Landesamt für Datenschutzaufsicht
in der Regierung von Mittelfranken

3. Tätigkeitsbericht

2008

Impressum

Herausgeber:

Landesamt für Datenschutzaufsicht
in der Regierung von Mittelfranken
Promenade 27
91522 Ansbach

Telefon: (0981) 53-1301
Telefax: (0981) 53-5301
E-Mail: datenschutz@reg-mfr.bayern.de

Dieser Tätigkeitsbericht kann auch unter
www.regierung.mittelfranken.bayern.de abgerufen werden.

Vorwort

Der 3. Tätigkeitsbericht der Bayerischen Datenschutzaufsichtsbehörde für den nichtöffentlichen Bereich erscheint in einer Zeit, in der der Datenschutz offensichtlich Hochkonjunktur hat. Damit soll nicht gesagt sein, dass die Verantwortlichen in den Wirtschaftsunternehmen und den sonstigen datenverarbeitenden Stellen dem Datenschutz stets besondere Beachtung schenken bzw. geschenkt haben. Die zahlreichen, in den vergangenen 12 Monaten publik gemachten Skandale und Verfehlungen weisen eher auf das Gegenteil hin.

Bei allem Unverständnis darüber, wie sorglos, man kann auch sagen eigenmächtig und rechtswidrig zuweilen mit den Daten anderer Menschen umgegangen wird, haben die vielen Negativschlagzeilen auch eine positive Wirkung gehabt. Der Datenschutz ist in den Focus des öffentlichen Interesses und der Medien gerückt. Die ständige Thematisierung hat ihn aus einem Schattendasein herausgeholt und ihm einen Stellenwert in der öffentlichen Diskussion und Wahrnehmung verliehen, wie er ihn seit dem Erlass des Bundesdatenschutzgesetzes im Jahr 1977 wohl noch nie hatte.

Bei der Datenschutzaufsicht machte sich diese neue Entwicklung dadurch bemerkbar, dass die Anfragen und Beratungen sowohl von Bürgerinnen und Bürgern als auch von Unternehmen im Jahr 2008 sprunghaft gestiegen sind. Auch in den Unternehmen wird den Anliegen der betrieblichen Datenschutzbeauftragten plötzlich mehr Aufmerksamkeit geschenkt als dies vorher der Fall war. Es scheint, als ob ein Ruck durch die Unternehmen gegangen ist. Viele sind sich ihrer Verantwortung und des Risikos datenschutzwidrigen Verhaltens für ihren wirtschaftlichen Erfolg wohl erst jetzt so richtig bewusst geworden. Der Datenschutz wird vermehrt als Qualitätsmerkmal erkannt.

Der vorliegende Bericht beschäftigt sich weniger mit Skandalen als vielmehr mit einzelnen Datenschutzverstößen und -problemen, die uns bekannt geworden sind. Mit unseren rechtlichen Beurteilungen möchten wir einen Beitrag zu den allgemeinen Diskussionen über den Datenschutz leisten und dabei auch die Dimension der datenschutzrechtlichen Fragestellungen aufzeigen. Wir erhoffen uns damit eine weitere Sensibilisierung für den Datenschutz sowohl bei den Verantwortlichen als auch bei den Bürgerinnen und Bürgern.

Ansbach, im März 2009

Dr. Thomas Bauer
Regierungspräsident

Inhaltsverzeichnis

Wir bitten um Verständnis, dass wir wegen der leichteren Lesbarkeit des Tätigkeitsberichts im Rahmen von allgemeinen Ausführungen bei geschlechtsspezifischen Bezeichnungen nur die männliche Form verwendet haben.

1 Die Datenschutzaufsicht im nicht-öffentlichen Bereich im Freistaat Bayern

1.1 Organisation

Die Bayerische Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich ist im Jahr 2002 in der Regierung von Mittelfranken in Ansbach eingerichtet worden. Dort ist die Wahrnehmung der sich insbesondere aus § 38 Bundesdatenschutzgesetz (BDSG) ergebenden Aufgaben der dem Regierungspräsidenten unterstellten Stabsstelle „Datenschutzaufsicht“ (DSA) übertragen worden.

Gemäß Beschluss des Ministerrats vom 03.02.2009 wird diese Stabsstelle ab sofort zu einem in der Regierung von Mittelfranken eingerichteten „Landesamt für Datenschutzaufsicht“ ausgebaut und personell erheblich verstärkt.

Die Besetzung stellte sich am 01.02.2009 wie folgt dar:

Leiter	Ltd. Regierungsdirektor Dorn
Stv. Leiter	Oberregierungsrat Meier
	Regierungsrat Ilgenfritz
	Regierungsrätin z. A. Lang (ab Januar 2009)
	Regierungsamtmann Andörfer
	Regierungsoberinspektor Fromm
	Regierungsoberinspektorin Dierauff
	Beschäftigte Scheiderer (ab Januar 2009)

Die Überprüfungen hinsichtlich der Datensicherheit führt in Bayern der Technische Überwachungsverein (TÜV Süd) durch.

1.2 Örtliche Zuständigkeit

Sie ist gemäß Art. 3 Bayerisches Verwaltungsverfahrensgesetz gegeben, wenn sich der Sitz, eine Betriebsstätte, eine Zweigniederlassung oder die Geschäftsstelle der verantwortlichen Stelle, um deren Umgang mit personenbezogenen Daten es geht, in Bayern befindet.

1.3 Sachliche Zuständigkeit

Der Aufsicht unterliegen grundsätzlich die nicht-öffentlichen Stellen im Sinne des § 1 Abs. 2 Nr. 3 in Verbindung mit § 2 Abs. 4 Satz 1 bzw. § 27 Abs. 1 Satz 1 Nr. 1 BDSG, wenn sie Daten automatisiert oder unter Einsatz einer manuellen Datei verarbeiten, nutzen oder dafür erheben.

Ausnahmen bestehen insbesondere für Telekommunikations- und Postdienste sowie für die Presse und den Rundfunk.

1.4 Tätigkeitsbericht

Die gesetzliche Verpflichtung der Aufsichtsbehörden, Tätigkeitsberichte zu erstellen, ergibt sich aus § 38 Abs. 1 Satz 7 BDSG.

*** * ***

2 Die Verpflichtung auf das Datengeheimnis

Es geht hier um weitaus mehr als nur um die Wahrung eines Geheimnisses!

Mit der förmlichen Verpflichtung durch ihren Arbeitgeber müssen alle bei der Datenverarbeitung beschäftigten Personen auf den rechtmäßigen Umgang mit den personenbezogenen Daten regelrecht „eingeschworen werden".

Gemäß § 5 Satz 2 BDSG sind die mit der Datenverarbeitung bei nicht-öffentlichen Stellen beschäftigten Personen bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.

Die vom Arbeitgeber einseitig vorzunehmende förmliche Verpflichtung der mit der Datenverarbeitung beschäftigten Personen bezieht sich darauf, dass diese beim Umgang mit personenbezogenen Daten die Rechtsordnung, das heißt insbesondere das Datenschutzrecht, beachten und sich dabei im Rahmen des geschäftlichen Zweckes und der ihnen zugewiesenen Aufgaben halten (§ 5 Satz 1 BDSG). Es geht hier um weitaus mehr als um die bloße Wahrung eines Geheimnisses!

Die förmliche Verpflichtung auf das Datengeheimnis ist einer von zahlreichen Bausteinen, die das BDSG in sein formales Systemgebäude zur Gewährleistung des Schutzes der personenbezogenen Daten eingebaut hat. Diesem Zweck dienen unter anderem auch der betriebliche Datenschutzbeauftragte, die Aufstellung eines Verfahrensverzeichnisses, die Meldepflichten und die staatliche Datenschutzaufsicht.

Der Inhaber bzw. die Unternehmensleitung ist für die ordnungsgemäße Durchführung der Verpflichtung verantwortlich. Die Durchführung kann auch auf den betrieblichen Datenschutzbeauftragten übertragen werden.

Bei unseren Unternehmenskontrollen stellen wir immer wieder fest, dass diese förmlichen Verpflichtungen nicht dem Sinn und Zweck der gesetzlichen Vorschrift entsprechend durchgeführt werden. In vielen Fällen kommt die ihr zukommende große Bedeutung für die Mitarbeiter nicht zur Geltung. So reicht es zum Beispiel nicht aus, wenn

- der Arbeitnehmer am ersten Arbeitstag neben vielen anderen Unterschriften lediglich auch die Empfangsbestätigung eines die Verpflichtung auf das Datengeheimnis enthaltenden Formblattes unterschreibt,

- die gesetzliche (!) Verpflichtung auf das Datengeheimnis nur als eine von vielen weiteren Verpflichtungen des Arbeitnehmers im Arbeitsvertrag steht oder

- nur am schwarzen Brett oder in der Betriebszeitung veröffentlicht ist.

