

18. Datenschutz in der Privatwirtschaft

18.1 Zu den Sitzungen der obersten Datenschutzaufsichtsbehörden

Die Sitzungen des so genannten Düsseldorfer Kreises, dem Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich, fanden in diesem Jahr turnusgemäß in Bremen statt. Die dringend einer Verständigung bedürftigen Themen nehmen weiter zu, weil auch in der Privatwirtschaft immer weitere Bereiche mit Informationstechniken automatisiert werden und dabei in zunehmendem Maße personenbezogene Daten, sei es der Beschäftigten, sei es der Kunden, in vielfältiger Weise mit einbezogen werden. Hinzu treten ein ansteigender Vertrieb von Waren, Dienstleistungen und Informationen über das Internet, die zunehmende Internationalisierung der Datenverarbeitung oder die technische Entwicklung neuer IT-Produkte, aber auch eine fortschreitende Vernetzung in der Wirtschaft und die Entstehung neuer Datenverbünde.

So waren denn die jeweils über 40 Punkte enthaltenden Tagesordnungen der Sitzungen des Düsseldorfer Kreises trotz straffer Führung nicht abzuarbeiten. Eine Darstellung würde den Bericht sprengen, auch wenn ich mich nur auf eine kurze Beschreibung beschränken würde. Allein das 60-seitige Protokoll der Frühjahrssitzung spricht Bände. Ich will an dieser Stelle daher exemplarisch nur einige Themenschwerpunkte des Düsseldorfer Kreises nennen:

Fragen des internationalen Datenverkehrs, wie Übermittlung sensibler Daten an Auftragnehmer in Drittstaaten, extraterritoriale Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG), Unternehmensregelungen zum Datenschutz, Standardvertragsklauseln, das Vertragsverletzungsverfahren der EU-Kommission gegen die Bundesrepublik Deutschland wegen Verstoßes gegen die EG-Datenschutzrichtlinie;

verschiedene Themen betreffend die Auskunfteien, hier z. B. Online-Auskunft über „MeineSCHUFA.de“, Nutzung von Daten aus dem Inkasso-Bereich für die Auskunftserteilung oder erweitertes Online-Auskunftsverfahren bei Online-Krediten;

die Kreditwirtschaft, hier z. B. Bonitätsanfragen durch Kreditinstitute ohne Einwilligung des Betroffenen, Datenübermittlung der SWIFT-Zentrale in Belgien an die USA, Weiterleitung von Bankverbindungsdaten des Überweisenden an den Begünstigten wie auch Fragen zum Scoring;

die Versicherungswirtschaft, hier u. a. Datenaustausch zwischen Versicherungen und Außendienstmitarbeitern, Gespräche beim Bundesverband Verbraucher-Zentrale e. V. über eine Einwilligungserklärung in der Versicherungswirtschaft oder Fragen der Benachrichtigung Dritter bei der Einmeldung in ein zentrales Warnsystem der Versicherungswirtschaft;

Fragen des Arbeitnehmerdatenschutzes, hier insbesondere Fragen von so genannten Whistleblowing-Hotlines und die Initiative zur Aufnahme von Vorschriften zum Arbeitnehmerdatenschutz in ein Arbeitsgesetzbuch;

verschiedene Fragen im Zusammenhang mit der Datenverarbeitung bei der Personenüberprüfung und dem Ticketing bei der Fußballweltmeisterschaft 2006;

verschiedene Fragen betreffend die Rechtsstellung und Aufgaben von betrieblichen Datenschutzbeauftragten, hier insbesondere Auslegung der neuen Regelungen im Mittelstandsentlastungsgesetz;

den Bereich Verkehr, hier Fehler- und Unfalldatenspeicher in Kraftfahrzeugen, Aufzeichnung telefonischer Taxibestellungen oder Datenschutz im öffentlichen Personennahverkehr;

Fragen der Datenschutzaufsicht bei Rechtsanwälten und Datenschutz bei Detekteien, Speicherfristen aufgrund des Allgemeinen Gleichbehandlungsgesetzes (AGG) sowie Fragen der Datenverarbeitung bei Markt- und Meinungsforschung.

Hervorheben möchte ich, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), der mittlerweile in einer ganzen Reihe von Feldern eigene Zuständigkeiten gegenüber Unternehmen der Privatwirtschaft hat, in 2006 volles Mitglied des Düsseldorfer Kreises geworden ist. Ein Durchbruch gelang auch bei der Informationspolitik des Düsseldorfer Kreises. War es bisher so, dass die Entscheidungen lediglich den Parteien in der Wirtschaft mitgeteilt wurden, die es anging, in der Regel also Wirtschaftsverbände und Dachorganisationen, hat sich der Düsseldorfer Kreis jetzt auf Regularien verständigt, um Beschlüsse auch der Öffentlichkeit zugänglich zu machen. Sie werden unter www.bfdi.bund.de für jedermann im Internet abrufbar zur Verfügung gestellt.

18.2 Voraussetzungen für den Einsatz von RFID-Chips

RFID-Systeme bestehen aus einem mobilen Datenspeicher (Transponder) und einem Lese- und/oder Schreibsystem. Sie dienen dazu, Gegenstände zu kennzeichnen. Die Technik ermöglicht die eindeutige Identifizierung eines Gegenstands. Auf dem Chip können je nach Leistungsfähigkeit verschiedene Informationen gespeichert und ggf. auch verändert werden. Die Bauformen der Bestandteile eines RFID-Systems können sehr unterschiedlich sein, in der Regel sind sie aber sehr klein. Für die Übermittlung der Daten über Funkwellen stehen verschiedene Frequenzbereiche zur Verfügung. Einfache Anwendungen befinden sich z. B. in Zugangssystemen wie den Fußballtickets zur WM 2006, in Skipässen oder Autoschlüsseln. Ein erheblich größeres Potenzial steckt jedoch im Einsatz der Technik bei der Kennzeichnung von Bauteilen und Einzelprodukten, weshalb RFID besonders für Produktion, Logistik und Handel von Interesse ist. Die RFID-Technologie wird den Barcode ersetzen, aber auch Anwendungen im medizinischen Bereich oder auch Autonummernschilder sind schon im Einsatz.

