Landtag Brandenburg **Drucksache 3/7723**
3. Wahlperiode

Neudruck

Bericht
der Landesregierung

Zwölfter Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht−öffentlichen Bereich zuständigen Aufsichtsbehörde an den Landtag des Landes Brandenburg

Datum des Eingangs: 30.06.2004 / Ausgegeben: 07.07.2004

1. Einleitung

Der Bericht gibt einen Überblick über die Tätigkeit der Aufsichtsbehörde für den Datenschutz im nicht−öffentlichen Bereich im Land Brandenburg. Aufsichtsbehörde ist das Ministerium des Innern des Landes Brandenburg.
Die Berichterstattung erstreckt sich über den Zeitraum vom 1. Januar 2003 bis 31. Dezember 2003.

1.1 Meldungen zum Register

Die Aufsichtsbehörde für den Datenschutz im nicht−öffentlichen Bereich führt das Register nach § 4 d
Bundesdatenschutzgesetz (BDSG).

Die Registerübersicht gliedert sich folgendermaßen:

Gesamtmeldungen:	12
davon	
Auskunfteien:	6
Markt− und Meinungs− forschungsinstitute:	6

1.2 Beschwerden

Im Berichtszeitraum gingen 81 schriftliche Beschwerden sowie 24 Informationsan−fragen bei der Aufsichtsbehörde ein, die durch die Mitarbeiter zeitnah bearbeitet wurden.
Hierbei sollte erwähnt werden, dass sich in diesem Zeitraum der Beschwerdeanteil

zum Vorjahr verdoppelt hat. Darunter waren auch einige Beschwerdeführer, die mit der ersten Bewertung der Behörde nicht zufrieden waren und um eine erneute Befassung mit der Angelegenheit baten.

Die Anzahl der Informationsanfragen ging tendenziell etwas zurück. Dies dürfte darauf zurückzuführen sein, dass seitens der Bürger oder Unternehmen verstärkt Informationen über das Internet eingeholt werden.
Beschwerden und Anfragen, die nicht der Zuständigkeit der Aufsichtsbehörde Brandenburg unterlagen, wurden an die dafür zuständigen Bundesländer weitergeleitet. Diese sowie telefonische Anfragen wurden nicht gesondert erfasst.
Unter Punkt 3 werden nähere Ausführungen zu einigen Beschwerden bzw. Anfragen gemacht.

2. Allgemeines

2.1 Internationaler Datenverkehr

Die Aufsichtsbehörde ist unter anderem zuständig für die Kontrolle des grenzüberschreitenden Datenverkehr sowohl innerhalb als auch außerhalb der Europäischen Union. Da internationale Datenverarbeitungen im Zuge der Globalisierung verstärkt an Bedeutung gewinnen werden, werden die grundlegenden Rechtsvorschriften nachfolgend erläutert:

Die Europäische Datenschutzrichtlinie verfolgt neben dem Ziel des Schutzes der Grundrechte der Menschen in Europa auch das Ziel, den freien Verkehr personenbezogener Daten innerhalb der Europäischen Union zu gewährleisten, in dem das Datenschutzniveau in den Mitgliedstaaten vereinheitlicht wird. Mit der Umsetzung der EG−Richtlinie durch die Novelle des Bundesdatenschutzgesetzes (BDSG) im Jahr 2001 ist nunmehr eine Übermittlung personenbezogener Daten an Stellen innerhalb der Europäischen Union, aber auch an Stellen in Länder des Europäischen Wirtschaftsraumes, die nicht gleichzeitig Mitglied der Europäischen Union sind (Island, Liechtenstein und Norwegen), erlaubt. Voraussetzung ist jedoch, dass auch

die sonstigen Zulässigkeitsvoraussetzungen für eine Datenübermittlung erfüllt sein müssen (§ 28 bis 30 BDSG).

Differenziert ist die Zulässigkeit der Datenübermittlung an Stellen außerhalb der EU, in die sogenannten Drittstaaten, zu sehen. Eine Datenübermittlung ist über die allgemeinen Voraussetzungen der Datenverarbeitung hinaus grundsätzlich nur dann zulässig, wenn bei der Stelle ein angemessenes Datenschutzniveau gewährleistet ist (§ 4b Abs. 2 Satz 2 BDSG). Daneben lässt das BDSG eine Datenübermittlung aber auch unter bestimmten Voraussetzungen zu. So ist die Datenübermittlung an Stellen in Drittstaaten ohne angemessenes Datenschutzniveau auch zulässig mit Einwilligung des Betroffenen, zur Erfüllung eines Vertragsverhältnisses mit oder im Interesse der betroffenen Person, zur Wahrung eines wichtigen öffentlichen Interesses oder zur Ausübung von Rechtsansprüchen und aus Registern, die der Information der Öffentlichkeit dienen und leicht zugänglich sind (§ 4c Abs. 1 Nr. 1 bis 6 BDSG). Sind diese Voraussetzungen nicht erfüllt, kann die zuständige Aufsichtsbehörde einzelne Übermittlungen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien für den Schutz der Persönlichkeitsrechte der betroffenen Person aufweist (§ 4c Abs. 2 BDSG).

Eine Datenübermittlung in Drittstaaten ist also nur zulässig wenn

a) ein angemessenes Datenschutzniveau bei der empfangenden Stelle gewährleistet ist,
b) bestimmte Ausnahmen vorliegen oder
c) die Aufsichtsbehörde diese genehmigt.

<u>a) angemessenes Datenschutzniveau im Drittstaat</u>

Nach § 4b Abs. 5 BDSG trägt die Verantwortung für die Zulässigkeit der Datenübermittlung die übermittelnde Stelle. Sie hat also nicht nur zu prüfen, ob die Voraussetzung für eine Datenübermittlung nach § 28 bis 30 BDSG vorliegen, sondern auch, ob bei der empfangenden Stelle ein angemessenes Datenschutzniveau vorliegt.

Unter welchen konkreten Voraussetzungen das Schutzniveau als angemessen qualifiziert werden kann, wird jedoch weder in der EG−Richtlinie noch im BDSG geklärt. Als Maßstab ist der Schutz der Grundrechte und Grundfreiheiten und insbesondere der Schutz der Privatsphäre anzusehen. Entscheidend hierfür ist, inwieweit der Drittstaat über eine Regelung verfügt, die den "harten Kern" der von der EG−Richtlinie bzw. dem BDSG aufgestellten Verarbeitungsbedingungen gewährleistet. Die Regelungen müssen nicht nur eine Zweckbindung sowie ein Mindestmaß an Transparenz vorschreiben, sondern genauso die Rechte der Betroffenen und eine unabhängige Kontrolle der Verarbeitungsvorgänge garantieren. Zudem muss das Datenschutzniveau für den konkreten Verarbeitungszusammenhang angemessen sein. Es ist deshalb denkbar, dass die Angemessenheit etwa bei der Verarbeitung im Gesundheits− oder Kreditbereich bejaht, ansonsten aber verneint werden muss. In Betracht kommen grundsätzlich lediglich Regelungen, die auf gesetzlichen, eindeutig auf die Verarbeitung personenbezogener Daten zugeschnittenen Vorgaben beruhen müssen. Gesetzliche Regelungen und vertragliche Abmachungen dürfen deshalb nicht auf eine Stufe gestellt werden. Der Ausnahmetatbestand des Art. 26 Abs. 2 EG−Richtlinie (Genehmigung aufgrund von Garantien) lässt sich also nicht über die "Adäquanz−Formel" in einen Regelfall verwandeln.[1] Zu dieser Problematik besteht unter den Aufsichtsbehörden keine einheitliche Auffassung. Es wird diesbezüglich auf die Ausführungen unter dem Punkt 4.3 verwiesen.

Neben der verantwortliche Stelle kann auch die Europäische Kommission feststellen, dass in einem Drittstaat ein angemessenes Datenschutzniveau gewährleistet ist. Bislang wurde dieses uneingeschränkt für die Länder Schweiz, Argentinien

[1] insgesamt siehe hierzu: Dammann, Dr. Ulrich; Simitis, Dr. Dr. h.c. Spiros: EG Datenschutzrichtlinie Kommentar, 1. Auflage, Nomos−Verlagsgesellschaft, Baden−Baden 1997., S. 77 f.

Guernsey und die Isle of Man sowie mit Einschränkungen für Kanada festgestellt.[2] Weiterhin hat die Europäische Kommission eine Entscheidung getroffen, die feststellt, dass das Safe−Harbor−Abkommen mit den USA ein "angemessenes Datenschutzniveau" für die Übermittlung an Unternehmen gewährleistet[3], die diesem Abkommen beigetreten sind.