Die gegenüber dem Mitarbeiter auszusprechende Verpflichtung muss mehr als nur eine unter vielen Formalien sein. Schließlich muss der Mitarbeiter beim Umgang mit personenbezogenen Daten im Hinblick auf die Risiken und Gefahren für das Persönlichkeitsrecht der Betroffenen besondere Sorgfaltspflichten beachten. Darauf muss er „regelrecht eingeschworen werden". Nur so wird er dem Datenschutz von Anfang an die nötige Aufmerksamkeit entgegenbringen.

Dem Mitarbeiter muss durch die förmliche Verpflichtung auch bewusst werden, dass der unbefugte Umgang mit personenbezogenen Daten als Ordnungswidrigkeit oder als Straftat geahndet werden kann und dass sich daraus ggf. Schadensersatzpflichten und arbeitsrechtliche Konsequenzen bis hin zur Kündigung ergeben können.

Um diesen Anforderungen gerecht zu werden, sollte die Verpflichtung in persönlicher Form, ggf. gruppenweise, in der Form einer persönlichen Ansprache etwa nach folgendem Muster vorgenommen werden:

(1) Am Beginn steht eine kurze überschlägige Belehrung an Hand eines gut verständlichen Merkblattes über die Bedeutung des Datengeheimnisses und die wichtigsten Vorschriften des BDSG einschließlich der Bußgeld-, Straf- und Schadensersatzbestimmungen.

Das bloße Vorlesen des Textes des § 5 BDSG reicht nicht aus!

Der Inhalt der Belehrung ist für die zu verpflichtende Person am besten arbeitsplatzbezogen zu gestalten.

(2) Daran schließt sich die förmliche Verpflichtung mit den Worten an: „Ich verpflichte Sie hiermit auf das Datengeheimnis". Die Wirkung dieses Vorganges kann unterstrichen werden, indem die Verpflichtung mit einem Händedruck besiegelt wird.

(3) Die schriftliche Ausfertigung der Verpflichtung wird von dem, der die Verpflichtung vornimmt, unterschrieben.

(4) Die Unterschrift des Verpflichteten bezieht sich nur auf die Bestätigung der Durchführung der Verpflichtung und des Erhalts einer Ausfertigung und eines Merkblattes.

Verweigert er seine Unterschrift, ist die Verpflichtung dennoch wirksam. Zu empfehlen ist dann allerdings ein entsprechender Vermerk dessen, der die Verpflichtung durchgeführt hat.

(5) Die schriftliche Ausfertigung ist zum Personalakt zu nehmen. Die Zweitausfertigung bekommt die verpflichtete Person.

Mit der Einhaltung eines gewissen Rituals wird letzten Endes das verwirklicht, was der Gesetzgeber mit dem Verpflichtungsvorgang erreichen will: Der Datenschutz soll im Bewusstsein eines Mitarbeiters von Anfang an einen hohen Stellenwert bekommen, so dass er bei seiner Haupttätigkeit auch auf den rechtmäßigen Umgang mit personenbezogenen Daten größten Wert legt. Die Beachtung des Datenschutzes darf nicht etwas sein, das „nur eben mal so nebenbei erledigt wird“. Sie gehört vielmehr zu den wesentlichen Pflichten der Mitarbeiter.

Mit den eingangs genannten – nicht ausreichenden – Arten von Verpflichtungen auf das Datengeheimnis allein wird dieses Ziel nicht erreicht. Zwar ist es sehr zu begrüßen, wenn diese Verpflichtung noch zusätzlich in den Arbeitsvertrag oder in die Arbeitsordnung aufgenommen oder am schwarzen Brett ausgehängt wird oder wenn auf sie immer wieder einmal in der Betriebszeitung hingewiesen wird. Eine formgerechte Verpflichtung kann dadurch aber nicht ersetzt werden.

Zusätzlich zu der förmlichen Verpflichtung und der damit verbundenen ersten Belehrung bei der Aufnahme der Tätigkeit müssen in der Folgezeit je nach der Art der Tätigkeit weitere Schulungen im Datenschutz folgen. Nur so ist gewährleistet, dass die Mitarbeiter mit dem Datenschutzrecht in dem erforderlichen Umfang vertraut werden.

*** * ***

3 Der betriebliche Datenschutzbeauftragte

Maßnahmen bei einer langen Erkrankung eines betrieblichen Datenschutzbeauftragten

1. Kann ein Datenschutzbeauftragter sein Amt wegen langer Krankheit nicht ausüben, ist die verantwortliche Stelle zunächst verpflichtet, einen Vertreter zu bestellen.

   Bleibt die verantwortliche Stelle in diesem Fall untätig, kann dies gemäß § 43 Abs. 1 Nr. 2 BDSG mit einem Bußgeld geahndet werden. Da der Datenschutzbeauftragte objektiv außerstande ist, seine Funktion wahrzunehmen, liegt keine Bestellung vor und damit ist der Tatbestand der genannten Bußgeldvorschrift erfüllt (vgl. Gola/Schomerus Rn 6 zu § 43 BDSG).

2. Darüber hinaus muss die verantwortliche Stelle prüfen, ob sie die Bestellung des lange erkrankten Datenschutzbeauftragten gemäß § 4f Abs. 3 Satz 4 BDSG in entsprechender Anwendung von § 626 BGB widerrufen kann (vgl. Urteil des Bundesarbeitsgerichts vom 13.03.2007, Az. 9 AZR 612/05). Im Hinblick auf ihre gesetzlichen Verpflichtungen aus dem BDSG ist es für sie sehr problematisch, wenn der Datenschutzbeauftragte seine gesetzlich vorgesehenen Tätigkeiten zum Schutz des Persönlichkeitsrechts der Betroffenen (§ 4g Abs. 1 Satz 1 i. V. m. § 1 Abs. 1 BDSG) aufgrund langer Erkrankung nicht wahrnehmen kann.

3. Des Weiteren stellt sich die Frage, ob die Datenschutzaufsichtsbehörde von der verantwortlichen Stelle die Abberufung des lange erkrankten Datenschutzbeauftragten auf Grund dessen fehlender Zuverlässigkeit verlangen kann (§ 38 Abs. 5 Satz 3 BDSG).

   Man wird wohl in diesem Zusammenhang den Begriff „Zuverlässigkeit“ im objektiven Sinn verstehen müssen. Schließlich geht es dem Gesetzgeber darum, dass der Datenschutzbeauftragte in dem Unternehmen seine Funktion ausübt. Ist er – egal aus welchem Grund – dazu objektiv für lange Zeit nicht in der Lage und kann deshalb die ihm übertragenen Aufgaben nicht wahrnehmen, ist er nicht zuverlässig im Sinne des § 4f Abs. 2 Satz 1 und des § 38 Abs. 5 Satz 3 BDSG.

Somit kann auch eine lange Erkrankung ein Grund dafür sein, die objektive Zuverlässigkeit des Datenschutzbeauftragten zur Erfüllung seiner Aufgaben zu verneinen. Die Datenschutzaufsichtsbehörde kann in diesem Fall gegenüber der verantwortlichen Stelle die Abberufung des Datenschutzbeauftragten verlangen.

* * *

4 Versicherungen

Übermittlung der Adresse der getrennt lebenden Ehefrau an den als Versicherungsbetreuer tätigen Ehemann

Liegt ein wirksamer Widerspruch der Ehefrau gemäß § 35 Abs. 5 BDSG vor, ist diese Übermittlung unzulässig.

Die Trennung von Eheleuten ist verschiedentlich mit nachwirkenden Konfliktsituationen verbunden, weshalb manche Ehegatten den persönlichen Kontakt mit dem früheren Partner absolut unterbinden wollen.

In einem Beschwerdefall war der getrennt lebende Ehemann als Versicherungsbetreuer bei einer Versicherungsgesellschaft beschäftigt. Die Ehefrau hatte die Versicherungsgesellschaft wegen zu befürchtender Belästigungen durch ihren Ehemann ausdrücklich gebeten, eine Adressenweitergabe an den Ehemann zu unterlassen und auch dafür Sorge zu tragen, dass er in Zukunft nicht mit der Betreuung ihrer Versicherungen befasst werde.

Trotzdem hat die Versicherungsgesellschaft dem getrennt lebenden Ehemann als Versicherungsbetreuer die neue Adresse seiner Frau mitgeteilt.

Die grundsätzlich zulässige Übermittlung der Adresse an einen Versicherungsbetreuer war in diesem speziellen Fall unzulässig, da die betroffene Ehefrau dem gemäß § 35 Abs. 5 BDSG wirksam widersprochen hatte. Nach dieser Bestimmung darf eine Übermittlung nicht stattfinden, soweit der Betroffene bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Übermittlung überwiegt. Diese Voraussetzungen liegen im Falle der getrennt lebenden Ehefrau vor. Auch wenn die Ehefrau den § 35 Abs. 5 BDSG gegenüber der Versicherungsgesellschaft nicht erwähnt, ist ihre Willensbekundung als Widerspruch im Sinne dieser Bestimmung zu werten.