Die RFID-Technologie steht erst am Anfang ihrer Entwicklung. Dabei geht man davon aus, dass in einer parallelen Welt der Dinge diese untereinander kommunizieren und sich selbstständig organisieren (z. B. der Kühlschrank bestellt den fehlenden Aufschnitt). Schon jetzt spricht man von einem Internet der Dinge, auch dem Web 2. Die mit der Technologie verbundenen neuen Möglichkeiten und Veränderungen, insbesondere aber die möglichen Arbeitserleichterungen und Kosteneinsparpotenziale werden dafür sorgen, dass diese Mikrochips in fast allen Bereichen zum Einsatz kommen werden. Ich erwarte eine rasche Verbreitung binnen kürzester Zeit. RFID wird alle Lebensbereiche durchdringen. Deshalb ist es wichtig, in der jetzigen Entwicklungsphase, in der noch gestaltend eingegriffen werden kann, die technischen Vorkehrungen zu implementieren, die das informationelle Selbstbestimmungsrecht der von dieser Technologie betroffenen Besitzer stärken. Darüber hinaus bleibt abzuwarten, ob die derzeitigen rechtlichen Regelungen ausreichen, um den Datenschutz auch beim Einsatz dieser Technologie zu garantieren. Gegebenenfalls muss der Gesetzgeber durch ergänzende rechtliche Regelungen die Hersteller und die Wirtschaft, die sich für den Einsatz dieser Technologie entscheidet, verpflichten, dass diese ausreichende Potenziale zur Sicherung des Datenschutzes zur Verfügung stellen. Es geht dabei nicht um die Verhinderung dieser Technologie, sondern um ihre Gestaltung. Die Datenschutzaufsichtsbehörden haben hierzu in Bremen einen Beschluss gefasst, in dem sie die notwendigen Parameter für die Entwicklung und den Einsatz der Technologie festlegen (vgl. Ziff. 20.2 dieses Berichts). Dieser Beschluss ist den einschlägigen Organisationen und Verbänden der Wirtschaft übermittelt worden und ich hoffe, dass er genügend Anreiz für weitere Diskussionen gibt.

18.3 Kreditwirtschaft, insbesondere SWIFT

Im Bereich der Kreditwirtschaft hat es verschiedene Aktivitäten auf Bundesebene gegeben. Unter anderem war auch eine Bürgereingabe aus Bremerhaven Auslöser für die Überprüfung der Praxis des Umfangs der Datenübermittlung an den Empfänger bei Überweisungen. Nach von mir geführten Verhandlungen mit dem führenden norddeutschen Rechenzentrum der Kreditwirtschaft wird die Frage nun mit dem Zentralen Kreditausschuss der Deutschen Kreditwirtschaft (ZKA) weiterverhandelt. Der Vorgang ist noch nicht abgeschlossen.

Hohe Wellen schlug die Mitteilung, dass die in Belgien ansässige SWIFT (Society for Worldwide Interbank Financial Telecommunication), über die weltweit der gesamte internationale Zahlungsverkehr der Banken abgewickelt wird, die dabei anfallenden Daten im SWIFT-Rechenzentrum in den USA spiegelt und dort den US-amerikanischen Behörden und dem Geheimdienst in vollem Umfang Daten zugänglich macht. Diese Praxis ist sowohl nach deutschem als auch nach EU-Datenschutzrecht unzulässig. Rechtlich verantwortlich sind dabei neben der SWIFT-Zentrale auch die deutschen Banken. Diese bündeln ihre Interessenvertretung im ZKA. Die Datenschutzaufsichtsbehörden haben in einem gemeinsamen Beschluss (vgl. Ziff. 20.1 dieses Berichts) die Praxis für rechtlich unzulässig erklärt und die Banken aufgefordert, unverzüglich Maßnahmen zu ergreifen. Der ZKA wurde von mir über diesen Beschluss unterrichtet. Wenig später hat auch die Artikel 29-Datenschutzgruppe der EU mit ähnlichem Inhalt dazu einstimmig die Stellungnahme WP128 verabschiedet.

18.4 Eingaben gegen die Handels- und Wirtschaftsauskunfteien

Erneut erhielt ich eine Vielzahl von Eingaben, die sich gegen die Speicherung und Datenweitergabe von Auskunfteien richteten. Soweit ich nicht unmittelbar helfen konnte, z. B. weil anderenorts Feststellungen gemacht werden mussten, gab ich die Eingaben an die Datenschutzaufsichtsbehörden ab, in deren Zuständigkeitsbereich die Auskunfteien ihren Sitz haben. Mehrere Eingaben, die die Verarbeitung personenbezogener Daten durch in Bremen ansässige Wirtschaftsauskunfteien betrafen, verfolgte ich selbst. Die Bürger beklagten sich dabei u. a., dass über sie unrichtige Daten hinsichtlich ihrer wirtschaftlichen Betätigung gespeichert, ihnen zustehende Betroffenauskünfte nicht oder nicht rechtzeitig erteilt oder aber zu beachtende Löschfristen nicht eingehalten würden. Nach den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) dürfen über den Betroffenen nur richtige Daten gespeichert werden. Außerdem hat der Betroffene einen umfassenden Auskunftsanspruch, dem auch die Auskunfteien gerecht werden müssen.

Zu diesen Eingaben führte ich Prüfungen bei den betreffenden Auskunfteien durch. Soweit sich hierbei die von den Petenten geschilderten Mängel bestätigten, gelang es, dass die Auskunfteien die von ihnen gespeicherten Daten berichtigten bzw. löschten oder aber die erbetenen Auskünfte erteilten.

18.5 Bericht zur Arbeitsgruppe Versicherungswirtschaft

Die Mitglieder der AG Versicherungswirtschaft haben sich im Berichtsjahr zu drei Sitzungen getroffen. Beraten wurden u. a. strittige Punkte mit der Versicherungswirtschaft, die die Verhandlungen ins Stocken gebracht hatten. Dies waren u. a. die aufgrund von Rechtsprechung notwendig gewordenen Änderungen der Einwilligungsklausel nach dem Bundesdatenschutzgesetz, die Frage der Benachrichtigung Dritter bei der Einmeldung in das Versicherungsinformationssystem Uniwagnis, die Zulässigkeit von Bonitätsauskünften an Versicherungen und Fragen des Scoring in der Versicherungswirtschaft.

Außerdem wurden folgende Themen beraten: die Übernahme von Geschäftstätigkeiten innerhalb einer Versicherungsgruppe, die Frage des Umfangs zulässiger Datenübermittlungen zwischen Versicherungswirtschaft und Auskunfteien sowie die Frage der Übermittlung von Arztberichten an Krankenversicherungsunternehmen.

Viele der Themen waren auch Gegenstand der Behandlungen in den Sitzungen der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (Düsseldorfer Kreis) in Bremerhaven und Bremen. Schließlich soll nicht unerwähnt bleiben, dass Mitte des Jahres der Vorsitz in der AG Versicherungswirtschaft von Hamburg auf das Unabhängige Landeszentrum für Datenschutz (ULD) in Schleswig-Holstein übergegangen ist.

18.6 Telefongesprächsaufzeichnung bei Schadensmeldung in der Versicherungswirtschaft

Ein Rechtsanwalt wies mich auf folgende Praxis hin: Sein Mandant habe seine Versicherung über einen Zentralruf über einen Rechtsschutzfall telefonisch informiert. Zunächst sei ihm von dort eine Deckungszusage gemacht worden. Wenige Tage später habe ihn sein örtlich zuständiger Versicherungsvertreter angerufen und ihm erklärt, er habe in dem fraglichen Fall keinen Anspruch auf Versicherungsschutz. In dem Telefonat mit dem Versicherungsvertreter seien die Worte hin und her gegangen, schließlich habe der Vertreter ihm gegenüber erklärt, er, der Versicherungsunternehmer, habe „das und das“ gesagt, er habe noch einmal in sein Gespräch mit dem Versicherungsunternehmen hineingehört.

