenverarbeitung

Nach der herrschenden Meinung kann eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG in der Regel nur dann angenommen werden, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten als Hilfstätigkeit oder EDV-technische Unterstützung durchgeführt wird. Bezieht sich der Auftrag auch auf weitere Tätigkeiten, z.B. auf die technische Organisation von Dienstreisen oder auf den Betrieb eines Callcenters, so dürfen dem Auftragnehmer auf Grund enger Vorgaben keine Spielräume bleiben.

Auftragsdatenverarbeitungen können somit, sofern sie durch einen weisungsgebundenen Dienstleister erbracht werden, u.a. sein:

- der EDV-technische Teil einer Lohn- und Gehaltsabrechnung
- Finanzbuchhaltung
- Werbeadressenverarbeitung
- Betrieb eines Callcenters
- E-Mail-Verwaltung

- Datenverwaltung für den Betreiber von Internetseiten
- Datenerfassung, Mikroverfilmung oder Datenkonvertierung
- Speicherung von Backup-Sicherungsdatenbeständen
- Datenträgerentsorgung

Die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen werden gemäß § 11 Abs. 5 BDSG der Datenverarbeitung im Auftrag gleichgestellt, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

5.1.2 Höhere Anforderungen bei der Auswahl und Überwachung von Auftragnehmern

Als Reaktion auf verschiedene „Datenschutzskandale" und „Datenpannen" bei Auftragnehmern in den letzten Jahren hat der Gesetzgeber seit 1. September 2009 die Regelungen im Bundesdatenschutzgesetz zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag in § 11 BDSG ausführlicher gefasst und die Verantwortlichkeit sowie die Prüfpflichten des Auftraggebers konkretisiert.

Die schon bisher bestehenden Kontrollpflichten des Auftraggebers gegenüber dem Auftragnehmer wurden gesetzlich nun dadurch herausgehoben, dass der Auftraggeber sowohl vor Beginn der Datenverarbeitung als auch im weiteren Verlauf der Auftragsdatenverarbeitung regelmäßig beim Auftragnehmer die Einhaltung der gebotenen Sicherheitsmaßnahmen zu prüfen hat.

Dies führte bei uns zu einer Vielzahl von Beratungsanfragen, insbesondere von Unternehmen und deren Datenschutzbeauftragten sowie von Verbänden und Rechtsanwälten.

Zur Auslegung der Vorschriften haben wir die nachfolgenden Rechtsauffassungen vertreten:

- Zuständig für die Prüfungen beim Auftragnehmer über die Einhaltung der gebotenen Sicherheitsmaßnahmen ist die Unternehmensleitung des Auftraggebers, die daraus bestimmte Prüfungsaufgaben je nach Art den Fachabteilungen, der Revision, ihrem Datenschutzbeauftragten oder auch einem externen Sachverständigen übertragen kann. Vor-Ort-Kontrollen durch den Auftraggeber bei einem in Aussicht genommenen Auftragnehmer können in manchen Fällen zweckmäßig sein, wer-

den aber nach der Gesetzesbegründung nicht für jeden Fall erwartet. Bei bekannten Rechenzentren, Dienstleistern, Systemhäusern oder Internet-/E-Mail-Providern mit „gutem Ruf“ können Vor-Ort-Prüfungen eher entfallen als bei bisher unbekannten Callcentern, Direktwerbeunternehmen oder Datenträgerentsorgern.

- Es kann im Einzelfall auch ein vom Dienstleister vorgelegtes schlüssiges Datensicherheitskonzept oder ein dort durchgeführtes externes Audit durch einen unabhängigen Auditor genügen. Soweit Testate die Vor-Ort-Kontrolle ganz oder teilweise ersetzen sollen, muss die verantwortliche Stelle die Qualifikation des Auditors überprüft haben. Aus dem Testat selbst muss sie nachvollziehen können, nach welchen Kriterien und mit welchem Ergebnis im Einzelnen die Prüfung des Auftrags durchgeführt wurde. Das Testat muss die verantwortliche Stelle in den Stand versetzen können, selbst zu beurteilen, ob der Auftrag ordnungsgemäß durchgeführt wird.

- Für den Prüfungsturnus in laufenden Auftragsverhältnissen können je nach Sachverhalt Prüfungsfristen zwischen ein und drei Jahren angemessen sein, wobei auch die öffentliche Berichterstattung zu Datenschutzverletzungen sowie eigene und bekannt gewordene fremde Erfahrungen mit einem Auftragnehmer bzw. einer Branche Anlass für eine Prüfung sein sollten.

- Wichtig ist für die Auftraggeber, die Einzelheiten der Auswahlentscheidung wie auch die zum Auftragnehmer herangezogenen Prüfungsergebnisse sorgfältig schriftlich zu dokumentieren, um gegenüber den Datenschutzaufsichtsbehörden und auch bei Rechtsstreitigkeiten schlüssige Belege für die Erfüllung der gesetzlichen Auswahl- und Prüfungsverpflichtungen vorlegen zu können.

5.1.3 Praxisfall: Auftragsdatenverarbeiter gibt Daten eigenmächtig weiter

Ein Auftragsdatenverarbeiter, der Kundendaten an einen Dritten weitergibt, wird selbst zur verantwortlichen Stelle.

Ein Unternehmen übergab einer Werbeagentur Kundendatensätze (Name und postalische Anschrift) und erteilte ihr den Auftrag zur Versendung postalischer Werbeanschreiben. Die Werbeagentur gab nach Auftragserledigung die Daten an einen Konkurrenten des Auftraggebers weiter, um diesem die Versendung eigener Werbeanschreiben an die Betroffenen zu ermöglichen.

Soweit die Werbeagentur zunächst auftragsgemäß tätig war, war ihre Tätigkeit als Auftragsdatenverarbeitung gemäß § 11 BDSG zu bewerten. Mit der Weitergabe der Daten an das Konkurrenzunternehmen ging sie in rechtswidriger Weise über den ihr erteilten Auftrag hinaus. Sie übernahm bei der Datenübermittlung an das Konkurrenzunternehmen eigenmächtig die Funktion einer verantwortlichen Stelle.

Diese Datenübermittlung war unzulässig. Eine Rechtfertigung durch die im Listenprivileg vorgesehene Übermittlungsbefugnis gemäß § 28 Abs. 3 Nr. 3 BDSG (alt) bzw. § 28 Abs. 2 Sätze 4 und 6 BDSG (neu) scheidet aus, da bei einem derartigen Datenmissbrauch die schutzwürdigen Interessen der Betroffenen am Unterbleiben einer derartigen Übermittlung ihrer Daten entgegenstanden.

5.2 Funktionsübertragung

Eine über die Auftragsdatenverarbeitung hinausgehende Funktionsübertragung liegt vor, wenn einem Unternehmen eine Aufgabe zur eigenverantwortlichen Erledigung übertragen wird. Dazu gehört zum Beispiel

- das Outsourcing der Personalverwaltung,
- Mitarbeiterrekrutierung,
- Vertragskundenbetreuung,
- Finanzberatung,
- Steuerberatung,
- Unternehmensberatung,
- Wirtschaftsprüfung oder
- Inkassotätigkeit für ein anderes Unternehmen.

Da für diese Tätigkeiten die in Nr. 3.1.1 genannten Merkmale nicht vorliegen, gilt hierfür die Privilegierung des § 11 BDSG nicht. Von einer Funktionsübertragung ist auszugehen, wenn das übernehmende Unternehmen die ausgelagerten Aufgaben weitgehend selbständig durchführt. Es handelt sich hier um die Ausgliederung von ganzen Funktionen, die von den ausführenden Unternehmen in eigener Verantwortung durchgeführt werden. Derartige Funktionsübertragungen sind nur unter den Voraussetzungen des § 4 Abs. 1 BDSG zulässig.

Im Rahmen unserer aufsichtlichen Überprüfungen stellen wir immer wieder fest, dass Unternehmen derartige Auslagerungen - im Widerspruch zur Rechtslage - gleichwohl als Auftragsdatenverarbeitungen qualifizieren. Eine datenschutzrechtliche Zulässigkeit kann dann ggf. dadurch erreicht werden, dass Einwilligungen von den Betroffenen eingeholt oder die vertraglichen Vereinbarungen so gestaltet werden, dass Anforderungen einer rechtfertigenden Rechtsvorschrift erfüllt werden.

Unter Umständen kann hierfür die „Abwägungsvorschrift“ des § 28 Abs. 1 Satz 1 Nr. 2 BDSG als gesetzliche Rechtsgrundlage für die erforderliche Datenübermittlung herangezogen werden. Entscheidend ist, dass auch hier eine vertragliche Vereinbarung getroffen wird, die unter Berücksichtigung der Interessenlagen der betroffenen Personen und unter Beachtung der Zweckbindung der Datenverwendung eine Gewährleistung des Datenschutzes und der Datensicherheit beim übernehmenden Unternehmen sicherstellt. Zu diesem Zweck empfiehlt es sich für das ausgliedernde Unternehmen, geeignete Maßgaben des § 11 Abs. 2 BDSG in den Vertrag mit dem durchführenden Unternehmen aufzunehmen, das insoweit ebenfalls verantwortliche Stelle ist.

Diese Grundsätze gelten auch bei der Auslagerung oder Inanspruchnahme von meist praktischen Tätigkeiten, bei denen dem Umgang mit personenbezogenen Daten nur eine untergeordnete Bedeutung zukommt oder eine Kenntnisnahme der Daten bei der Leistungserbringung nicht ausgeschlossen ist, so zum Beispiel bei Post- oder Kurierdiensten, Transportleistungen von öffentlichen Telekommunikationsdiensten, Bankdienstleistungen als „Transportleistungen von Geld", Bewachungsdiensten, Reinigungsdienstleistungen oder Handwerkereinsätzen in Unternehmen. Hier müssen vor allem eine sich inhaltlich an der Verpflichtung auf das Datengeheimnis nach § 5 BDSG orientierende Verpflichtung sowie etwaige besondere Geheimhaltungsverpflichtungen in die entsprechenden Verträge aufgenommen werden.

6 Versicherungen

6.1 Fahrlässige Veröffentlichung von Gesundheitsdaten eines Kunden im Internet

Die Veröffentlichung von Gesundheitsdaten eines auch nur potentiellen Versicherungsnehmers im Internet durch einen Versicherungsvermittler stellt einen erheblichen datenschutzrechtlichen Verstoß dar, der, selbst wenn er nur fahrlässig begangen worden ist, mit einem Bußgeld zu ahnden ist.

Ein Kunde hatte über ein Webportal eines Versicherungsvermittlers eine Vorabanfrage zur Erstellung eines Angebots für eine Berufsunfähigkeitsversicherung gestellt. In seinem Antwortschreiben informierte der Vermittler den Kunden darüber, dass neben einem 25%-igen Prämienzuschlag wegen Bluthochdrucks ein Leistungsausschluss im Hinblick auf psychische und psychosomatische Erkrankungen mit den daraus resultierenden Störungen der körperlichen und psychischen Befindlichkeit einschließlich eventueller Folgen und Komplikationen erforderlich sei. Dieses Schreiben verschob der Vermittler versehentlich in einen falschen Dateiordner und stellte damit das Schreiben an den Kunden auf seiner Internetseite online.

Die Veröffentlichung dieser zum Teil äußerst sensiblen Gesundheitsdaten im Internet stellt eine Datenübermittlung an Dritte im Sinne des § 3 Abs. 4 Nr. 3b BDSG in der Form dar, dass die Dritten die zur Einsicht oder zum Abruf bereitgehaltenen Daten einsehen oder abrufen können. Da sie unbefugt und auch fahrlässig erfolgte, erfüllt sie den Tatbestand einer Ordnungswidrigkeit gemäß § 43 Abs. 2 Nr. 1 BDSG. Das Landesamt hat diesen Verstoß mit der Verhängung eines Bußgeldes geahndet.

6.2 Unbefugte und zweckwidrige Verwendung von Versicherungsdaten durch eine Beschäftigte eines Lebensversicherungsunternehmens

Sämtliche Angaben, die sich auf eine private Personenversicherung, hier eine Lebensversicherung, beziehen, unterliegen einem besonderen Schutz.

Die Beschäftigte eines Versicherungsunternehmens griff ohne Berechtigung auf die Versichertendaten ihres geschiedenen Ehemannes zu, der eine Lebensversicherung beim betreffenden Unternehmen unterhielt. Sodann übermittelte sie die Daten, unter

denen sich keine Gesundheitsdaten befanden, an ihren Rechtsanwalt, damit dieser die Informationen aus dem Lebensversicherungsvertrag im Rahmen eines familiengerichtlichen Verfahrens gegen den geschiedenen Ehemann verwenden konnte.

Aus der Abwägungsvorschrift des § 28 Abs. 1 Satz 1 Nr. 2 BDSG ergibt sich keine Rechtfertigung für diese Datenverwendungen. Zum einen kann weder ein berechtigtes Interesse der Frau am unbefugten Zugriff auf die Daten ihres Ex-Ehemannes noch an deren Übermittlung an den Rechtsanwalt anerkannt werden. Zum anderen steht das schutzwürdige Interesse des geschiedenen Ehemannes diesen rechts- und zweckwidrigen Aktionen entgegen. Es kommt noch hinzu, dass der Bundesgerichtshof in seinem Urteil vom 10. Februar 2010 (Az. VII ZR 53/09) zur strafrechtlichen Verschwiegenheitspflicht von Angehörigen privater Lebensversicherungsunternehmen gemäß § 203 Abs. 1 Nr. 6 Strafgesetzbuch (StGB) festgestellt hat, dass dort nicht nur die von der betroffenen Person preiszugebenden Gesundheitsdaten geschützt sind. Auch der Umstand, dass ein Betroffener zur Absicherung bestehender oder künftiger gesundheitlicher Risiken finanzielle Vorsorgemaßnahmen getroffen hat, unterfällt der Geheimhaltungspflicht, da er Auskunft über die persönliche, der Öffentlichkeit nicht zugängliche wirtschaftliche Lebensgestaltung des Versicherungsnehmers gibt.

Unter Berücksichtigung all dieser Umstände haben wir gegen die Beschäftigte ein Bußgeldverfahren wegen einer vorsätzlichen unbefugten Übermittlung personenbezogener Daten durchgeführt (§ 43 Abs. 2 Nr. 1 BDSG).

6.3 Erhebung von Gesundheitsdaten durch Versicherer bei Dritten im Rahmen der Risiko- oder Leistungsprüfung

Auch Reiserücktrittskostenversicherer dürfen vom Versicherungsnehmer Gesundheitsdaten nur in dem Umfang erheben, wie sie für die Feststellung der Leistungspflicht erforderlich sind. Umfängliche Krankenhausentlass- oder Arztberichte gehören in der Regel nicht dazu.

Wir erhalten zahlreiche Beschwerden, insbesondere zu privaten Krankenversicherungen und Reiserücktrittskostenversicherungen, die den Umfang der von einem Versicherungsunternehmen bei der Risiko- oder Leistungsprüfung angeforderten Gesundheitsangaben und ärztlichen Unterlagen zum Gegenstand haben.

Ein Versicherungsunternehmen darf nach § 213 Abs. 1 Versicherungsvertragsgesetz (VVG) Gesundheitsdaten bei Dritten nur erheben, soweit die Kenntnis der Daten für die Beurteilung des zu versichernden Risikos oder der Leistungspflicht **erforderlich** ist und die betroffene Person eine **Einwilligung** erteilt hat. Die Einwilligung kann bereits bei Vertragsschluss oder später im Einzelfall erteilt werden, wobei die betroffene Person vor einer Erhebung ihrer Gesundheitsdaten zu unterrichten ist und ihre Entscheidung jederzeit ändern kann (§ 213 Abs. 2 und 3 VVG).

Die Frage, ob eine Datenerhebung im konkreten Einzelfall für die Risiko- oder Leistungsprüfung tatsächlich erforderlich ist, stellt sowohl eine versicherungsvertragsrechtliche als auch eine datenschutzrechtliche Frage dar. Versicherungsvertragsrechtlich korrespondiert § 213 Abs. 1 VVG mit § 31 Abs. 1 VVG, demzufolge der Versicherer von dem Versicherungsnehmer jede Auskunft verlangen kann, die zur Feststellung des Versicherungsfalles oder des Umfangs der Leistungspflicht **erforderlich** ist. Datenschutzrechtlich hat der Versicherer bei der Prüfung der Erforderlichkeit den Grundsatz der Verhältnismäßigkeit sowie das Gebot der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) zu beachten.

Bei Beschwerden hinsichtlich des Umfangs der von einem Versicherungsunternehmen verlangten Gesundheitsdaten fordern wir den Versicherer regelmäßig auf, uns die Erforderlichkeit der Datenerhebung im konkreten Fall darzulegen.

Bei der Geltendmachung von Ansprüchen aus Reiserücktrittskostenversicherungen halten wir es in aller Regel für zulässig, dass der Versicherer die Diagnose erhebt, die für den Nichtantritt der Reise ursächlich war. Der Versicherer muss die Möglichkeit haben, seine tatsächliche Leistungspflicht zu prüfen. Dies ist ihm ohne Angabe der Diagnose regelmäßig nicht möglich.

Dagegen sehen wir die pauschale Anforderung eines Krankenhausentlassberichts im Rahmen des Formulars der Schadensanzeige bzw. des ärztlichen Berichtes mangels Erforderlichkeit für datenschutzrechtlich nicht zulässig an. Der Entlassbericht enthält nämlich eine Vielzahl von Daten, die in den meisten Fällen weit über den Informationsbedarf des Reiserücktrittskostenversicherers hinausgehen.

Lediglich in Ausnahmefällen, bei denen eine Einsichtnahme in den gesamten Entlassbericht bzw. eine umfänglichere ärztliche Dokumentation besonders zu begründen ist, beispielsweise um das Vorliegen einer in der Reiserücktrittskostenversicherung regelmäßig ausgeschlossenen chronischen Erkrankung zu erkennen, kann ggf. eine derartige Anforderung gerechtfertigt sein.