Die Übermittlung der neuen Adresse war somit unzulässig. Wir haben eine Beanstandung ausgesprochen und die Versicherungsgesellschaft gebeten, durch eine entsprechende Sensibilisierung der Mitarbeiter dafür Sorge zu tragen, dass in derartigen Fällen die Widersprüche der betroffenen Versicherungsnehmer beachtet werden.

*** * ***

5 Banken

5.1 Diskretion am Bankschalter

Sensible Gespräche am Bankschalter sind so zu führen, dass Dritte nicht mithören können.

Am Bankschalter werden Gespräche über finanzielle Angelegenheiten des Kunden geführt, beispielsweise bei einer Kreditanfrage.

Aus Gründen der Datensicherheit müssen Vorkehrungen getroffen werden, dass Dritte keine Gespräche zwischen den Mitarbeitern der Bank und den Kunden über problematische Gesichtspunkte mithören können. So darf es nicht vorkommen, dass Dritte im Schalterraum mitbekommen, dass die Gewährung eines Kredits wegen eines bestimmten Grundes abgelehnt wird.

Um die erforderliche Diskretion zu erreichen, kommen vor allem folgende Maßnahmen in Betracht:

- Abstandslinien
- Hinweisschilder mit der Bitte um Diskretion
- Besprechungstische und -zimmer für die Fälle, in denen die finanzielle Situation eines Kunden besprochen wird
- Schulung der Mitarbeiter

5.2 Auswertung der Kontobewegungen

Eine Bank darf die Kontobewegungsdaten ihrer Kunden nur mit deren Einwilligung für eine über den jeweiligen Vertrag hinausgehende Beratung oder für Werbezwecke auswerten.

Aufgrund der beim bargeldlosen Zahlungsverkehr anfallenden personenbezogenen Daten ihrer Kunden sind Banken theoretisch in der Lage, Auswertungen vorzunehmen und dabei umfassende Persönlichkeitsprofile ihrer Kunden zu erstellen. Eine derartige Verarbeitung und Nutzung ist jedoch nur zulässig, wenn eine Einwilligung eines Kunden gemäß § 4a BDSG vorliegt oder eine Rechtsvorschrift dies erlaubt oder anordnet.

Die Auswertung der Kontobewegungen eines Kunden (Empfänger oder Auftraggeber, Verwendungszweck, Betrag) für dessen über den jeweiligen Vertrag hinausgehende,

umfassende Beratung und Betreuung in sämtlichen Vermögensangelegenheiten ist durch keine Rechtsvorschrift gerechtfertigt.

Dies gilt auch für eine gezielte Werbeansprache für Zwecke der Bank oder ihrer Verbundpartner, z. B. Bausparkassen oder Versicherungen. Eine derartige Werbung kann - ohne gesonderte Vereinbarung - insbesondere nicht gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG auf den Girovertrag gestützt werden, da sie nicht der Zweckbestimmung dieses Vertrages dient.

Im Rahmen einer Interessenabwägung gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG müssen die berechtigten Interessen der Bank oder der Verbundpartner an einer Werbung bei ihren Kunden gegenüber deren entgegenstehenden schutzwürdigen Interessen zurückstehen. Die Kunden dürfen davon ausgehen, dass ihre Bank die im Rahmen des bargeldlosen Zahlungsverkehrs anfallenden Daten nur für die vertragsgemäße Durchführung der Bankdienstleistung verwendet.

Die Kontodaten dürfen somit nur dann für eine über den jeweiligen Vertrag hinausgehende Beratung genutzt werden, wenn der Kunde sich mit einer Auswertung seiner Daten für diese Zwecke gemäß § 4a BDSG einverstanden erklärt hat.

Eine angesprochene Bank teilte unsere Rechtsauffassung nicht und sah im Rahmen von Beratungserwartungen der Kunden eine datenschutzrechtliche Grundlage für die Auswertung der Kontobewegungsdaten.

Wir wurden in der letzten Zeit mit folgenden Beschwerden betroffener Bankkunden befasst:

5.2.1 Auswertung für Werbezwecke

Der Kundenbetreuer einer Bank hatte aus den Kontobewegungen eines Kunden ausgelesen, bei welcher Gesellschaft er privat krankenversichert ist und wie hoch sein Beitrag ist. In Kenntnis dessen hatte er ihm ein günstigeres Angebot einer mit der Bank zusammenarbeitenden Krankenversicherung unterbreitet.

Wir haben diese unzulässige Datennutzung beanstandet.

5.2.2 Übermittlung von Informationen an Dritte

In einem weiteren Fall hatte ein Bankkunde bei einer Bausparkasse seine dortigen Verträge gekündigt und dafür einen Vertrag mit einer anderen Bausparkasse abgeschlossen. Ein Bankmitarbeiter konnte dies aus den Kontobewegungen ersehen und informierte die Bausparkasse, die ihren Kunden verloren hatte. Der Bankkunde erfuhr davon, als er von seiner ehemaligen Bausparkasse darauf angesprochen wurde.

Die Datenübermittlung an die Bausparkasse war nicht zulässig, weil sie weder auf eine Rechtsvorschrift gestützt werden kann (siehe oben) noch eine Einwilligung des Kunden vorlag.

5.3 Werbung mit Meldedaten von Neubürgern

Die Verwendung von Meldedaten von Neubürgern für Werbezwecke ist unzulässig.

Auf ihre Bitte hin haben ortsansässige Banken vom Meldeamt einer Gemeindeverwaltung Listen der zugezogenen Bürger erhalten und sie für ihre Neukundenwerbung genutzt.

Die Übermittlung solcher Adresslisten von der Meldebehörde an private Stellen ist nach dem Bayerischen Meldegesetz unzulässig. Der dafür zuständige Bayerische Landesbeauftragte für den Datenschutz hat die Gemeinde beanstandet, worauf diese die Weitergabe der genannten Adresslisten eingestellt hat.

Auch auf Seiten der Banken war dieser Umgang mit den Adressdaten unzulässig, weil weder eine rechtfertigende Rechtsvorschrift noch eine Einwilligung der Betroffenen vorgelegen hat (§ 4 Abs. 1 BDSG).

Insbesondere kann im Rahmen der Interessenabwägung gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG ein berechtigtes Interesse der Banken an der Erhebung, Speicherung und Nutzung von Daten der Neubürger nicht anerkannt werden, wenn diese Daten vom Meldeamt an die Banken rechtswidrig übermittelt worden sind.

Zudem sind die schutzwürdigen Interessen der Neubürger am Ausschluss einer derartigen Verwendung als hoch einzustufen. Die Tatsache und damit das personenbe-

zogene Datum des Neuzuzuges ist eine höchstpersönliche Angelegenheit. In aller Regel möchten die Menschen – von gesetzlichen und vertraglichen Verpflichtungen abgesehen – selbst entscheiden können, ob und wen sie von ihrem Umzug informieren (vgl. auch 7.3). Darüber hinaus haben sie ein Interesse daran, dass ihre von der Gemeindeverwaltung unzulässigerweise übermittelten Daten von den Banken nicht weiter verwendet werden.

*** * ***

6 Auskunfteien

6.1 Fortlaufende Bonitätsauskünfte an den Versandhandel

Sog. Nachmeldungen der Auskunfteien an den Versandhandel sind grundsätzlich unzulässig.

Eine Ausnahme von diesem Verbot gilt jedoch dann, wenn ein Ratenzahlungskredit vereinbart wurde oder noch ein offener Saldo besteht.

Versandhäuser haben in der Vergangenheit häufig bei Bestellungen gegen Rechnung in Erwartung einer längerfristigen Kundenbeziehung ein sog. Versandhauskonto angelegt, das mit einem Girokonto der Banken mit Kreditlinie verglichen werden konnte. Ohne dass der Kunde datenschutzrechtlich eingewilligt hat, meldeten sie dieses Konto bei Auskunfteien ein. Diese sollten künftig negative Erkenntnisse zur Bonität des Kunden dem Versandhaus automatisch mitteilen, d. h. zur ursprünglichen Bonitätsprüfung "nachmelden". So sollte das Versandhaus in die Lage versetzt werden, ggf. entsprechend zu reagieren, z. B. mit einer Einschränkung oder Schließung des für den Rechnungskauf eingerichteten Kontos.

Insbesondere Kunden, die nur einmal bei einem Versandhaus bestellt hatten, haben sich über diese Praxis bei uns beschwert, nachdem sie durch eine Eigenauskunft nach § 34 BDSG aus dem Datenbestand der Auskunftei davon erfahren hatten.