Der Versicherungsnehmer war erstaunt, dass sein Telefongespräch ohne sein Wissen aufgezeichnet worden war. Auf Rat des Rechtsanwalts wies er seinen Versicherungsagenten darauf hin, dass die Praxis der Gesprächsaufzeichnung nicht zulässig sei. Ihm wurde daraufhin in dem fraglichen Fall eine Deckungszusage erteilt mit der Maßgabe, den Fall nicht „an die große Glocke zu hängen“. Bei diesem Gespräch sei ihm deutlich gemacht worden, dass es wohl in der gesamten Versicherungsbranche gängige Praxis sei, telefonische Schadensmeldungen aufzuzeichnen. Wegen der Besonderheit des Falles bat der Rechtsanwalt, das fragliche Versicherungsunternehmen noch nicht bekannt zu geben, um Schaden von seinem Mandanten abzuwenden.

Wegen der behaupteten generellen Praxis in der Versicherungswirtschaft habe ich angeregt, die Frage mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) zu erörtern. Aus meiner Sicht sollte dabei überlegt werden, wie dem Interesse der Versicherungswirtschaft einerseits und der Unterrichtung und Transparenz für den Betroffenen vor einer möglichen Aufzeichnung andererseits Rechnung getragen werden kann. So könnte ein dem Gespräch vorgeschalteter Sprachcomputer eingesetzt werden, mit dem die Versicherungswirtschaft ermittelt, ob der Betroffene mit einer Aufzeichnung des Gesprächs einverstanden ist oder nicht. Alternativ könnte auch eine bloße Ansage vorgeschaltet werden, die darauf hinweist, dass das Gespräch aufgezeichnet werden soll und er seine Entscheidung dem Sachbearbeiter mitteilen soll. Der Sachbearbeiter könnte dann bei Zustimmung die Aufzeichnung manuell starten.

Weiter habe ich, um einen Ausgleich zu erreichen, angeregt, durch Verfahrensregelungen zu ermöglichen, solche Aufzeichnungen auf Wunsch auch den jeweiligen Versicherten zugänglich zu machen. In jedem Fall muss festgelegt sein, wer zu welchen Zwecken solche Gesprächsaufzeichnungen im Unternehmen nutzen darf. Voraussetzung hierfür wäre eine revisions sichere Speicherung der Aufzeichnung. Innerhalb des Versicherungsunternehmens müssen die aufgezeichneten Gespräche einem Zugriffsschutz unterliegen, um die Gefahr des Missbrauchs zu minimieren. Weiterhin wären Löschrufen für die Gesprächsmitschnitte und die zugehörigen Protokoll Daten zu definieren und umzusetzen.

18.7 Mittelstandsentlastungsgesetz

Ende August 2006 trat das Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft (BGBl. I S. 1970) in Kraft. Durch das Artikelgesetz wurden auch verschiedene Regelungen des Bundesdatenschutzgesetzes (BDSG) geändert.

Im Wesentlichen geht es um die Erhöhung des Schwellenwertes für die Ausnahme von der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten von derzeit vier auf nunmehr neun Mitarbeiter, die mit der Verarbeitung personenbezogener Daten beschäftigt sind. Entsprechend trifft auch die Meldepflicht für automatisierte Verfahren nur noch Unternehmen, die mehr als neun Mitarbeiter besitzen, die mit der Verarbeitung personenbezogener Daten beschäftigt sind. Ferner können externe Datenschutzbeauftragte, die bei Berufsheimnisträgern eingesetzt sind, sich auf ein abgeleitetes Zeugnisverweigerungsrecht berufen. Andererseits unterliegen sie nun auch der Strafandrohung bei Verletzung von Amts- und Berufsheimnissen (§ 203 Abs. 1 StGB). Klargestellt wird, dass die erforderliche Fachkunde des betrieblichen Datenschutzbeauftragten abhängig vom Umfang der Datenverarbeitung und dem Schutzbedarf der personenbezogenen Daten ist. Für die Datenschutzaufsichtsbehörden wird neben der Kontrollfunktion explizit neu eine Beratungsfunktion für betriebliche Datenschutzbeauftragte festgelegt. Aus Sicht der Datenschutzaufsichtsbehörden stellt sich das Gesetz als Abbau von Schutzvorschriften dar, ohne dass der angestrebte Entlastungseffekt für die mittelständische Wirtschaft erkennbar ist. So befreit die Lockerung von der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten die nicht öffentliche Stelle nicht von den inhaltlichen Anforderungen an den Datenschutz. Diese gelten unverändert und in vollem Umfang und sind durch den Leiter der Stelle in anderer Weise sicherzustellen. Daher wird es absehbar für die Aufsichtsbehörden zu mehr Beratungsaufwand kommen. Zwar enthält das Gesetz einige Klarstellungen, jedoch auch verschiedene neu zu bestimmende Rechtsbegriffe, die neuen Klärungsbedarf aufwerfen.

18.8 Weitergabe von Patientendaten durch den Insolvenzverwalter einer Pflegeeinrichtung

Mit einer Eingabe wurde mir zur Kenntnis gebracht, dass der Insolvenzverwalter einer ambulanten Pflegeeinrichtung, ein Rechtsanwalt aus Bremen, eine Liste mit den Daten aller von der insolventen Pflegeeinrichtung betreuten Patienten an die Arbeitsgemeinschaft der Krankenkassenverbände in Bremen und an eine Krankenkasse geschickt hatte, um für den Fall, dass ein Versicherungsverhältnis besteht, die Begleichung etwaiger offener Rechnungsbeträge zu erreichen. Tatsächlich bestand jedoch nur ein Versicherungsverhältnis mit einer einzigen Patientin.

Unter Hinweis darauf, dass es sich bei der Offenlegung der Eigenschaft der Pflegebedürftigkeit einer Vielzahl von Patienten um ein unbefugtes Offenbaren von Gesundheitsdaten handelt, forderte ich ihn zur Stellungnahme auf. Er trug vor, aufgrund fehlenden Personals keine Möglichkeit gehabt zu haben festzustellen, bei welcher Krankenkasse die Patienten jeweils versichert sind. Vor dem Hintergrund, dass durch einfache Einsicht in die Unterlagen bzw. Kontaktaufnahme mit den Patienten die Frage nach deren Krankenversicherungsverhältnissen hätte geklärt werden können, leitete ich ein Ordnungswidrigkeitsverfahren gegen den Insolvenzverwalter ein.