7 Banken

7.1 Schülerpraktikum bei Banken

Kommt ein Schüler als Praktikant mit Daten von Bankkunden in Berührung, sind besondere organisatorische Maßnahmen zur Einhaltung des Datenschutzes notwendig.

Bankkunden haben bei uns angefragt, wie die Tätigkeit von Praktikanten in Banken datenschutzrechtlich zu bewerten sei. Schließlich seien die Daten zu ihren finanziellen Verhältnissen oder zu ihren Kredit-, Spar- und Anlageverträgen besonders vertraulich zu behandeln.

Beim Einsatz von - meist minderjährigen - Schülerpraktikanten in Banken sehen wir deshalb neben der allgemein gebotenen Sorgfalt bei der Auswahl und Beschäftigung von Praktikanten sowie deren Verpflichtung auf das Datengeheimnis gemäß § 5 BDSG insbesondere folgende organisatorische Maßnahmen der Bank für erforderlich an:

- Die datenschutzrechtliche Belehrung zu Beginn des Praktikums darf nicht "nebenbei" abgehandelt werden oder sich gar auf eine Unterschrift beschränken, sondern soll Schülern die große Verantwortung der Beschäftigten im Kredit- und Bankenwesen anschaulich und nachhaltig vermitteln.
- Den Praktikanten dürfen keine eigenen EDV-Zugriffsrechte eingeräumt werden.
- Die Einsichtsmöglichkeiten in personenbezogene Daten (z.B. beim Einsatz am Schalter) sind so weit wie möglich zu begrenzen.
- Im Kundenkontakt muss der Praktikant klar als solcher erkennbar sein.
- Vor einem Kundengespräch ist die Zustimmung des Kunden zur Anwesenheit des Praktikanten einzuholen.

7.2 Einwilligung in die Auswertung von Kontobewegungen für Kundenbetreuung

Kontobewegungsdaten dürfen von der Bank für die Kundenbetreuung nur mit einer rechtswirksamen Einwilligung der Kunden ausgewertet werden.

Im 3. Tätigkeitsbericht haben wir im Kapitel 5.2. bereits dargestellt, dass die Nutzung der Kontobewegungsdaten für Zwecke der Kundenbetreuung und der Werbung für eigene Angebote der Bank sowie für ihre Verbundpartner nur mit Einwilligung des betroffenen Bankkunden zulässig ist. Das (entgegenstehende) schutzwürdige Interesse des Kunden daran, dass die Bank seine aus den Kontobewegungen ersichtlichen Lebensverhältnisse nicht auswertet und die Möglichkeit zur Erstellung eines Persönlichkeitsprofils nicht nutzt, ist höher anzusetzen.

Aus diesem Grund sind Banken dazu übergegangen, für die von manchen Kunden gewünschte umfassende Betreuung in Finanzfragen und für eine zielgerichtete Werbeansprache eine Einwilligung der Kunden einzuholen.

Eine derartige datenschutzrechtliche Einwilligung ist nur wirksam, wenn die Maßgaben des § 4a BDSG beachtet werden. Insbesondere muss die Erklärung freiwillig sein. Ferner müssen die Kunden über die geplanten Kontoauswertungen sowie deren Zwecke deutlich und in verständlicher Weise informiert werden.

7.3 Prüfung von Mitarbeiterkonten

Auch die Mitarbeiter einer Bank dürfen davon ausgehen, dass die im Rahmen ihrer Bankverträge anfallenden Daten grundsätzlich nur für die vertragsgemäße Durchführung der Bankdienstleistung verwendet werden.

Mehrfach haben sich Mitarbeiter von Banken an uns gewandt, weil ihre Arbeitgeber offensichtlich ihre Finanztransaktionen ausgewertet hatten.

Soweit eine Überprüfung der Geldtransaktionen und Konten von Mitarbeitern auf gesetzlicher Grundlage, wie z.B. dem Geldwäschegesetz erfolgt, sind die Vorgaben dieses Gesetzes maßgeblich. Allerdings dürfen die dabei gewonnenen Erkenntnisse - wie bei jedem anderen Kunden auch - nur zur Erfüllung der gesetzlichen Verpflichtung und im Rahmen der Erforderlichkeit verwendet werden.

Eine darüber hinaus gehende Verwendung im Rahmen des Arbeitsverhältnisses ist grundsätzlich nicht erlaubt. Die gewonnenen Informationen dürfen beispielsweise nicht dazu verwendet werden, die Mitarbeiter auf den Geldabfluss an eine andere

Bank und die möglicherweise dahinter stehende Kundenbeziehung zur Konkurrenz anzusprechen.

Auch eine Einsicht in die Girokontobewegungen eines Mitarbeiters, um während einer Krankschreibung dessen Kontoaktivitäten zu prüfen (z.B. im Hinblick auf den Einsatz der EC-Karte in einem Geschäft oder an einer Tankstelle), ist unzulässig.

7.4 Herausgabe von Bankunterlagen an Dritte, deren Empfangsvollmacht vom Kontoinhaber widerrufen worden ist

Bei der Herausgabe von Bankunterlagen an einen Dritten ist zu prüfen, ob er über eine Vollmacht verfügt und diese noch besteht.

Es wurde uns wiederholt vorgetragen, dass Bankunterlagen, z.B. Kontoauszüge oder Zweitausdrucke davon, ohne jegliche Prüfung an Dritte herausgegeben worden sind. In anderen Fällen war die Herausgabe an Dritte darauf zurückzuführen, dass der Kunde eine Vollmacht widerrufen hatte und der Bankmitarbeiter die Berechtigung des Empfängers nicht aktuell überprüft hatte.

Die Herausgabe von Bankunterlagen an nicht (mehr) bevollmächtigte Personen stellt eine unbefugte Übermittlung personenbezogener Daten dar und erfüllt damit einen Bußgeldtatbestand.

Um eine unbefugte Herausgabe zu verhindern, ist sicherzustellen, dass die Berechtigung zum Empfang der Unterlagen in jedem Fall geprüft wird. Keinesfalls darf sich der Bankmitarbeiter - wie geschehen - darauf verlassen, dass der Anfragende schon öfters befugtermaßen Unterlagen in Empfang genommen hat.

7.5 Bildschirmanzeigen am Geldautomat bzw. Kontoauszugsdrucker

Bei den Bildschirmanzeigen an den Selbstbedienungsgeräten der Banken ist sicherzustellen, dass Dritten keine Angaben über den Kunden unbefugt offenbart werden.

An manchen Geldausgabeautomaten und Kontoauszugdruckern werden Bildschirme eingesetzt, deren Anzeige nicht nur von der unmittelbar davor stehenden Person gelesen werden können, sondern auch von dahinter wartenden Dritten. Dies gilt sowohl für die Anzeige des Kontostandes oder des Auszahlungsbetrages als auch für eine namentliche Begrüßung des Kunden auf dem Bildschirm. Es kann damit zu Datenübermittlungen der auf dem Bildschirm gezeigten Informationen kommen.

Wir raten von namentlichen Begrüßungen der Kunden auf dem Bildschirm ab. In jedem Fall haben aber die Banken hier durch organisatorische Maßnahmen zu gewährleisten, dass unberechtigte Dritte Bildschirminformationen nicht einsehen können. Dies kann durch die Art und Weise der Aufstellung der Geräte wie auch durch die Gestaltung und den Inhalt der Bildschirmanzeigen erfolgen.

7.6 Aufzeichnung von Telefongesprächen mit Banken

Der Inhalt eines Telefongesprächs darf nur nach einer rechtswirksam erteilten Einwilligung des Gesprächspartners aufgezeichnet werden.

Bürger beschwerten sich bei uns, weil sie mit einer Bank nur unter der Voraussetzung telefonieren können, dass sie vorher ihre Zustimmung zu einer Gesprächsaufzeichnung erteilt haben.

Die Aufzeichnung des Inhalts eines Telefongesprächs ist, auch wegen der Regelungen im Strafgesetzbuch, in jedem Fall grundsätzlich nur auf Grund einer vorher erteilten rechtswirksamen Einwilligung des Gesprächspartners zulässig.

Soweit am Telefon Bankgeschäfte abgewickelt werden, ergeben sich aus dem Bankrecht entsprechende Dokumentationspflichten. Hierbei kann eine im Kontoeröffnungsantrag enthaltene und den Anforderungen des § 4a BDSG entsprechende Einwilligung oder die Tatsache, dass der Anrufer in Kenntnis der Aufzeichnung das Gespräch führt, eine Gesprächsaufzeichnung rechtfertigen. In der Regel beginnen solche Telefongespräche für den Kunden mit einem vorgeschalteten Begrüßungstext der Bank, der auf die Gesprächsaufzeichnung hinweist.

Das Gleiche gilt für allgemeine Telefongespräche mit einer Bank, z.B. für Anfragen zu Vertragskonditionen. Auch hier ist eine ausdrücklich oder konkludent erklärte vorherige Einwilligung des Gesprächspartners vor der Aufzeichnung des Gesprächs erforderlich.

7.7 Berechtigungskonzepte und Protokollierungen der Kontenzugriffe

Zugriffe von Mitarbeitern auf Bankkonten müssen so weit wie möglich beschränkt und in jedem Fall protokolliert werden.

Gerade bei Banken mit einem regionalen oder gar bundesweiten Einzugsbereich möchten manche Kunden nicht, dass die Kundenberater aller Filialen auf ihre Kontendaten zugreifen können. Dies gilt vor allem für Rechtsanwälte, Ärzte usw. im Hinblick auf die ihnen obliegende Schweigepflicht und die Sensibilität der auf den Konten gespeicherten Daten sowie für prominente Persönlichkeiten wegen der nicht auszuschließenden Neugier an ihren Daten.

Einige Banken kommen solchen Kundenwünschen nach Zugriffsbeschränkungen ohne weiteres nach. Andere Banken lehnen dies ab oder haben nach ihren Angaben (noch) nicht die technischen Umsetzungsmöglichkeiten hierfür.

Aus der Sicht des Datenschutzes sehen wir es als erforderlich an, Zugriffsmöglichkeiten auf Konten so weit wie möglich zu beschränken; zumindest dann, wenn der Kunde dies ausdrücklich wünscht.

Aus präventiven Gründen müssen Kontenzugriffe einschließlich der nur lesenden Zugriffe protokolliert werden, um missbräuchliche Zugriffe aufdecken zu können. Die erzeugten Protokolle müssen ohne großen technischen Aufwand auswertbar sein.

8 Auskunfteien

8.1 Mehr Transparenz im Auskunfteiwesen

Seit dem 1. April 2010 haben die Bürger gegenüber Auskunfteien erweiterte Auskunftsrechte.

In unserem 3. Tätigkeitsbericht haben wir im Einzelnen aufgeführt, welche Rechte den betroffenen Bürgern gegenüber Auskunfteien zustehen. Durch eine Änderung des Bundesdatenschutzgesetztes wurde zum 1. April 2010 das Auskunftsrecht der Bürger erweitert. So kann jeder nunmehr sehr einfach in Erfahrung bringen, welche Informationen der Auskunftei zur eigenen Person vorliegen, ob diese Daten richtig sind, welche Stellen Auskünfte eingeholt haben und ob dies jeweils gerechtfertigt war.

Die Bürger können von Auskunfteien nun folgende Auskünfte verlangen:

- **über die zu ihrer Person gespeicherten Daten**

  Das Auskunftsrecht der Bürger umfasst sämtliche zur Person gespeicherte Daten, auch wenn sie weder automatisiert verarbeitet werden noch in einer nicht-automatisierten Datei gespeichert sind, z.B. in schriftlichen Unterlagen jeder Art.

- **über die Herkunft und Empfänger der Daten**

  Diese Auskunft kann nur verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

- **über den Zweck der Speicherung**

- **über gespeicherte und bisher schon übermittelte Scorewerte (= Wahrscheinlichkeit, mit der ein Zahlungsausfall eintreten kann) nach der Maßgabe des § 34 Abs. 4 ff. BDSG.**

  Als Scoring bezeichnet man ein Verfahren, mit dem auf Grund bestimmter tatsächlicher Erkenntnisse eine Prognose für ein bestimmtes zukünftiges Verhalten erstellt wird. So könnte z.B. aus der Kenntnis, das sich jemand in einem Privatin-

solvenzverfahren befindet, schon länger arbeitslos ist oder in einer Obdachlosenwohnung lebt, die Prognose erstellt werden, dass ein diesem Menschen gewährter größerer Kredit im Regelfall wohl nicht mehr zurückbezahlt werden dürfte.

Das Bundesdatenschutzgesetz räumt nunmehr jedem das Recht ein, zu den für ihn berechneten Scorewerten, also der Wahrscheinlichkeit, mit der bei ihm nach Meinung der Auskunftei ein Zahlungsausfall eintreten kann, Auskunft zu verlangen. Konkret kann er Informationen insbesondere über

- die innerhalb der letzten zwölf Monate übermittelten Scorewerte,
- den Namen und die letztbekannte Anschrift der Empfänger der Scorewerte,
- den aktuell sich ergebenden Scorewert,
- die zur Berechnung der Scorewerte genutzten Datenarten sowie
- das Zustandekommen und die Bedeutung der Scorewerte

einzelfallbezogen in nachvollziehbarer und allgemein verständlicher Form verlangen. Dieses Auskunftsrecht zu Scorewerten gilt auch dann, wenn eine Auskunftei die Scorewert-Informationen nicht zur betroffenen Person konkret schon speichert, sondern nur die Datengrundlagen vorhält, anhand derer bei einer Anfrage ein Scorewert berechnet werden kann.

Die Bürger können einmal im Jahr kostenlos die o.g. Auskünfte verlangen und überprüfen, welche Informationen der Auskunftei zur eigenen Person vorliegen, ob diese Daten alle richtig sind, welche Stellen Auskünfte eingeholt haben und ob dies jeweils gerechtfertigt war. Für jede weitere Auskunft innerhalb eines Jahres kann ein kostendeckendes Entgelt für den Aufwand verlangt werden.

8.2 Das berechtigte Interesse an einer Auskunfteiabfrage

Das Einholen einer Bonitätsauskunft über eine Person bei Auskunfteien ist nur dann zulässig, wenn der Anfragende ein berechtigtes Interesse an der Kenntnis der Daten hat. Der typische Fall eines berechtigten Interesses ist die Prüfung eines finanziellen Ausfallrisikos, z.B. vor der Gewährung eines Kredits, vor dem Abschluss eines Ratenkaufvertrages oder einer Lieferung gegen Rechnung. Mit Hilfe der gewonnenen

Erkenntnisse über den potentiellen Vertragspartner kann geprüft werden, ob und ggf. unter welchen Bedingungen der Vertrag geschlossen werden kann.

In den nachfolgend geschilderten Fällen wurden Bonitätsauskünfte ohne ausreichendes berechtigtes Interesse und damit unbefugt abgerufen. Dies haben wir beanstandet und in den gravierenden Fällen auch mit einem Bußgeldverfahren geahndet.

8.2.1 Vor einer Probefahrt

Für die Entscheidung, ob von einem Autohaus eine Probefahrt gewährt werden soll, besteht kein berechtigtes Interesse, eine Bonitätsauskunft über den potentiellen Interessenten einzuholen.

Ein Autohaus hatte vor Abschluss eines Fahrzeugnutzungsvertrages für eine Probefahrt mit einem hochwertigen PKW-Cabrio eine Bonitätsprüfung des Interessenten durch eine Anfrage bei einer Auskunftei vorgenommen. Dies wurde damit begründet, dass der Interessent Neukunde gewesen sei und über ihn bislang keinerlei Informationen vorgelegen hätten. Aufgrund des negativen Ergebnisses der Bonitätsprüfung sei von der Gewährung einer Probefahrt Abstand genommen worden.

Wir haben ein berechtigtes Interesse des Autohauses an einer Auskunfteiabfrage verneint. Zum einen bestand für das Autohaus aus dem Probefahrtvertrag kein finanzielles Ausfallrisiko, da der Interessent keine finanziellen Verpflichtungen übernehmen musste. Zum anderen kann möglichen Fahrzeugunterschlagungen oder -beschädigungen nicht mit einer Wirtschaftsauskunft wirksam begegnet werden. Eine Wirtschaftsauskunft zeigt auf, wie der Interessent in der Vergangenheit seinen finanziellen Verpflichtungen verschiedenster Art nachgekommen ist. Für die Beurteilung der allgemeinen Zuverlässigkeit des Betroffenen oder der Einschätzung der Gefahr einer Unterschlagung des überlassenen Fahrzeuges ist eine Wirtschaftsauskunft dagegen in aller Regel nicht geeignet.

8.2.2 Bonitätsauskünfte über Mieter im Rahmen einer Immobilienbewertung

Es besteht kein berechtigtes Interesse, für die Bewertung einer größeren vermieteten Immobilie Bonitätsauskünfte über die Mieter der Immobile einzuholen.

Ein Unternehmen, das mit der Bewertung einer größeren Immobilie beauftragt war, hat dazu Bonitätsauskünfte von einer Auskunftei zu sämtlichen privaten Wohnungsmietern in dieser Immobilie eingeholt. Das berechtigte Interesse an der Kenntnis der Daten der Mieter wurde darin gesehen, dass es bei der Ermittlung des Wertes einer vermieteten Immobilie auch darauf ankomme, wie die einzelnen Mieteinheiten vermietet seien, ob also die Mieter solvent seien oder finanzielle Belastungen hätten.

Es ist bereits fraglich, ob eine Bonitätsauskunft für den genannten Zweck geeignet ist. Ausreichend und angemessen wäre es in diesem Fall gewesen, wenn sich das mit der Immobilienbewertung beauftragte Unternehmen vom derzeitigen Vermieter darüber hätte informieren lassen, ob bzw. zu welchem Anteil die Mieter insgesamt ihren Zahlungsverpflichtungen pünktlich nachkommen. Weil es hier um die Bewertung der gesamten Immobilie geht, wäre ein Bezug auf die einzelnen Mieter entbehrlich gewesen. Ein berechtigtes Interesse an einer Auskunfteiabfrage bestand deshalb nicht.