Im Zuständigkeitsbereich der Aufsichtsbehörde erfolgen beispielsweise durch das Unternehmen eBay Datenübermittlungen in die USA. Diese basieren auf einer Einwilligung der eBay−Mitglieder, so dass sich die Frage der Angemessenheit des Schutzniveaus für die personenbezogenen Daten bei diesen Übermittlungen nicht stellt. Näheres ist den Ausführungen unter dem Punkt 3.2 zu entnehmen.

b) Datenübermittlung auf der Grundlage der Ausnahmebestimmungen des § 4c Abs. 1 BDSG

Liegt bei der Stelle, an die die Daten übermittelt werden sollen, kein angemessenes Datenschutzniveau vor, kann eine Datenübermittlung erfolgen, wenn einer der in § 4c Abs. 1 BDSG genannten Fälle vorliegt. Hierbei ist die Stelle darauf hinzuweisen, dass die Daten nur für die Zwecke, für die sie übermittelt wurden, verwendet werden dürfen.

c) Genehmigungen durch die Aufsichtsbehörde

Liegt bei der empfangenden Stelle weder ein angemessenes Datenschutzniveau vor, noch eine der o.g. Ausnahmen, kann eine Datenübermittlung durch die Aufsichtsbehörde genehmigt werden. Dabei wird jedoch nur die Frage geprüft, ob bei der empfangenden Stelle ausreichende Garantien für die Gewährleistung des Datenschutzes vorliegen. Solche Garantien könne sich aus vertraglichen Vereinbarungen zwischen den beteiligten Stellen oder verbindlichen Unternehmensreglungen ergeben.
Bei der Beurteilung solcher Vereinbarungen können die Entscheidungen der Europäischen Kommission über die Standardvertragsklauseln herangezogen werden. Bisher hat die Europäische Kommission 2 Entscheidungen über Standardvertragsklauseln getroffen, die ein angemessenes Datenschutzniveau bei der empfangen−

[2] siehe: http://europa.eu.int/comm/internal_market/privacy/adequacy_de.htm
[3] Entscheidung der Kommission 2000/520/EG vom 26.7.2000 − ABl. L 215/7 vom 25.8.2000

den Stelle gewährleisten. Diese betreffen

1. Datenübermittlungen in Drittstaaten ohne angemessenes Datenschutzniveau[4]
2. Datenübermittlungen an Auftragsdatenverarbeiter in Drittstaaten ohne angemessenes Datenschutzniveau[5].

Wenn Datenverarbeiter diese Standardvertragsklauseln anwenden, können die darauf beruhenden Datenübermittlungen nicht aus Gründen des mangelnden Datenschutzniveaus untersagt werden.

In Brandenburg wurde bisher kein Antrag auf Genehmigung einer Datenübermittlung in Drittstaaten ohne angemessenes Datenschutzniveau gestellt.

2.2 Regelmäßige Gespräche mit Vertretern des Internetauktionshauses eBay

Auch in diesem Berichtszeitraum fanden Gespräche mit eBay statt, die zum Ziel haben, die Einhaltung der datenschutzrechtlichen Vorschriften zu begeleiten und auftretende Rechtsfragen zu klären.

Insgesamt war festzustellen, dass die Beschwerden und Anfragen im Zusammenhang mit der Tätigkeit von eBay in erheblichem Umfang zugenommen haben. Dies dürfte zum einen auf die ständig wachsende Mitgliederzahl bei eBay zurückzuführen sein. Zum anderen ist aber auch die Sensibilität der Menschen in bezug auf die Modalitäten der Verarbeitung ihrer personenbezogenen Daten gewachsen.

Die Gespräche wurden genutzt, um grundsätzliche Fragestellungen anzusprechen und eine Lösung herbeizuführen. So wurde im Berichtszeitraum u.a. die Einführung einer Einwilligungslösung für ein "Fraud Management" bei eBay thematisiert. Hintergrund hierfür war, dass der öffentliche Druck auf eBay, zum Schutz der Ver-

---

[4] Entscheidung der Kommission 2001/497/EG unter: http://europa.eu.int/comm/internal_market/privacy/modelcontracts_de.htm

[5] Entscheidung der Kommission (2002/16/EG) unter: http://europa.eu.int/comm/internal_market/privacy/modelcontracts_de.htm

braucher vor betrügerischen Angeboten tätig zu werden, sehr stark gestiegen ist. Da eBay bestrebt ist, den Schutz seiner Mitglieder weiter zu verbessern, wurde es für notwendig erachtet, eine Einwilligung in die Erhebung, Verarbeitung und Nutzung von Bestands− und Nutzungsdaten für Zwecke der Betrugsbekämpfung einzuholen. Nunmehr geben die Mitglieder u.a. die folgende Einwilligungserklärung ab:

Ich willige ein, dass eBay, soweit es im Einzelfall erforderlich ist, bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte, die Bestands− und Nutzungsdaten erheben, verarbeiten und nutzen darf, die zum Aufdecken sowie Unterbinden von in betrügerischer Absicht eingestellten Angeboten und sonstiger rechtswidriger oder vertragswidriger Inanspruchnahme der Leistungen von eBay erforderlich sind. Zu diesem Zweck darf eBay auch Nutzungsdaten, unter anderem mit Hilfe von Cookies, erheben und in der Weise verarbeiten und nutzen, dass aus dem Gesamtbestand aller aktuellen Angebote, diejenigen ermittelt werden können, bei denen tatsächliche Anhaltspunkte bestehen, dass sie in Missbrauchsabsicht eingestellt wurden.

Seitens der Aufsichtsbehörde bestehen gegen eine solche Erklärung keine Bedenken. Vielmehr wird anerkannt, dass hierdurch eine Verbesserung bei der Betrugsbekämpfung erreicht werden kann. Die Missbrauchsbekämpfung ist als Verbraucherschutz zu beurteilen wie der Datenschutz. Insoweit ist es von großer Bedeutung Lösungen zu finden, die beiden Zielrichtungen gleichermaßen gerecht werden.

2.3 Datenschutz in Gemeinschaftspraxen / Praxis−Gemeinschaften

Die Datenschutzbehörde für den nicht−öffentlichen Bereich führte im Berichtszeitraum eine Aktion zur Einhaltung des Datenschutzes im Gesundheitswesen durch. Schwerpunkt war dabei der Umgang mit Patientendaten in Gemeinschaftspraxen bzw. Praxisgemeinschaften.
Die Auswahl der in die Prüfung einbezogenen Gemeinschaftspraxen erfolgte nach dem Zufallsprinzip und nicht aufgrund von Beschwerden von Patienten. Zur Vorbereitung der Prüfung wurde ein "Selbst−Check" (s.Anlage) übergeben, der zeigen sollte, inwieweit in den Praxen Arztgeheimnis und Datenschutz beachtet werden.

Bei einem gemeinsamen Gespräch in der Praxis wurde dann dieser "Selbst−Check" ausgewertet und geprüft, wie die Bedingungen zum Schutz der Patientendaten ausgestaltet sind. Dabei wurden Vorschläge für Veränderungen im Praxisbereich unterbreitet, die zu einer Verbesserung des Datenschutzes führen sollten.
Geprüft wurden 2 Kinderarztpraxen, 2 Internistische Praxisgemeinschaften, 1 All−gemeinmedizinische Praxisgemeinschaft, 1 Psychotherapeutische Gemeinschafts−praxis, 1 HNO−Gemeinschaftspraxis sowie 1 Praxisgemeinschaft für Logopädie.
Leider war im Vorfeld der Wille zum Ausfüllen des "Selbst−Checks" nicht bei allen Praxen vorhanden bzw. wurde von zwei Praxen anfangs sogar verweigert.

Folgende wesentliche Erkenntnisse wurden bei den Prüfungen gewonnen:
Bei einer Praxisgemeinschaft wurde festgestellt, dass die Patientenunterlagen nicht in verschließbaren Schrank gelagert werden und Faxmitteilungen an die BfA aus den Privaträumen übermittelt werden. Hier wurde im Interesse der Sicherheit der Patientendaten gebeten, die Mängel abzustellen und die Aufsichtsbehörde über das Veranlasste zu unterrichten.

In einigen Gemeinschaftspraxen wurde festgestellt, dass gerade im Empfangsbe−reich eine Einsichtnahme auf den Computerbildschirm durch die Patienten leicht möglich war. Hier wurde geraten, die Computer anders aufzustellen oder einen Sichtschutz anzubringen.

In einigen Praxen wurde darauf hingewiesen, das vorhandene Passwort für den Computer in regelmäßigen Abständen zu wechseln bzw. dieses durch eine Kombi−nation von Buchstaben und Zahlen zu ersetzen, da hier eine größere Sicherheit bestehe.

Alle Angestellten der Gemeinschaftspraxen waren auf die Wahrung des Arztge−heimnisses verpflichtet.

Nach Prüfung der verschiedenen Gemeinschaftspraxen kann zusammengefasst werden, dass in den von der Aufsichtsbehörde aufgesuchten Gemeinschaftspraxen

bzw. Praxisgemeinschaften keine gravierenden Verstöße gegen den Datenschutz bei Patientenunterlagen vorlagen. Auch wenn nicht in allen Praxen das Bewusstsein für die Bedeutung des Schutzes der Rechte der Patienten in gleichem Maße ausgeprägt war, kann doch festgestellt werden, dass die Ärzte und das Praxispersonal sehr sensibel im Umgang mit den Daten ihrer Patienten sind.

2.4 Videobeobachtung öffentlich zugänglicher Räume durch private Stellen

Auch in Bezug auf die Videoüberwachung öffentlich zugänglicher Räume war festzustellen, dass die Anzahl der Anfragen zugenommen hat. Aus diesem Grund werden nachfolgend die Zulässigkeitsvoraussetzungen und die Rahmenbedingungen hierfür beleuchtet.

§ 6b Abs. 1 BDSG definiert die Videoüberwachung als Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen. Das heißt, eine Videoüberwachung findet nicht erst dann statt, wenn die Bilder aufgezeichnet und gespeichert werden, sondern sobald die tatsächliche Möglichkeit der Beobachtung gegeben ist. Die Überwachung setzt schon mit der Installation von Kameras ein, auch wenn die Geräte nur im Bedarfsfall aufzeichnen oder wenn sie zur bloßen Beobachtung genutzt werden.