18.9 Personenverwechslung bei der Ausstellung eines Rezepts

Im Rahmen meiner Bürgersprechstunde wandte sich eine Frau an mich, der von einem Versicherungsunternehmen eine für sie ausgestellte ärztliche Verordnung zugeschickt worden war. Das Versicherungsunternehmen, das im Übrigen keine Krankenversicherungssparte hat, teilte ihr mit, dass das Rezept zu dem Versicherungsunternehmen fehlgeleitet worden sei. Die ärztliche Verordnung war mit einem Apothekenstempel versehen, was die Aushändigung des Medikaments nahelegt. Es handelte sich dabei um ein Medikament gegen Wechseljahresbeschwerden, das sich die Frau jedoch nie hat verschreiben lassen, zumal sie es in ihrem Alter gar nicht benötigt. Bei dem ausstellenden Arzt war sie ebenfalls nicht gewesen. Auch die naheliegende Vermutung, ihre Versichertenkarte sei in fremde Hände gelangt, konnte sie ausschließen. Ich rief den Arzt an, in dessen Praxis das Rezept ausgestellt worden war, berichtete ihm den Sachverhalt und bat ihn um Aufklärung. Er bestätigte mir, das Rezept für die Frau ausgestellt zu haben und vermutete zunächst, dass diese in Vertretung für eine von ihm genannte Gynäkologin in seiner Praxis gewesen sei und er ihr ohne Untersuchung das Rezept ausgestellt habe. Eine Rücksprache bei der Patientin ergab zwar, dass sie bei der vom ausstellenden Arzt genannten Gynäkologin in Behandlung sei, die Praxis des Arztes jedoch hatte sie niemals betreten. Ich rief daher die Gynäkologin an, die sich sehr verwundert zeigte, da der Arzt für sie keine Vertretung durchführe. Stattdessen führe er für sie Zelluntersuchungen durch, wie auch im Fall der genannten Patientin. Zu diesem Zweck habe sie dem Arzt die Daten der Beschwerdeführerin übermittelt. Sie bestätigte auch, dass ihre Patientin das verschriebene Medikament nicht benötige. Kurz darauf meldete sich der Arzt, der zwischenzeitlich mit der Gynäkologin gesprochen hatte, erneut und konnte die Angelegenheit endlich aufklären: Es hatte in seiner Praxis eine Verwechslung mit einer anderen Patientin mit gleichem Nachnamen gegeben. Diese sei bei ihm Privatpatientin und habe das verschriebene Medikament auch bekommen.

18.10 Prüfung der Datenverarbeitung in Sanitätshäusern

Im Berichtsjahr habe ich die Datenverarbeitung in Sanitätshäusern in Bremerhaven und Bremen geprüft. Bei der Bestellung und dem Verkauf von Sanitätsartikeln werden Daten über den Gesundheitszustand der Kunden verarbeitet. Es handelt sich hierbei im Wesentlichen um Daten, die sich auf den Rezepten befinden. Diese sind im Einzelnen: Name der Krankenkasse, Name, Adresse und Geburtsdatum der Kunden, Kassen-Nummer, Versichertennummer, Versichertenstatus, Vertragsarzt Nummer, Gültigkeitsdatum der Versichertenkarte, Ausstellungsdatum, verordnetes Hilfsmittel und Diagnose.

Diese Daten werden elektronisch und in Papierform gespeichert. Die Speicherung dient der Erstellung der Kostenvoranschläge für die Krankenkassen und der Abrechnung. Die elektronisch erstellten Abrechnungen enthalten nur für die Abrechnung relevante Daten, die Diagnose wird darin z. B. nicht mehr genannt. Sowohl die Aufbewahrung und Versendung der Rezepte mit der Bezeichnung der verordneten Hilfsmittel und den Diagnosen als auch die Speicherung der ausgelieferten Hilfsmittel im System stellen eine Verarbeitung von Gesundheitsdaten dar, die nach § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG) zu den besonderen Arten von Daten zählen und deshalb einer besonderen Schutzbedürftigkeit unterliegen.

Ich konnte feststellen, dass die durch die Sanitätshäuser erhobenen Daten für die Versorgung mit Hilfsmitteln erforderlich waren. Die Papierunterlagen wurden für den erforderlichen Zeitraum sicher aufbewahrt und nach der Auslieferung der Hilfsmittel datenschutzgerecht vernichtet. Auch elektronisch wurden nur die für die Erfüllung des Vertragsverhältnisses erforderlichen Daten verarbeitet. Hier habe ich auf der Ebene der technischen Datenschutzmaßnahmen die Absicherung des EDV-Netzes gegenüber unbefugten Zugriffen und die Möglichkeiten der für die Sanitätshäuser speziell entwickelten Fachanwendungen geprüft. Hierzu gehörte die Zugangskontrolle (Anlage § 9 BDSG) zum System, die über angemessene Authentisierungsmechanismen (Benutzername, sicheres Passwort) gewährleistet werden muss. Ebenso geprüft wurden die Verfügbarkeitskontrolle, d. h., der Schutz von Kundendaten gegen zufällige Zerstörung oder Verlust, die Zugriffskontrolle (wer von den Mitarbeitern darf mit welchen Funktionen auf die Kundendaten zugreifen) und insgesamt die Absicherung gegenüber dem Internet.

Ich konnte eine Reihe von wirkungsvollen technischen Schutzmaßnahmen feststellen. Dazu gehörten u. a. Maßnahmen zur physikalischen, unwiderruflichen Löschung der Daten auf den Festplatten, Maßnahmen zum Schutz des In-House-Netzes gegenüber externen Anschlüssen durch die Bildung eines Grenznetzes, Einsatz von Schutzsoftware zur Erkennung von Viren, Spyware und Trojanern, Firewallfunktionen sowie verschlüsselte Datenspeicherung.

Mängel konnte ich bei organisatorischen Maßnahmen erkennen, wie etwa die vorgeschriebene Dokumentation der technischen und organisatorischen Maßnahmen im Rahmen einer Verfahrensbeschreibung (§ 4 e Abs. 1 BDSG). Auch gab es im Fall eines an das Internet angeschlossenen Stand-alone-Rechners keine eindeutig sichere Trennung von im Rahmen eines Terminkalenders eingetragenen Kundendaten. Allerdings waren hier keine Diagnosen gespeichert. Es

bestand aber die Möglichkeit, über dort eingetragene Tätigkeiten mit vorhandenem Zusatzwissen auf die Art der gesundheitlichen Störung zu schließen. In einem anderen Fall wurden für den Betrieb der Fachanwendung noch DOS-PC verwendet, die über deutlich weniger Sicherheitsmaßnahmen verfügen als Windows-Systeme. Beispielsweise kann jede Person, die Zugang zu diesem Rechner hat, diesen auch administrieren, also z. B. Einstellungen ändern und Software einspielen. Auch Auftragsverhältnisse zu Supportfirmen mussten hinsichtlich der Handhabung personenbezogener Daten präzisiert werden.

Insgesamt wurde bis auf die oben genannten Mängel ein angemessenes, z. T. hohes Datenschutzniveau vorgefunden. Die Sanitätshäuser wurden im Rahmen der von mir zugestellten Prüfberichte aufgefordert, die festgestellten Mängel zu beseitigen.

18.11 Konzeption eines Arbeitsgesetzbuches und Arbeitnehmerdatenschutz

Im August 2006 hat das Forschungsinstitut für Deutsches und Europäisches Sozialrecht an der Universität Köln im Auftrag der Bertelsmann Stiftung den Diskussionsentwurf eines Arbeitsvertragsgesetzes (ArbVG) vorgelegt. Im Vorfeld dazu hatten mehrere Aufsichtsbehörden für den Datenschutz – auch die in Bremen – unter Federführung der Aufsichtsbehörde Nordrhein-Westfalen dem Institut Vorschläge zur Aufnahme von Regelungen zum Arbeitnehmerdatenschutz unterbreitet. Grundlage waren die Beschlüsse der Konferenz der Datenschutzbeauftragten „zum Datenschutz im Recht des öffentlichen Dienstes“ und „zum Arbeitnehmerdatenschutz“ aus den Jahren 1991 und 1992 sowie das Datenschutzniveau des Bundesdatenschutzgesetzes, der Landesdatenschutzgesetze sowie der Beamtengesetze des Bundes und der Länder.