In jedem Fall besteht Grund zu der Annahme, dass die betroffenen Mieter hier ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung ihrer Daten durch eine Auskunftei hatten. Ein privater Mieter muss es im Regelfall nicht hinnehmen, dass sich ein Dritter in dem Stadium der bloßen Bewertung einer Immobilie Informationen über seine allgemeine Bonität beschafft.

8.2.3 Vor einem reinen Beratungsgespräch für einen Küchenkauf

Es besteht kein berechtigtes Interesse, bereits nach der Terminvereinbarung für ein Beratungsgespräch über einen Küchenkauf eine Bonitätsauskunft über die potentiellen Kunden einzuholen.

Ein Küchenfachgeschäft hatte bereits nach der Terminvereinbarung für ein erstes Beratungsgespräch über einen Küchenkauf die Bonität des Interessenten überprüft. Dies wurde damit begründet, dass bei der Terminvereinbarung ein „vorgezogenes Verkaufsgespräch" geführt worden sei. Mit Hilfe der Bonitätsprüfung hätte dem Kun-

den beim erwarteten nachfolgenden Vertragsabschluss bereits eine Lieferzusage gegeben und die Zahlungsbedingungen hätten vereinbart werden können.

Ein finanzielles Ausfallrisiko und damit ein berechtigtes Interesse an einer Auskunfteiabfrage wird beim Verkauf einer Küche erst dann begründet, wenn der Kunde einen entsprechenden Auftrag erteilt oder zumindest echtes Kaufinteresse bekundet, d.h. er sich eindeutig dahingehend äußert oder anderweitig klar zum Ausdruck bringt, dass er eine Küche kaufen möchte. In einem vorhergehenden Stadium, wie bei einer allgemeinen Terminvereinbarung oder beim ersten Beratungsgespräch kann ein derartiges finanzielles Ausfallrisiko regelmäßig noch nicht gesehen werden.

8.2.4 Überlegungen bezüglich einer Beendigung der Geschäftsbeziehung wegen häufiger unberechtigter Beschwerden des Kunden

Es besteht kein berechtigtes Interesse für ein Kreditinstitut, für die Entscheidung über die Fortführung der Geschäftsbeziehung eine Bonitätsauskunft einzuholen.

Ein Kreditinstitut hatte eine Bonitätsprüfung eines Kunden damit begründet, dass aufgrund mehrerer Beschwerdefälle überlegt worden sei, die Geschäftsbeziehung zu beenden.

Anlass für die Bonitätsprüfung war also weder das finanzielle Ausfallrisiko des Kunden noch eine anstehende Entscheidung mit finanziellem Hintergrund, für die im Rahmen der Entscheidungsfindung Informationen über die finanzielle Situation des Kunden erforderlich gewesen wären. Ein berechtigtes Interesse für eine Bonitätsprüfung hat somit nicht vorgelegen.

8.2.5 Aus privatem Anlass

Die private Nutzung der dienstlich eröffneten Möglichkeit, Bonitätsauskünfte über Dritte einzuholen, stellt eine datenschutzrechtliche Ordnungswidrigkeit dar.

Immer wieder kommt es vor, dass Mitarbeiter, die im Rahmen der Erledigung ihrer dienstlichen Aufgaben in einem Unternehmen oder einer Bank die Möglichkeit haben, bei Auskunfteien Bonitätsauskünfte einzuholen, diese Berechtigung missbrauchen

und unbefugt für rein private Zwecke und unter Vorspiegelung falscher Tatsachen Bonitätsauskünfte einholen, beispielsweise für die private Vermietung einer Wohnung oder im Rahmen einer privaten Streitigkeit.

Dieses Erschleichen personenbezogener Daten mittels unrichtiger Angaben gegenüber einer Auskunftei ahnden wir regelmäßig mit einem Bußgeld.

9 Werbung, Adressenhandel

Die rechtlichen Vorschriften für die persönliche Werbung wurden im Jahr 2009 strenger geregelt.

Seit Jahren ist bei allen Datenschutzaufsichtsbehörden der Umgang mit personenbezogenen Daten wie Postadresse, E-Mail-Adresse oder Telefon-/Fax-Nummer für Zwecke der werblichen Ansprache von Personen ein Dauerthema.

Die großen Fallzahlen an Beschwerden beruhen insbesondere darauf, dass sich die mit Werbung angesprochenen Personen belästigt fühlen, speziell durch Telefon- und E-Mail-Werbung, oder generell nicht wollen, dass ihre Kontaktdaten für eine werbliche Ansprache verwendet bzw. von ihren Vertragspartnern hierfür an Dritte weitergegeben werden.

Um diese Missstände zu unterbinden, hat der Bundestag im Jahr 2009 das Gesetz gegen unlauteren Wettbewerb (UWG) und im BDSG die Zulässigkeitsvoraussetzungen für die Datenverwendung zu Werbezwecken enger gefasst, wobei die bisherigen Vorschriften des BDSG für die vor dem 1. September 2009 erhobenen oder gespeicherten Daten bis zum 31. August 2012 weiter anzuwenden sind.

9.1 Telefon- und Faxwerbung

Telefon- und Faxwerbung ist grundsätzlich nur nach vorheriger Einwilligung erlaubt.

9.1.1 Wettbewerbsrechtliche Kriterien der Telefon- und Faxwerbung

Nach dem neuen Wettbewerbsrecht sind Werbeanrufe oder Fax-Werbung gegenüber Verbrauchern nur noch mit deren vorheriger ausdrücklicher Einwilligung erlaubt.

Für die Meldung von unerlaubter Telefon- und Faxwerbung hat die Bundesnetzagentur (http://www.bundesnetzagentur.de) eine Beschwerdeseite "Rufnummernmissbrauch" eingerichtet. Die Bundesnetzagentur kann nach dem Telekommunikationsrecht unter anderem Rufnummern, von denen aus unerlaubte Telefon- oder Faxwerbung erfolgt, abschalten lassen oder Bußgelder verhängen.

9.1.2 Datenschutzrechtliche Kriterien der Telefon- und Faxwerbung

Auch datenschutzrechtlich dürfen Telefon- oder Faxnummern nur mit einer Einwilligung der betroffenen Personen für werbliche Ansprachen verwendet werden. Dies wird häufig von Unternehmen ignoriert und führt in der Folge zu Beschwerden, denen wir dann nachgehen und für Abhilfe sorgen.

9.2 E-Mail-/SMS-Werbung

Abgesehen von einer Ausnahme gegenüber Bestandskunden bedarf die E-Mail- und SMS-Werbung einer Einwilligung.

9.2.1 Wettbewerbsrechtliche Kriterien der E-Mail- und SMS-Werbung

Wettbewerbsrechtlich ist eine Werbung per E-Mail und die damit vergleichbare Werbung per SMS gegenüber Verbrauchern grundsätzlich nur mit einer vorherigen ausdrücklichen Einwilligung zulässig.

Hierzu gibt es allerdings gemäß § 7 Abs. 3 UWG die Ausnahmeregelung für sogenannte Bestandskunden dahingehend, dass E-Mail- und SMS-Werbung dann erlaubt ist,

- wenn ein Unternehmen im Zusammenhang mit dem Verkauf von Waren oder Dienstleistungen die Kontaktdaten für elektronische Post von einem Kunden erhalten hat,

- dieses Unternehmen für ähnliche Waren oder Dienstleistungen wirbt,

- der Kunde der werblichen Verwendung seiner Daten für elektronische Post nicht widersprochen hat, und

- der Kunde schon bei der Erhebung seiner Daten wie auch bei jeder werblichen Verwendung klar und deutlich auf sein Widerspruchsrecht hingewiesen wird.

9.2.2 Datenschutzrechtliche Kriterien der E-Mail- und SMS-Werbung

Aus dem Datenschutzrecht ergibt sich gemäß § 28 Abs. 3 BDSG ebenfalls, dass eine Nutzung oder Übermittlung von Adressen der elektronischen Post für Werbeansprachen grundsätzlich einer vorherigen Einwilligung der beworbenen Personen bedarf.

Eine Ausnahme ergibt sich lediglich aus § 28 Abs. 3 Satz 3 BDSG, der das Hinzuspeichern und damit auch die Nutzung weiterer Daten, z.B. einer E-Mail-Adresse, für Werbeansprachen an eigene Kunden vorsieht. Einer E-Mail- oder SMS-Werbung entgegenstehende Interessen der Kunden sind in der Regel dann nicht gegeben, wenn die obengenannten vier Anforderungen aus dem Wettbewerbsrecht (§ 7 Abs. 3 UWG) eingehalten werden.

Diese Regelungen werden in der Praxis oft missachtet. Uns erreichen deshalb viele Beschwerden. Kürzlich haben wir in einem solchen Fall gegen einen Verkäufer von E-Mail-Adressen einen Strafantrag gestellt, weil dieser die Einwilligungen der betroffenen Personen für die werbliche Verwendung der E-Mail-Adressen nicht nachweisen konnte und den E-Mail-Adressenbestand trotzdem zum Verkauf angeboten hatte.

9.3 Briefwerbung

Die Zulässigkeit der Briefwerbung kann sich aus einer Einwilligung oder aus einem der in § 28 Abs. 3 Sätze 2 bis 7 geregelten Tatbestände des „Listenprivilegs“ ergeben.

9.3.1 Wettbewerbsrechtliche Kriterien der Briefwerbung

Nach dem Wettbewerbsrecht ist Briefwerbung dann zulässig, wenn sie den Angeschriebenen nicht in unzumutbarer Weise belästigt. Eine unzumutbare Belästigung besteht laut UWG insbesondere dann, wenn Briefwerbung erfolgt, obwohl erkennbar ist, dass der Angeschriebene diese Werbung nicht wünscht.

9.3.2 Datenschutzrechtliche Kriterien der Briefwerbung

Die Verwendung der Postadresse für eine Briefwerbung ist gemäß § 28 Abs. 3 BDSG zulässig, wenn eine sich darauf beziehende Einwilligung des Beworbenen vorliegt

oder wenn sich eine Erlaubnis aus den Sätzen 2 bis 7 dieser Bestimmung ergibt. Im Rahmen dieser gesetzlichen Erlaubnistatbestände dürfen nur folgende „Listendaten“ verwendet werden:

> Berufs-, Branchen- oder Geschäftsbezeichnung
> Namen, Titel, akademischer Grad
> Anschrift
> Geburtsjahr
> ein Merkmal über die Zugehörigkeit zu einer Personengruppe, wie z.B. Haustierbesitzer, sport- oder reiseinteressiert oder ähnliches.

Die Verwendung dieser Listendaten ist unter folgenden Voraussetzungen zulässig:

- Eigenwerbung an Bestandskunden sowie an sonstige Personen, wenn deren Kontaktdaten aus allgemein zugänglichen Verzeichnissen stammen (nicht: aus sonstigen Veröffentlichungen wie Presse oder Internet). Weitere Daten dürfen hinzugespeichert werden, um z.B. den Interessentenkreis für eine bestimmte Werbung einzugrenzen.

- Geschäftliche Werbung an geschäftliche Kontaktadressen

- Spendenwerbung durch steuerbegünstigte Organisationen

- Empfehlungswerbung/Beipackwerbung, d. h. die Nutzung der eigenen Kontaktdaten für Werbezwecke von dritten Unternehmen. Dabei muss für den Angeschriebenen erkennbar sein, wer seine Adresse gespeichert und genutzt hat.

- Übermittlung von Listendaten für Zwecke der Werbung **und** Werbung des Empfängers mit diesen Daten. In diesem Fall muss die ursprüngliche Quelle dieser Daten aus der Werbung eindeutig hervorgehen. Außerdem muss die Datenübermittlung vom Adressenlieferanten sowie dem Werbenden für eventuelle Auskunftswünsche der betroffenen Personen dokumentiert werden.

In all diesen Fällen dürfen die schutzwürdigen Interessen der beworbenen Personen nicht entgegenstehen und es darf auch kein Werbewiderspruch vorliegen.

Auf das Widerspruchsrecht gegen eine werbliche Verwendung der Daten muss schon beim Abschluss eines Vertrages und darüber hinaus in jeder einzelnen Werbesendung hingewiesen werden. Wird gegen diese Hinweisverpflichtungen verstoßen, kann dies mit einem Bußgeld geahndet werden.

10 Handel, Dienstleistung

10.1 Elektronisches Lastschriftverfahren als Zahlungsform

Für das elektronische Lastschriftverfahren (ELV), d.h. Zahlung unter Hingabe der ec-Karte und Unterschreiben des Lastschriftbelegs (im Gegensatz zum hier nicht angesprochenen electronic-cash-Verfahren, d.h. Hingabe der ec-Karte und Eingabe der PIN-Nummer) sollen einheitliche datenschutzrechtliche Anforderungen definiert werden.

10.1.1 Problemstellung

Der Bundesverband der Verbraucherzentralen hat sich im Laufe des vergangenen Jahres mehrfach kritisch zu den Texten geäußert, die Handels- und andere Unternehmen Kunden bei Bezahlung im elektronischen Lastschriftverfahren auf den sog. Lastschriftbelegen zur Unterschrift vorlegen. Bemängelt wurde unter anderem, dass für die Kunden nicht hinreichend transparent sei, was mit ihren Daten geschehe. Die Kritik wurde auch in den Medien aufgegriffen und war für die Datenschutzaufsichtsbehörden Anlass, das ELV in seiner aktuellen praktischen Ausgestaltung einer näheren Überprüfung unter datenschutzrechtlichen Gesichtspunkten zu unterziehen. Hierzu wurde im Herbst 2010 eine Arbeitsgruppe des Düsseldorfer Kreises gegründet, deren Leitung dem Bayerischen Landesamt für Datenschutzaufsicht übertragen wurde. Ziel der Arbeitsgruppe ist es, die Datenflüsse im ELV im Einzelnen festzustellen, eine einheitliche datenschutzrechtliche Bewertung der Datenflüsse zu erreichen und dann den betreffenden Unternehmen entsprechende Vorgaben für die Gestaltung ihrer Verfahren zu machen.

Das ELV ist ein bargeldloses Zahlungsverfahren, das der Handel als Alternative zu dem bankenabhängigen electronic-cash-Verfahren (Bezahlung mit der ec-Karte und Geheimzahl/PIN) entwickelt hat, und bei dem der Kunde durch seine Unterschrift eine Ermächtigung zu einem Lastschrifteinzug von seinem Konto erteilt. Der Kunde gibt an der Kasse seine ec-Karte hin, die von der Kassenkraft in das Lastschrift-Terminal gesteckt wird. Das Terminal liest aus dem Magnetstreifen der ec-Karte die dort gespeicherte Kontonummer und Bankleitzahl sowie die so genannte Kartenfolgenummer (diese dient der Zuordnung zu einer bestimmten Karte bei mehreren zu einem Konto ausgegebenen Karten) aus. In den meisten Fällen werden für die fol-

genden Arbeitsschritte andere Unternehmen eingeschaltet, für die in den Fachkreisen die Bezeichnung „Netzbetreiber“ gebräuchlich ist.

Der Netzbetreiber gleicht diese Daten innerhalb weniger Sekunden mit bei ihm gespeicherten Datenbeständen ab, die in der Regel aus Positivdaten (Zahlungsdaten, die ihnen bei jeder ELV-Transaktion übermittelt werden) sowie einer Sperrdatei (Daten zu ec-Karten, bei denen es zu einer Rücklastschrift gekommen ist und Daten aus der sog. KUNO-Sperrdatei [Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nicht polizeilicher Organisationsstrukturen]) der Polizei bestehen. Nach dem Abgleich gibt der Netzbetreiber eine Rückmeldung an das Händlerterminal dahingehend, ob eine Zahlung im ELV empfohlen werden kann oder nicht.

Die eigentliche Bedeutung der Netzbetreiber im ELV liegt darin, dass sie Systeme zur Verhinderung von Zahlungsausfällen entwickelt haben und den Händlern zur Verfügung stellen. Diese Systeme bauen auf der Auswertung von Daten aus dem ELV auf. Da die großen Netzbetreiber ihre Dienste für das ELV einer Vielzahl von Unternehmen anbieten, verfügen sie über händlerübergreifende Bestände von Daten, die aus ELV-Transaktionen der bei ihnen angeschlossenen Händler stammen.

10.1.2 Interessen des Handels, Rechtsposition des Kunden

Indem beim Netzbetreiber Rücklastschrift-Meldungen und Positivdaten von allen an seinem System angeschlossenen Händlern eingehen und dort verwendet werden, kann dieser den angeschlossenen Händlern ein System zur Verhinderung von Zahlungsausfällen zur Verfügung stellen, das deutlich leistungsfähiger ist, als wenn er hierfür lediglich die Daten aus den bei dem jeweiligen Händler stattfindenden ELV-Transaktionen verwenden würde.

Dem Kunden dürfte in der aktuellen Praxis häufig nicht bewusst sein, was geschieht, wenn er seine ec-Karte zur Zahlung abgibt. Dies gilt sowohl für die unterschiedlichen Zahlungsweisen, ELV oder PIN-Verfahren, als auch für die Zahlungsabwicklungen im jeweiligen Fall.

10.1.3 Sachstand und Zielsetzung der Arbeitsgruppe

Die Arbeitsgruppe der Aufsichtsbehörden hat festgehalten, dass

- auf die vom Händlerterminal an den Netzbetreiber übermittelten Daten (Kontonummer, Bankleitzahl, Kartenfolgenummer, Terminal-Kennnummer, Datum und Uhrzeit des Vorgangs) das Bundesdatenschutzgesetz Anwendung findet, weil im Falle einer Rücklastschrift der Händler oder Netzbetreiber unter Nennung von Kontoverbindung und Bankleitzahl von der Kundenbank in der Regel Name und Anschrift des Kunden erfahren kann. Es handelt sich somit um Daten einer zumindest bestimmbaren Person und damit um personenbezogene Daten.