Nicht unter die Videoüberwachung i.S.v. § 6b BDSG fällt die Überwachung von Eingangsbereichen von Wohnhäusern oder Werksgeländen zur Zugangsüberwachung, weil es sich hierbei i.d.R. nicht um öffentlich zugängliche Räume handelt. Ebenso fällt nicht unter den Anwendungsbereich des § 6b BDSG die private Videoüberwachung privater Wohnhäuser durch den Eigentümer oder Besitzer, auch wenn hierbei Teile der Straße oder des Gehweges (und damit öffentlich zugänglicher Räume) erfasst werden. In diesen Fällen erfolgt die Videoüberwachung ausschließlich für persönliche Zwecke, die ohnehin nicht der Anwendung des BDSG unterfällt (§ 1 Abs. 2 Nr. 3 BDSG). Allerdings darf die Videoüberwachung in diesen Fällen nicht für eine über die private Tätigkeit hinausgehende Sekundärnutzung eingesetzt werden. Auch die im Auftrag einiger Städte durchgeführten Aufnahmen von Gebäuden und ganzen Straßenzügen durch private Unternehmen fällt nicht

unter den Anwendungsbereich des § 6b BDSG. Sofern es sich nicht ausschließlich um eine Datenverarbeitung im Auftrag der Kommunen (z.B. Anfertigung der Auf−nahmen für Zwecke der Katasterverwaltung) nach § 11 BbgDSG handelt, werden in diesen Fällen die Aufnahmen zusätzlich zur Erfüllung eigener Geschäftszwecke bzw. zum Zweck der geschäftsmäßigen Übermittlung angefertigt. Deren Zulässigkeit richtet sich nach den §§ 28 oder 29 BDSG.

Öffentlich zugängliche Räume sind Bereiche innerhalb oder außerhalb von Ge−bäuden, die frei oder nach allgemein erfüllbaren Voraussetzungen (z.B. durch das Lösen von Eintrittskarten) zugänglich sind. Hierzu gehören u.a. Bahnhöfe, Kinos, Kaufhäuser sowie Restaurants aber auch Erlebnis− und Erholungsparks und Zoos.

Eine Videoüberwachung durch Private ist nur zulässig, wenn dies zur Wahrneh−mung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen (§ 6b Abs. 1 Nr. 2 und 3 BDSG).
Ein berechtigtes Interesse kann dabei ideeller, wirtschaftlicher oder rechtlicher Natur sein. Es liegt beispielsweise dann vor, wenn die Videoüberwachung dem Schutz des Eigentums oder der Vermeidung von Inventurdifferenzen dient. Weiterhin muss die Videoüberwachung für die Erreichung des Zweckes erforderlich sein. Dies ist dann der Fall, wenn der beabsichtigte Zweck nicht mit einem anderen zumutbaren Mittel, das weniger in die Rechte der Person eingreift, erreicht werden kann. Dies kann beispielsweise für die Überwachung von Verkaufsräumen zum Schutz vor konkreten Straftaten bejaht werden. Der Zweck der Videoüberwachung ist vor der Inbetrieb−nahme festzulegen und zu dokumentieren. Dabei muss beachtet werden, dass die Videoüberwachung möglicherweise mehreren Zwecken dient, weil anderenfalls eine Nutzung der Daten für andere Zwecke, wie die Verfolgung von Straftaten, nicht möglich ist (§ 6b Abs. 3 BDSG).

Vor Beginn der Überwachung ist zu prüfen, ob dieser Anhaltspunkte für ein über−wiegendes schutzwürdiges Interesse der betroffenen Personen entgegenstehen. Werden Personen so überwacht, wie dies ein Beobachter mit bloßem Auge auch tun

könnte, werden im Regelfall keine schutzwürdigen Interessen verletzt. Geht die Videoüberwachung jedoch über dieses normale Beobachten hinaus, werden z.B. Umkleidekabinen in einem Schwimmbad überwacht und damit in die Intimsphäre der Betroffenen eingegriffen, werden schutzwürdige Interessen verletzt. Auch die schutzwürdigen Belange der Mitarbeiter, die von der Videoüberwachung betroffen sein können, sind zu berücksichtigen.

Der Umstand der Videobeobachtung und die verantwortliche Stelle sind nach § 6b Abs. 2 BDSG durch geeignete Maßnahmen erkennbar zu machen. Dieser Hinweis ist deutlich sichtbar anzubringen, er erfüllt nur dann seinen Zweck, wenn er für den Kunden ohne weiteres wahrnehmbar ist und von ihm nicht erst gesucht werden muss.

Das Deutsche Institut für Normung (DIN) hat ein Normungsverfahren für ein einheitliches Piktogramm zur Kennzeichnung einer Videoüberwachung eingeleitet, mit dessen Abschluss im Herbst 2004 gerechnet werden kann. Im Mai 2003 setzten sich Vertreter des privatwirtschaftlichen Bereiches und öffentlicher Stellen im Normungsausschuss Gebrauchstauglichkeit und Dienstleistungen zusammen. Als Zwischenergebnis ist nun im Mai 2004 der Normungsentwurf DIN 33450 "Graphisches Symbol zum Hinweis auf Beobachtung mit optisch−elektronischen Einrichtungen (Video−Infozeichen)" erschienen. Neben potentiellen Anwendern aus der Privatwirtschaft ist das Projekt von den Aufsichtsbehörden aus Berlin und Brandenburg aktiv begleitet worden. Bei einer Nutzung dieses Piktogramms kann davon ausgegangen werden, dass man als nicht−öffentliche Stelle seine Verpflichtung zur Kenntlichmachung der Videobeobachtung erfüllt. Die Presseerklärung zu diesem Projekt kann unter http://www2.din.de/Pressemitteilungen − Pressemitteilungen 2003 nachgelesen werden.

Die Verarbeitung oder Nutzung der durch die Videoüberwachung gewonnen Daten ist nur zulässig, wenn sie für einen der festgelegten Zwecke erforderlich ist und keine Anhaltspunkte für überwiegende schutzwürdige Interessen des Betroffenen bestehen. Nach § 6b Abs. 4 BDSG ist der Betroffene zu benachrichtigen, wenn die mit der Videoüberwachung erhobenen Daten einer bestimmten Person zugeordnet werden können. Darunter fällt immer der Verdächtige, aber auch das Opfer z.B. eines Taschendiebstahls oder sonstige namentlich bekannte Personen wie beispielsweise Zeugen.

Nach Erreichung des Aufnahmezwecks sind die Daten unverzüglich zu löschen (§ 6b Abs. 4 BDSG). Bei einer vollständigen Aufzeichnung eines Geschäftstages (z.B. mit einer Black Box) muss die Aufzeichnung innerhalb von ein bis zwei Arbeitstagen ausgewertet werden. Aufzeichnungen, die nicht für die festgelegten Zwecke genutzt werden, sind unverzüglich zu löschen.

Im Übrigen hat die Art. 29 Datenschutzgruppe am 11. Februar eine Stellungnahme zum Thema Verarbeitung personenbezogener Daten aus der Videoüberwachung angenommen.[6]

3. Kontrolltätigkeit der Aufsichtsbehörde

3.1 Gemeinsame Prüfung eines Unternehmens im Einzugsgebiet Berlin/Brandenburg

Am 14.05.2003 wurde das Unternehmen gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit geprüft.
Der Anlass ergab sich durch ein anderes Bundesland, in welchem bei der Prüfung eines der konzernangehörigen Unternehmen Mängel festgestellt wurden. Es wurde davon ausgegangen, dass die festgestellten Mängel (Nichtbeachtung eines Wider−spruches gegen eine Nutzung oder Übermittlung der Daten für Werbezwecke gem. § 28 Abs. 4 Satz 1 BDSG) alle Unternehmensteile gleichermaßen betreffen würde und deshalb auch hier eine Kontrolle angeraten sei. Im Land Brandenburg gab es zu diesem Unternehmen bereits mehrere Datenschutzbeschwerden, so dass ein zusätzlicher Anlass zu dieser Prüfung vorlag.

Bei der gemeinsamen Prüfung wurden folgende Problemkreise erörtert:

− Bezahlung mit ec−Karte

[6] http://europa.eu.int/comm/internal_market/privacy/news_de.htm.

Bei der Bezahlung mit ec−Karte praktiziert man ein sogenanntes "wildes Last−schriftverfahren" zur Absicherung der Fälle, in denen der Rechnungsbetrag nicht eingezogen werden kann und die entsprechende Bank die Kundendaten nicht übermittelt. Name, Anschrift und Geburtsdatum würden notiert, um so der Kunden habhaft zu werden. Die Daten werden nicht bei jeder ec−Zahlung erhoben, sondern in der Regel nur bei größeren Rechnungsbeträgen.
Hier wurde dem Datenschutzbeauftragten des Unternehmens erläutert, dass das Speichern des Geburtsdatums zweifelhaft sei. Ein Notieren dieses Datums zusätz−lich zu Name und Anschrift sei nur in Ausnahmefällen von Nutzen. In Betracht kä−men nur die beiden Fälle, dass im selben Haus mehrere Personen mit demselben Namen wohnten oder innerhalb einer Familie mehrfach der selbe Name existiere (Peter Meier sen. und Peter Meier jun). Diese Fälle seien aber höchst selten, so dass eine Speicherung des Geburtsdatums nicht erforderlich und damit rechtlich bedenklich sei.