Leider enthält der Diskussionsentwurf nur einzelne Datenschutzregelungen, z. B. zur Datenerhebung im Bewerbungsverfahren und eine allgemeine Regelung zur Einsicht in Personalakten. Erhebliche Bedenken bestehen gegen eine Schlussvorschrift, wonach erlaubt werden soll, dass zu Ungunsten des Arbeitnehmers per Tarifvertrag, Betriebsvereinbarung oder Arbeitsvertrag von Bestimmungen des Gesetzes abgewichen werden kann. Es ist im Datenschutzrecht unumstritten, dass derartige Regelungen das gesetzliche Datenschutzniveau nicht unterschreiten dürfen.

Die Projektverantwortlichen des Instituts rechnen mit einer weiterhin regen Beteiligung von Interessengruppen (Verbände, Gewerkschaften, Berufsvereinigungen etc.) und haben dargelegt, es sei hilfreich, wenn die Aufsichtsbehörden für den Datenschutz ihre Vorstellungen zum Arbeitnehmerdatenschutz mitteilen könnten und um ergänzende Vorschläge gebeten. Das wird zu prüfen sein. Das Institut hat unter der Homepage www.arbvg.de ein Portal eingerichtet, in dem sich interessierte gesellschaftliche Gruppen und Personen zu dem Entwurf äußern können.

18.12 Meldung unzulässiger Verhaltensweisen im Betrieb durch Beschäftigte (Whistleblowing)

In zunehmendem Maße setzen international tätige Unternehmen Whistleblowing Hotlines ein, die auch für die jeweiligen Niederlassungen in Deutschland - also auch im Land Bremen - gelten sollen. Zwecke dieser Hotlines sind u. a., Unregelmäßigkeiten im Finanzsektor oder Korruptionsfälle aufzudecken. Wegen der Unsicherheiten über die Zulässigkeit dieser Hotlines und zur Wahrung der schutzwürdigen Interessen Betroffener vor unzulässiger Denunziation etc. hat die Arbeitsgruppe „Beschäftigtendatenschutz“ der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich ein Papier erarbeitet, das für Unternehmen, Personalvertretungen und Betroffene eine Orientierungshilfe darstellen soll. Es berücksichtigt die Stellungnahme 1/2006 bzw. WP117 der Artikel-29-Datenschutzgruppe (Datenschutzbeauftragte der Mitgliedstaaten der EU), abrufbar unter www.europa.eu.int/comm/justice-home/fsj/privacy/docs/wpdocs/2006/wp117-de.pdf. Das nationale Arbeitspapier wird zurzeit noch im Kreise der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich abgestimmt.

Rechtsgrundlage für derartige Hotlines ist § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG), wonach derartige Hotlines zulässig sind zur Wahrung der berechtigten Interessen der Unternehmen, Regelverstöße aufzudecken oder zu vermeiden. Hierbei dürfen jedoch die schutzwürdigen Interessen der Beschäftigten, über die von anderen Kollegen Meldungen erfolgen, nicht überwiegen.

Als zulässige Zwecke kommen Verhaltensweisen in Betracht, die einen sich gegen das Unternehmensinteresse richtenden Straftatbestand erfüllen (z. B. Korruption und Unterschlagung) oder Verhaltensweisen, die gegen die Menschenrechte verstoßen (z. B. Ausnutzung günstiger Produktionsbedingungen im Ausland durch in Kauf genommene Kinderarbeit und Umweltverstöße). Nicht dagegen sind Verhaltensweisen als Regelverstöße zu betrachten, die unternehmensinterne Verhaltensregeln beeinträchtigen, wie z. B. ein unzulässiges Verbot privater Kontakte unter Beschäftigten.

Eine Regelung über derartige Hotlines sollte den angesprochenen Personenkreis und den Zweck der jeweiligen Hotline konkret bestimmen. Außerdem müssen die Beschäftigten über Zweck, Organisation und Nutzungsbedingungen sowie Auskunfts-, Berichtigungs- und Lösungsrechte der Betroffenen unterrichtet werden. Anonyme Anzeigen (auch Hinweise) sollten nur in Ausnahmefällen akzeptiert werden. Anonymität widerspricht dem Transparenzgebot und begünstigt gegenüber der namentlichen Nennung eher Missbrauch und Denunziation. Durch anonyme Hinweise gemeldete Personen können sich gegen eine etwaige Verleumdung in einem rechtsstaatlichen Verfahren nicht wehren. Den Hinweisgebern muss verdeutlicht werden, dass ihre Identität den Personen, die an weiteren Überprüfungen oder ggf. anschließend eingeleiteten Gerichtsverfahren beteiligt sind, enthüllt werden kann. Dies gilt hinsichtlich entsprechender Akteneinsichtsrechte in evtl. Strafverfahren. Eine betroffene Person ist erst dann über Anzeigen zu informieren, wenn kein Risiko besteht, dass Beweise für ein Fehlverhalten vernichtet werden oder ein Missbrauch der Hotline offensichtlich ist. Außerdem sollten die Daten innerhalb von zwei Monaten nach Abschluss der Untersuchung gelöscht werden.

Bedeutsam ist auch, dass vor dem Einsatz eines derartigen automatisierten Verfahrens wegen der besonderen Risiken für die Rechte und Freiheiten der Betroffenen eine Vorabkontrolle durch den Beauftragten für den Datenschutz vorgenommen wird und entsprechende technische und organisatorische Maßnahmen zur Wahrung der Vertraulichkeit (z. B. Einsatz von Verschlüsselungsverfahren) und der Löschungsverpflichtung getroffen werden.

18.13 E-Mail-Weiterleitung nach Ausscheiden aus dem Betrieb

Die Weiterleitung von E-Mails nach Ausscheiden eines Mitarbeiters aus dem Unternehmen ist grundsätzlich zulässig, wenn die E-Mail-Nutzung nur zu betrieblichen Zwecken erlaubt und die Nutzung zu privaten Zwecken ausdrücklich untersagt worden ist. Allerdings ist nicht auszuschließen, dass trotzdem private E-Mails über die personengebundenen E-Mail-Adressen von Mitarbeitern eingehen. Diese unterliegen dem Fernmeldegeheimnis nach § 88 Telekommunikationsgesetz (TKG), wonach dem Arbeitgeber nicht erlaubt ist, Einsicht in private E-Mails zu nehmen.

Hierbei sind die Voraussetzungen des § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) zu beachten. Zur Wahrung der schutzwürdigen Interessen eines ausscheidenden Mitarbeiters aus dem Unternehmen sollte folgende Vorgehensweise beachtet werden:

Wenn ein Mitarbeiter das Unternehmen verlässt, sollte er vorher die in seinem E-Mail-Fach vorhandenen persönlichen bzw. privaten E-Mails löschen, während die betrieblichen E-Mails entweder an den Vertreter oder Nachfolger weitergeleitet oder ggf. ebenfalls gelöscht werden, soweit sie für betriebliche Zwecke nicht mehr benötigt werden.