- Netzbetreiber im ELV, jedenfalls soweit sie Positiv- und Rücklastschriftdaten aus Transaktionen bei unterschiedlichen Händlern zusammengefasst auswerten, um daraus Empfehlungen zu erteilen, datenschutzrechtlich als verantwortliche Stellen tätig sind. Hieraus folgt, dass Daten an die Netzbetreiber nur bei Einhaltung der datenschutzrechtlichen Voraussetzungen für die Zulässigkeit von Datenübermittlungen weitergegeben werden dürfen.

- sich ein Einvernehmen darüber abzeichnet, dass die Auswertung der ELV-Daten von unterschiedlichen Händlern durch die Netzbetreiber und die darauf aufbauende Erteilung von Empfehlungen an die angeschlossenen Händler der Tätigkeit einer Auskunftei entspricht oder ihr zumindest weitgehend ähnlich ist und daher an § 29 BDSG zu messen ist.

Es ist nachvollziehbar, dass sich Handels- und andere Unternehmen mittels Schutzmechanismen vor Zahlungsausfällen im ELV schützen wollen. Grundsätzlich ist auch anzuerkennen, dass der Handel bemüht ist, mit dem ELV einen eigenen alternativen Zahlungsweg gegenüber der in der Regie der Banken liegenden Bezahlung mit ec-Karte und PIN zu etablieren. Ein derartiges Konkurrenzverhältnis kann nicht zuletzt - etwa unter Kostengesichtspunkten - auch den Kunden zugute kommen. Indessen dürfte dem Kunden bei der heutigen Praxis des ELV häufig nicht hinreichend klar werden, dass neben dem Händler eine weitere Stelle - der Netzbetreiber - seine Daten erhält und für welche Zwecke dies geschieht. Auch ist fraglich, inwieweit der Kunde in der Drucksituation an der Kasse wirksame datenschutzrechtliche Einwilligungserklärungen abgeben kann.

In den weiteren Beratungen der Arbeitsgruppe wird zu entscheiden sein, inwieweit die geschilderten Vorgänge im Rahmen des ELV datenschutzrechtlich auf eine gesetzliche Grundlage gestützt werden können und welche Anforderungen an die Information der Kunden zu stellen sind. Die Arbeitsgruppe hat sich zum Ziel gesetzt, dem Düsseldorfer Kreis einen Beschlussvorschlag mit dem Ziel zu unterbreiten, sich auf einheitliche datenschutzrechtliche Anforderungen an das ELV zu einigen.

10.2 Fahrzeugdatenspeicher

In Kraftfahrzeuge werden in zunehmendem Maße elektronische Bauteile eingebaut, die nicht nur ein Funktionieren des Fahrzeugs sicherstellen sollen, sondern auch der Speicherung und Nutzung von Daten für eine spätere Auswertung dienen. Dabei ist es nicht ausgeschlossen, dass auch datenschutzrelevante personenbezogenen Daten erfasst und ausgewertet werden können, die datenschutzgerechte Schutzkonzepte erfordern.

Im Rahmen einer Arbeitsgruppe der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, deren Leitung das Bayerische Landesamt für Datenschutzaufsicht innehat, beschäftigen wir uns mit den datenschutzrechtlichen Fragen, die sich im Zusammenhang mit so genannten Fahrzeugdatenspeichern ergeben.

Moderne Kraftfahrzeuge enthalten eine Vielzahl elektronischer Steuerungsgeräte, in denen Datenverarbeitungsprozesse stattfinden. Beispiele hierfür sind etwa das Antiblockiersystem (ABS), das Elektronische Stabilitätsprogramm (ESP), die Antriebs-Schlupfregelung (ASR) oder das Airbag-Steuergerät. Solche Bauteile erfassen physikalische Kenngrößen (z.B. Geschwindigkeit, Lenkwinkel, Beschleunigungswerte, Drehzahl usw.), vergleichen die erfassten Werte mit Sollwerten und lösen im Falle von Abweichungen eine Nachsteuerung aus. Viele dieser Steuerungsgeräte verfügen über Speichermodule und können damit Daten speichern. Aufgezeichnete Daten können aus dem Fahrzeug durch spezielle Lesegeräte ausgelesen werden. Die meisten Lesegeräte stehen nur dem Hersteller und Werkstätten zur Verfügung. Jedoch gibt es inzwischen auch im Handel Lesegeräte, die von jedermann erworben und genutzt werden können.

Wir sind davon überzeugt, dass bestimmte auslesbare Fahrzeugdaten Rückschlüsse auf das Verhalten oder die Wahrnehmung der Verantwortung von Fahrer oder

Halter ermöglichen und zum Beispiel für Zwecke der Rekonstruktion von Unfällen oder zur Abwehr von Produkthaftungsansprüchen verwendet werden können.

Die Fahrzeugdaten sind aber erst dann personenbezogen und fallen in den Anwendungsbereich des BDSG, wenn sie einer bestimmten Person zugeordnet werden können. Die Arbeitsgruppe hat hierzu festgehalten, dass es sich jedenfalls dann um personenbeziehbare Daten handelt, wenn das Fahrzeug immer von derselben Person gefahren wird. Bei mehreren Fahrern einer Familie oder eines Unternehmens kommt es für den Personenbezug der Daten darauf an, ob der Zeitpunkt ihrer Erfassung und die seinerzeit fahrende Person festgestellt werden kann. Relativ eindeutig dürfte der Personenbezug bei der Auswertung der Daten eines Unfallgeschehens sein.

Mit Unterstützung der Fahrzeugindustrie sind wir z.Zt. noch darum bemüht, zu klären, von welcher Bandbreite und Intensität der in den einzelnen Fahrzeugtypen verwendeten Systeme einer Fahrzeugdatenverwendung wir ausgehen müssen. Es sind deshalb weitere Untersuchungen in tatsächlicher Hinsicht erforderlich.

Den meisten Fahrern und Haltern dürfte nicht klar sein, welche Datenverarbeitungsprozesse in modernen Kraftfahrzeugen stattfinden. Deshalb steht aus unserer Sicht - ungeachtet zahlreicher rechtsdogmatischer und rechtstechnischer Fragen - vor allem eine gewisse Transparenz dieser Datenverarbeitungen für die Kunden im Vordergrund unserer Verhandlungen.

Ferner muss die Frage geklärt werden, wie der Kfz-Benutzer die zu seiner Person im Fahrzeug gespeicherten Daten in Erfahrung bringen kann. Die Umsetzung des datenschutzrechtlichen Auskunftsanspruchs wirft für die Praxis eine Reihe schwieriger Fragen auf. Insbesondere kann ein solcher Anspruch nur dann bestehen, wenn sicher feststeht, dass es sich bei den Daten, zu denen im konkreten Fall etwa ein Fahrer Auskunft begehrt, tatsächlich nur um die Daten der anfragenden Person handeln kann.

Die Arbeitsgruppe befindet sich derzeit in Gesprächen mit dem Verband der Automobilindustrie (VDA). Im Wesentlichen müssen die Fragen abgeklärt werden, welche Daten mit Personenbezug ausgelesen werden können, wie eine gewisse Transparenz des Umgangs mit den Fahrzeugdaten für die Halter und Fahrer hergestellt werden kann und wie die rechtlichen Auskunftsansprüche gestaltet werden können.

10.3 Übermittlung von Kundendaten bei Geschäftsveräußerungen u.a.

10.3.1 Fitness-Studio verkauft Kundendaten

Die Weitergabe von Kundendaten an das übernehmende Unternehmen zu Werbezwecken muss sich an den Maßgaben des Listenprivilegs orientieren.

Ein Fitness-Studio veräußerte im Rahmen des Insolvenzverfahrens Teile seiner Geschäftsausstattung (u.a. Trainingsgeräte) an einen Erwerber, der das Studio unter eigenem Namen weiterführen wollte, und gab auch Namen und Adressen von Kunden an ihn weiter. Der Erwerber schrieb die Kunden daraufhin mit einem Begrüßungsschreiben an und bot an, einen Vertrag mit ihnen abzuschließen.

Es handelt sich hier um eine Übermittlung und Nutzung der Kundendaten für Werbezwecke. Die Zulässigkeit dieser Datenverwendungen orientiert sich, soweit die Daten vor dem 1. September 2009 erhoben worden waren, an § 28 Abs. 3 Satz 1 Nr. 3 BDSG in der bis zum 31. August 2009 geltenden Fassung. Bei den verwendeten Daten handelt es sich um Listendaten im Sinne der genannten Vorschrift. Es besteht kein Grund zur Annahme, dass schutzwürdige Interessen der Kunden entgegenstanden. Die Übermittlung und die Nutzung waren somit für Werbezwecke zulässig.

Waren diese Listendaten ab dem 1. September 2009 erhoben worden, ergibt sich die Zulässigkeit aus § 28 Abs. 3 Satz 4 i.V.m. Satz 2 BDSG in der ab dem 1. September 2009 geltenden Fassung, allerdings mit der Maßgabe des § 34 Abs. 1a Satz 1 BDSG, demzufolge die Übermittlung gemäß § 34 Abs. 1a Satz 1 gespeichert wird und die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgeht.

Das erwerbende Unternehmen darf die Daten derjenigen Kunden, die mit ihm keinen Vertrag abschließen, nicht unbegrenzt speichern. Die im konkreten Fall beabsichtigte Speicherung für insgesamt sechs Monate haben wir als vertretbar angesehen.

10.3.2 Übernahme eines Online-Shops incl. Kundendaten, die über das Listenprivileg hinausgingen

Die Weitergabe von Kundendaten, die über die sog. Listendaten hinausgehen, an das übernehmende Unternehmen zu Werbezwecken ist unzulässig, sofern keine Einwilligung vorliegt.

In einem anderen Fall übergab ein Handelsunternehmen seinen Online-Shop für Elektronikprodukte an einen Konkurrenten einschließlich der Kundendaten. Zu diesen gehörten auch die nicht unter das Listenprivileg fallenden Kundennummern, Telefonnummern und E-Mail-Adressen.

Da weder eine Einwilligung der Kunden vorlag noch das Listenprivileg zur Rechtfertigung herangezogen werden konnte, war die Datenübermittlung und -nutzung zu Werbezwecken unzulässig.

10.3.3 Weitergabe von Abonnentendaten

Die Übermittlung von Abonnentendaten einer Zeitschrift, die eingestellt wird, an einen anderen Verlag, mit dem erklärten Ziel, dass die Abonnements „übergehen“ sollen, wenn die Abonnenten nicht widersprechen, ist datenschutzrechtlich unzulässig.

Ein Zeitschriftenverlag stellte die Veröffentlichung einer bestimmten Zeitschrift ein und übermittelte die Abonnentendaten an einen anderen Verlag, der eine thematisch ähnliche Zeitschrift herausgibt. Den Abonnenten teilte der übermittelnde Verlag in einem Informationsschreiben mit, dass sie fortan mit der anderen Zeitschrift beliefert werden würden, und nannte dabei auch den dafür zu entrichtenden Preis. Der Preis, den die Abonnenten für die eingestellte Zeitschrift bereits vorab entrichtet hatten, sollte hierauf angerechnet werden. Kunden, die sich nicht für die neue Zeitschrift "entschieden", so der Verlag, würden um einen entsprechenden Hinweis gebeten. Kurze Zeit später erhielten die Abonnenten vom übernehmenden Verlag ein inhaltsgleiches Schreiben. Übermittelt wurden offenbar jedenfalls die Daten von Abonnenten, die keine Rückmeldung gegeben hatten.

Die Übermittlung der Abonnentendaten haben wir aus folgenden Gründen als unzulässig bewertet:

In zivilrechtlicher Hinsicht hatte der jeweilige Abonnent nur ein Vertragsverhältnis mit dem übermittelnden Verlag, nicht jedoch mit dem übernehmenden Verlag. Der übermittelnde Verlag hatte zivilrechtlich keine Möglichkeit, die bestehenden Verträge einseitig auf einen Dritten zu übertragen. Ein Vertrag zwischen dem jeweiligen Betroffenen und dem neuen Verlag hätte vielmehr nur aufgrund einer entsprechenden Willenserklärung des jeweiligen Abonnenten zustande kommen können. Da somit kein Vertragsverhältnis zwischen den Abonnenten und dem neuen Verlag zustande gekommen war, konnten die Datenübermittlungen nicht auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG gestützt werden.

Auch das Listenprivileg kann weder in der aktuellen noch in der vor dem 1. September geltenden Fassung als Rechtsgrundlage herangezogen werden, da hier der erklärte Zweck der Übermittlung gerade nicht die bloße werbliche Ansprache war. Vielmehr diente die Datenübermittlung der sofortigen Belieferung der Kunden mit einer anderen Zeitschrift.

Wir haben gegen das übermittelnde Unternehmen ein Bußgeldverfahren eingeleitet, das noch nicht rechtskräftig abgeschlossen ist.

10.4 Versendung von E-Mails mit offenem „Verteiler"

Bei geschäftlichen Sammel-E-Mails dürfen die Namen der einzelnen Empfänger nicht den anderen Empfängern bekannt gegeben werden.

Immer wieder kommt es vor, dass Unternehmen E-Mails an Kunden und Geschäftspartner mit offenem Empfängerfeld (an-Feld oder cc-Feld) an eine Vielzahl von Empfängern („Verteiler") versenden, so dass alle Empfänger erkennen können, an welche anderen Adressaten die E-Mail ebenfalls verschickt wurde.

In einem uns bekannt gewordenen Fall umfasste der Text der Mitteilung zwei kurze Sätze. Den einzelnen Empfängern der Sendung wurden als „Beigabe" insgesamt sieben (!) Seiten personenbezogener Daten, bestehend aus E-Mail-Adressen, die im wesentlichen Vor- und Familiennamen enthielten, übermittelt.

In einem anderen Fall lud ein Unternehmen per E-Mail einen größeren Kreis von Personen zu einer Veranstaltung ein. Auch hier enthielten die meisten E-Mail-

Adressen der Empfänger deren Vor- und Nachnamen. Einige der E-Mail-Adressen hatte das Unternehmen von Homepages der Angeschriebenen entnommen, andere aus der eigenen Kundendatei.

Soweit in den E-Mail-Adressen Namen und Vornamen enthalten waren, stellen sowohl die E-Mail-Adressen selbst als auch die Inhalte der E-Mails auf die jeweiligen Empfänger bezogene Daten im Sinne des § 3 Abs. 1 BDSG dar. Da die E-Mail-Adressen aller Empfänger für jeden der Empfänger sichtbar waren, wurden diese personenbezogenen Daten letztlich an alle Empfänger gemäß § 3 Abs. 4 Satz 2 Nr. 4 BDSG übermittelt.

Die Übermittlungen waren unzulässig, da hierfür weder Einwilligungen vorlagen noch eine rechtfertigende Rechtsvorschrift einschlägig war. Eine Interessenabwägung gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG ergibt bei den genannten Fällen ein überwiegendes entgegenstehendes schutzwürdiges Interesse der Adressaten.

Die Übermittlung war auch insoweit unzulässig, als es sich um allgemein zugängliche E-Mail-Adressen handelte, wie bei denjenigen Adressen, die das Unternehmen den Internetpräsenzen der Angeschriebenen entnommen hatte. Zwar kann gemäß § 28 Abs. 1 Satz 1 Nr. 3 BDSG die Übermittlung allgemein zugänglicher Daten für die Erfüllung eigener Geschäftszwecke grundsätzlich zulässig sein. Bei der hier vorzunehmenden Abwägung war im vorliegenden Fall davon auszugehen, dass die entgegenstehenden Interessen der Betroffenen am Unterbleiben der Übermittlung offensichtlich überwogen. Denn es spricht vieles dafür, dass auch solche Betroffene, die ihre E-Mail-Adresse auf ihrer Homepage allgemein zugänglich gemacht hatten, nicht möchten, dass andere Personen Kenntnis davon erlangen, dass eine Geschäftsbeziehung zu einem bestimmten Unternehmen besteht.

Zur Vermeidung einer unbefugten Übermittlung personenbezogener Daten sind die mit der Verteilung von Massensendungen beauftragten Mitarbeiter auf den gesetzeskonformen Umgang mit Daten ausdrücklich hinzuweisen. Im Rahmen der unternehmensinternen datenschutzrechtlichen Schulung sind insbesondere die möglichen Fehlerquellen zu erläutern und beim Massenversand von E-Mails der Eintrag der Empfänger entweder einzeln im „an-Feld" oder bei einer Rundmail im „bcc-Feld" (blind-carbon-copy Feld) vorzugeben. Bei letzterem Verfahren ist für die im bcc-Feld enthaltenen E-Mail-Empfänger nicht erkennbar, wer die Mail sonst noch erhalten hat.

Im Gegensatz zu den genannten - unzulässigen - Fällen von offenen Sammeladressierungen von E-Mails sind auch datenschutzrechtlich zulässige Fallgestaltungen denkbar. Dies gilt vor allem für den E-Mail-Verkehr innerhalb von Gremien oder bei Geschäftsprozessen und Projekten, bei denen mehrere Personen beteiligt sind bzw. zusammenarbeiten. Dort ist jeder Adressat einer E-Mail oft geradezu darauf angewiesen, zu wissen, auf welchem Informationsstand die anderen Beteiligten sind.

Die Interessenabwägung gemäß § 28 Abs.1 Satz 1 Nr. 2 BDSG ergibt in diesen Fällen, dass entgegenstehende Interessen der Adressaten nur sehr gering oder gar nicht vorhanden sind und dass somit die Bekanntgabe aller Adressaten in der E-Mail zulässig ist.

10.5 Versendung einer CD-ROM mit Kundendaten durch ein Software-Unternehmen

Datenträger, die an Kunden verschickt werden, müssen vorab von personenbezogenen Daten Dritter bereinigt werden.