Wegen der bundesweit verbreiteten Verfahrensweise des Versandhandels hat sich der "Düsseldorfer Kreis", das Gremium der Datenschutzaufsichtsbehörden, mit dieser Thematik befasst und folgenden einstimmigen Beschluss gefasst:

> "Auskunfteien dürfen Bonitätsauskünfte gemäß § 29 Abs. 2 Nr. 1a BDSG grundsätzlich nur erteilen, wenn der Dritte, dem die Daten übermittelt werden sollen, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat.
>
> Besteht zwischen diesem Dritten (also dem anfragenden Unternehmen) und dem Betroffenen ein Dauerschuldverhältnis, aufgrund dessen das anfragende Unternehmen während der gesamten Dauer des Bestehens ein finanzielles Ausfallrisiko trägt (z. B. Ratenzahlungskredit, Girokonto, Energielieferungs-, Telekommunikationsvertrag), so dürfen Bonitätsauskünfte nicht nur zu dem Zeitpunkt erteilt werden, zu dem der Betroffene ein solches Vertragsverhältnis

beantragt hat, sondern während der gesamten Laufzeit des Vertragsverhältnisses und bis zur Erfüllung sämtlicher Pflichten des Betroffenen.

Ein Versandhandelsgeschäft stellt als solches kein Dauerschuldverhältnis dar. Die aufgrund der bisherigen Erfahrungen mit den Kunden möglicherweise bestehende Wahrscheinlichkeit und darauf gegründete Erwartung, dass der Kunde nach der ersten Bestellung wiederholt bestellen wird, und die zur Erleichterung der Bestellvorgänge möglicherweise erfolgte Einrichtung eines „Kundenkontos“ rechtfertigten es nicht, ein Versandhandelsgeschäft mit einem Dauerschuldverhältnis gleichzusetzen.

Ein berechtigtes Interesse seitens des Versandhandels gem. § 29 BDSG ist demnach nur gegeben, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko vorliegt.

Nach Vertragsschluss sind Bonitätsauskünfte an Versandhändler dann nicht zu beanstanden, wenn ein Ratenzahlungskredit vereinbart wurde oder noch ein offener Saldo besteht. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäftes für den Versandhandel abgeschlossen, ein berechtigtes Interesse an Bonitätsauskünften ist dann nicht mehr zu belegen. Damit sind Nachmeldungen oder sonstige Beauskunftungen in dieser Konstellation rechtlich unzulässig."

Die einschlägigen Unternehmen und Auskunfteien haben sich bereit erklärt, diese gesetzlichen Vorgaben für das Nachmeldeverfahren ab Oktober 2008 zu beachten.

6.2 Transparenz im Auskunfteiwesen

6.2.1 Benachrichtigung des Betroffenen im Fall der ersten Datenübermittlung

Auskunfteien sind gemäß § 33 Abs. 1 Sätze 2 und 3 BDSG verpflichtet, die Betroffenen von der erstmaligen Datenübermittlung und der Art der übermittelten Daten zu benachrichtigen sowie über die Kategorien von Empfängern zu unterrichten, soweit sie nicht mit der Übermittlung an diese rechnen müssen.

Da Auskunfteien personenbezogene Daten in vielen Fällen zunächst ohne Kenntnis des Betroffenen speichern, erfahren diese erst mit der Benachrichtigung, dass Daten zu ihrer Person bei der Auskunftei gespeichert sind. Die Benachrichtigung durch die

Auskunftei ist deshalb für die Betroffenen von großer Bedeutung. Nur wenn sie wissen, dass Daten zu ihrer Person gespeichert sind, können sie von den ihnen zustehenden Rechten Gebrauch machen.

6.2.2 Auskunft an den Betroffenen

Im Gegensatz zur Benachrichtigung, die nur allgemeine Informationen enthält, gibt der § 34 Abs. 1 und 2 BDSG dem Betroffenen einen Anspruch gegenüber einer Auskunftei auf folgende konkrete Auskünfte:

1. **Die zu seiner Person gespeicherten Daten**
   Es sind sowohl die im Auskunftsdatensatz als auch die intern zur Person gespeicherten Daten mitzuteilen. Das Auskunftsrecht des Betroffenen erstreckt sich auch auf solche Daten, die weder in einer automatisierten Verarbeitung noch in einer nicht automatisierten Datei gespeichert sind (§ 34 Abs. 2 Satz 1 BDSG).

2. **Die Herkunft und Empfänger der Daten, soweit nicht das Interesse der Auskunftei an der Wahrung ihres Geschäftsgeheimnisses überwiegt.**
   Die Herkunft von Daten ist in vielen Fällen nicht aufklärbar, da es im BDSG keine allgemeine Pflicht gibt, die Herkunft zu speichern. In den anderen Fällen werden von den Auskunfteien häufig Geschäftsgeheimnisse geltend gemacht.

   Auskunft über den Empfänger müssen die Auskunfteien in aller Regel dann erteilen, wenn er einer Branche angehört, bei der die Zusammenarbeit mit Auskunfteien allgemein bekannt ist, z. B. wenn es sich um Versicherungen, Banken, den Versandhandel, die Telekommunikation oder Leasing-/Factoringgesellschaften handelt. Dasselbe gilt grundsätzlich dann, wenn der Betroffene begründete Zweifel an der Richtigkeit der Daten oder am Vorliegen eines berechtigten Interesses vorträgt oder gegen den Empfänger Schadensersatz- oder Richtigstellungsansprüche geltend machen will oder dieser die Auskunft missbräuchlich verwendet hat.

3. **Der Zweck der Speicherung**
   Hier sind allgemeine Erläuterungen zur Tätigkeit der Auskunftei zu geben.

6.2.3 Erhebung eines Entgelts für eine Auskunft

Auskunfteien können für eine Eigenauskunft an den Betroffenen ein Entgelt verlangen, wenn dieser die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Dadurch soll verhindert werden, dass der Geschäftstätigkeit der Auskunfteien die Grundlage entzogen wird, indem potentielle Geschäftspartner Informationen zur wirtschaftlichen Lage des Betroffenen nicht von der Auskunftei beziehen, sondern den Interessenten dazu auffordern, eine (für ihn kostenfreie) Eigenauskunft vorzulegen.

Die Auskunft ist jedenfalls dann kostenfrei, wenn besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergibt, dass die Daten zu berichtigen oder unter den Voraussetzungen des § 35 Abs. 2 Satz 2 Nr. 1 BDSG (unzulässige Datenspeicherung) zu löschen sind (§ 34 Abs. 5 Satz 4 BDSG).

6.2.4 Berichtigung und Bestreiten unrichtiger Daten bei Auskunfteien

Stellt der Betroffene fest, dass bei einer Auskunftei in seinem Datensatz unrichtige Daten gespeichert sind, sieht das BDSG folgendes vor:

1. Bei Daten, die aus allgemein zugänglichen Quellen, z. B. Presseveröffentlichungen, entnommenen sind, können zwar die bestrittenen Daten unverändert im Datensatz der Auskunftei belassen werden. Auf Verlangen des Betroffenen ist diesen Daten aber für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

2. In allen anderen Fällen hat der Betroffene einen Rechtsanspruch auf Berichtigung (§ 35 Abs. 1 BDSG), den er ggf. gerichtlich durchsetzen kann.

Für eine Berichtigung muss der Betroffene der Auskunftei die richtigen Daten nennen, damit diese die entsprechenden Korrekturen durchführen kann.

Der Betroffene kann es jedoch auch dabei belassen, die unrichtigen Daten zu bestreiten. In diesem Fall muss die Auskunftei die Daten überprüfen. Kann weder die Richtigkeit noch die Unrichtigkeit der Daten festgestellt werden, muss die Auskunftei die Daten sperren (§ 35 Abs. 4 BDSG).

3. Im Falle einer Berichtigung oder einer Sperrung bestrittener Daten ist bezüglich einer Benachrichtigung der Stellen, an die Daten übermittelt worden sind, § 35 Abs. 7 BDSG zu beachten.

6.2.5 Löschung und Sperrung

Sind personenbezogene Daten bei einer Auskunftei zulässigerweise gespeichert, hat der Betroffene, vom Ausnahmefall des § 35 Abs. 5 BDSG abgesehen, keinen Anspruch auf Löschung oder Sperrung.

Der Betroffene kann eine Löschung allerdings dann verlangen, wenn ihre Speicherung unzulässig ist. Dies ist auch dann der Fall, wenn die Daten für die Beurteilung der Kreditwürdigkeit nicht geeignet sind.

Im Übrigen muss eine Auskunftei die Daten löschen, wenn eine Prüfung am Ende des vierten Kalenderjahres - beginnend mit dem 1. Januar des auf die erstmalige Speicherung folgenden Jahres - ergibt, dass eine länger währende Speicherung nicht erforderlich ist (§ 35 Abs. 2 Nr. 4 BDSG). Bis zum Ablauf dieser Frist dürfen Negativdaten, auch wenn sie schon erledigt sind, noch gespeichert bleiben.