Sollte dies z. B. bei einer fristlosen Kündigung nicht mehr möglich sein, hängt es von den jeweiligen Umständen des Einzelfalls ab, ob eine Einsichtnahme in das E-Mail-Fach erforderlich ist, um betriebliche E-Mails bearbeiten zu können. Hierbei empfiehlt es sich, eine verantwortliche Person zu bestimmen, die zur Wahrung der schutzwürdigen Interessen des ehemaligen Mitarbeiters nur Einsicht in das E-Mail-Fach nimmt, um betriebliche E-Mails auszusortieren und offensichtlich private E-Mails unverzüglich zu löschen.

Nach dem Ausscheiden eines Mitarbeiters aus dem Unternehmen sollte die E-Mail-Adresse unverzüglich gelöscht werden, so dass keine weiteren E-Mails mehr unter dieser Adresse eingehen. Alternativ besteht die Möglichkeit, über den Abwesenheitsassistenten den Hinweis anzubringen, dass unter dieser E-Mail-Adresse keine E-Mails mehr bearbeitet werden und auf eine andere E-Mail-Adresse zu verweisen.

18.14 Weitergabe von Personalakten

Eine Vielzahl von Beschäftigten eines privatrechtlich organisierten Unternehmens hatte moniert, ihre Personalakten seien an eine Dienststelle der bremischen Verwaltung weitergegeben worden, ohne dass sie darüber informiert oder gar ihre Einwilligungen eingeholt worden wäre.

Das Unternehmen hat erklärt, die Weitergabe sei auf Anforderung der Dienststelle zur Rückführung der Beschäftigten in den bremischen Dienst erforderlich gewesen. Die die Personalakten anfordernde Dienststelle hat auf Anfrage erklärt, nur mit Hilfe der Personalakten sei eine qualifikationsorientierte Rückführung und Einweisung der Beschäftigten möglich. Eine Aufstellung erforderlicher Daten sei für diesen Zweck nicht ausreichend gewesen.

Das Unternehmen hat daraufhin auf Anfrage zugesichert, in ähnlich gelagerten Fällen des § 28 Abs. 3 Nr. 1 Bundesdatenschutzgesetz (BDSG) zukünftig die Beschäftigten unmittelbar nach der Weitergabe ihrer Personalakten darüber zu informieren.

18.15 Prüfung der Datenverarbeitung in Fahrschulen

Im Berichtsjahr habe ich die Verarbeitung personenbezogener Daten von Fahrschülern in den Geschäftsräumen von fünf Fahrschulen geprüft. Bei den Prüfungen sind jeweils die Formulare „Ausbildungsvertrag“, „Antrag auf eine Fahrerlaubnis“ und eine „Bewerberliste“ zur Anmeldung von Führerscheinprüfungen an den Technischen Überwachungsverein (TÜV) Nord vorgelegt worden.

Zu den rechtlichen Anforderungen: Rechtsgrundlagen zur Zulässigkeit der Datenverarbeitung sind § 28 Abs. 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) und § 18 Fahrlehrergesetz (FahrIG) i. V. m. § 6 Durchführungsverordnung zum Fahrlehrergesetz (FahrIGDV) einschließlich der Anlagen 3 und 4 (Ausbildungsnachweis und Tagesnachweis für Fahrlehrer). Die Fahrschule schließt mit einer/einem sich meldenden Fahrschülerin/Fahrschüler einen Ausbildungsvertrag ab. Hierzu wird ein Formular verwendet, in das die erforderlichen Daten (Stammdaten und andere) eingetragen werden.

Zweifel an der Zulässigkeit der Datenverarbeitung habe ich hinsichtlich des Datums „Staatsangehörigkeit“ bei einer Fahrschule in Bremerhaven geäußert. Hierzu erklärte der Fahrlehrer, dieses Datum benötige die Fahrerlaubnisbehörde. Diese würde ggf. beim Ausländeramt nachfragen, ob eine befristete oder unbefristete Aufenthaltsgenehmigung vorliege. Auf Anfrage hat die Fahrerlaubnisbehörde mitgeteilt, diese Angabe sei nie von dort verlangt worden. Daraufhin hat der Fahrlehrer erklärt, dieses Datum zukünftig nicht mehr zu erheben.

Bei einer anderen Fahrschule sind in der Datenmaske eines Fahrlehrerprogramms die Felder „Staatsangehörigkeit“ und „Sprache“ aufgeführt. Dort wurde die jeweilige Sprache des Fahrschülers in das Feld „Staatsangehörigkeit“ eingetragen. Die Aufnahme der Sprache ist stets freiwillig und deshalb bedeutsam, weil die Fahrprüfer den Fahrschülern ermöglichen wollen, die schriftliche Prüfung in ihrer Muttersprache abzulegen. Wegen des Grundsatzes der Richtigkeit der Daten habe ich empfohlen, die Sprache in das entsprechende Feld einzutragen und das Feld „Staatsangehörigkeit“ zu löschen. Die Fahrschule hat dies zugesagt.

Die im Ausbildungsvertrag enthaltenen Daten werden bei allen geprüften Fahrschulen elektronisch gespeichert und nach Abschluss der Fahrausbildung bzw. nach Bestehen der Fahrprüfung zehn Jahre lang aufbewahrt. Diese Frist ergibt sich aus § 257 Abs. 4 Handelsgesetzbuch (HGB).

Ich habe Zweifel geäußert, ob auch die elektronisch gespeicherten Daten neben den übrigen Unterlagen in Papierform zehn Jahre lang aufbewahrt werden müssen. Die Fahrschulen haben jeweils zugesagt zu klären, ob die Daten nach zwei bis drei Jahren gelöscht werden können, so dass nur noch die in Papierform zur Steuerprüfung zu verwendenden Daten zehn Jahre lang aufbewahrt werden. Da diese Unterlagen Belege i. S. des § 257 Abs. 1 Nr. 4 HGB sind, werden sie von allen Fahrschulen in Papierform aufbewahrt.

Technische Sicherungsmaßnahmen: Die für die Erfüllung des Ausbildungsvertrages erforderlichen Daten wurden bei allen geprüften Fahrschulen elektronisch auf Stand-alone-Rechnern unter dem Betriebssystem Windows XP oder Rechnern mit Internet-Zugang mit unterschiedlichen Fachanwendungen für Fahrschulen verarbeitet, teilweise mit einer Online-Verbindung zum TÜV Nord zur Terminbestellung. Diese Online-Verbindung war datenschutzgerecht abgesichert.

Bei den Prüfungen wurden von mir außerdem Fragen zur Zugangskontrolle einer angemessenen Authentifizierung und Verfügbarkeitskontrolle, d. h., dem Schutz der Fahrschülerdaten gegen zufällige Zerstörung oder Verlust, geklärt.