Ein Software-Hersteller, dessen Software von anderen Unternehmen für betriebliche Zwecke verwendet wird, wurde von einem dieser Unternehmen gebeten, ihm eine Sicherheitskopie des sog. Entwicklungsverzeichnisses der Software zur Verfügung zu stellen. Das Softwareunternehmen übermittelte daraufhin eine CD-ROM, auf der sich jedoch außer dem Entwicklungsverzeichnis auch Dokumentationen zu anderen Unternehmen befanden, die ebenfalls Kunden des Softwarehauses waren. Das Softwarehaus hatte es infolge mangelhafter Organisation der betreffenden Arbeitsprozesse versäumt, vor Versendung der CD-ROM die kundenspezifischen Dokumentationen aus dem Entwicklungsverzeichnis zu entfernen.

Die Dokumentationen enthielten eine jeweils zweistellige Anzahl von Namen, Mobiltelefonnummern, Adressen und Geburtsdaten von Kunden eines dritten Unternehmens sowie von Namen, Geburtsdaten, Anschriften, Telefonnummern, E-Mail-Adressen und - vereinzelt - Anmerkungen von Mitarbeitern eines vierten Unternehmens.

Die Übermittlung der personenbezogenen Daten war eindeutig unzulässig. Das Unternehmen hat aus Anlass unseres Tätigwerdens seine internen Arbeitsprozesse

beim Umgang mit Entwicklungsverzeichnissen überarbeitet, um ähnliche Vorfälle zukünftig zu vermeiden.

Wir haben im vorliegenden Fall ein Bußgeldverfahren durchgeführt, das inzwischen durch bestandskräftigen Bußgeldbescheid abgeschlossen wurde.

10.6 Offenlegung von Adressdaten und Beteiligungsquoten innerhalb einer Kommanditgesellschaft

Kommanditisten dürfen die personenbezogenen Daten ihrer Mitgesellschafter erfahren, auf die sie zur Ausübung ihrer Gesellschafterrechte angewiesen sind.

Ein Kommanditist einer GmbH & Co. KG forderte von der Komplementärin und Geschäftsführerin die Offenlegung der Namen aller anderen Kommanditisten nebst Kontaktdaten und Beteiligungsquoten.

Der Gesellschaftsvertrag enthielt nur eine allgemeine Klausel, wonach jeder Kommanditist Auskunft in Angelegenheiten der Gesellschaft verlangen kann. In der zivilgerichtlichen Rechtsprechung zu den Personengesellschaften ist, soweit ersichtlich, zumindest grundsätzlich anerkannt, dass ein Gesellschafter einer Personengesellschaft Auskunft über die Namen und Anschriften von Mitgesellschaftern verlangen kann. Allerdings gibt es auch anderslautende Entscheidungen, wobei sich die den Entscheidungen zugrunde liegenden Sachverhalte etwa im Hinblick auf die konkreten Regelungen im jeweiligen Gesellschaftsvertrag zum Teil erheblich voneinander unterscheiden können.

Wir haben die Übermittlung von Namen, postalischen Anschriften und Beteiligungsquoten im vorliegenden Fall als datenschutzrechtlich zulässig angesehen, da der anfragende Kommanditist seine grundlegenden Gesellschafterrechte nur dann wirksam ausüben konnte, wenn er die Möglichkeit zur Kontaktaufnahme mit den anderen Kommanditisten erhielt. Denn nach dem Gesellschaftsvertrag war die jeweilige Geltendmachung wichtiger Gesellschafterrechte an die Erfüllung eines bestimmten Quorums geknüpft. So konnten Kommanditisten die Einberufung einer außerordentlichen Gesellschafterversammlung nur dann verlangen, wenn sie mindestens 20 % des Kommanditkapitals hielten. Daher musste der einzelne Kommanditist die Mög-

lichkeit haben, neben den Kontaktdaten auch die Beteiligungsquoten anderer Kommanditisten zu erfahren, um gemeinsam mit diesen etwa die Einberufung einer außerordentlichen Gesellschafterversammlung erzwingen zu können.

An dieser Bewertung änderte auch der Umstand nichts, dass es sich um eine sog. „Publikums-KG“ handelte, das heißt einer Kommanditgesellschaft, deren Komplementär eine GmbH ist. Der Zweck einer Publikums-KG liegt typischerweise darin, eine möglichst große Anzahl von Kapitalgebern für die Finanzierung von Projekten mit erheblichem Kapitalbedarf zu erschließen. Die Kapitalgeber erhalten die Stellung von Kommanditisten. Die Publikums-KG ist auf eine unbestimmte Vielzahl von Kommanditisten angelegt, so dass unter den Kommanditisten typischerweise keine persönlichen Bindungen bestehen und diese sich in der Regel auch nicht kennen. Dieser Umstand könnte gegen eine Offenlegung zumindest von Teilen ihrer Daten an andere Kommanditisten sprechen. Ein solches Interesse von Kommanditisten an Anonymität hätte aber nach unserer Bewertung ausdrücklich vertraglich vereinbart werden müssen, woran es hier fehlte. Damit blieb es dabei, dass die Kommanditisten aufgrund der im Gesellschaftsvertrag geregelten Quoren betreffend die Ausübung wesentlicher Gesellschafterrechte die Offenlegung ihrer Kontaktdaten und Beteiligungsquoten gegenüber anderen Kommanditisten für diese Zwecke hinnehmen mussten.

Die Übermittlung von Namen, postalischen Adressen und Beteiligungsquoten war damit zulässig. Die Übermittlung von E-Mail-Adressen und Telefonnummern haben wir dagegen als nicht erforderlich angesehen, weil die Kontaktaufnahme mit den Mitgesellschaftern auch auf postalischem Weg möglich war.

11 Internationaler Datenverkehr

11.1 Datenübermittlung in die USA für Zwecke eines Gerichtsverfahrens

Fernmeldegeheimnis und deutsches Datenschutzrecht haben in einem Fall die Offenlegungspflichten für Daten aus dem Inland im Rahmen eines US-Prozesses beschränkt.

Ein deutsches Unternehmen wurde in einem Zivilrechtsstreit vor einem US-amerikanischen Gericht im Wege eines Beweisantrags der Klägerin - einem US-amerikanischen Konkurrenzunternehmen - aufgefordert, bestimmte in Deutschland befindliche Geschäftsunterlagen an das Gericht sowie an die Prozessparteien und deren Prozessvertreter in den USA zu übermitteln. Die Aufforderung bezog sich auf Geschäftsunterlagen einschließlich geschäftlicher Korrespondenz, auch in Form von E-Mails, die einen Bezug zur Klägerin oder deren Produkten oder Geschäftsgeheimnissen hatten, sowie auf bestimmte Unterlagen über Entwicklung und Vertrieb von Produkten des deutschen Unternehmens. Das deutsche Unternehmen war nicht selbst Prozesspartei. Die Beklagte war jedoch ein mit ihm eng verbundenes US-Unternehmen desselben Konzerns. Die Klägerin behauptete, dass sich die Beklagte und das deutsche Unternehmen unbefugten Zugang zu Geschäftsgeheimnissen der Klägerin verschafft hätten und wollte dies mit Hilfe der angeforderten Unterlagen belegen.

Das US-Gericht hat den Beweisantrag als zulässig bewertet, auch wenn er sich nicht gegen eine Prozesspartei richtete. Das deutsche Unternehmen fragte uns, ob und unter welchen Voraussetzungen es personenbezogene Daten übermitteln dürfe.

Der Schwerpunkt unserer Empfehlung an das deutsche Unternehmen bestand darin, sicherzustellen, dass nur Daten im erforderlichen Umfang übermittelt werden. Dies konnten von vorneherein nur Daten sein, die den inhaltlichen Kriterien des Beweisantrags tatsächlich entsprachen und zur Klärung der mit der Klage behaupteten Ansprüche beitragen konnten. Um dies zu gewährleisten, haben wir bestimmte Anforderungen gestellt. Wir teilten dem Unternehmen mit, dass es zunächst - zum Beispiel mittels einer Stichwortsuche - seine Unterlagen daraufhin überprüfen müsse, welche davon überhaupt die Kriterien des Beweisantrags erfüllen. Diese Unterlagen waren herauszufiltern und anschließend nochmals per Hand auf Relevanz, gemes-

sen an den Kriterien des Beweisantrags, zu überprüfen. Beide Arbeitsschritte mussten nach unserer Bewertung grundsätzlich im Inland stattfinden, soweit nicht konkret begründet wurde, dass dies unzumutbar wäre. Nur die so selektierten Unterlagen durften in die USA übermittelt werden. Jedoch war auch bei diesen Unterlagen die Übermittlung zunächst grundsätzlich auf pseudonymisierte Daten zu beschränken. Nur wenn eine Prozesspartei oder das Gericht näher begründeten, dass in konkreten Fällen eine Aufhebung der Pseudonymisierung erforderlich sei, konnten insoweit personenbezogene Daten im Klartext übermittelt werden.

Das Unternehmen hat - neben anderen Argumenten - diese Bewertung dem Antrag der Klägerin auf umfassende Offenlegung von Geschäftsunterlagen entgegengehalten und Daten nur in dem darin aufgezeigten Umfang übermittelt. Das deutsche Unternehmen teilte uns anschließend mit, dass das US-Gericht unsere Darstellung berücksichtigt habe. Das Gericht hat ausgeführt, dass die Klägerin nicht belegen konnte, dass unzumutbare Nachteile für ihre Beweissituation entstehen würden, wenn sich das deutsche Unternehmen an die - von uns dargestellten - Bestimmungen des deutschen Rechts halte und daher dem Beweisantrag nur in dem von uns dargestellten Umfang nachkomme. Das Gericht lehnte unter anderem mit dieser Begründung den Antrag der Klägerin auf weitergehende Offenlegung von Geschäftsunterlagen ab.

11.2 Neue Standardvertragsklauseln für die Datenübermittlung an Auftragsdatenverarbeiter in Drittstaaten

Neue Standardvertragsklauseln ermöglichen es einem in einem Drittstaat ansässigen Auftragsdatenverarbeiter mit vorheriger schriftlicher Einwilligung des Datenexporteurs einen Verarbeitungsauftrag an einen Unterauftragnehmer zu vergeben.

Mit Wirkung zum 15. Mai 2010 hat die Europäische Kommission die Standardvertragsklauseln vom 27. Dezember 2001 für die Datenübermittlung an Auftragsdatenverarbeiter in Drittländer aufgehoben und durch neue Standardvertragsklauseln vom 5. Februar 2010 ersetzt. Die neuen Klauseln enthalten erstmals auch eine Regelung, die die Vergabe von Unteraufträgen durch den Auftragsdatenverarbeiter ermöglicht. Demnach kann der in einem Drittstaat ansässige Auftragsdatenverarbeiter mit vorheriger schriftlicher Einwilligung des Datenexporteurs einen Verarbeitungs-

auftrag an einen Unterauftragnehmer vergeben. Hierzu ist eine schriftliche Vereinbarung mit dem Unterauftragnehmer erforderlich, die diesem die gleichen Pflichten auferlegt, denen auch der (Haupt-) Auftragnehmer nach den Standardvertragsklauseln unterworfen ist.

Die neuen Standardvertragsklauseln können allerdings „als solche" (also als Standardvertragsklauseln, die somit die Genehmigungspflicht für den Datenexport entfallen lassen) nicht von Auftragsdatenverarbeitern **mit Sitz in einem Mitgliedstaat der EU oder des Europäischen Wirtschaftsraums (EWR)** für die Erteilung von Unteraufträgen verwendet werden. Die Artikel-29-Gruppe der Datenschutzaufsichtsbehörden der EU-Mitgliedsstaaten hat in ihrem Arbeitspapier (Working Paper) Nr. 176 (im Internet abrufbar unter http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm) ausdrücklich darauf hingewiesen, dass die neuen Standardvertragsklauseln für diese Fallgestaltung keine - auch keine entsprechende - Anwendung finden können. Angesichts des klaren Wortlauts der neuen Klauseln haben wir uns dieser Auffassung angeschlossen. Für derartige Fälle bleibt es dabei, dass ein direkter Vertragsschluss zwischen dem Auftraggeber in der EU bzw. im EWR und dem Unterauftragnehmer im Drittstaat erforderlich ist. Hierzu können die neuen Standardvertragsklauseln vom 5. Februar 2010 verwendet werden, jedoch muss der Auftraggeber insoweit Vertragspartei sein. Eine Stellvertretung des Auftraggebers durch den (Haupt-) Auftragsdatenverarbeiter ist bei diesem Vertragsschluss - wie schon bislang - allerdings möglich.

11.3 Auftragsdatenverarbeitung in Drittstaaten

Die Anforderungen des § 11 BDSG müssen auch bei der Weitergabe von Daten an Auftragsdatenverarbeiter in Drittstaaten eingehalten werden.

Deutsche Unternehmen, die Daten auf der Grundlage der neuen Standardvertragsklauseln vom 5. Februar 2010 an Auftragsdatenverarbeiter in Drittstaaten exportieren wollen, müssen neben den Zulässigkeitsvoraussetzungen der "zweiten Stufe" (§§ 4b, 4c BDSG) auch die Anforderungen des § 11 BDSG in der seit 1. September 2009 geltenden Fassung erfüllen. Denn die Voraussetzungen des § 11 BDSG betreffen die sog. erste Stufe des Datenumgangs und müssen daher unabhängig davon eingehalten werden, wo die Datenverarbeitung im Auftrag stattfindet. Andernfalls stünden die Personen, deren Daten verarbeitet werden, bei einer Auftragsver-

arbeitung im Drittstaat zum Teil schlechter als bei einer Verarbeitung im Inland oder innerhalb der EU bzw. des EWR.

In der Praxis können bei Verwendung der Standardvertragsklauseln die nach § 11 Abs. 2 Satz 2 BDSG erforderlichen schriftlichen Festlegungen, soweit sie nicht bereits in den Standardvertragsklauseln vom 5. Februar 2010 selbst enthalten sind, zum Beispiel in den Anhängen des Standardvertrags, als sog. geschäftliche Klauseln als Ergänzung des Hauptvertrags oder in einem gesonderten Dienstleistungsvertrag, auf den Bezug genommen wird, getroffen werden. So kann etwa die gemäß § 11 Abs. 2 Satz 2 Nr. 1 BDSG erforderliche Festlegung des Gegenstands und die Dauer des Auftrags im Anhang 1 des Standardvertrags im Rahmen der dort vorzunehmenden näheren Beschreibung der Verarbeitung ergänzt werden. Diese Ergänzungen des Standardvertrags lösen keine Genehmigungspflicht gemäß § 4c Abs. 2 BDSG für die auf Grundlage des so ergänzten Standardvertrags vorgenommenen Datenübermittlungen aus.

12 Beschäftigtendatenschutz

12.1 Unternehmensinterne Veröffentlichung von Rankings

Eine unternehmensinterne, personenbezogene Veröffentlichung von Rankings in Form sog. Rennlisten ist datenschutzrechtlich unzulässig.

Ein Unternehmen möchte bei Außendiensttagungen die Umsatzzahlen aller Mitarbeiter mit den dazugehörigen Namen bekanntgeben.

Maßstab für die Zulässigkeit der Datennutzung ist § 32 Abs. 1 Satz 1 BDSG. Bei der Frage, ob die Datennutzung für die Durchführung des Beschäftigungsverhältnisses erforderlich ist, ist auch der Grundsatz der Verhältnismäßigkeit zu beachten. In diesem Rahmen ist auch auf die Interessenlage abzustellen. Ein Interesse des Unternehmens, seine Mitarbeiter mit solchen Vergleichslisten zu motivieren, kann durchaus gesehen werden. Allerdings überwiegt in der Regel das entgegenstehende Interesse der Mitarbeiter daran, dass die Umsatzzahlen nicht personenbezogen veröffentlicht werden. Um das Ziel eines Leistungsanreizes zu erreichen, genügt es auch, diese Daten zu anonymisieren. Damit wäre eine personenbezogene Veröffentlichung unverhältnismäßig und damit unzulässig.

12.2 Online-Bewerbung

Bei Online Bewerbungen muss eine Einwilligungserklärung der Bewerber, dass die Bewerbungen an andere Stellen weitergeleitet werden dürfen, den Vorgaben des § 13 Telemediengesetz entsprechen.

Ein Kandidat, der sich bei einem Unternehmen online für eine ausgeschriebene Stelle bewarb, beschwerte sich darüber, dass das Unternehmen seine Daten innerhalb der Firmengruppe weitergeleitet hat. Das Unternehmen beruft sich darauf, dass die Bewerber in der Datenschutzerklärung über diese Verwendung ihrer Daten informiert würden. Bewirbt sich jemand in Kenntnis dieser Tatsache, so willige er in die Weiterleitung ein.

Es handelt sich hier um eine Datenübermittlung, für die eine Rechtsvorschrift als Rechtsgrundlage nicht zur Verfügung steht und die deshalb nur aufgrund einer wirksamen Einwilligung zulässig ist.

Eine wirksame elektronische Einwilligung liegt jedoch nur vor, wenn das Unternehmen gemäß § 13 Abs. 1 Telemediengesetz (TMG) den Betroffenen vorher über Art, Umfang und Zweck der Erhebung und Verwendung der personenbezogenen Daten informiert und die Vorgaben der Nr. 2 dieser Vorschrift einhält. Danach muss das Unternehmen bei einer elektronischen Einwilligung sicherstellen, dass

- der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird und
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann.

Vorliegend wurden die Bewerber über die Weiterleitung ihrer Daten nur über Betätigen eines Hinweis-Links auf der "Datenschutzerklärung" informiert. Dies erfüllte die oben genannten Anforderungen nicht. Es fehlte an einer ausreichenden Information ebenso wie an einer bewussten und eindeutigen Einwilligungserklärung der Bewerber.

12.3 Weiterleitung einer Absage an Mitbewerber

Die fahrlässige Weiterleitung einer an einen bestimmten Bewerber gerichteten Absage an die anderen Mitbewerber ist datenschutzrechtlich unzulässig und erfüllt den Tatbestand einer Ordnungswidrigkeit.

Im Rahmen eines Auswahlverfahrens für eine Stellenbesetzung gab ein Unternehmen seine Absage an einen Bewerber nicht nur diesem, sondern auch den anderen Bewerbern per E-Mail unter „cc“ zur Kenntnis.