Abweichend davon gelten in verschiedenen Fällen besondere Löschungsvorschriften, z. B. für die aus dem Schuldnerverzeichnis entnommenen Daten (§ 915g i. V. m. § 915a Zivilprozessordnung).

*** * ***

7 Handel, Dienstleistung

7.1 Kundenbindungsprogramme

Einige Hinweise zur datenschutzgerechten Gestaltung von Kartensystemen

In Bayern haben die Betreiber großer unternehmensübergreifender Kundenbindungsprogramme ihren Sitz. Wir sind deshalb in die damit verbundenen Datenschutzfragen intensiv eingebunden.

Die Betreiber der Kundenbindungsprogramme geben Rabattkarten aus, die Kunden bei den beteiligten Unternehmen beim Kauf von Waren oder der Nutzung von Dienstleistungen einsetzen, um Rabattpunkte zu sammeln, die sie später gegen Prämien einlösen können.

Bei der Beantragung und dem Einsatz der Rabattkarten erheben die Betreiber der Kundenbindungsprogramme zahlreiche personenbezogene Daten, von den erforderlichen Stammdaten (z. B. Name, Adresse) über freiwillig mitgeteilte Kontaktdaten (E-Mail-Adresse, Telefonnummer, Handy-Nummer) bis hin zu den Einkaufsdaten (Waren, Warengruppen) und den Daten über genutzte Dienstleistungen.

Für die Erhebung, Verarbeitung und Nutzung der Stamm- und der Einkaufsdaten gelten die datenschutzrechtlichen Grundsätze der Erforderlichkeit, der Datenvermeidung und Datensparsamkeit sowie der Zweckbindung. Insbesondere dürfen weder bei dem Betreiber des Kundenbindungsprogramms noch bei den beteiligten Unternehmen "gläserne Kunden" mit detaillierten Konsumprofilen entstehen.

Zur Erfüllung der datenschutzrechtlichen Grundsätze haben wir die Betreiber von Kundenbindungsprogrammen beraten und notwendige Änderungen durchgesetzt. So legen wir bei den Antragsformularen Wert auf eine klare Trennung und Kennzeichnung von Pflichtangaben für das Vertragsverhältnis einerseits und von den Kunden auf freiwilliger Basis abgefragten Daten andererseits.

Die von den Kunden in den Antragsformularen erbetenen Einwilligungserklärungen für eine Datenverwendung über den eigentlichen Zweck des Rabattkartenvertrags hinaus zu Werbe- oder Marktforschungszwecken müssen gemäß § 4a BDSG inhaltlich klar formuliert, deutlich erkennbar und schnell überschaubar sein (siehe Tätig-

keitsbericht 2006 unter 4.1). Detaillierte Erläuterungen dazu können für den interessierten Leser in ergänzende Datenschutzhinweise aufgenommen werden.

Der Bundesgerichtshof hat in seinem Urteil vom 16.07.2008, Az. VIII ZR 348/06, festgestellt, dass unter diesen Umständen eine Einwilligungserklärung mit einem Kartenantrag verbunden werden kann und dass eine sogenannte Auskreuzlösung, die eine Streichung der Einwilligung im Formular ermöglicht (sog. opt-out), rechtlich unbedenklich ist. Lediglich für die Einwilligung in Werbezusendungen per E-Mail und SMS verlangt das Gericht eine eigene positive Erklärung, die vom Kunden gesondert zu unterschreiben oder durch individuelles Markieren eines entsprechenden Feldes abzugeben ist (sog. opt-in).

7.2 Mahnung durch Computeranruf

Telefonische Mahnungen durch Computeranruf sind wegen der Gefahr, dass eine andere Person als der vorgesehene Gesprächspartner das Gespräch entgegennimmt, unzulässig.

Um die Kosten für das Mahnverfahren zu reduzieren, gingen Unternehmen dazu über, ausstehende Forderungen durch Computeranrufe anzumahnen. Wurde eine fällige Forderung gegen einen Kunden, dessen Telefonnummer bekannt war, nicht beglichen, wurde automatisch ein Anruf an ihn generiert.

Nach § 9 Satz 1 BDSG hat die verantwortliche Stelle die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften des BDSG, insbesondere die in der Anlage zum BDSG genannten Anforderungen, zu gewährleisten. Gemäß Nr. 4 der Anlage zu § 9 BDSG (Weitergabekontrolle) muss die verantwortliche Stelle gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies gilt entsprechend auch für die telefonische Weitergabe personenbezogener Daten. Auch hier muss sichergestellt werden, dass diese Daten nicht von Dritten unbefugt zur Kenntnis genommen werden können.

Bei Mahnungen per Computeranruf kann nicht ausgeschlossen werden, dass Dritte vom Inhalt des Anrufs etwas erfahren. Man kann nämlich in vielen Fällen nicht davon ausgehen, dass der säumige Zahler das Gespräch entgegennimmt. Schließlich werden viele Telefonanschlüsse von mehreren Personen genutzt, z. B. in der Familie, in

der Wohngemeinschaft, im Büro usw. Es kann das Persönlichkeitsrecht des Betroffenen verletzen, wenn Dritte von seinen Zahlungsrückständen etwas mitbekommen.

Wir kamen deshalb zu dem Ergebnis, dass Mahnungen durch Computeranruf der gebotenen Datensicherung im Sinn des § 9 Satz 1 BDSG mit Anlage nicht entsprechen.

Der Düsseldorfer Kreis, das Gremium der deutschen Datenschutzaufsichtsbehörden, hat sich auf unseren Antrag hin mit diesem Thema befasst und in Übereinstimmung mit unserer Auffassung folgenden Beschluss gefasst:

> "Eine telefonische Mahnung durch Computeranruf ist wegen der hohen Gefahr, dass ein anderer als der vorgesehene Empfänger die Nachricht erhält und so personenbezogene Daten einem Dritten unbefugt offenbart werden, unzulässig."

Die Unternehmen haben diese Praxis zwischenzeitlich eingestellt.

7.3 Übermittlung von Umzugsdaten

Die Übermittlung der neuen Anschrift eines Kunden an andere Unternehmen, die mit dem Kunden in einer Geschäftsbeziehung stehen, ist nur zulässig, wenn der Kunde in diese Übermittlung gemäß § 4a BDSG eingewilligt hat.

Um Fehlsendungen zu Kunden oder bei Werbeaussendungen zu vermeiden, setzte eine Reihe von Unternehmen einen auf Adressaktualisierungen spezialisierten Dienstleister ein, der seinen Adressenbestand gegen die Adressdaten der Unternehmen abgleicht und veraltete Adressen berichtigt.

Die Information über die neuen Adressen stammte auch von den angeschlossenen Unternehmen. Stellte ein am System beteiligtes Unternehmen fest, dass sein Kunde ihm gegenüber eine neue Adresse angegeben hat, so leitete es diese Adressänderung über den Dienstleister an die an dem System beteiligten Unternehmen weiter, bei denen dieser Kunde registriert war. Es berief sich dabei auf die gesetzlichen Rechtsgrundlagen des § 28 Abs. 1 Satz 1 Nr. 2 oder des Abs. 3 Nr. 1 BDSG.

Auf diese Vorschriften kann die Übermittlung der Adressänderung an die anderen Unternehmen allerdings nicht gestützt werden. Zwar besteht seitens der dem System

angeschlossenen Unternehmen ein berechtigtes Interesse an einem stets aktuellen Datenbestand. Auf diese Weise können Fehlsendungen, die jährlich für die einschlägigen Unternehmen hohe Kosten verursachen, vermieden werden. In vielen Fällen vergessen diejenigen, die umgezogen sind, ihre neue Adresse den Unternehmen mitzuteilen, mit denen sie in geschäftlicher Beziehung stehen. Im Bereich der Werbung sind die Unternehmen daran interessiert, dass ihre Werbepost auch ankommt.

Im Rahmen der Interessenabwägung ist allerdings das schutzwürdige Interesse derjenigen, die umgezogen sind, höher zu bewerten als das Interesse der Unternehmen. Die Frage, ob man die Tatsache und damit das personenbezogene Datum des Umzugs - abgesehen von gesetzlichen und vertraglichen Verpflichtungen - einem anderen mitteilt, ist eine höchstpersönliche Angelegenheit. In aller Regel möchten die Menschen selbst entscheiden können, ob sie ihren Umzug weitererzählen, wem sie dies mitteilen und zu welchem Zeitpunkt sie sich äußern bzw. ihre Einwilligung dazu erteilen (vgl. auch unter 5.3). Es gibt immer wieder - abgeschlossene - Geschäftsbeziehungen, lästige Zusendungen von Werbepost und sonstige Verbindungen, die man auf diese Weise ("unbekannt verzogen") elegant beenden kann.