− Löschung von Kundendaten
Im weiteren Gesprächsverlauf wurde auch über die Löschung von Daten aus schriftlichen Kaufverträgen gesprochen. Hier wurde seitens des betrieblichen Da−tenschutzbeauftragten erklärt, dass diese inaktiven Daten theoretisch "ewig" auf−bewahrt würden, eine Löschungsregelung bestehe nicht. Allerdings seien 1999 alle damals vorhandenen Datensätze gelöscht worden, da aufgrund alter Postleitzahlen etc. die Angaben nur schlecht verwertbar waren. Seither würden alle Daten der schriftlichen Kaufverträge unbegrenzt in den "inaktiven Daten" gespeichert. Dies geschehe insbesondere zur Gewährleistung des Kundenservice. Weiterhin möchte man in der Lage sein, den Kunden auch noch nach dem Ablauf längerer Zeiträume zu helfen, wenn es darum gehe, dass Produkte nachgekauft werden sollen, Repa−raturen erforderlich sind etc. Hier wurde von den Aufsichtsbehörden darauf hinge−wiesen, dass eine solche unbegrenzte Speicherung der Daten unzulässig ist und von dem betrieblichen Datenschutzbeauftragten ein Löschungskonzept erstellt werden muss.

Bei der Löschung der Kundendaten, die mit ec−Karte bezahlt haben, wurde darauf

aufmerksam gemacht, dass die 2−jährige Aufbewahrung der Daten unzulässig ist. Die Pflicht der Löschung der gewonnen Daten ergibt sich bezüglich dieser Kun−dendaten aus § 35 Abs. 2 Nr. 3 BDSG. Danach sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Da bei Ab−schluss der Kaufverträge als Zahlungsmodalität das sogenannte "wilde Lastschrift−verfahren" mittels ec−Karte vereinbart wird, gehört es mit zur Zweckbestimmung dieser Vertragsverhältnisse, dass die Erfüllung der vertraglichen Verpflichtung zur Zahlung des Kaufpreises sichergestellt wird. Insofern ist die Speicherung von Name und Anschrift von § 28 Abs. 1 Nr. 1 BDSG gedeckt. Allerdings ist die Legitimati−onswirkung dieser Vorschrift auf die Zeit bis zum wirksamen Eintritt der Zahlung begrenzt. Da der Kontoinhaber innerhalb von sechs Wochen die Möglichkeit hat, gegen den Lastschrifteinzug Widerspruch einzulegen, ist erst nach diesen sechs Wochen von einer wirksamen Zahlung auszugehen. Anschließend ist eine Spei−cherung der Daten unter Rücksicht auf das bestehende Vertragsverhältnis nicht mehr erforderlich.
In Anbetracht der möglichen Unregelmäßigkeiten hinsichtlich des Zeitpunkts der Abbuchungen der Rechnungsbeträge dürfte eine Frist zur Löschung innerhalb von drei Monaten nach Abschluss des Kaufvertrages noch angemessen sein.

− Datenverarbeitung zu Werbezwecken

Zur Werbung des Unternehmens konnte festgestellt werden, dass die verwendeten Daten ausschließlich von einer Firma mit Sitz außerhalb der Länder Berlin und Brandenburg stammen. Wenn Personen sich gegen die Verwendung der Daten aussprechen, wird diesem Unternehmen mitgeteilt, dass diese Datensätze "auszu−sortieren" sind. Sofern es sich um eigene Kundendaten handelt, werden diese intern entsprechend gekennzeichnet, so dass diese Daten auch nicht mehr zu Werbe−zwecken verwendet werden.

− Datenverarbeitung innerhalb der Unternehmensgruppe

Vom Geschäftsführer des Unternehmens wurde erläutert, dass die Datenabwicklung

aller Firmen über eine zentrale EDV−Anlage erfolgt. Dabei haben aber die einzelnen Firmen jeweils eigene Kundennummern, einen eigenen Buchhaltungskreis, eigene Bankkonten, etc. Die Datenverarbeitung erfolgt also jeweils in eigenen Bearbeitungskreisen, sie wird allerdings von einem zentralen Unternehmen durchgeführt. Die Entscheidung über die Daten treffen allerdings jeweils die einzelnen Firmen. Danach kommt für diese Datenverarbeitung die Anwendung von § 11 BDSG in Betracht.
Voraussetzung für die Anwendbarkeit des § 11 BDSG als Rechtsgrundlage der Datenverarbeitung durch den Unternehmenssitz für alle anderen Häuser ist, dass die Verarbeitung lediglich als Hilfsfunktion für die Erfüllung der Aufgaben und Geschäftszwecke der einzelnen Firmen als verantwortlichen Stelle ausgelagert wird. Würden die den Verarbeitungsvorgängen zugrunde liegenden Aufgaben oder Geschäftszwecke ganz oder teilweise mit abgegeben oder erfüllte das zentrale Unternehmen als der externe Datenverarbeiter überwiegend eigene Geschäftszwecke, insbesondere, indem es über die technische Durchführung der Verarbeitung hinaus materielle vertragliche Leistungen mit Hilfe der überlassenen Daten erbrächte, dann wäre sie nicht mehr bloß Auftragnehmer, sondern würde selbst zur insoweit verantwortlichen Stelle. Eine derartige Datenverarbeitung setzt mithin eine Übermittlung voraus und wäre nicht mehr von § 11 BDSG erfasst.

Vorliegend treffen nach Auskunft des Geschäftsführers alle Häuser eigenständig ihre Personalentscheidungen, schließen jeweils eigene Kaufverträge ab, haben eigene Bankkonten etc.

Bei der Verarbeitung der Daten werden in der Hauptgeschäftsstelle die Daten mittels der vorhandenen EDV−Anlage so verarbeitet und aufbereitet, dass sie von den einzelnen Häusern entsprechend ihrer Geschäftszwecke eingesetzt und verwendet werden können. Eigene Geschäftszwecke erfüllt die zentrale Stelle dabei jedoch nicht.

Daraus schlussfolgernd liegt nach der bisherigen Bewertung der beteiligten Aufsichtsbehörden eine Auftragsdatenverarbeitung nach § 11 BDSG vor. Der nach § 11 Abs. 2 S. 2 BDSG vorgeschriebene Vertrag existiert jedoch nicht.

Seitens der Aufsichtsbehörden wurde festgestellt, dass es dringend eines solchen Vertrages bedarf, da der gegenwärtige Zustand rechtswidrig sei. Die Anforderungen nach § 11 BDSG wurden erläutert. Der Vertrag müsse so konkret und detailliert wie möglich sein und der Rückzug auf eine Generalklausel wie etwa "die Daten sind den gesetzlichen Vorgaben entsprechend zu verarbeiten" sei nicht zulässig.
Da die Firmen, die die Datenverarbeitung bei der zentralen Stelle in Auftrag geben, gem. § 11 Abs. 1 BDSG die für die Datensicherheit verantwortlichen Stellen sind, obliegt ihnen auch die Sicherstellung der Rechtmäßigkeit der vorgenommenen Datenverarbeitung. Daher bedarf es eines auf der Grundlage des § 11 Abs. 2 Satz 2 BDSG erteilten schriftlichen Auftrages, damit die Auftraggeber gegenüber dem Auftragnehmer die Erfüllung des Vertrages kontrollieren aber auch einfordern können.

Der Mindestinhalt dieses Vertrages umfasst die Festlegung von Art und Gegenstand der vom Auftragnehmer erwarteten Datenverarbeitungstätigkeit, insbesondere welche Phasen der Datenverarbeitung ihm für welche Datenbestände übertragen werden. Weiterhin müssen die technischen und organisatorischen Maßnahmen der Datensicherung fixiert werden. Sie müssen den Zeitraum vom Eingang der Daten beim Auftragnehmer bis zum Eingang der Arbeitsergebnisse beim Auftraggeber erfassen. Klarzustellen sind z. B. Zeitpunkt, Ort und Berechtigte für die Übergabe der Datenbestände, die Versendung, die Aufbewahrung der Datenträger, die Löschung von Restdaten usw. Weiterhin ist die Zulässigkeit von etwaigen Unterauftragsverhältnissen zu regeln, falls solche in Betracht kommen.
Da die zentrale Stelle mit den anderen Firmen mehrere Auftraggeber hat, muss sie zudem gemäß Nr. 8 der Anlage zu § 9 BDSG eine Vermischung der jeweiligen Datenbestände verhindern, also den ungenehmigten Zugriff auf die Datenbestände der anderen Firmen ausschließen können.

Im Gespräch wurde auch die Notwendigkeit der Erstellung eines öffentlichen Verfahrensverzeichnisses erörtert. Der behördliche Datenschutzbeauftragte merkte an, dass man sich mit diesem Thema noch nicht befasst habe.
Der Vertreter der Berliner Aufsichtsbehörde erklärte, dass aufgrund der gesetzlichen Übergangsvorschriften noch bis zum Jahre 2004 Zeit für die Erstellung des Ver-

zeichnisses sei, dass aber andere Unternehmen davon berichten, dass diese Auf−gabe sehr viel Zeit beanspruche und man anrate, bereits jetzt mit der Erstellung zu beginnen.

Der Geschäftsführer des Unternehmens wurde gebeten, binnen zwei Monaten erste Informationen darüber zu geben, wie die Empfehlungen ungesetzt wurden bzw. weiter umgesetzt werden.

Leider gibt es noch immer offene Fragen mit dem geprüften Unternehmen, die es in Zusammenarbeit mit der Berliner Behörde zu klären gilt.