Zur Zugangs-, Zugriffs- und Weitergabekontrolle nach Nr. 2 – 4 und 7 der Anlage zu § 9 Satz 1 BDSG habe ich bei einer Verbindung der Rechner mit dem Internetanschluss der Fahrschule die Installation einer „Personal Firewall“ empfohlen. Sie ermöglicht u. a., die Zugänge zum Rechner und die auf den Festplatten der Rechner gespeicherten Programme zu schützen. Auch ein Virenschutz zur Prüfung von E-Mail-Attachments ist dort in der Regel integriert. Informationen über entsprechende Produkte finden sich auch im Internet; für grundlegende Informationen über „Personal Firewalls“ habe ich auf meine Homepage www.datenschutz.bremen.de verwiesen.

18.16 Bonitätsprüfung bei der Bezahlung von Parkgebühren per Handy

Durch einen Pressebericht der Bremer Tageszeitungen wurde ich darauf aufmerksam, dass in Bremen die Bezahlung von Parkgebühren per Handy ermöglicht werden soll. Ich nahm daraufhin Kontakt mit der Firma auf, um mich über die geplanten Datenverarbeitungsvorgänge unterrichten zu lassen. Die Firma erklärte mir in diesem Zusammenhang, neben der Übermittlung von personenbezogenen Daten an die beteiligten Banken, Kreditkartenunternehmen und Mobilfunknetzbetreiber des Nutzers sei auch eine Überprüfung der Kreditwürdigkeit bei Auskunfteien vorgesehen. Grundlage für die Bonitätsprüfung seien §§ 28, 29 Bundesdatenschutzgesetz (BDSG). Um die wirtschaftliche Situation eines Unternehmens bei Kleinbetragsgeschäften nicht zu gefährden, müsse eine entsprechende Prüfung des Nutzers auf sein Bezahlverhalten vor Geschäftsabschluss erfolgen. Bei Nichtzahlung mit anschließender Verfolgung (Mahnwesen, Vollstreckung usw.) stehe der Aufwand in keinem wirtschaftlichen Verhältnis zum Ertrag. Keine Verfolgung fordere zum Missbrauch durch den Nutzer auf. Eine Prüfung des Zahlungsverhaltens sei daher immer vor der Gewährung des „Kredites“ zwingend. Außerdem informiere sie den Nutzer darüber, dass im Falle der Nichteinlösung der Lastschrift diese Tatsache in eine Sperrdatei aufgenommen werde, so dass er faktisch bis zur Begleichung der Forderungen von zukünftigen Zahlungen per Handy ausgeschlossen werde. Das Unternehmen berief sich dabei auch auf seine im Internet veröffentlichten Allgemeinen Geschäftsbedingungen (AGB).

Da wohl kein Nutzer, der mit seinem Fahrzeug auf einen Parkplatz fährt, vor der Bezahlung zunächst im Internet nach den AGB der Firma sucht, wäre die Bonitätsprüfung ohne Wissen und Kenntnis hinter dem Rücken der Betroffenen vonstatten gegangen und schon allein aus diesem Grund unzulässig. Weiter ist zu beachten, dass die Datenerhebung bei anderen Personen oder Stellen nur zulässig wäre, wenn sie zur Wahrung des Geschäftszwecks erforderlich wäre und keine Anhaltspunkte dafür bestünden, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt würden (§ 28 Abs. 1 Nr. 2 i. V. m. § 4 Abs. 2 b BDSG). Es ist zumindest strittig, ob Kleinstbeträge zum Anlass einer Bonitätsprüfung dienen dürfen. Im vorliegenden Fall war ohnehin beabsichtigt, säumige Nutzer in eine Sperrdatei aufzunehmen.

Zu einer Klärung dieser Fragen kam es nicht, weil zwischenzeitlich das Unternehmen aus wirtschaftlichen Gründen diesen Dienst einstellen musste, weil dieser von zu wenig Kunden in Anspruch genommen wurde. Die beteiligten Geschäftspartner erklärten dann auch, sie wollten kein Nachfolgeprojekt auflegen.

18.17 Herausgabe von Mitgliederdaten an Vereinsmitglieder und Dritte

Im vergangenen Jahr haben sich verschiedentlich Vereine und Vereinsmitglieder mit datenschutzrechtlichen Fragestellungen an mich gewandt. Dabei ging es z. B. um die datenschutzkonforme Gestaltung der Vereinssatzung und der Einwilligungsklauseln in den Beitrittserklärungen oder um die Rechtmäßigkeit der Übermittlung von Mitgliederdaten an andere Vereine und Verbände.

Ein weiteres Dauerthema ist die Herausgabe von Mitgliederdaten an Vereinsmitglieder zum Zweck der Kontaktaufnahme oder zur Wahrnehmung von satzungsmäßigen Rechten, etwa der Einberufung außerordentlicher Mitgliederversammlungen oder der Ergänzung der Tagesordnung.

So haben sich Mitglieder eines als Verein geführten Kindergartens an mich gewandt und um Mitteilung gebeten, ob ihnen vom Vorstand des Vereins eine Mitgliederliste zur Verfügung zu stellen ist, um die Vereinsmitglieder im Vorfeld einer Mitgliederversammlung über einen Tagesordnungspunkt zu informieren und ggf. einen abweichenden Antrag zu formulieren. Nach Einsicht in die Satzung des Vereins ergab sich, dass Anträge zur Behandlung in der Tagesordnung der Mitgliederversammlung ohne Quorum gestellt werden konnten. Eine Mobilisierung der Mitglieder und Übersendung der Mitgliederdaten war daher nicht erforderlich. Die Bestimmungen der Satzung ließen sich zudem dahin auslegen, dass fristgerecht eingegangene Anträge im Vorfeld der Mitgliederversammlung an alle Mitglieder zu versenden waren. Damit war auch ausgeschlossen, dass eine ad-hoc Behandlung von Gegenanträgen auf der Mitgliederversammlung, zu der mangels näherer Kenntnis unter Umständen nur ein Teil der Mitglieder erscheint, zu verfälschten Ergebnissen führt.

In einem ähnlichen Fall hat das Amtsgericht Bremen mit Urteil vom 28. November 2005 (Az. 1 C 0061/05), bestätigt durch Beschluss des Landgerichts Bremen vom 1. Juni 2006 (Az. 1 S 406/05), die Klage eines Vereinsmitglieds als unbegründet zurückgewiesen, das auf Herausgabe bzw. Bekanntgabe einer Namen und Anschriften enthaltenen Mitgliederliste eines Vereins geklagt hatte, dessen Ziel die Aufklärung zu gesundheitlichen Risiken sowie die Verbesserung der Vorsorge und Unterstützung Betroffener ist. Das Gericht hat anerkannt, dass zur Durchsetzung der Einberufung einer außerordentlichen Mitgliederversammlung eine Kommunikation zwischen den Vereinsmitgliedern zur Mobilisierung von Mitinteressenten nötig ist. Nach Auffassung des Gerichts gewährleistete der Verein diese Kommunikation jedoch durch ein Rundbriefverfahren. Zudem überwog das Datenschutzinteresse der Vereinsmitglieder vorliegend das berechnete Interesse an der Herausgabe der Mitgliederliste, da aufgrund der Thematik des Vereins davon auszugehen war, dass ein Teil der Mitglieder persönlich betroffen ist und in hohem Maße Anspruch auf sensiblen Umgang mit ihren Daten hatte. Eine Umfrage unter den Mitgliedern hatte ergeben, dass nur ein Bruchteil der Datenweitergabe zustimmte. Die Klägerin selbst gehörte nicht dazu.