Es handelt sich hier um eine unzulässige Datenübermittlung, weil dafür weder eine Einwilligung der Bewerber vorlag noch eine gesetzliche Rechtsgrundlage dies rechtfertigte.

Wir beanstandeten das Verhalten und leiteten, da es sich um einen gravierenden datenschutzrechtlichen Verstoß handelte, ein Ordnungswidrigkeitenverfahren gegen den verantwortlichen Mitarbeiter des betreffenden Unternehmens ein.

12.4 Anzeige von Krankheitstagen im Intranet

Die offene Anzeige von Krankheitstagen im Intranet ist unzulässig.

Ein Unternehmen zeigte die Krankheitstage seiner Beschäftigten personenbezogen im Intranet an.

Die Zulässigkeit dieser Datenverwendung richtet sich nach § 32 Abs. 1 Satz 1 BDSG. Sie ist für die Durchführung des Beschäftigungsverhältnisses nicht erforderlich, da unverhältnismäßig, und somit unzulässig. Es darf außerhalb der personalverantwortlichen Stelle nicht als allgemeine Information zugänglich sein, wenn ein Beschäftigter aufgrund von Krankheit fehlt.

Wenn die An- oder Abwesenheit aufgrund von Arbeitseinteilung und Organisation im Unternehmen bekannt sein muss, kann dies im Intranet neutral vermerkt werden.

13 Gesundheitswesen

13.1 Übermittlung einer Behandlungsakte durch einen Arzt an seinen Rechtsanwalt im Rahmen einer rechtlichen Auseinandersetzung mit einem Patienten

Ein Arzt darf nur solche Teile der Behandlungsakte, die er zur Klärung des Rechtsstreits für erheblich hält, an seinen Rechtsanwalt weitergeben.

Im Rahmen einer Rechtsstreitigkeit mit einem Patienten übermittelte ein Arzt die vollständige zur psychiatrischen bzw. psychotherapeutischen Behandlung des Patienten geführte Dokumentation an seinen Rechtsanwalt. Der Patient beschwerte sich bei uns darüber, dass der Arzt seinem Rechtsanwalt die gesamte Akte übersandte und nicht nur diejenigen Teile davon, die für die Wahrnehmung seiner rechtlichen Interessen erforderlich waren.

Im Zuge unserer datenschutzrechtlichen Überprüfung kamen wir nach eingehender Diskussion mit der Bayerischen Landesärztekammer und der Rechtsanwaltskammer München über die Beachtung des Datenschutzrechts bei derartigen Übermittlungen zu folgendem einvernehmlichen Ergebnis:

Soweit keine wirksame Einwilligung des Patienten vorliegt, ist Maßstab für eine zulässige Übermittlung von medizinischen Behandlungsunterlagen durch einen Arzt an einen Rechtsanwalt bei Rechtsstreitigkeiten mit einem Patienten die **Erforderlichkeit.**

Unterlagen, die ein Rechtsanwalt für eine angemessene Vertretung der rechtlichen Interessen seines Mandanten benötigt, dürfen an ihn auf der gesetzlichen Grundlage des § 28 Abs. 6 Nr. 3 BDSG herausgegeben werden. Dagegen kann die Übermittlung von Aktenteilen, die für die rechtliche Auseinandersetzung mit den streitgegenständlichen Fragen nicht erforderlich sind, nicht auf diese Vorschrift gestützt werden.

Durch eine Prüfung im konkreten Einzelfall ist sicherzustellen, dass an den Rechtsanwalt nur die zur Rechtsverteidigung erforderlichen Unterlagen übermittelt werden und es zu keiner „überschießenden" Weitergabe sensibler Daten kommt. Dies gilt im besonderen für psychiatrische Behandlungsakten, die äu-

ßerst sensible Daten des betroffenen Patienten und im Regelfall auch Angaben von am Rechtsstreit nicht beteiligter Dritter enthalten.

Aus den genannten Gründen darf ein Arzt medizinische Behandlungsunterlagen nicht ungeprüft an seinen Rechtsanwalt übergeben. Er muss vielmehr in jedem Einzelfall ggf. mit seinem Rechtsanwalt zusammen prüfen, welche Teile der Akte der Anwalt **zur Vertretung seiner Mandantschaft** benötigt. Nur diese **erforderlichen Teile** darf der Arzt dem Anwalt übergeben (§ 28 Abs. 6 Nr. 3 BDSG, § 3a Satz 1 BDSG).

Diese Vorgehensweise des Arztes ist auch vor dem Hintergrund seiner ärztlichen Schweigepflicht aus § 203 Abs. 1 Satz 1 Strafgesetzbuch (StGB) geboten. Zwar darf ein Arzt zur Wahrnehmung seiner berechtigten Interessen, beispielsweise zur Durchsetzung von Honoraransprüchen, Patientendaten gegenüber seinem Rechtsanwalt preisgeben. Nach der Rechtsprechung des Bundesgerichtshofs (Urteil vom 23.06.1993, Az. VIII ZR 226/92) ist der Arzt dabei jedoch zu einer sorgfältigen, am Grundsatz der Verhältnismäßigkeit ausgerichteten Abwägung zwischen seinen eigenen berechtigten wirtschaftlichen Interessen und dem Geheimhaltungsbedürfnis des Patienten gehalten. Die Preisgabe von Behandlungsdaten hat er insoweit auf das angemessene, zur Beitreibung seiner Honoraransprüche erforderliche Maß zu beschränken.

13.2 Überschießende Datenübermittlung durch behandelnden Arzt an ein Versicherungsunternehmen

Ein Arzt darf auch bei Vorliegen einer Schweigepflichtentbindung nur die Patientendaten an eine Versicherung übermitteln, die für die Versicherung für die Entscheidung, ob und zu welchen Konditionen eine Berufsunfähigkeitsversicherung angeboten werden kann, erforderlich sind.

Ein Versicherungsunternehmen bat im Rahmen der Prüfung eines Antrags auf Abschluss einer Berufsunfähigkeitsversicherung den behandelnden Arzt anhand eines Fragebogens um Auskunft zur Antragstellerin. Diese hatte ihren Arzt im Versicherungsantrag von seiner ärztlichen Schweigepflicht entbunden. Neben dem Fragebogen übersandte der Arzt dem Versicherungsunternehmen unaufgefordert die ge-

samte und sehr umfangreiche Behandlungsdokumentation der letzten sechs Jahre, die auch persönliche und nicht fachliche Bemerkungen zur Antragsstellerin enthielt.

Rechtsgrundlage für die Übermittlung der vom Versicherungsunternehmen **angeforderten** und zur Prüfung des Antrags **erforderlichen** Gesundheitsdaten durch den Arzt war die im Versicherungsantrag erteilte Einwilligungs- und Schweigepflichtentbindungserklärung der Antragsstellerin (§ 4a Abs. 1 und 3 BDSG). Nicht gedeckt von dieser Einwilligung war jedoch die überschießende Erteilung von Auskünften, d.h. eine Übermittlung von Gesundheitsdaten, die vom Versicherer gar **nicht angefordert** wurden und zur Antragsprüfung **nicht erforderlich** waren, insbesondere die persönlichen und nicht fachlichen Anmerkungen des Arztes zu seiner Patientin. Insoweit war die Datenübermittlung unzulässig.

Hat ein Arzt Zweifel, welche Angaben das Versicherungsunternehmen benötigt, so muss er bei diesem nachfragen und sich auch mit seinem Patienten diesbezüglich abstimmen.

14 Vereine und Verbände

14.1 Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen

Die Übermittlung personenbezogener Daten von Vereinsmitgliedern an ein Versicherungsunternehmen, mit dem der Verein einen sogenannten Gruppenversicherungsvertrag geschlossen hat, ist nur mit deren Einwilligung zulässig. Dies gilt sowohl für Mitglieder, die erst nach Abschluss des Gruppenversicherungsvertrages dem Verein beigetreten sind, als auch für Mitglieder, die zu diesem Zeitpunkt bereits Mitglied waren.

Bei sog. Gruppenversicherungsverträgen handelt es sich um Rahmenverträge zwischen Vereinen bzw. Verbänden und Versicherungsunternehmen, die den Mitgliedern der Vereine bzw. Verbände unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen.

Werden für die Werbung zum Abschluss solcher Verträge personenbezogene Daten der Mitglieder an ein Versicherungsunternehmen übermittelt, setzt dies die Einwilligung der Betroffenen voraus, da sich eine gesetzliche Erlaubnis hierfür in aller Regel nicht finden lässt.

Die Weitergabe der Mitgliederdaten zum Zweck der Werbung durch ein Versicherungsunternehmen dient normalerweise nicht den in der Satzung festgelegten Zielen eines Vereins und damit auch nicht dem rechtsgeschäftsähnlichen Schuldverhältnis zwischen Mitglied und Verein (§ 28 Abs. 1 S. 1 Nr. 1 BDSG). Auch die Voraussetzungen des § 28 Abs. 3 BDSG liegen nicht vor. Die Mitglieder vertrauen darauf und dürfen auch darauf vertrauen, dass die Daten, die sie im Rahmen ihres Vereinsbeitritts angegeben haben, nicht ungefragt für Werbezwecke an Dritte weitergegeben werden. Insofern überwiegt hier das schutzwürdige Interesse der Betroffenen.

Vor allem im Hinblick darauf, dass Betroffene in uns bekannt gewordenen Fällen von Versicherungsvertretern sogar in ihrer Privatwohnung aufgesucht worden sind, halten wir es auch bei Alt-Mitgliedern nicht mehr für ausreichend, sie lediglich unter Einräumung eines Widerspruchsrechts über die Datenweitergabe zu informieren.

In der gleichen Weise hat sich der Düsseldorfer Kreis in seinem Beschluss vom 24./25. November 2010 zum Umgang mit Gruppenversicherungsverträgen geäußert.

14.2 Übermittlung von Spenderdaten bei Anlassspenden

Datenschutzrechtliche Vorschriften stehen einer Auskunft an den Spendenveranlasser darüber, wer in welcher Höhe gespendet hat, nicht entgegen.

Immer häufiger wird bei verschiedenen Anlässen (Geburtstag, Jubiläum, Beerdigung) um Spenden an eine gemeinnützige Organisation anstelle von Geschenken oder Blumen gebeten. Die begünstigte gemeinnützige Organisation erfährt, wer in welcher Höhe gespendet hat, derjenige jedoch, der zu den Spenden aufgerufen hat (Spendenveranlasser), nicht.

Eine Bekanntgabe der Spenderdaten an den Spendenveranlasser bzw. im Fall einer Beerdigung an die Hinterbliebenen ist in diesen Fällen datenschutzrechtlich nicht zu beanstanden.

Die Übermittlung der Namen der Spender einschließlich der Spendenbeträge durch die begünstigte Organisation ist von der Erlaubnis des § 28 Abs. 2 Nr. 2 a BDSG gedeckt. Nach dieser Vorschrift ist die Übermittlung personenbezogener Daten für einen anderen als den eigenen Geschäftszweck zulässig, wenn es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an einem Ausschluss der Übermittlung hat.

Ein berechtigtes Interesse des Spendenveranlassers ergibt sich daraus, dass die Spende als Ersatz für eine Zuwendung an ihn zu sehen ist. Dies zeigt sich daran, dass sich die Höhe der Spende in erster Linie nach der Wertschätzung bemisst, die dem Spendenveranlasser gegenüber zum Ausdruck gebracht werden soll, und weniger nach der Motivation des Spenders, die angegebene Organisation zu unterstützen. Es kann sogar vorkommen, dass der Spender von der Organisation gar nicht viel hält, gleichwohl aber einen ansehnlichen Betrag spendet, um seiner Verbundenheit Ausdruck zu verleihen. Der Spendenveranlasser befindet sich also in der gleichen Situation wie derjenige, der ein Geschenk erhält und muss demzufolge die

Möglichkeit haben, seinen sich aus dem Geschenk ergebenden Verpflichtungen nachzukommen. Hierzu gehört, dass er sich bei einem Spender in angemessener Weise bedanken kann, beispielsweise in besonderem Maß bei denjenigen, deren Spenden weit über dem Durchschnitt liegen. Dies gilt sinngemäß auch im Fall einer Beerdigung für die Hinterbliebenen.

Ein Grund zu der Annahme, dass der Spender ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung der Daten an den Spendenveranlasser hat, besteht in aller Regel nicht. Vielmehr wird man sogar annehmen müssen, dass der Spender in gleicher Weise wie jemand, der einem anderen ein persönliches Geschenk macht oder bei einer Beerdigung Blumen stiftet, davon ausgeht und es letzten Endes auch so haben will, dass der Beschenkte bzw. die Hinterbliebenen davon erfahren. Schließlich möchte er in vielen Fällen mit seinem Geschenk Verpflichtungen gegenüber dem Beschenkten erfüllen (z.B. Dank für die Einladung, Revanchieren für ein früher erhaltenes Geschenk usw.) bzw. seine Wertschätzung und Verbundenheit ausdrücken.

15 Wohnungswirtschaft und Mieterdatenschutz

15.1 Mieterselbstauskünfte

Die Erhebung und Verwendung der im Vorfeld der Vermietung einer Wohnung über eine Mieterselbstauskunft abgefragten Daten ist zulässig, soweit die Daten für die Begründung oder Durchführung des Mietvertrages erforderlich sind.

In regelmäßigen Abständen erreichen uns Anfragen von Bürgern, die sich über die Art und den Umfang der Fragen irritiert zeigen, die ihnen im Vorfeld der Vermietung einer Wohnung - oft in Form einer standardisierten Mieterselbstauskunft - zur Beantwortung vorgelegt werden.

Vermieter sind meist bestrebt, so viele Informationen wie möglich über den jeweiligen Mietinteressenten zu gewinnen, um sich ein umfassendes Bild von einem potentiellen Mieter machen zu können. Dabei wird jedoch oftmals über das Ziel hinausgeschossen. Die befragten Personen zeigen sich verunsichert, ob jede gestellte Frage tatsächlich beantwortet werden muss.

Die Zulässigkeit der Erhebung von personenbezogenen Daten mittels Mieterfragebögen bewegt sich im Spannungsfeld zwischen dem auf Grund der Privatautonomie bestehenden legitimen Interesse des Vermieters, einen ihm entsprechenden Mieter zu finden, der insbesondere seinen Verpflichtungen aus dem Mietvertrag nachkommen kann (Zahlung der Miete, pfleglicher Umgang mit dem Mietobjekt, Eingliederung in die Hausgemeinschaft), und auf der anderen Seite dem informationellen Selbstbestimmungsrecht des Mietinteressenten.

Der Maßstab aus datenschutzrechtlicher Sicht ist § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Das Erheben, Speichern und Nutzen personenbezogener Daten des Mietinteressenten durch den Vermieter ist danach zulässig, „wenn es für die Begründung oder Durchführung des Mietvertrages erforderlich ist". Nach dieser gesetzlichen Regelung ist die Erhebung der Daten erlaubt, die für den Vermieter bei verständiger Würdigung für den Abschluss des Mietvertrages wesentlich sind, so zum Beispiel die Identität des Mietinteressenten (Name, Vorname, Anschrift), seine Einkommensverhältnisse, eventuelle Mietrückstände im aktuellen Mietverhältnis, seine berufliche Stellung, die Zahl der mit einziehenden Kinder und deren Alter.

Keine Erforderlichkeit sehen wir aber beispielsweise für die verpflichtende Angabe zur Höhe etwaiger Ersparnisse oder einer Bankverbindung bereits im Vorfeld der Entscheidung über den künftigen Mieter.

Vermieter, die mehr als 50 Wohnungen vermieten, müssen außerdem § 19 des Allgemeinen Gleichbehandlungsgesetzes (AGG) im Hinblick auf die Benachteiligung aus Gründen der Rasse oder der ethnischen Herkunft, wegen des Geschlechts, der Religion, einer Behinderung, des Alters oder der sexuellen Identität beachten.

15.2 Einholen von Auskünften über die Bonität von Mietinteressenten bei Auskunfteien

Neben der direkten Befragung der Bewerber besteht für Vermieter die Möglichkeit, bei Auskunfteien Informationen zur Bonität der Mietinteressenten einzuholen. Auch hier setzt das Datenschutzrecht Grenzen.

Wie oben ausgeführt, sind Vermieter bestrebt, so viele Informationen wie möglich über den jeweiligen Mietinteressenten zu gewinnen, um sich ein umfassendes Bild von einem potentiellen Mieter machen zu können. Dabei werden in erheblichem Umfang auch Anfragen bei Auskunfteien in Auftrag gegeben.

Nach § 29 Absatz 2 Nr. 1a BDSG ist die Erteilung von Bonitätsauskünften nur zulässig, wenn der Vermieter ein berechtigtes Interesse hieran hat und wenn kein Grund zu der Annahme besteht, dass der betroffene Mietinteressent ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Da Vermieter mit dem Abschluss eines Mietvertrages das Risiko eingehen, dass ein Mieter aufgrund von Zahlungsunfähigkeit oder -unwilligkeit den Mietzins oder Nebenkosten nicht begleicht, erkennen die Aufsichtsbehörden an, dass Vermieter aufgrund dieses finanziellen Ausfallrisikos grundsätzlich ein berechtigtes Interesse an einer Bonitätsauskunft über einen Mietinteressenten haben. Bei der erforderlichen Abwägung sind allerdings auch die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung zu berücksichtigen. Ferner ist zu beachten, dass Mietkautionen in Höhe von bis zu drei Monatsmieten, das Vermieterpfandrecht und die bei nachträglicher Zahlungsunfähigkeit vielfach in die Zahlungspflicht eintretenden Sozialbehörden das finanzielle Risiko der Vermieter teilweise reduzieren.

Der Düsseldorfer Kreis, das bundesweite Gremium der obersten Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, hat dazu im Oktober 2009 mit Zustimmung des Landesamtes den folgenden Beschluss gefasst:

Häufig holen Vermieter Informationen bei Auskunfteien über die Bonität von Mietinteressenten ein, bevor sie Wohnraum vermieten. Hierfür gelten folgende Anforderungen:

1. Vermieter dürfen erst dann eine Auskunft zu einem Mietinteressenten einholen, wenn der Abschluss des Mietvertrags mit diesem Bewerber nur noch vom positiven Ergebnis einer Bonitätsprüfung abhängt.