3.2 Schwerpunkte aus Beschwerden

− Bekanntmachung der Post von Mitgliedern einer Kleingartenanlage

Ein Petent beschwerte sich, dass in einer Streitsache mit dem Kreisverband einer Kleingartenanlage Post vervielfältigt und den Mitgliedern ohne Einwilligung der Ab−sender zum Lesen überreicht worden sein soll. In dem geschilderten Fall fand das Bundesdatenschutzgesetz (BDSG) jedoch keine Anwendung. Nach § 1 Abs. 3 und § 27 Abs. 2 BDSG wäre der Anwendungsbereich nur eröffnet, wenn die personen−bezogenen Daten zunächst in einem automatisierten Verfahren gespeichert worden wären.

Eine Verletzung des Postgeheimnisses war auch nicht zu erkennen, da der § 39 des Postgesetzes lediglich die Umstände des Postverkehrs regelt.
Inwieweit in dem geschilderten Fall eine strafrechtliche Relevanz vorlag, war von der Aufsichtsbehörde nicht zu prüfen. Der betroffene Verband wurde jedoch in einem gesonderten Schreiben von der Aufsichtsbehörde über den Datenschutz in Vereinen informiert.

Eine Veröffentlichung von Mitgliederdaten in Aushängen und Vereinspublikationen wäre zulässig, soweit es dabei um Informationen geht, die in engem Zusammen−

hang mit dem Verein stehen und keine überwiegenden schutzwürdigen Interessen der Mitglieder entgegenstehen (§ 28 Abs. 1 Nr. 2 BDSG). Datenschutzrechtlich problematisch ist jedoch die Mitteilung von Daten aus dem persönlichen Lebensbereich der Mitglieder. Bei der Veröffentlichung solcher Daten ist immer Zurückhaltung geboten.

- **Vorlage des Personalausweises bei Kauf einer DVD FSK 18**

Der Petent wollte sich eine DVD mit der Altersfreigabe ab 18 Jahre kaufen und wurde aufgefordert seinen Personalausweis vorzuzeigen. Nun wurden beim Kauf auch die personenbezogenen Daten, wie die Personalausweisnummer aufgeschrieben. Gleichzeitig wurde er aufgefordert, eine Belehrung zu unterschreiben, dass er diese DVD nicht Minderjährigen zugänglich mache.
In der Stellungnahme des Einkaufscenters wurde mitgeteilt, dass bei den Kunden, wo eine Alterseinschätzung unsicher ist, durch das Vorzeigen des Personalausweises geprüft wird, ob das Alter mit der Altersfreigabe nach § 7 Jugendschutzgesetz übereinstimmt.
Das Verkaufspersonal habe dann aus Vorsicht die Personalausweisnummer notiert. Die Geschäftsführung sicherte jedoch zu, die Belege mit den handschriftlichen Aufzeichnungen innerhalb von 3 Tagen zu vernichten. Seit geraumer Zeit würde diese Praxis auch nicht mehr gehandhabt.
Verwiesen wurde auch auf Geschehnisse wie beispielsweise in Erfurt, wo man sich verpflichtet fühlte, die Kunden darauf hinzuweisen, dass diese Ware nicht an Jugendliche unter 18 Jahren weiterverkauft werden darf und dass ein Produkt der Klasse FSK 18 den gesetzlichen Bestimmungen unterliegt. Diesen Hinweis hat man sich deshalb unterzeichnen lassen, weil es oft vorkam, dass Minderjährige auf dem Parkplatz ältere Kunden angesprochen haben mit der Bitte, für sie eine DVD FSK 18 käuflich zu erwerben. Diese schriftlichen Hinweise wurden grundsätzlich nach 3 Tagen durch einen Reißwolf vernichtet.

- **Abgabe des Personaldokumentes beim Betreten eines Industrieparks**

Der Beschwerdeführer gab an, dass er dem Wachpersonal vor dem Betreten des Geländes sein Personaldokument aushändigen sollte, dafür wurde ein Besucher−ausweis ausgeteilt. Beim Verlassen des Geländes wurde dann der Personalausweis wieder übergeben. Der Petent fühlte sich durch diese Maßnahme in seiner Persön−lichkeit eingeschränkt.
Aus der Stellungnahme des Industrieparks wurde jedoch deutlich, dass diese Maßnahme auf Sicherheitsüberlegungen beruhte. Es werden dort Explosivstoffe gelagert und vernichtet. Obwohl man für die Sicherheit der Mitarbeiter und der Be−sucher alles getan hat, ereignete sich 2002 ein schwerer Unfall, bei dem auch Menschenleben zu beklagen waren. Nach diesem Ereignis war erst einmal das Wichtigste, festzustellen, wo sich Besucher und eigene Mitarbeiter befanden und dass diese unverletzt waren.
In Auswertung dieser Erkenntnisse wurde auf der Grundlage des Hausrechts die Verfahrensweise bei der Objektwache geändert. Diese ist in Räumen untergebracht, zu denen nur der im Dienst befindliche Wachmann Zutritt hat.
Der Personalausweis wird für die Zeit des Besuches auf der Wache hinterlegt, mit der Absicht, im Notfall eine sofortige Übersicht über die auf dem Gelände befindli−chen Personen zu haben. Ferner werden vom Wachmann Datum, Name, Vorname, Geburtsdatum , Firma bzw. Institution, Besuchsgrund, Uhrzeit Besuchbeginn und Urzeit Besuchende im Besucherbuch vorgenommen. Eine missbräuchliche Nutzung der personenbezogenen Daten ist ausgeschlossen.
Bei Besuchende bekommt der Besucher seinen Personalausweis zurück und gibt den Besucherausweis an der Wache ab.

Die Verfahrensweise der Eintragung im Besucherbuch wurde seitens der Auf−sichtsbehörde nicht beanstandet. Es handelt sich hierbei um kein automatisiertes Verfahren und keine Verarbeitung mittels einer nicht−automatisierten Datei. Ein Verstoß gegen § 4 Personalausweisgesetz (PersAuswG) liegt demnach hier nicht vor.

- **Gruppensterbegeldversicherungsangebot über einen Verband**

Eine Petentin schilderte in ihrem Anliegen, dass sie von Vertretern einer Versicherung aufgesucht wurde und man ihr ein Angebot zu einer Gruppensterbegeldversicherung überreicht hätte. Zum Erstaunen der Beschwerdeführerin verfügten die Vertreter bereits über ihre personenbezogenen Daten.

Der Verband hatte gemeinsam mit einer Versicherung seine Mitglieder angeschrieben und eine Sterbegeld- und Unfallversicherung für die Mitglieder des Landesverbandes und deren Ehegatten angeboten. Es wurde den Mitgliedern auch mitgeteilt, welche Kosten bei einem Begräbnis entstehen und was dann auf die Angehörigen zukomme. Es lohne sich deshalb Vorsorge zu treffen. Diese "Sterbegeldversicherung" biete eine günstige Gelegenheit.
Gleichzeitig teilte man mit, dass bei einer solchen Versicherung anfallende Überschussanteile gespendet werden könnten. Beim Beitritt zu einer Gruppenversicherung würde keine Spende notwendig werden.

In den Stellungnahmen des Verbandes und des Versicherungsunternehmens kam zum Ausdruck, dass die Mitglieder im Vorfeld in der "Verbandszeitung" über die bestehenden Vereinbarungen informiert wurden. In dem speziellen Fall wurde darüber hinaus ein Informationsblatt im Schaukasten des Vereins ausgehängt. Widersprüche zur Übermittlung der personenbezogenen Daten seien listenmäßig erfasst worden.
Abschließend konnte der Beschwerdeführerin mitgeteilt werden, dass die Datenübermittlung in diesem Fall nach § 28 BDSG zu beurteilen sei. Danach ist die Übermittlung personenbezogener Daten zulässig, soweit sie zur Wahrung berechtigter Interessen der übermittelnden Stelle oder eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung überwiegt. Dies war hier nicht der Fall.

Datenschutzrechtlich problematisch wäre die Mitteilung von Daten aus dem persönlichen Lebensbereich der Mitglieder (etwa Angaben über runde Geburtstage, Eheschließungen, Geburt von Kindern, Abschluss von Schul- oder Berufsausbildungen). Bei der Übermittlung solcher Daten ist Zurückhaltung geboten.

Zusammenfassend gilt, dass die Verarbeitung personenbezogener Daten im Verein dem BDSG unterliegt. Ein Verein darf beim Vereinsbeitritt (Aufnahmeantrag oder Beitrittserklärung) und während der Vereinsmitgliedschaft nur solche Daten von Mitgliedern erheben, die er auch verarbeiten oder nutzen darf und hat sich dabei unter Beachtung des Grundsatzes der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) grundsätzlich auf Daten zu beschränken, die im Rahmen des Vereinszwecks liegen.

In der Praxis ergeben sich bei Vereinen häufig Probleme mit der Weitergabe von Mitgliederdaten an Versicherungsunternehmen oder Versicherungsvertreter im Rahmen von Gruppenversicherungsverträgen, da diese nicht vom Vereinsrecht umfasst wird. Dabei handelt es sich um Rahmenverträge zwischen Vereinen und Versicherungsunternehmen, die den Vereinsmitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen. Nach den zwischen den Datenschutzaufsichtsbehörden und den Verbänden der Versicherungswirtschaft getroffenen Absprachen darf ein Verein im Rahmen eines Gruppenversicherungsvertrages dem Versicherungsunternehmen bzw. dem Versicherungsvertreter die Daten seiner Mitglieder nur unter folgenden Voraussetzungen übermitteln:

- Bei **Neumitgliedern**, die nach Abschluss des Gruppenversicherungsvertrages dem Verein beitreten, muss die Einwilligung eingeholt werden. Dies sollte zweckmäßigerweise in der Beitrittserklärung oder im Aufnahmeantrag vorgesehen werden, wobei das Mitglied darüber aufzuklären ist, welche Daten an welches Unternehmen weitergegeben werden sollen.
- Bei **Altmitgliedern**, die bei Abschluss des Gruppenversicherungsvertrages bereits Vereinsmitglied waren, genügt es, wenn der Verein sie vor der Übermittlung ihres Namens und ihrer Anschrift an die Versicherung in einem Schreiben informiert und ihnen den Besuch eines Versicherungsvertreters ankündigt. In dem Schreiben muss auf die Möglichkeit des Widerspruchs gegen die Datenübermittlung und den Vertreterbesuch hingewiesen und dem Vereinsmitglied ausreichend Zeit eingeräumt werden, von dieser Widerspruchsmöglichkeit Gebrauch zu machen.