Man kann auch nicht sagen, dass jemand, der seine Adresse bei irgendeiner Gelegenheit weitergegeben hat, damit rechnet, dass von dem Empfänger all seine künftigen Umzüge nachverfolgt werden können. Die seinerzeitige Einwilligung bezog sich selbstverständlich nur auf eine, d. h. auf die damals aktuelle Adresse, nicht jedoch auf alle folgenden Adressen. Der Betroffene wollte nur seine aktuelle Adresse preisgeben, nicht jedoch sein künftiges Umzugsverhalten. Auch aus diesem Grund steht der Adressenweitergabe das schutzwürdige Interesse des Betroffenen entgegen.

Dies muss man nicht zuletzt auch deshalb annehmen, weil bei derartigen Datenweitergaben ohne Einwilligung der Betroffenen ein gewisses Risiko besteht, dass fehlerhafte Daten übermittelt werden. Derartige Fälle wurden uns in einigen Eingaben vorgetragen.

Für die Zulässigkeit der Übermittlung der Umzugsadressen an andere Unternehmen kann aus diesen Gründen eine gesetzliche Rechtsgrundlage nicht herangezogen werden. Eine derartige Datenübermittlung ist deshalb nur mit Einwilligung des Betroffenen zulässig.

Auf unsere Veranlassung hin hat sich der Düsseldorfer Kreis, das Gremium der deutschen Datenschutzaufsichtsbehörden, mit diesem Thema befasst und in Übereinstimmung mit unserer Rechtsauffassung einstimmig folgenden Beschluss gefasst:

> "Übermittelt ein Unternehmen Umzugsadressen seiner Kunden an andere Unternehmen zur weiteren Übermittlung dieser Adressänderungen an angeschlossene Unternehmen zum Zwecke des Adressabgleichs, so ist dies nur mit einer ausdrücklichen Einwilligung der Betroffenen gemäß § 4a BDSG zulässig.
>
> Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandelsunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen."

Die beteiligten Unternehmen haben die Übermittlung von Umzugsdaten, soweit keine Einwilligungen der Kunden vorliegen, zwischenzeitlich eingestellt.

7.4 Einkauf mit Fingerabdruck

Eine datenschutzgerechte Gestaltung eines derartigen Bezahlsystems ist denkbar.

Neuerdings können Kunden in Geschäften alternativ zu herkömmlichen Zahlungsformen mittels ihres unverwechselbaren Fingerabdrucks bezahlen.

Unter der Voraussetzung, dass das Erkennungssystem für die Fingerabdrücke die notwendige technische Sicherheit bietet, hat das Handelsunternehmen eine sehr sichere Identifikationsmöglichkeit. Auch für die Kunden hat das System Vorteile. Da sie ihr Zahlungsmittel "Fingerabdruck" immer dabei haben, benötigen sie weder Bargeld noch Karten und haben damit auch kein Diebstahlsrisiko.

Im Rahmen der Zweckbestimmung dieses Bezahlsystems erhebt und speichert das Unternehmen die notwendigen Fingerabdrucke, Personalien und Kontodaten des Kunden, um die anfallenden Beträge abbuchen zu können.

Datenschutzrechtliche Rechtsgrundlage für diese Vorgänge ist eine Einwilligungserklärung gemäß § 4a BDSG oder ein spezieller Vertrag, in dem sich der Kunde mit dem erforderlichen Umgang mit seinen genannten personenbezogenen Daten in entsprechender Anwendung des § 4a BDSG einverstanden erklärt. In beiden Fällen muss der Kunde in allgemein verständlicher Form über alle Umstände der Fingerabdruck-Zahlung informiert worden sein. Die Einverständniserklärung hat freiwillig und schriftlich zu erfolgen und muss für den Kunden frei widerrufbar sein. Darüber hinaus ist die technische Sicherheit des Bezahlsystems zu gewährleisten.

7.5 Weitergabe eines Zeitungsabonnements an einen anderen Verlag

Ohne Einwilligung der Abonnenten dürfen deren Daten nicht an andere Verlage übermittelt werden.

Ein Verlag stellte die Herausgabe einer Fachzeitschrift ein und übertrug, ohne seine Abonnenten zu fragen, die Lieferverträge einschließlich der Daten der Abonnenten an einen anderen Verlag, der die Abonnenten künftig mit einer ähnlichen Fachzeitschrift beliefern sollte.

Die damit verbundenen Datenübermittlungen konnten weder auf eine gesetzliche Rechtsgrundlage noch auf eine Einwilligung der Betroffenen gestützt werden und waren somit unzulässig.

Beide Verlage hatten zwar ein berechtigtes Interesse daran, dass die Abonnements unterbrechungslos fortgeführt und Rückabwicklungen der laufenden Verträge vermieden wurden.

Der Übermittlung der Abonnentendaten standen jedoch die schwerer wiegenden schutzwürdigen Interessen der Abonnenten entgegen. Aus dem informationellen Selbstbestimmungsrecht ergibt sich für sie, dass es allein ihrer Entscheidung oblag, ob ihre Daten an den anderen Verlag weitergegeben werden durften.

7.6 Detektiv ortet Person heimlich mit Hilfe eines GPS-Senders

Ein Detektiv hatte heimlich einen Peilsender in der Form eines GPS-Senders und GSM-Moduls an dem PKW einer Person, die er beobachten sollte, angebracht. Der Sender funkte die Bewegungsdaten des Fahrzeugs an den Detektiv. So konnte er die empfangenen Informationen auf seinem PC speichern oder per Handy abrufen und

damit ohne großen Zeitaufwand Weg- und Zeitskizzen über alle Bewegungen des Fahrzeuges erstellen. Die erfassten Daten ergaben zunächst ein umfassendes Bewegungsprofil des mit dem Peilsender versehenen Fahrzeuges.

Die Frage, ob diese Daten auch personenbezogen sind und damit das BDSG anwendbar ist, hängt davon ab, ob sie sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Da ein unmittelbarer Bezug von diesen Fahrzeug-Bewegungsdaten auf eine bestimmte Person nicht gegeben ist, kommt es darauf an, ob die Person, die das Fahrzeug gefahren hat, wenigstens bestimmbar war. Das ist dann der Fall, wenn der Personenbezug mit einem konkreten personenbezogenen Zusatzwissen hergestellt werden kann.

In dem von uns überprüften Fall war dem Detektiv bekannt, welcher Fahrer das Fahrzeug fuhr, an dem er den Peilsender angebracht hatte. Damit konnte er die erfassten Fahrzeug-Bewegungsdaten einem bestimmten Betroffenen zuordnen. Mit den Bewegungsdaten des Fahrzeugs erhob, verarbeitete und nutzte daher der Detektiv gleichzeitig personenbezogene Daten in der Form von Bewegungsdaten des Fahrers.

Diese Schlussfolgerung kann allerdings dann nicht gezogen werden, wenn ein Fahrzeug in dem Überwachungszeitraum von mehreren Personen gefahren wurde und von dem Detektiv auch mit dem entsprechenden Zusatzwissen nicht festgestellt werden kann, von welchem Fahrer das Fahrzeug auf den einzelnen Fahrtstrecken gefahren worden ist.

Soweit es sich jedoch um die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gehandelt hat, ist festzustellen, dass hierfür keine Rechtsgrundlage vorhanden ist. Es war weder die Einwilligung des betroffenen Fahrers eingeholt worden noch ist eine rechtfertigende Rechtsvorschrift ersichtlich. Insbesondere ergibt sich eine Zulässigkeit nicht aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG.

Es ist schon sehr zweifelhaft, ob sich der Detektiv auf ein berechtigtes Interesse berufen kann, mit solchen Ermittlungsmethoden mit den Bewegungsdaten der betroffenen Fahrer umzugehen. In jedem Fall überwiegt jedoch das entgegenstehende schutzwürdige Interesse des Betroffenen. Dieser muss eine heimliche Überwachung seiner PKW-Fahrten nicht hinnehmen. Eine heimliche Überwachung aller Bewegungen mit dem Fahrzeug sei es aus beruflichen oder privaten Gründen beeinträchtigt das informationelle Selbstbestimmungsrecht und damit das allgemeine Persönlichkeitsrecht in

erheblicher Weise (so auch OLG Oldenburg im Beschluss vom 20.05.2008, Az. 13 WF 93/08).

Die Erhebung, Verarbeitung und Nutzung der PKW-Bewegungsdaten durch den Detektiv waren somit unzulässig.

7.7 Datenerhebung an der Kasse eines Einkaufsmarktes

Aus Datensicherheitsgründen ist darauf zu achten, dass unbefugte Dritte keine Kenntnis von personenbezogenen Daten erhalten.