2. Es dürfen nur folgende Datenkategorien nach Darlegung eines konkreten berechtigten Interesses an Vermieter übermittelt werden, sofern diese Daten zulässigerweise an die Auskunftei übermittelt bzw. von dieser erhoben wurden:

   - Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen;

   - sonstige Daten über negatives Zahlungsverhalten, bei denen

     - die dem jeweiligen Eintrag zugrunde liegende Forderung noch offen ist oder – sofern sie sich zwischenzeitlich erledigt hat – die Erledigung nicht länger als ein Jahr zurückliegt und
     - eine Bagatellgrenze von insgesamt 1.500 € überschritten wird.

3. Die Übermittlung von Scorewerten an Vermieter ist unzulässig, sofern darin andere als die unter 2. erwähnten Daten verwendet werden.

4. Vermieter dürfen weitergehende als die unter 2. genannten Daten grundsätzlich auch nicht im Wege einer Einwilligung oder einer Selbstauskunft des Mietinteressenten von einer Auskunftei erheben.

15.3 Benennung einer Wohnung als Vergleichsobjekt im Mieterhöhungsverfahren

Die Benennung einer Wohnung als Vergleichsobjekt im Mieterhöhungsverfahren ist im Regelfall auch ohne Einwilligung der Bewohner datenschutzrechtlich zulässig.

Um eine Mieterhöhung durchzusetzen, muss der Vermieter das Mieterhöhungsverlangen gegenüber seinem Mieter begründen (§ 558a BGB).

Hierfür genügt nach der Vorschrift des § 558a Abs. 2 Nr. 4 BGB die Benennung von drei vergleichbaren Wohnungen für die ein der Mieterhöhung entsprechender Mietzins entrichtet wird. Nach der Rechtsprechung des Bundesgerichtshofs müssen die Vergleichsobjekte so genau beschrieben werden, dass sie für den Mieter identifizierbar sind, um eine Nachprüfung zu ermöglichen. Regelmäßig wird eine solche Aufstellung, sofern sie nicht ohnehin mit Hilfe eines Computers erstellt wird, den manuellen Dateibegriff erfüllen, so dass die Vorschriften des Bundesdatenschutzgesetzes Anwendung finden.

Ist die Wohnung identifizierbar, so sind die Angaben als Einzelangaben über die sachlichen Verhältnisse der dort lebenden Person zu bewerten. Durch die genaue Beschreibung der Wohnung kann auf die Lebensumstände der Bewohner geschlossen werden. Sie stellen damit personenbezogene Daten i.S.d. Datenschutzrechts dar.

Im Regelfall ist die Benennung einer Wohnung als Vergleichsobjekt im Mieterhöhungsverfahren auf der Grundlage von § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig.

Im Rahmen dieser Vorschrift sind die berechtigten Interessen des Vermieters mit den entgegenstehenden schutzwürdigen Interessen der Bewohner der Vergleichsobjekte abzuwägen. Festzuhalten ist, dass es sich um relativ sensible Daten aus dem grundrechtlich besonders geschützten häuslichen Lebensbereich handelt. Allerdings kommt es nur in dem eher seltenen Fall der Nachprüfung durch den Mieter zu einer fühlbaren Beeinträchtigung. Zu Gunsten des Vermieters spricht der Grundsatz der Einheit der Rechtsordnung: Von den rechtlichen Instrumenten, die der Gesetzgeber zur Verfügung stellt, muss Gebrauch gemacht werden können, ohne von der Einwilligung eines Dritten abhängig zu sein. Vor diesem Hintergrund überwiegen

die berechtigten Interessen des Vermieters - von Ausnahmen wegen besonderer Umstände im Einzelfall abgesehen - die schutzwürdigen Interessen der Bewohner.

15.4 Datenschutz bei „intelligenter“ Stromverbrauchsmessung - Smart Metering

Beim Einsatz „intelligenter Zähler“ (Smart Meter) zur Messung des Energieverbrauchs sind die Ableseintervalle an die Anzahl der angebotenen Tarife des Energieversorgers anzupassen. Ein häufigeres Ablesen bedarf der Einwilligung des Anschlussnutzers.

Seit dem 1. Oktober 2010 müssen in Neubauten oder Gebäuden, die in größerem Umfang renoviert worden sind, Messeinrichtungen eingebaut werden, die dem Anschlussnutzer den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit anzeigen. Für die übrigen Gebäude muss ein Einbau solcher Messeinrichtungen angeboten werden. Diese „intelligenten" Zähler werden auch Smart Meter genannt.

Die gesetzliche Verpflichtung zum Einbau von Smart Metern verfolgt klimapolitische Ziele: Der Einzelne soll besser über seinen Energieverbrauch informiert sein, um Einsparpotentiale erkennen und nutzen zu können.

In diesem Zusammenhang ist auch eine weitere Maßnahme des Gesetzgebers zu sehen: Die Energieversorgungsunternehmen mussten bis spätestens 30. Dezember 2010 den Verbrauchern Tarife anbieten, die einen Anreiz zur Energieeinsparung oder Steuerung des Energieverbrauchs bieten. Dies sind insbesondere lastvariable und tageszeitabhängige Tarife. Auch hierfür ist eine detailliertere Verbrauchserfassung als bislang notwendig. Das vorgesehene Ableseintervall beträgt 15 Minuten. Dies bedeutet ca. 35.000 Messpunkte pro Jahr. Die Daten werden über Funk oder via Internet übertragen.

Die so gewonnenen Verbrauchsdaten sind jedenfalls bei Ein-Personen-Haushalten als personenbezogene Daten zu bewerten. Sie geben Auskunft über die persönlichen und sachlichen Verhältnisse des Bewohners. Die meisten menschlichen Aktivitäten sind in unserer heutigen Gesellschaft mit dem Verbrauch von Energie verknüpft. Anhand der charakteristischen Verbrauchskurven von Haushaltsgeräten

lässt sich sogar mit großer Treffsicherheit bestimmen, welches Gerät zu welcher Zeit im Einsatz war. Daraus lässt sich auf Lebensgewohnheiten schließen:

- Wie häufig wird gekocht?
- Wird hierbei der Backofen benutzt?
- Wann wird aufgestanden?
- Wann wird das Haus verlassen?
- Wann kommen die Bewohner zurück?
- Wann wird ins Bett gegangen?
- Gibt es nächtliche Toilettenbesuche?
- usw.

Bislang fehlt eine spezielle Regelung zum Datenschutz in den Energiegesetzen. Daher sind die allgemeinen Vorschriften und Grundsätze aus dem BDSG zu beachten. Soweit die Messdaten zu Abrechnungszwecken benötigt werden, ist ihre Erhebung und Verarbeitung auf gesetzlicher Grundlage zulässig. Es gilt das Prinzip der Erforderlichkeit, d.h. die Häufigkeit der Messungen pro Tag muss sich an der Anzahl der angebotenen Tarife orientieren. Bietet beispielsweise ein Energieversorger drei Tarife am Tag tageszeitabhängig an, so rechtfertigt der Zweck der Abrechnung lediglich drei Messungen pro Tag.

Darüber hinaus erfolgende Messungen bedürfen der Einwilligung des Anschlussnutzers. Die Einwilligung bedarf der Schriftform. Sie kann zusammen mit dem Energielieferungsvertrag abgegeben werden. In diesem Fall ist sie jedoch besonders hervorzuheben. Der Anschlussnutzer muss auf die vorgesehenen Zwecke der Erhebung, Verarbeitung oder Nutzung seiner Messdaten hingewiesen werden. Eine Verwendung der Daten zu anderen Zwecken ist unzulässig. Der Anschlussnutzer kann die Einwilligung mit Wirkung für die Zukunft jederzeit widerrufen.

Zur Gewährleistung der Datensicherheit sind Vorkehrungen zu treffen, die ein unbefugtes Auslesen verhindern.

16 Videoüberwachung

16.1 Videoüberwachung der Außenbestuhlung eines Cafes

Vandalismusschäden außerhalb der Betriebszeit können die Videoüberwachung der Außenbestuhlung eines Cafes in der Zeit von 22.00 bis 07.00 Uhr rechtfertigen.

Ein Eiscafe hatte immer wieder durch Vandalismus verursachte Schäden an seiner Außenbestuhlung sowie an Pflanztrögen mit Zierbäumen und an Blumenkästen zu beklagen. Die Betreiber des Eiscafes richteten dazu eine Videoüberwachung für diese Bereiche ein.

Die an die Gehsteigfläche angrenzende Bestuhlung ist öffentlich zugänglich, so dass sich die Zulässigkeit der Videoüberwachung nach § 6b BDSG bemisst. Danach muss die Videoüberwachung für die Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen erforderlich sein und es dürfen keine Anhaltspunkte vorliegen, dass schutzwürdige Interessen der Betroffenen überwiegen. Wir bejahten hier aufgrund der geschilderten Vorfälle ein berechtigtes Interesse der Betreiber an der Videoüberwachung und hielten dieses auch für überwiegend im Verhältnis zum Persönlichkeitsrecht von aufgenommenen Personen. Dies galt jedoch unter der Voraussetzung, dass die Überwachung nur außerhalb der Betriebszeit von 22.00 bis 7.00 Uhr stattfindet.

16.2 Videoüberwachung in Aufzugskabine oder Waschküche

Die Videoüberwachung einer Aufzugskabine oder einer Waschküche in einem Mehrfamilienhaus ist nur zulässig, wenn immer wieder Schäden festgestellt werden. Auf die Videoüberwachung muss deutlich hingewiesen werden.

Eine Eigentümergemeinschaft beabsichtigte, wegen Vandalismus die Aufzugskabine und die Waschküche mit Videokameras zu überwachen.

Da es sich bei der Aufzugskabine und der Waschküche in einem Mehrfamilienhaus um nicht öffentlich zugängliche Bereiche handelt, kommt § 6b BDSG nicht in Betracht. Für die Anwendbarkeit der allgemeinen datenschutzrechtlichen Regelungen

ist Voraussetzung, dass es sich bei der Videoüberwachung um eine automatisierte Datenverarbeitung handelt. Dies ist nur bei einer digitalen Aufzeichnung gegeben. Prüfungsmaßstab ist dann § 28 Abs. 1 Nr. 2 BDSG. Die Überwachung ist zulässig, wenn sie zur Wahrung berechtigter Interessen der Eigentümergemeinschaft erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Überwachung überwiegt. Um eine Zulässigkeit der Überwachung im Aufzug bejahen zu können, müssten gewichtige Vorfälle von Vandalismus vorliegen, da auch hausfremde Personen den Aufzug benutzen. Da Benutzer des Aufzugs davon ausgehen, unbeobachtet zu sein, ist ein deutlich erkennbares Schild nötig, das auf die Überwachung hinweist.

Weil sich in der Waschküche keine hausfremden Personen aufhalten, kann der Kameraeinsatz mit sich wiederholenden Schadensereignissen gerechtfertigt werden.

16.3 Videoüberwachung in einer Gaststätte

Wenn sich in einer Gaststätte, bedingt durch ihre besondere Lage, oft alkoholisierte Gäste aufhalten, die in der Vergangenheit vermehrt Straftaten begingen, ist die Kameraüberwachung des Kassenbereichs und ausnahmsweise auch des Gastraums zulässig.

Eine Gaststätte, die sich im gleichen Haus wie eine sehr große Disco befindet, überwachte mit Videokameras den Gastraum und den Kassenbereich.

Eine Videoüberwachung des Gastraums einer Gaststätte ist gemäß § 6b BDSG grundsätzlich unzulässig, weil dort das schutzwürdige Interesse der Gäste überwiegt, da die Videoüberwachung die ungestörte Kommunikation und einen unbeobachteten Aufenthalt stört. Der Gastwirt trug allerdings vor, wegen der besonderen Situation befänden sich häufig alkoholisierte Jugendliche in der Gaststätte, die andere Gäste belästigen oder Sachbeschädigungen begingen. Wegen dieses Sonderfalls hielten wir eine Überwachung des Gastraums für gerechtfertigt.

Mit Hilfe der Überwachung des Kassenbereichs besteht die Möglichkeit, Personen, die die Gaststätte verlassen haben, ohne an der Kasse zu bezahlen, zu identifizieren und die offene Rechnung einzufordern. Wir hielten diese Überwachung im Rahmen der Prüfung nach § 6b BDSG für zulässig. Die berechtigten Interessen des Wirts überwiegen in diesem Fall die schutzwürdigen Interessen der aufgenommenen Personen.

16.4 Videoüberwachung des Küchenpersonals

Die Videoüberwachung des Küchenpersonals einer Gaststätte ist unzulässig.

Ein Gaststätteninhaber überwachte sein Küchenpersonal mit einer Videokamera.

Maßstab für die Zulässigkeit einer Videoüberwachung in der Küche ist § 32 Abs. 1 Satz 1 BDSG. Danach muss sie für die Durchführung des Beschäftigungsverhältnisses erforderlich sein. Im Rahmen der Erforderlichkeit ist auch der Grundsatz der Verhältnismäßigkeit zu beachten. Wir hielten die Überwachung für unzulässig, weil die dort tätigen Mitarbeiter einer permanenten Überwachung ausgesetzt werden und damit eine - unzulässige - Verhaltens- und Leistungskontrolle durchgeführt werden kann.

16.5 Videoüberwachung in einem Fitness-Studio

Die Videoüberwachung in einem Fitness-Studio kann im Eingangsbereich, in den Zugängen zu den Umkleiden und im Trainingsbereich zulässig sein.

Die Videoüberwachung in einem Fitness-Studio betraf digitale Aufzeichnungen des Eingangsbereichs, der Zugänge zu den Umkleiden sowie von Teilen des Trainingsbereichs. Die Betreiber des Studios wiesen ihre Mitglieder in den Allgemeinen Geschäftsbedingungen auf die Videoüberwachung hin, außerdem brachten sie Hinweisschilder an.

Da nur Mitglieder Zutritt zu den Räumen des Fitness-Studios haben, handelt es sich um nicht öffentlich zugängliche Bereiche, so dass sich die Zulässigkeit der Überwachung nach § 28 Abs. 1 Nr. 1 bzw. Nr. 2 BDSG richtet. Die Kamera im Eingangsbereich soll das Betreten Unbefugter verhindern (das Fitness-Studio ist rund um die Uhr geöffnet). Da wiederholt Spinde aufgebrochen und die darin befindlichen Sachen entwendet worden waren, wurde die Überwachung der Zugänge zu den Umkleiden vorgenommen. Die Überwachung von Teilen des Trainingsbereichs sollte der Sicherheit der Mitglieder dienen, da wegen der geringen Zahl des anwesenden Personals nur auf diese Weise gesundheitliche Probleme oder Belästigungen von Personen an den Trainingsgeräten zeitnah festgestellt werden konnten. Außerdem befanden sich im Trainingsbereich Fluchttüren, die sehr leicht geöffnet werden

konnten und teilweise offen standen, so dass die Gefahr bestand, dass Unbefugte ins Studio gelangen konnten. Im Hinblick auf diese Begründungen hielten wir das berechtigte Interesse des Kamerabetreibers für überwiegend gegenüber den Persönlichkeitsrechten der betroffenen Mitglieder und somit die Kameraüberwachung für zulässig.

16.6 Videoüberwachung in Lagerräumen

Lagerräume, in denen vorübergehend Möbel eingelagert werden, können unter bestimmten Voraussetzungen mit Videokameras überwacht werden.

Ein Unternehmen, das Flächen für Einlagerungen anbietet, richtete im Kunden- und Lagerbereich eine Videoüberwachung ein. In der Vergangenheit war es zu Diebstählen und Sachbeschädigungen gekommen.

Da es sich um nicht öffentlich zugängliche Bereiche handelt, richtet sich die Zulässigkeit der Videoüberwachung nach § 28 Abs. 1 Nr. 2 BDSG bzw. § 28 Abs. 2 Nr. 2a BDSG. Ein berechtigtes Interesse des Unternehmens und auch der Kunden ist wegen der Vorfälle zu bejahen. Bei der Interessenabwägung ist jeweils zu berücksichtigen, dass die Überwachung einerseits dem Schutz der Kunden und ihrer eingelagerten Waren dient, andererseits den Interessen des Unternehmens. Darüber hinaus können die Mitarbeiter die Funktionen der Kameras sowie die Auswahl der gezeigten Bilder selbst festlegen. Eine Verhaltens- oder Leistungskontrolle der Mitarbeiter findet nicht statt. Unter diesen Umständen haben wir die Videoüberwachung für zulässig gehalten.

16.7 Veröffentlichung des Bildes einer Ladendiebin

Die Veröffentlichung des mit einer Videokamera aufgenommenen Bildes einer Ladendiebin im Tankstellenbereich ist nicht zulässig.

In einer Tankstelle verübte eine Frau einen Ladendiebstahl. Eine für den Tankstellenbesitzer tätige Detektei möchte das von der Videokamera an der Kasse aufgenommene Bild der Frau veröffentlichen, um über Hinweise aus der Bevölkerung deren Identität aufzuklären.

Nach § 6b Abs. 3 BDSG kann eine Videoüberwachung zwar der Aufklärung von Straftaten dienen, weil mit den Aufnahmen eine Identifizierung des Täters ermöglicht wird. Derartige Ermittlungen sind jedoch den Strafverfolgungsbehörden vorbehalten. Eine Veröffentlichung von Bildaufnahmen zur Identifizierung des Täters kann daher nicht als berechtigtes Interesse einer privaten Stelle angesehen werden.

16.8 Videoüberwachung in Bierzelten

Eine Videoüberwachung in Bierzelten ist in der Regel zulässig.

Wegen der erfahrungsgemäß immer wieder vorkommenden Schlägereien und Sachbeschädigungen werden in Bierzelten zunehmend Videoüberwachungen eingesetzt.