Aufgrund des anhaltend hohen Beratungsbedarfs habe ich in Zusammenarbeit mit verschiedenen anderen Landesbeauftragten für den Datenschutz bereits im Jahr 2002 ein Faltblatt „Datenschutz im Verein“ erstellt und im Anschluss daran eine ausführlichere Broschüre „Datenschutz im Verein“, in der sich u. a. auch Beispielformulierungen für eine Datenschutzregelung in der Satzung und das Muster

einer Einwilligungserklärung befinden. Die Broschüre ist auf meiner Webseite www.datenschutz.bremen.de abrufbar.

18.18 Einsatz von Videoüberwachung und Webcams

Im letzten Jahr erreichten mich mehr als 20 Anfragen, die sich gegen die Videoüberwachung von Wohn- und Geschäftsgebäuden wandten. Es wäre zu aufwändig, jeden Fall hier ausführlich darzustellen, so dass ich mich auf einige exemplarische Fälle beschränke.

In Spielhallen: Ein Kunde beschwerte sich z. B. über das Vorhandensein von Kameras in einer Spielhalle, sowohl in den Kabinen als auch am Geldwechselautomat. Das Unternehmen erklärte, die Videoüberwachung sei vorwiegend zur Abschreckung von Übergriffen oder Manipulationen in den Kabinen und am Geldwechselautomat durch Gäste erforderlich. Darüber hinaus verlangten die Berufsgenossenschaften aufgrund der besonderen Gefahrensituation in Spielstätten die Videoüberwachung. Meine Aufforderung ist umgesetzt worden, an mehreren Stellen entsprechende Hinweise anzubringen.

Eingang und Fahrstuhl eines Wohn- und Geschäftshauses: Eine Einwohnerversammlung einer Großwohnanlage hatte per Mehrheitsbeschluss über den Einsatz der Videoüberwachung entschieden. Daraufhin haben mehrere Eigentümer und Mieter dargelegt, dadurch würden ihre schutzwürdigen Interessen beeinträchtigt; außerdem würden regelmäßig Patienten einer in der Wohnanlage befindlichen Arztpraxis überwacht werden.

Der Beschluss einer Eigentümerversammlung ist keine Befugnis zur Videoüberwachung. Entscheidend ist, ob eine Vorabkontrolle zum Ergebnis hat, dass die materiell- und formalrechtlichen Voraussetzungen des § 6 b Bundesdatenschutzgesetz (BDSG) vorliegen bzw. eingehalten werden. Insbesondere wegen der schutzwürdigen Interessen der die Arztpraxis aufsuchenden Patienten ist, neben den allgemeinen Anforderungen, auf meine Empfehlung hin festgelegt worden, die Videoüberwachung nur außerhalb der Geschäftszeiten dieser Praxis zu aktivieren.

Kamera-Attrappen: Aufgrund der Hinweise von Passanten auf eine an einem Wohngebäude angebrachte auf die öffentliche Straße gerichtete Videokamera hat die Hausverwaltung auf Nachfrage erklärt, es handele sich um eine Attrappe, die den gewünschten Abschreckungseffekt gegen Einbruch und Vandalismus entfalte. Auf meinen Vorschlag hin wurde die Attrappe ausschließlich auf den zum Privatgrundstück gehörenden Eingangsbereich gerichtet und ein Hinweis auf den Umstand der Videoüberwachung angebracht.

Die zumindest analoge Anwendung des § 6 b BDSG ist insbesondere aufgrund des Urteils des Landgerichts Bonn vom 16. November 2006 (Az. 8 S 1389/04) angemessen. Das Gericht kommt zu dem Schluss, die Attrappe einer Kamera erwecke den Eindruck der Überwachung, der den gleichen Überwachungsdruck auslöse wie eine echte Kamera, aber auch die gleiche abschreckende Wirkung habe. Soweit die Attrappe auf den öffentlichen Straßenraum gerichtet sei, beeinträchtige sie das Persönlichkeitsrecht des Betroffenen ebenso wie es echte Kameras täten.

Webcams auf Baustellen: Mehrere Hinweise auf diese Webcams waren verbunden mit der Befürchtung, hier würden die Bauarbeiter einer permanenten Kontrolle durch den Arbeitgeber ausgesetzt sein. Hierzu habe ich die jeweils angegebenen Webcams auf den Homepages angesehen (z. B. Neubau eines Kultur- und Dienstleistungszentrums in der Bremerhavener Innenstadt und der

Neubau von Radio Bremen in der Faulenstraße). Zweck dieser Webcams ist, regelmäßig die Öffentlichkeit über den Fortschritt von Neubauten zu informieren.

Es handelte sich in beiden Fällen um feststehende Bilder, die erst nach ca. 15 bis 30 Minuten aktualisiert wurden. Keine Bedenken bestehen, wenn die Personen auf der Baustelle nicht erkennbar sind und nur feststehende Bilder, die in länger andauernden Intervallen aktualisiert werden, veröffentlicht werden. Abgesehen davon kann jeder betroffene Beschäftigte direkt bei den Baufirmen Auskunft nach § 34 Bundesdatenschutzgesetz (BDSG) darüber erhalten, ob und ggf. zu welchen Zwecken die Firmen ihre Bilddaten verarbeiten. Außerdem muss die Baufirma als Arbeitgeberin die auf ihrer Baustelle tätigen Beschäftigten nach § 4 Abs. 3 BDSG über die Zwecke etwaiger Videoaufnahmen unterrichten.

18.19 Ordnungswidrigkeitsverfahren

In zwei Fällen verhängte ich im Berichtsjahr nach § 43 Bundesdatenschutzgesetz (BDSG) Bußgelder wegen begangener Ordnungswidrigkeiten. In einem Fall war das betroffene Unternehmen mehrfach meiner Aufforderung nicht nachgekommen, zu einer Eingabe, die ich zuvor erhalten hatte, Stellung zu nehmen. Die dem Unternehmen übersandten Anschreiben wurden nicht beantwortet, obwohl es gem. § 38 Abs. 3 Satz 1 BDSG hierzu verpflichtet war. Der Bußgeldbescheid ist zwischenzeitlich rechtskräftig geworden. Da das Unternehmen nicht bereit war, in der ihm dafür eingeräumten Frist das verhängte Bußgeld zu entrichten, ist das Mahn- und Beitreibungsverfahren eingeleitet worden.

In dem anderen Fall übermittelte ein Insolvenzverwalter vorsätzlich unzulässigerweise eine Vielzahl von Daten pflegebedürftiger Personen an eine Krankenkasse, was einen Verstoß gegen § 28 Abs. 6 BDSG darstellt (vgl. Ziff. 18.8 dieses Berichts). Gegen den gegen ihn verhängten Bußgeldbescheid hat der Insolvenzverwalter Einspruch eingelegt. Der Bußgeldvorgang ist zur weiteren Bearbeitung an die Staatsanwaltschaft Bremen abgegeben worden.