− Rechnungserstellung eines Krankenhauses

Eine Petentin hat sich mit dem Problem an die Aufsichtsbehörde gewandt, dass sie nach einer Behandlung eines Familienangehörigen im Krankenhaus die Rechnung per Post erhalten hat. Auf dem Briefumschlag waren im Sichtfenster neben der Adresse auch die Informationen "Rechnung" sowie der Name des Patienten sichtbar.

Auch die Information, dass ein Patientenverhältnis besteht, stellt eine vom Bundesdatenschutzgesetz (BDSG) geschütztes Datum dar, dessen Offenbarung nur unter sehr eingeschränkten Voraussetzungen zulässig ist. Das Krankenhaus wurde zu dieser Problematik um Stellungnahme gebeten.
Dort wurde der Sachverhalt geprüft und dabei festgestellt, dass durch ein Update des Rechnungsprogramms die Abstände zwischen den Zeilen automatisch verkleinert wurden. Da die Rechnungen maschinell erstellt würden, hätte es in den Händen der Mitarbeiter/innen der Patientenverwaltung gelegen, durch entsprechende Faltung des Briefes nur die Adresse des Empfängers im Fenster des Briefumschlages sichtbar zu machen. Da es hierbei zu Fehlern gekommen sei, habe man nun die Maske des Rechnungsprogramms umgestaltet und die Zeilenabstände vergrößert. Bei einfacher und ordnungsgemäßer Faltung würde dieser Fehler nicht mehr auftreten. Darüber hinaus seien alle Mitarbeiter/innen, die den Postversand veranlassen, angewiesen worden, die ausgehende Post auf Unkorrektheiten zu kontrollieren. Die Mitarbeiter/innen seien auf die Brisanz der Thematik hingewiesen worden.

Im Krankenhaus wurde offenbar das Notwendige veranlasst, um derartige Fehler zukünftig zu vermeiden. Aus der Sicht der Aufsichtsbehörde wurde daher kein weiterer Handlungsbedarf gesehen.

− Beschwerden und Anfragen bezüglich eBay

- SCHUFA−Abgleich zum Zweck der Identifikation

Mehrere Anfragen bzw. Beschwerden bezogen sich im Berichtszeitraum auf die Identifikation der Mitglieder durch einen SCHUFA−Abgleich.

Zur Identifizierung der Mitglieder führt eBay bei allen Anmeldungen einen Daten−abgleich mit der SCHUFA durch. Nur in den Fällen, in denen von den zukünftigen Mitgliedern E−Mail−Adressen verwendet werden, deren Anbieter selbst ein "starkes" Authentifizierungsverfahren durchführen, erfolgt eine solche Abfrage nicht. Diese Anbieter befinden sich auf einer sogenannten White−List. eBay verlässt sich in diesen Fällen auf das von den entsprechenden Anbietern durchgeführte Authentifi−zierungsverfahren.

Bei der Identifizierung durch die SCHUFA übermittelt eBay die Angaben, die das Mitglied im Anmeldeformular macht, an die SCHUFA. Diese Daten umfassen den Vor− und Nach−namen, Straße und Hausnummer, Postleitzahl und Ort sowie das Geburtsdatum. Diese von eBay übermittelten Daten werden nicht von der SCHUFA gespeichert oder genutzt.

Nur wenn persönliche Daten des Mitglieds bereits bei der SCHUFA gespeichert sind, ergänzt die SCHUFA den vorhandenen Datensatz um die Information, dass eine Anfrage von eBay beantwortet wurde. Die SCHUFA ist hierzu gesetzlich verpflichtet, da sie den eBay−Mit−gliedern gemäß § 34 Abs. 1 Nr. 2 BDSG gegebenenfalls mitteilen muss, an wen sie Aus−künfte über die betroffene Person erteilt hat. eBay nutzt die SCHUFA−Prüfung jedoch nicht, um die Kreditwürdigkeit zukünftiger Mitglieder abzufragen oder andere Auskünfte über de−ren finanzielle Situation einzuholen.

Gegen dieses Identifizierungsverfahren bestehen seitens der Aufsichtsbehörde keine Beden−ken. Im Zusammenhang mit dem Ansteigen der Fälle, in denen unter der Nutzung fremder Identitäten in betrügerischer Absicht Handel auf eBay betrieben wird, muss jedoch die Frage gestellt werden, ob dieses Verfahren die höchst mögliche Sicherheit bietet. Dieser Frage wird die Aufsichtsbehörde in der Zukunft vor dem Hintergrund des Grundsatzes der Verhältnis−mäßigkeit nachgehen.

- Einwilligungserklärung der Mitglieder

Weitere Anfragen erfolgten im Zusammenhang mit einer Änderung der Allgemeinen Geschäftsbedingungen von eBay und der damit verbunden Einwilligungserklärung in die Verarbeitung der personenbezogenen Daten. In dieser Erklärung heißt es u.a.

" Ich willige ein, dass

- die eBay International AG, Bubenbergplatz 5, CH−3011 Bern, Schweiz, meine personenbezogenen Daten erhebt und an die eBay Inc., 2145 Hamilton Avenue, San Jose 95125, USA, übermittelt.
- die eBay Inc., die eBay International AG und die eBay GmbH, Markt−platz 1, D−14532 Europarc Dreilinden, (im Folgenden zusammen als "eBay" bezeichnet) die bei der eBay Inc. gespeicherten Daten für die Begründung, Durchführung und Abwicklung meines Nutzungsver−hältnisses mit der eBay International AG verarbeiten und nutzen.
- andere eBay−Gesellschaften, wie die Betreiber weiterer eBay−Websi−tes (z.B. eBay.com, eBay.co.uk), die bei der eBay Inc. gespeicherten Daten für die Durchführung und Abwicklung meines Nutzungsver−hältnisses mit der eBay International AG verarbeiten und nutzen. ...
- Personenbezogene Daten sind Bestandsdaten, wie beispielsweise Name und Adresse sowie Nutzungsdaten wie beispielsweise Mit−gliedsname, Kennwort und IP−Adresse. ..."

Die Anfragen richteten sich darauf, ob es zulässig sei, dass eBay die Daten in die USA übermittelt.
Da die Datenübermittlung in die USA auf der Einwilligung der Mitglieder beruhen, bestehen gegen ebendiese Übermittlungen keine Bedenken.

- Vorratsspeicherung durch eBay?

Ein Petent wies auf einen möglichen Verstoß von eBay Deutschland gegen § 3 Abs. 4 Teledienstedatenschutzgesetz und das daraus resultierende sogenannte Kopp−lungsverbot hin. Die von eBay verlangte Einwilligung erstrecke sich nicht nur auf die Datenverarbeitung, die zur Abwicklung von Käufen/Verkäufen erforderlich ist, son−dern decke unbeschränkt die Speicherung personenbezogener Daten in den USA ab, also auch die Speicherung zu anderen Zwecken als zur Erbringung der ange−botenen Teledienste. So speichere eBay Nutzungsdaten auf Vorrat, um bei dem bloßen Verdacht eines Verstoßes gegen die eBay−AGB das gesamte Verhalten des

Nutzers in der Vergangenheit nachvollziehen zu können. Bei der Speicherung von Nutzungsdaten über den Abschluss einer Transaktion (Kauf/Verkauf) hinaus handele es sich um eine Speicherung für andere Zwecke als für die Erbringung der Teledienste, weil der Teledienst nach Abschluss einer Transaktion (Kauf/Verkauf) bereits erbracht ist.

Es ist richtig, dass sich die Datenverarbeitung der Teleddiensteanbieter nach dem Grundsatz der Zweckbindung zu richten hat. Die Daten der Kunden dürfen nur insoweit verwendet werden, wie ein gesetzlicher Erlaubnistatbestand existiert oder der Betroffene eingewilligt hat. Dieser Grundsatz wird noch um das Koppelungsverbot erweitert.
Die Nutzung der Teledienste der eBay−Website setzt die Anmeldung als Mitglied voraus. Sie erfolgt durch Eröffnung eines Mitgliedskontos unter Zustimmung u.a. zu den AGB. Mit der Anmeldung kommt zwischen eBay und dem Mitglied ein Vertrag über die Nutzung der eBay−Website zustande. eBay fragt dazu Bestands− und Nutzungsdaten ab.