Bierzelte sind öffentlich zugängliche Räume. Rechtsgrundlage für die Zulässigkeit ist deshalb § 6b BDSG. Wegen der dort vorkommenden Zwischenfälle liegt ein berechtigtes Interesse des Wirts vor, Vorfälle aufzuklären. Das Interesse der Besucher, nicht mit einer Kamera beobachtet zu werden, muss insoweit zurückstehen. Es muss sichergestellt sein, dass nur Leitungspersonen Zugriff auf die Aufzeichnungen haben. Im Zelt sind Hinweise auf die Videoüberwachung anzubringen.

17 Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten (§ 42a BDSG, § 93 Abs. 3 TKG, § 15a TMG)

Bei bestimmten Datenschutzverstößen und Datenschutzpannen müssen die verantwortlichen Stellen die Datenschutzaufsichtsbehörden und die betroffenen Personen informieren.

Eine der Reaktionen des Gesetzgebers auf die bekannt gewordenen Datenschutzverstöße und Datenschutzpannen war die Einführung einer „Verpflichtung zur Selbstanzeige“, wenn Dritte unrechtmäßig von bestimmten sensiblen Daten Kenntnis erlangt haben und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der betroffenen Personen drohen.

17.1 Voraussetzungen für die Informationspflicht

Die Informationspflicht tritt ausschließlich ein, wenn folgende, im Gesetz abschließend genannte Arten personenbezogener Daten von einem Datenschutzverstoß bzw. einer Datenpanne betroffen sind:

- besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG, z.B. Gesundheitsdaten oder Religionszugehörigkeit,
- personenbezogene Daten, die z.B. bei Ärzten, Apothekern, Rechtsanwälten, Steuerberatern oder Personenversicherern einem Berufsgeheimnis unterliegen,
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder auf einen Verdacht hierauf beziehen,
- personenbezogenen Daten zu Bank- und Kreditkartenkonten, z.B. Kontonummern mit Bankleitzahl oder Kreditkartennummern,
- Bestands- und Verkehrsdaten im Bereich der Telekommunikation und
- Bestands- und Nutzungsdaten im Bereich der Telemedien (Internet).

Die unrechtmäßige Kenntniserlangung von Daten durch Dritte kann auf einer unrechtmäßigen Übermittlung von Daten beruhen (z.B. Fehl-Versendungen, illegale Datenweitergaben oder Datenabrufe). Die Daten können aber auch auf sonstige Weise dritten Personen unrechtmäßig zur Kenntnis gelangen, insbesondere beim Verlust von Datenträgern durch Einbrüche, Diebstähle und Fundunterschlagungen oder beim Internethacking (das sind z.B. illegale Online-Datenzugriffe über das Internet).

17.2 Umsetzung der Informationspflicht

Bei der Anwendung des § 42a BDSG in der Praxis hat sich die Frage gestellt, ob in wörtlicher Auslegung der Vorschrift im Einzelfall der Beweis erbracht werden muss, dass dritte Personen von den Daten tatsächlich Kenntnis erlangt haben, was z.B. durch bereits eingetretene Schadensfälle wie illegale Lastschrifteinzüge von Bankkonten oder Internetbestellungen auf Kosten der Geschädigten bewiesen werden könnte, oder ob es im Rahmen einer etwas weiteren Auslegung ausreicht, dass aufgrund der Lebenserfahrung eine hohe Wahrscheinlichkeit dafür besteht, dass die Daten von einem Dritten zur Kenntnis genommen wurden bzw. hätten genommen werden können.

Wir entschieden uns bisher für die letztere Alternative und ließen es für das Tatbestandsmerkmal „zur Kenntnis eines Dritten gelangen“ ausreichen, dass die Daten unrechtmäßig, insbesondere durch eine kriminelle Handlung, in den Verfügungsbereich Dritter gelangt sind. Es besteht damit eine hohe Wahrscheinlichkeit dafür, dass z.B. Diebe oder ihre Abnehmer die gespeicherten Daten unrechtmäßig zur Kenntnis nehmen und damit für die Betroffenen eine konkrete Gefahr droht.

Man würde dem Schutzzweck des § 42a BDSG, der vor allem darin besteht, die Betroffenen vor drohenden Schäden zu bewahren, nicht genügen, wenn man gerade in den typischen Hacking- und Diebstahlsfällen vor der Anwendung der Vorschrift erst den Eintritt von Schäden abwarten müsste. § 42a BDSG würde weitgehend leer laufen, wenn man ihn nicht in vorgenanntem Sinne auslegen würde.

Bei der Frage, ob schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der betroffenen Personen drohen, ist eine Prognoseentscheidung zu treffen, ob eine schwerwiegende Beeinträchtigung in eine bedrohliche Nähe

gerückt ist. Dabei ist zu berücksichtigen, um welche Art von Daten es geht, wer - vermutlich - in den Besitz der Daten gelangt ist ("vertrauenswürdige Umgebung", kriminelle Personen) und welche potentiellen Auswirkungen sich für die betroffenen Personen ergeben können, z.B. finanzielle Schäden, Identitätsbetrug, soziale Nachteile, Erpressbarkeit.

Mit der Begrenzung der Anwendung der Vorschrift auf drohende schwerwiegende Beeinträchtigungen sollen Bagatellfälle ausgeschlossen werden.

Die verantwortliche Stelle muss die zuständige Datenschutzaufsichtsbehörde und die betroffenen Personen, um deren Daten es geht, informieren. Dabei muss sie mitteilen, was konkret geschehen ist, welche Maßnahmen zur Abhilfe inzwischen getroffen wurden und was die betroffenen Personen selbst für ihren Schutz noch tun können.

Aufgrund der Information sollen die betroffenen Personen die Möglichkeit haben, Schaden von sich abzuwenden oder Schutzmaßnahmen zu treffen. Die zuständige Datenschutzaufsichtsbehörde kann nach der Information prüfen, ob die meldende Stelle die möglichen bzw. gebotenen Abhilfe-, Schutz- und Sicherheitsmaßnahmen schon getroffen hat und bei Bedarf weitere Maßnahmen einfordern.

17.3 Praxisfälle

Seit dem Inkrafttreten des § 42a BDSG am 1. September 2009 sind wir mit einer Reihe von Anfragen hierzu befasst worden. 20 Sachverhalte einer unrechtmäßigen Kenntniserlangung von Daten sind gemeldet worden. In zehn Fällen aus den folgenden Bereichen haben wir eine Pflicht zur Information bejaht:

- Diebstahl von Notebooks mit Arbeitnehmer- bzw. Versichertendaten einschließlich Gesundheits- und Bankkontodaten aus einem Firmengebäude oder einem PKW, wobei für die personenbezogenen Datenbestände keine Festplattenverschlüsselung vorhanden war.

- Auf dem Transportweg verschwundene bzw. aus Bankbriefkästen entwendete Bankunterlagen mit Kontodaten.

- Von Internetplattformen rechtswidrig beschaffte ("gehackte") Zugangs- bzw. Vertragsdaten (Passworte, Konto- und Kreditkartendaten etc.), die von den Tätern dann für Betrugshandlungen genutzt wurden bzw. genutzt werden könnten. Neben Betrugshandlungen wurden die von Tätern erlangten Informationen auch für Erpressungsversuche verwendet oder auf ausländischen Internetseiten veröffentlicht (wobei eine Datenlöschung teilweise nicht durchsetzbar ist).

Durch die neue gesetzliche Verpflichtung zur Information bei Datenschutzverstößen und Datenschutzpannen soll vor allem auch eine präventive Wirkung dahin gehend erreicht werden, dass die verantwortlichen Stellen sich noch mehr um den rechtmäßigen Umgang mit personenbezogenen Daten und um die Sicherheit für diese Daten kümmern, um derartige Selbstanzeigen und insbesondere im Falle einer Vielzahl der betroffenen Fälle die Information der Öffentlichkeit durch große Anzeigen in mindestens zwei bundesweit erscheinenden Tageszeitungen von vornherein zu vermeiden.

Auf mobilen Datenträgern und Geräten sollten personenbezogene Daten jedenfalls nur mit einer ausreichenden Verschlüsselung gespeichert sein, so dass eine Kenntnisnahme durch Dritte im Falle des Verlusts oder eines Diebstahls ausgeschlossen oder zumindest sehr unwahrscheinlich bleibt.

Für den Fall, dass es trotz aller getroffenen Maßnahmen doch zu einer unrechtmäßigen Kenntnisnahme durch Dritte kommt, sollte die verantwortliche Stelle organisatorisch gerüstet sein und ein geeignetes Prüfungs- und Meldesystem vorbereitet haben.

Schließlich ist zu beachten, dass ein Verstoß gegen die Informationsverpflichtung bußgeldbewehrt ist.

18 Entsorgung bzw. Rückgabe von Datenträgern

18.1 Entsorgung von Geschäftsakten in einem Altpapier- und Bauschuttcontainer

Bei der Entsorgung von Unterlagen mit personenbezogenen Daten muss der Datenschutz beachtet werden.

Immer wieder werden wir über Fälle informiert, in denen Altunterlagen mit zum Teil sehr sensiblen personenbezogenen Daten von dritten Personen an öffentlich zugänglichen Orten aufgefunden werden. So hatte ein Bauleiter in dem von seinem Unternehmen aufgestellten Bauschutt-Container diverse Unterlagen zu Telekommunikationsverträgen, wie Kopien von Auftragserteilungen, Meldebescheinigungen, Bank- und Kreditkartendaten sowie Telefonnummern, vorgefunden; mehrere Schriftstücke waren zudem von Windböen bereits auf die Straße geweht worden.

In einem weiteren Fall wurden ausgesonderte Bankunterlagen mit Kreditanträgen und den dazugehörigen Unterlagen (Lohnabrechnungen, Ausweiskopien, Kontoauszüge usw.) in einem öffentlichen Altpapiercontainer einer Wohnanlage entdeckt.

In einem dritten Fall befanden sich über 20 Ordner mit verschiedenen Dokumenten von Firmen (Steuerbescheide, Lohnabrechnungen, Kontoauszüge, Versicherungsunterlagen usw.) in einem öffentlichen Altpapiercontainer, die von einer Unternehmensberatung auf diese Weise entsorgt werden sollten.

Das Bundesdatenschutzgesetz ist auf Sachverhalte anzuwenden, wenn Papierdatenträger offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind (wie EDV-Ausdrucke, Kontoauszüge usw.) bzw. wenn Papierunterlagen eine sogenannte nicht-automatisierte Datei darstellen, wie eine Sammlung von Ausweiskopien oder anderen gleichartigen Formularen.

Wir haben hier zunächst für die Sicherstellung bzw. für eine ordnungsgemäße Entsorgung der Alt-Materialien gesorgt.

Weil die Papierunterlagen in den genannten Fällen von den Verantwortlichen der betroffenen Unternehmen durch ihr Handeln aktiv auf einen ungeeigneten Entsorgungsweg gegeben wurden und damit die unbefugte Kenntnisnahme personenbe-

zogener Daten durch Dritte geradezu in Kauf genommen bzw. herausgefordert wurde, was sich durch die Beschwerden der Finder bei uns bestätigt hatte, haben wir jeweils ein Bußgeldverfahren wegen unbefugter Datenübermittlung eingeleitet.

18.2 Rückgabe von (defekten) Geräten mit Datenspeicherungen an den Handel oder Abgabe beim Wertstoffhof

Bei der Rückgabe von Geräten und Datenträgern an den Handel oder bei einer Abgabe an Wertstoffhöfe ist darauf zu achten, dass auf den Geräten und Datenträgern noch gespeicherte Daten gelöscht sind.

Wer sich in Geschäften oder im Internet gebrauchte DV-Geräte oder Datenträger (insbesondere PC, Laptop, Festplatten) kauft oder hierfür das Depot eines Wertstoffhofes nutzt, stellt bei deren Einsatz manchmal fest, dass darauf noch umfangreiche persönliche Daten des Vorbesitzers gespeichert sind, der offensichtlich keine Löschung vorgenommen hat.

Aus solchen Sachverhalten haben sich bei uns einige Beschwerdefälle ergeben. Wir haben diese Fälle wie folgt bewertet:

Wenn ein beim Handel zurückgegebenes oder am Wertstoffhof entsorgtes Gerät bzw. ein sonstiger Datenträger noch voll funktionsfähig ist, liegt es in der Verantwortung der betroffenen Person, gespeicherte Daten vorher wirksam zu löschen (z.B. mittels einer Lösch-Software).

Wegen der oft sorglosen und wenig überlegten Verhaltensweise von Kunden haben wir bei Handelsunternehmen angeregt, bei der Rückgabe von Geräten oder Datenträgern (Garantiefälle, Umtausch, freiwillige Rücknahme) die Kunden auf die vorherige Löschung ihrer Daten aufmerksam zu machen, z.B. durch Hinweise auf Formularen, mittels Informationen im Internet oder bei Gesprächen mit den Kunden. Als Serviceleistung können Handelsunternehmen hier auch die Datenlöschung im Auftrag der Kunden anbieten.

Sind Geräte oder Datenträger aufgrund einer technischen Störung nicht mehr löschbar, kann der betroffene Bürger entweder eine mechanische Zerstörung vornehmen oder er muss sich bei der Rückgabe an den Handel eine Löschung seiner Daten vertraglich zusichern lassen, falls dort eine Untersuchung des Geräts oder eine Reparatur mit nachfolgendem Wiederverkauf in Betracht kommt.

Stichwortverzeichnis

A

Abonnentendaten 64
Access-Provider 29
Adressdaten 68
Adressenhandel....54
Allgemein zugängliche Daten....33
Analyseverfahren....30
Anlassspenden 81
Audit....37
Auftragsdatenverarbeiter....37, 71
Auftragsdatenverarbeitung....32, 35
Auftragsdatenverarbeitung in Drittstaaten....72
Auskunftei....84
Auskunfteien....48
Auskunftsrecht....48

B

Bankdienstleistung 44
Banken....43
Bankunterlagen 45
Beratung 14
Beschäftigtendatenschutz 74
betriebliche Datenschutzbeauftragte....20
Bewertung....26
Bewertungsplattformen....22
Bewertungsportale....27
BITKOM....26
Bonitätsauskunft 49, 50, 51, 52, 84
Bonitätsprüfung 85
Briefwerbung 56
Bundesnetzagentur 54
Bußgeld 53, 68
Bußgeldverfahren 41

C

Callcenter....35
Cookies....30

D

Datengeheimnis....21, 39, 43
Datenschutzbeauftragter 14
Datenschutzschulung 21
Datenübermittlung in die USA 70
Dienstleistung 58
Düsseldorfer Kreis 17, 31, 85

E

Eingaben 12
Einwilligung 23, 28, 32, 42, 75, 77, 85
Elektronische Einwilligung 75
Elektronisches Lastschriftverfahren 58
E-Mail 55
Entsorgung von Datenträgern.... 98
Erfa-Kreise 18
Europäischer Gerichtshof 11

F

facebook 34
Fahrzeugdatenspeicher 61
Faxwerbung 54
Finanzberatung 38
Flyer 34
Fotos 23
Funktionsübertragung 38

G

Geldausgabeautomaten 46
Geodatendienst.... 26
Georeferenz 26
Gesellschaft für Datenschutz und Datensicherung e. V. 17
Gesundheitsdaten.... 40, 41, 79
Gesundheitswesen 77
Google Street View.... 24

H

Handel.... 58

I

Informationspflicht.... 94
Inkasso.... 38
Intelligente Stromverbrauchsmessung 87
Interessenabwägung.... 26
Internationaler Datenverkehr 70
Internet.... 22
IP-Adressen 29

K

Kontoauszugdrucker.... 46
Kontrollpflichten 36

Kontrolltätigkeit 15
Krankheitstage im Intranet 76
Kunsturhebergesetz 23

L

Landesbeauftragter für den Datenschutz 10
Listendaten 57, 63
Listenprivileg 63

M

MAC-Adresse 32
Meinungsfreiheit 27
Meldepflicht 16
Mieterselbstauskünfte 83
Mobile Internetnutzung 32
Muster-Widerspruchsschreiben 26

N

Nutzerdaten 29
Nutzungsprofil 31

O

Öffentliches Register 16
Öffentlichkeitsarbeit 18
Online-Bewerbung 74
Ordnungswidrigkeitenverfahren 16
Outsourcing 35

P

Personalverwaltung 38
Personenbezogene Daten 22
Privatinsolvenz 28
Pseudonym 31, 71

R

Rechts auf informationelle Selbstbestimmung 27
Rote-Linie-Gesetz 4
Rückgabe von Geräten 99

S

Sammel-E-Mail 65
schülerVZ 34
Schweigepflichtentbindung 78
Scorewert 48, 85
Scoring 48
Smart Metering 87
SMS-Werbung 55
Soziale Netzwerke 34
Spenderdaten 81
spickmich.de-Urteil 22, 26
SSID 32
Standardvertragsklauseln 71
Statistik 12
Steuerberatung 38
Strafanträge 16
Straßenansichten im Internet 24
studiVZ 34

T

Telefon 54
Telemediengesetz 29, 31, 74

U

Übermittlung 22
Übermittlung von Kundendaten 63
Unrechtmäßige Kenntniserlangung von Daten 94
Unterauftragnehmer 71

V

Verantwortliche Stelle 14, 37
Verbände 80
Vereine 80
Verpixelung 25
Versicherungen 40
Versicherungsdaten 40
Versicherungsvertragsgesetz 42
Videoüberwachung 89
Vorabwiderspruch 25

W

Werbeagentur 38
Werbewiderspruch 57
Werbung 54
Widerruf 24
Widerspruch 25, 31
WLAN 32
WLAN-Daten 25
Wohnungswirtschaft 83

Impressum

Herausgeber:

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach

Telefon: 0981 53-1428
Telefax: 0981 53-5428
E-Mail: datenschutz@reg-mfr.bayern.de

Diesen Tätigkeitsbericht können Sie auch abrufen unter
www.datenschutzaufsicht.bayern.de