In einem Einkaufsmarkt war die EC-Karten-Anlage ausgefallen. Um den Kunden dennoch das bargeldlose Bezahlen anbieten zu können, wurde an der Kasse eine Liste ausgelegt, in die Kunden die für die Abbuchung erforderlichen Daten eingetragen haben. Dabei konnten sie auch die Eintragungen der vorherigen Kunden einsehen.

Die Erhebung der für die Abbuchung erforderlichen Daten durch den Einkaufsmarkt war zwar aufgrund des § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig.

Bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten müssen aber die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten getroffen werden. Unter anderem muss die verantwortliche Stelle sicherstellen, dass personenbezogene Daten während ihrer Speicherung auf Datenträgern nicht unbefugt gelesen werden können (vgl. § 9 BDSG i. V. m. Nr. 4 der Anlage zu § 9 BDSG, Weitergabekontrolle).

Durch die Verwendung einer fortlaufend geführten Liste konnten Kunden von personenbezogenen Daten Dritter unbefugt Kenntnis erlangen.

Dies haben wir beanstandet. Eine unbefugte Einsichtnahme hätte durch die Verwendung von Einzelbelegen auf einfache Weise verhindert werden können.

7.8 Versehentliche Übermittlung von Kundendaten

Bei der Versendung von Anlagen per E-Mail ist größte Sorgfalt anzuwenden, um Verwechslungen zu vermeiden.

Im Zusammenhang mit dem Kauf eines Notebooks hatte sich der Käufer beim Verkäufer nach einer Finanzierungsmöglichkeit erkundigt. In Beantwortung seiner Anfrage wurde ihm per E-Mail ein entsprechendes Antragsformular zugesandt.

Beim Ausfüllen des Formulars stellte er fest, dass darauf bereits die Daten eines anderen Kunden, u. a. Namen, Adresse, Geburtsdatum, Telefonnummer, Personalausweisnummer, Familienstand, Zahl der Kinder, Bankverbindungsdaten, Kreditkartennummer, Beruf, Nettoeinkommen usw. eingetragen waren. Eine Mitarbeiterin des Unternehmens hatte an ihn versehentlich an Stelle eines Leerformulars eine von einem Kunden bereits ausgefüllte PDF-Datei übermittelt.

Diese Datenübermittlung war unzulässig.

* * *

8 Werbung, Adressenhandel

8.1 Zusendung von Werbung nach der Erhebung eines Widerspruchs

Innerhalb einer Übergangsfrist von 8 Wochen seit Einlegung eines Werbewiderspruchs werden unzulässige Werbezusendungen von uns nicht beanstandet.

Die Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung ist unzulässig, wenn jemand gemäß § 28 Abs. 4 Satz 1 BDSG widersprochen hat. In vielen Fällen bestätigt das angesprochene Unternehmen die Einstellung dieser Nutzung.

Gleichwohl kommt es immer wieder vor, dass diese Person in den darauffolgenden Wochen von dem Unternehmen noch weitere Werbung erhält. Sie bekommt dadurch den Eindruck, dass ihr Werbewiderspruch nicht beachtet wird und wendet sich deshalb an die Datenschutzaufsicht.

Tatsächlich ist diese „Nichtbeachtung“ darauf zurückzuführen, dass Werbeaktionen mit persönlich adressierten Briefen meist einer längeren Vorlaufzeit bedürfen. Es können nur diejenigen Werbewidersprüche berücksichtigt werden, die zum Zeitpunkt der Adressenauswahl eingetragen waren. Da diese sechs bis acht Wochen vor dem Zugang eines Werbeschreibens liegen kann, kann es in dieser Zeitspanne zu weiterer Werbepost kommen.

Während einer laufenden Aktion würde es für ein Unternehmen einen nicht vertretbaren Aufwand bedeuten, ein einzelnes Werbeschreiben aus der Gesamtzahl der Anschreiben zu selektieren. Wir gestehen deshalb den Unternehmen eine Übergangsfrist von acht Wochen zu, bevor wir eine auf Grund eines Werbewiderspruches unzulässige Werbung beanstanden.

8.2 Freundschaftswerbung

Name und Anschrift dürfen bei Dritten erhoben werden, nicht aber Telefonnummern und E-Mail-Adressen.

Ein Fitnessstudio forderte seine Mitglieder im Rahmen einer Werbeaktion auf, von möglichen Interessenten aus ihrem Bekanntenkreis Name, Anschrift, Telefonnummer und E-Mail-Adresse anzugeben.

Die Erhebung, Verarbeitung und Nutzung der Interessentendaten richtet sich nach § 4 Abs. 2 Nr. 2a und § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Die Erforderlichkeit einer Erhebung bei anderen Personen kann hier wegen des Geschäftszwecks ebenso anerkannt werden wie das berechtigte Interesse des Fitnessstudios an einer derartigen Werbemaßnahme. Im Bekanntenkreis der Mitglieder bestehen bessere Chancen als dies bei ungezielt versendeter Werbepost der Fall ist.

Die von beiden Vorschriften geforderte Interessenabwägung ergibt, dass entgegen stehende schutzwürdige Interessen der Betroffenen nur dann nicht überwiegen, wenn nur der Name und die Anschrift, nicht aber noch zusätzlich die Telefonnummer und die E-Mail-Adresse erhoben werden. Diese Auslegung rechtfertigt sich aus einem Vergleich mit dem in § 28 Abs. 3 Satz 1 Nr. 3 BDSG geregelten Listenprivileg. Dort können der Name und die Adresse ohne Einwilligung des Betroffenen für Zwecke der Werbung genutzt und übermittelt werden.

Ob und inwieweit das Wettbewerbsrecht einer Freundschaftswerbung entgegensteht, ist nicht Gegenstand dieser datenschutzrechtlichen Beurteilung und muss gesondert geprüft werden.

8.3 Geburtstagsglückwünsche an Kunden

Unternehmen müssen bei der Zusendung von Geburtstagsglückwünschen an Kunden darauf achten, dass Dritten weder das Alter noch das Geburtsdatum des Kunden offenbart wird.

Die Zusendung von Geburtstagsglückwünschen zur Förderung der Kundenbeziehung ist grundsätzlich zulässig.

Dabei kommt es aber immer wieder vor, dass ein Unternehmen einem Kunden mit offener Postkarte zum 60. Geburtstag am 13.08.2008 gratuliert oder dass auf dem Briefumschlag aufgedruckt ist: "Alles Gute zum 50. Geburtstag".

Derartige Glückwunschschreiben sind datenschutzrechtlich nicht zulässig. Die Unternehmen müssen vielmehr sicherstellen, dass niemand unbefugt vom Alter und vom Geburtsdatum des angeschriebenen Kunden Kenntnis erhalten kann. Sie müssen deshalb von offenen Glückwunschkarten und von entsprechenden Kuvertaufdrucken absehen.

8.4 Werbesendung an den Adressbestand eines anderen Unternehmens

Gegen den Einsatz des Adressbestandes eines anderen Unternehmens für eine Werbeaktion bestehen bei Beachtung der Vorgaben des BDSG keine datenschutzrechtlichen Bedenken.

Erhält eine Person von einem Unternehmen, mit dem sie bisher noch keinen Kontakt hatte, ein persönlich adressiertes Werbeschreiben, erweckt dies bei ihr zunächst den Eindruck, dass das Unternehmen die bei ihm gespeicherte Adresse für diese Werbeaktion genutzt hat. Die Vermutung eines Datenschutzverstoßes liegt für sie nahe.

Spricht sie das Unternehmen darauf an oder macht sie von ihrem Auskunftsanspruch Gebrauch, erhält sie jedoch in zahlreichen Fällen die Antwort, dass das Unternehmen die Adresse nicht gespeichert, sondern zur einmaligen Verwendung nur angemietet hat und dabei das im Folgenden beschriebene Verfahren angewandt hat.

Das Unternehmen A bedient sich des Adressbestandes des Unternehmens B in der Weise, dass es sein Werbematerial dem Unternehmen B mit dem Auftrag übergibt, es an die dort vorhandenen Adressen zu versenden. Das Unternehmen B nutzt damit seinen eigenen Adressenbestand für die Werbeaktion des Unternehmens A.

Die Zulässigkeit dieser Datennutzung durch das Unternehmen B ist nach § 28 Abs. 3 Nr. 3 BDSG zu beurteilen. Danach muss die Auswahl der Adressen den abschließenden Kriterienkatalog des sog. Listenprivilegs beachten und es darf kein Grund zu der Annahme bestehen, dass die Beworbenen ein schutzwürdiges Interesse an dem Ausschluss dieser Werbenutzung haben.

Soweit im Einzelfall diese Voraussetzungen erfüllt sind, handelt es sich um eine aus datenschutzrechtlicher Sicht zulässige Werbung. Das werbende Unternehmen A hat mit den verwendeten Adressen nichts zu tun. Es lernt in der Folgezeit nur diejenigen Beworbenen kennen, die auf die Werbung reagieren.