Bestandsdaten, die zum Teil auch als Vertragsdaten bezeichnet werden, sind die personenbezogenen Daten, die erforderlich sind, um ein Vertragsverhältnis über Teledienste zu begründen, inhaltlich auszugestalten oder zu ändern. Diese Daten dürfen nur zu den Zwecken genutzt werden, die in den gesetzlichen Regelungen als zulässige Zwecke normiert sind oder zu denen der Benutzer eingewilligt hat. Die Bestandsdaten dürfen zunächst zur Aufnahme und Änderung des zwischen Diensteanbieter und Kunden bestehenden Vertragsverhältnisses verwendet werden. Dieser Zweck ist als selbstverständlich zu bezeichnen, denn ohne die Erhebung der Bestandsdaten zu diesem Zweck ist nur schwerlich ein Vertragsverhältnis mit nachträglicher Abrechnung vorstellbar, denn jeder Diensteanbieter braucht diese Daten, um später seine Leistungen abzurechnen und seinen Anspruch auf die Rechnungsbeträge durchzusetzen.

Nutzungsdaten sind die Daten, die benötigt werden, um dem Nutzer die Inanspruchnahme von Telediensten zu ermöglichen. Zu den Nutzungsdaten zählen alle Daten die bei der Nutzung anfallen, wie Name oder Pseudonym des Nutzers, Zeit−

punkt und Dauer der Nutzung sowie Passwörter und Zugangscodes. Auch für die Nutzung der Nutzungsdaten gilt das Prinzip der Zweckbindung. Die Daten dürfen nur für gesetzlich geregelte Zwecke benutzt werden. Einziger gesetzlich geregelter legitimer Zweck ist die Verarbeitung, um die Nutzung des Teledienstes zu ermöglichen. Die Nutzungsdaten dürfen ferner, soweit sie der Abrechnung dienen, für die Abrechnung verwendet werden.

Für das Anbieten von Artikeln erhebt eBay von dem Anbieter eine Angebotsgebühr. Für zusätzliche Leistungen von eBay, insbesondere für die Hervorhebung einzelner Angebote, hat der Anbieter Zusatzgebühren zu zahlen. Kommt es über die eBay−Website zum Abschluss eines Vertrags mit einem anderen Mitglied, fällt zugunsten von eBay eine Provision an, die von dem Anbieter zu begleichen ist.

Die Speicherung von Bestands− und Nutzungsdaten in den USA − beim Hauptsitz des Unternehmens −erscheint aus den oben dargelegten Gründen legitim und zweckentsprechend.

Das Kopplungsverbot besagt ferner, dass der Zugang zu einem Angebot im Internet nicht von der Erteilung der Einwilligung zur Verwendung persönlicher Daten des Nutzers für einen anderen Zweck abhängig gemacht werden darf, wenn dem Nutzer der Zugang zu dem konkreten Dienst anders nicht möglich ist.

Auch ein Verstoß gegen das Kopplungsverbot konnte in diesem Fall nicht festgestellt werden, da die personenbezogenen Daten zur Erbringung der Dienstleistung und nachträglichen Abrechung, also nicht für einen anderen Zweck, auf dem Server von eBay verarbeitet werden.

4. Zusammenarbeit mit den Datenschutzaufsichtsbehörden der Länder

4.1 Besondere Beratungsthemen des Düsseldorfer Kreises

Im Berichtszeitraum fanden zwei Sitzungen des Düsseldorfer Kreises statt. Unter anderem wurde dort die Zulässigkeit des Einsatzes von Webcams in gastronomischen Einrichtungen erörtert.

Unter den Aufsichtsbehörden bestand dahingehend Einigkeit, dass diese nicht auf § 6b BDSG als gesetzliche Rechtsgrundlage gestützt werden kann. Wegen der Veröffentlichung der Bilder im Internet überwiegen hier schutzwürdige Belange der betroffenen Personen ein angenommenes wirtschaftliches Interesse des Betreibers einer gastronomischen Einrichtung an der Veröffentlichung der Bilder.
Die Installation von Webcams und eine Übertragung der Bilder ins Internet ist daher nur mit einer Einwilligung der Gäste zulässig. Diese Einwilligung kann grundsätzlich auch konkludent erfolgen. Dies ist dann der Fall, wenn beim Betreten des Restaurants ein deutlich sichtbarer Hinweis auf die Aufnahme des Restaurantbetriebes und die Veröffentlichung dieser Bilder im Internet angebracht ist.
Mehrheitlich ist der Düsseldorfer Kreis nicht der Auffassung, dass innerhalb des gastronomischen Bereichs eine Aufenthaltsfläche angeboten werden muss, die nicht webcamüberwacht ist. Allerdings wird in den Fällen, in denen der Besuch als so genanntes sensitives Datum zu werden ist (z.B. beim Besuch einer einschlägigen Szenebar), eine schriftliche Einwilligung für erforderlich gehalten.

4.2 Arbeitgruppe "Auskunfteien"

Im Jahr 2003 trat die Arbeitsgruppe zwei mal zusammen. In der Sitzung im März in Wiesbaden wurden Themen besprochen, die sich speziell auf die SCHUFA bezogen. Im September in Potsdam wurden mit dem Verband der Handelsauskunfteien Themen besprochen, die in diesem Wirtschaftszweig von Bedeutung sind.

4.2.1 SCHUFA

− Widerspruch gegen die Übermittlung des SCHUFA−Scores
In der Vergangenheit wurde mit der SCHUFA das Scoreverfahren und die Mög−lichkeit, der Übermittlung des Score−Wertes an Dritte zu widersprechen, erörtert. In den Fällen, in denen der Betroffene einer Übermittlung des Score−Wertes wider−sprochen hat, sollte der anfragende Vertragspartner die Information: "Über die an−gefragte Person erfolgt keine Score−Wertermittlung" erhalten.

Demgegenüber wurde jedoch in diesen Fällen der folgende Text übermittelt:
"Betroffener widerspricht Scoreberechnung. Über angefragte Person erfolgt keine Scoreermittlung."
Die SCHUFA erklärte, dass die Angabe "Betroffener widerspricht Scoreermittlung" zum einen der Erklärung für den Vertragspartner diene. Zum anderen erscheine dieser Text auch in einer Selbstauskunft, um gegenüber dem Betroffenen zu bele−gen, dass sein Widerspruch beachtet werde.

Die Mitglieder der Arbeitsgruppe haben gegen die Übermittlung des Filtertextes "Betroffener widerspricht Scoreermittlung" Bedenken erhoben. Dieser Hinweis kann für den Betroffenen nachteilig wirken, ohne dass der Vertragspartner ein berechtig−tes Interesse am Erhalt dieser Information hat.

Die Vertreter der SCHUFA sagten zu, auf die Übermittlung des Filtertextes "Betrof−fener widerspricht Scoreermittlung" verzichten zu wollen. Für die Selbstauskunft werde man einen geeigneten Weg suchen, den Betroffenen über die Beachtung seines Widerspruches zu informieren.

4.2.2 sonstige Auskunftei−Themen

Auch in diesem Berichtszeitraum hatte sich die Arbeitsgruppe mit der Problematik der ungekennzeichneten Übermittlung von Schätzdaten zu beschäftigen. Nachdem im Jahr 2002 die Vereinbarung getroffen wurde, dass jedes einzelne geschätzte Datum mit einem (*) als solches gekennzeichnet werden sollte, rückte der Verband

im Berichtszeitraum hiervon wieder ab. Nunmehr wurde in der Arbeitsgruppe der Vorschlag unterbreitet, dass in jeder Auskunft der folgende Text deutlich sichtbar zu integrieren sei:

" Bei den in den Auskünften enthaltenen Unternehmenszahlen kann es sich teil−weise um auf Basis von Branchendurchschnittswerten geschätzte Angaben han−deln."

Diesem Kompromiss wurde seitens der Arbeitsgruppe als Mindestanforderung an die Kennzeichnung von Schätzdaten zugestimmt und mit dem Hinweis verbunden, dass eine entsprechende Musterauskunft zeitnah mit den Aufsichtsbehörden ab−gestimmt wird. Stattdessen hat der Verband jedoch eine Stellungnahme übermittelt, in der auch von diesem Kompromiss wieder abrückt und geringere Anforderungen für die Kennzeichnung vereinbart werden sollen.

Die Gespräche mit dem Verband der Handelsauskunfteien bezüglich der Handha−bung der Übermittlung von Schätzdaten reichen bereits in das Jahr 2000 zurück. Während dieser Zeit hat die Arbeitsgruppe die von ihr als rechtswidrig eingeschätzte Praxis der ungekennzeichneten Übermittlung von Schätzdaten[7] im Interesse eines mit den Vertretern der Wirtschaft abgestimmten Verfahrens toleriert. Die Arbeits−gruppe Auskunfteien, in der Brandenburg den Vorsitz für die alle Auskunfteien − mit Ausnahme der SCHUFA − betreffenden Fragen führt, wird diese Frage abschlie−ßend im Jahr 2004 klären. Möglicherweise wird von der bisherigen Linie der Ar−beitsgruppe abgerückt werden müssen, einvernehmlich Lösungen mit der Wirtschaft zu finden.

4.3 Arbeitsgruppe "Internationaler Datenverkehr"

Die Arbeitsgruppe "Internationaler Datenverkehr" trat im Berichtszeitraum zwei mal zusammen. Auch im Jahr 2003 stand im Mittelpunkt der Arbeit die Bewertung ver−bindlicher Unternehmensregeln, die ausreichende Garantien für den Schutz der

[7] Diese Auffassung wird auch durch ein entsprechendes Urteil des OLG Hamm, NVwz 2001, 235 f. gestützt.

Grundrechte von Personen bei internationalen Datenübermittlungen in Länder ohne angemessenes Datenschutzniveau bieten sollen (§ 4c Abs. 2 BDSG).

In diesem Zusammenhang stand auch die Diskussion in der Arbeitsgruppe, ob beim Vorliegen von verbindlichen Unternehmensregeln davon auszugehen ist, dass ein angemessenes Datenschutzniveau vorliegt, mit der Folge, dass für etwaige Daten−übermittlungen kein Genehmigungserfordernis besteht. Diese Problematik wird un−ter den Aufsichtsbehörden unterschiedlich gesehen.

Einige sprechen sich dafür aus, dass verbindliche Unternehmensregeln ein ange−messenes Datenschutzniveau bei der empfangenden Stelle gewährleisten können. In diesen Fällen wäre eine Datenübermittlung bereits nach § 4b Abs. 2 BDSG zu−lässig und eine Genehmigung nicht erforderlich.

Dagegen spricht jedoch, dass § 4c Abs. 2 BDSG explizit die verbindlichen Unter−nehmensregeln nennt, die die für eine Genehmigung erforderlichen ausreichenden Garantien bieten können. Weiterhin kann unter Berücksichtigung der Art. 25 und 26 der EG−Datenschutzrichtlinie ein angemessenes Datenschutzniveau i.S.v. § 4b Abs. 2 und 3 BDSG nur dann angenommen werden, wenn es durch einen allgemeinen rechtlichen Rahmen gewährleistet wird. Gesetzliche Regelungen und vertragliche Abmachungen dürfen jedoch nicht auf eine Stufe gestellt werden.[8]

Aus der Sicht des Innenministeriums Brandenburg ist von einem angemessenen Datenschutzniveau i.S.v. § 4b Abs. 2 und 3 BDSG nur dann auszugehen, wenn es durch einen allgemeinen gesetzlichen Rahmen gewährleistet wird, der auf die kon−krete Übermittlung anzuwenden ist. Verbindliche Unternehmensregeln können demgegenüber ausreichende Garantien für den Schutz der Persönlichkeitsrechte und der Ausübung der damit verbundenen Rechte der betroffenen Personen bieten. Auf der Grundlage derartiger Unternehmensregeln können Datenübermittlungen genehmigt werden (§ 4c Abs. 2 BDSG).

[8] Dammann; Simitis: EG Datenschutzrichtlinie Kommentar, a.a.O., S. 77 f.

4.4 AG Tele− und Mediendienste

Im Berichtszeitraum fand im April eine Sitzung der Arbeitsgruppe "Telekommunikation, Tele− und Mediendienste" in Berlin statt. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist der Vorsitzende dieser Arbeitsgruppe. An der Sitzung nahm ein Vertreter der Aufsichtsbehörde aus Brandenburg teil.

Im Vordergrund der Sitzung standen Anwendungsprobleme des Teledienstegesetzes (TDG) und Teledienstedatenschutzgesetzes (TDDSG) sowie des Mediendienste−Staatsvertrages (MDStV). So wurde z.B. über die Speicherung von IP−Adressen von P2P−Nutzern durch Access−Provider, über die Zulässigkeit der Speicherung von Nutzungsdaten sowie über die Abgrenzung von Inhalts− (BDSG) und Dienstebene (TDDSG/MDStV) diskutiert.

Ferner wurde über die Entwicklung von rechtlichen Grundlagen wie das Telekommunikationsgesetz (TKG) berichtet.

Anlage

Datenschutz in der Arztpraxis − Selbst−Check

1. Empfang

Wird durch eine ausreichende Diskretionszone oder durch organisatorische Maß−nahmen sichergestellt, dass die Patientinnen und Patienten ihre Anliegen schildern können, ohne dass neugierige Ohren mithören können?

Werden die Daten der Patienten (Anschrift, Kassenart, Grund des Besuchs...) so erhoben, dass Unbefugte nicht mithören können?

Kann das Personal Telefongespräche führen, ohne dass wartende Patientinnen und Patienten dadurch von Daten anderer Personen Kenntnis erlangen?

Sind Telefaxgeräte und Bildschirme so aufgestellt, dass diese nicht von Unbefugten eingesehen werden können?

Sind Patientenakten und Karteikarten vor dem Zugriff Unbefugter geschützt?

Wird die Patientin bzw. der Patient darauf hingewiesen, dass er einen Anamnese−bogen auf freiwilliger Basis individuell ausfüllen kann?

2. Wartebereich

Ist der Wartebereich vom Empfang und dem Behandlungsbereich so getrennt, dass wartende Patienten nicht unbefugt Kenntnis von Patientendaten erhalten?

3. Behandlungsbereich

Können Behandlungsräume so abgeschottet werden, dass neugierige Augen und Ohren ausgeschlossen werden?

Erfolgen vertrauliche Arzt−Patienten−Gespräche in geschlossenen Räumen?

Sind Patientendaten in den Behandlungsräumen gegen unbefugte Kenntnisnahme geschützt?

4. EDV

Ist der Zugang zum Computer durch ein Passwort geschützt?

Entspricht das Passwort dem aktuellen Sicherheitsstandard (8 Stellen, bestehend aus Buchstaben, Zahlen und Sonderzeichen)?

Ist vorgesehen, dass das Passwort nach einer gewissen Zeit geändert werden muss (Alterung)?

Ist ein passwortgeschützter Bildschirmschoner aktiviert?

Kennt nur das befugte Personal dieses Passwort?

Sind Computer mit Patientendaten, die mit dem Internet verbunden sind, tatsächlich ausreichend geschützt ("firewall")?

Wird regelmäßig eine Sicherungskopie der Daten gefertigt (möglichst jeden Tag, mindestens einmal die Woche)?

Bietet Ihre Praxis−Software die Möglichkeit, Patientendaten verschlüsselt zu spei−chern?

Wird das Patientengeheimnis beachtet, wenn Systemverwaltung und Wartung der EDV durch externe Stellen erfolgt (siehe auch Mitteilung in: Deutsches Ärzteblatt 93, Heft 43, 25.10.1996 −91, A−2809 ff.)?

5. Patientenrechte

Werden Patienten auf Wunsch über ihre Datenschutzrechte informiert?

Sind Sie darauf vorbereitet, was zu veranlassen ist, wenn ein Patient von seinem Recht auf Einsicht in die objektiven Aufzeichnungen zu seiner Person Gebrauch macht und/oder Kopien aus der Patientenakte verlangt?

Ist Ihnen bekannt, dass Patientendaten nach 30 Jahren zu löschen sind, unter be−stimmten Voraussetzungen, so auf Wunsch des Patienten, auch schon nach 10 Jahren (im letzteren Fall unter Umkehr der Beweispflicht zu Lasten des Patienten)?

6. Datenübermittlung

Achten Sie darauf, dass bei der Übermittlung von Patientendaten die Empfänger nicht mehr Informationen erhalten, als diese zur Erfüllung ihrer spezifischen Auf−gaben benötigen?

Prüfen Sie, bevor Sie Anfragen von Dritten direkt beantworten, ob die Auskünfte, Berichte oder Bescheinigungen nicht auch über den Patienten schriftlich weiterge−geben werden können?

Achten Sie darauf, dass Privatärztliche Verrechnungsstellen nur rechtswirksam beauftragt werden, wenn die Patientin bzw. der Patient zuvor schriftlich eingewilligt hat?

Benutzen Sie (geprüfte) Mustererklärungen zur Entbindung von der ärztlichen

Schweigepflicht, die dem Patienten hinreichend erkennbar machen, welche Daten für welche Zwecke an welche Empfänger weitergegeben werden sollen (siehe Muster der Ärztekammer bzw. Zahnärztekammer)?

Können Sie gesetzlich Krankenversicherten auf Anfrage Auskunft geben, welche Daten für welche Zwecke an die Kassen(zahn)ärztliche Vereinigung weitergegeben werden?

Haben Sie sichergestellt, dass in Ihrer Praxis bei Zweifeln über die Zulässigkeit vor der Übermittlung von Patientendaten eine rechtliche Klärung erfolgt (z.B. über einen Anwalt, die Zahn−/Ärztekammer oder die Aufsichtsbehörde)?

Informieren Sie die Patienten über mit− und nachbehandelnde Ärzte (auch Labor−ärzte) und vergewissern Sie sich, dass die Patienten keine Einwände gegen deren Einbeziehung und mit deren Unterrichtung über Behandlungsergebnisse haben?

7. Praxisverwaltung

Sind Karteikarten und Patientenakten vor dem Zugriff Unbefugter geschützt?

Werden Karteikarten etc. am Empfang oder in den Behandlungsräumen ohne ent−sprechende Aufsicht bereit gelegt?

Sind abschließbare Aktenschränke vorhanden? Werden diese nach Dienstschluss verschlossen?

Haben Sie daran gedacht, Ihre Praxis, insbesondere die Räume, in denen sich Pa−tientendaten/Ab−rechnungsdaten befinden, ausreichend gegen Einbruch zu schüt−zen?

Ist sichergestellt, dass das Reinigungspersonal keinen Zugang zu Patientendaten hat?

Ist die Aufbewahrung von "alten Akten" sicher organisiert (kein "offener Keller")?

Wie erfolgt eine sichere Vernichtung von Patientendaten (keine Daten in den Hausmüll)?

Wird bei der Versendung von Patientendaten per Fax sichergestellt, dass aus−schließlich berechtigte Dritte beim Empfänger Kenntnis von diesem Fax erhalten (z.B. Ankündigung beim Empfänger, regelmäßige Kontrolle von programmierten Nummern)?

Sind Mitarbeiterinnen und Mitarbeiter über ihre Befugnisse und gesetzlichen Pflich−ten bei der Wahrung der Schweigepflicht ausreichend (schriftlich) informiert?