Ebenso zulässig ist es, wenn das beauftragte Unternehmen B die technischen Arbeiten dieser Werbeaktion bis hin zur Versendung von einem Dienstleister im Rahmen einer Auftragsdatenverarbeitung gemäß § 11 BDSG durchführen lässt und dabei den Adressbestand an den Dienstleister übergibt. Es handelt sich dabei um ein sog. Lettershopverfahren.

Auch in diesen Fällen muss § 28 Abs. 4 BDSG beachtet werden. Die Betroffenen sind bei der Ansprache zum Zwecke der Werbung zu unterrichten, dass sie einer Werbung widersprechen können. Dem Betroffenen ist dabei ggf. auch Auskunft zur Herkunft der Adresse zu erteilen. Eine Nichtbeachtung dieser Verpflichtungen ist gemäß § 43 Abs. 1 Nr. 3 BDSG bußgeldbewehrt.

Macht jemand von seinem Werbewiderspruchsrecht Gebrauch, ist eine künftige Werbung unzulässig.

*** * ***

9 Internationaler Datenverkehr

Auftragsdatenverarbeitung in einem Staat außerhalb der Europäischen Union und des Europäischen Wirtschaftsraumes

Die Datenübermittlung in das Drittland muss durch eine Einwilligung oder durch eine Rechtsvorschrift gerechtfertigt sein.

Ein Unternehmen übermittelte unter anderem Gesundheitsdaten zur weiteren Verarbeitung an ein in einem Staat außerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraumes (EWR) - also in einem Drittland - gelegenes Dienstleistungsunternehmen, ohne dass die dafür geltenden datenschutzrechtlichen Regelungen der §§ 4b und 4c BDSG beachtet wurden. Darüber hinaus erfolgte die Übermittlung auf einer ungesicherten Datenleitung.

Bei der dabei erfolgenden Datenweitergabe seitens des deutschen Unternehmens handelt es sich um eine Datenübermittlung im Sinne des § 3 Abs. 4 Nr. 3 BDSG, die einer Rechtfertigung gemäß § 4 Abs. 1, § 4b und § 4c BDSG bedarf. Die Privilegierung des § 11 BDSG für weisungsgebundene Datenverarbeitung im Auftrag kann hier nicht zur Anwendung kommen. Dies ergibt der Umkehrschluss aus der Ausnahmevorschrift des § 3 Abs. 8 Satz 3 BDSG, die sich nur auf Personen und Stellen im Inland, in einem Mitgliedsstaat der EU oder in einem EWR-Staat bezieht.

Die Prüfung, ob die Auftragsdatenverarbeitung in einem sog. Drittland zulässig ist, findet zweistufig statt.

Die erste Stufe betrifft die Voraussetzungen, die auch bei einer Übermittlung innerhalb Deutschlands beachtet werden müssen. Es muss also eine Einwilligung oder eine Rechtsvorschrift, die die Übermittlung erlaubt, vorliegen (§ 4 Abs. 1 BDSG).

Die zweite Prüfungsstufe bezieht sich auf den speziellen Auslandsaspekt. Grundsätzlich muss beim Datenempfänger zum Schutz der von der Datenverarbeitung betroffenen Personen ein angemessenes Datenschutzniveau (oder ein Ausnahmetatbestand des § 4c Abs.1 BDSG) vorliegen.

Deutsche Unternehmen können ein solches angemessenes Datenschutzniveau für Dienstleister in Drittstaaten unter bestimmten Voraussetzungen mit vertraglichen Lösungen erreichen, wofür ein Mustervertrag der EG zur Verfügung steht (vgl. im

Internet unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:DE:PDF)

Da diese gesetzlichen Vorgaben nicht beachtet worden sind, waren die Datenübermittlungen unzulässig.

* * *

10 Arbeitnehmerdatenschutz

10.1 Unternehmensinterne Weitergabe von Dienstreisedaten

In einem Unternehmen wurde festgestellt, dass immer wieder Mitarbeiter dienstliche Flugreisen, für die bereits Flugtickets bestellt waren, nicht angetreten haben, ohne die Reisen rechtzeitig zu stornieren. Dadurch entstanden dem Unternehmen im Laufe der Zeit nicht unerhebliche Kosten.

Um einen Überblick über die aufgetretenen Fälle zu bekommen, wurde eine Liste erstellt, die neben den Namen der betroffenen Mitarbeiter die gebuchten, aber nicht angetretenen und nicht abgesagten Flüge sowie einzelne Vermerke über die Gründe des Nichtantritts, z. B. „wegen Erkrankung", enthielt. Die vollständige Liste übersandte eine Mitarbeiterin per E-Mail an alle dort Genannten mit der Bitte, fehlende Begründungen für den Nichtantritt und die unterlassene vorherige Anzeige nachzureichen und künftige Dienstreisen möglichst effizient zu planen.

Aus datenschutzrechtlicher Sicht handelt es sich bei diesem Vorgang um eine Nutzung von Arbeitnehmerdaten, für die gemäß § 4 Abs. 1 BSDSG eine Rechtsgrundlage vorhanden sein muss.

Hier lag weder eine Einwilligung der betroffenen Mitarbeiter noch eine Rechtsvorschrift vor, die die Nutzung der Daten in Form der unternehmensinternen Weiterleitung erlaubte.

Aus § 28 BDSG ist für die fragliche Datennutzung eine Rechtsgrundlage nicht ersichtlich. So diente es nicht dem Arbeitsvertragsverhältnis mit den betroffenen Bediensteten im Sinne von § 28 Abs. 1 Satz 1 Nr. 1 BDSG, wenn das Unternehmen ihre „Flugdaten“ anderen Mitarbeitern, die sich in der gleichen Situation befanden, mitteilte.

Im Rahmen der Prüfung von § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist festzustellen, dass es zum einen an einem berechtigten Interesse des Unternehmens fehlte, die Flugdaten an alle betroffene Bedienstete zu "verteilen". Eine dienstliche Erforderlichkeit für die Datenweiterleitungen durch die fragliche E-Mail ist nicht ersichtlich. Darüber hinaus standen einer Datenweiterleitung an die anderen Bediensteten die schutzwürdigen Interessen des einzelnen Mitarbeiters entgegen, der einen Anspruch auf vertrauliche Behandlung seiner Arbeitnehmerdaten und auf eine Verwendung dieser Daten nur im Rahmen des Notwendigen durch den Arbeitgeber hat.

Diese Datennutzung war somit nicht zulässig.

10.2 Erschleichen von Daten über die wirtschaftlichen Verhältnisse eines Mitarbeiters

Der Geschäftsführer eines Unternehmens wollte Erkundigungen über die wirtschaftlichen Verhältnisse eines Mitarbeiters einziehen. Er richtete zu diesem Zweck eine fingierte Finanzierungsanfrage für „einen Kunden“ an die Bank, mit der das Unternehmen in Geschäftsverbindung steht. Dabei gab er den Mitarbeiter als Kunden aus und übermittelte dessen Daten an die Bank, von der er daraufhin Daten zur Kreditwürdigkeit des Mitarbeiters erhielt.

Zunächst war die mit der fingierten Finanzierungsanfrage verbundene Übermittlung der Arbeitnehmerdaten an die Bank unzulässig, da sie nicht der Zweckbestimmung des Arbeitsvertrages diente (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Auch die Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG lagen nicht vor.

Darüber hinaus hat der Geschäftsführer mit der fingierten Finanzierungsanfrage vorsätzlich ein Datum zur Bonität des Betroffenen erschlichen und damit gegen den § 43 Abs. 2 Nr. 4 BDSG verstoßen. Nach dieser Vorschrift handelt ordnungswidrig, wer vorsätzlich oder fahrlässig durch unrichtige Angaben die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, erschleicht.

10.3 Mitarbeiterfotos im Intranet

Die Veröffentlichung von Mitarbeiterfotos im Intranet ist nur mit Einwilligung unter ausdrücklichem Hinweis auf die Freiwilligkeit zulässig.

Ein Unternehmen veröffentlicht Fotos aller Mitarbeiter im Intranet. Die Mitarbeiter waren gebeten worden, ein Foto für diesen Zweck zur Verfügung zu stellen.

Es kann dahinstehen, ob es sich bei diesem Vorgang noch um eine innerbetriebliche Nutzung oder bereits um eine Übermittlung von Arbeitnehmerdaten an Dritte gehandelt hat. In jedem Fall lag eine Datenverwendung vor, für die gemäß § 4 Abs. 1 BDSG eine Rechtsgrundlage vorhanden sein muss.

§ 28 Abs. 1 Nr. 1 BDSG kann nicht als Rechtsgrundlage herangezogen werden, da eine derartige unternehmensinterne Bildveröffentlichung nicht der Zweckbestimmung des Arbeitsvertragsverhältnisses dient. Sie ist - auch unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit - hierfür nicht erforderlich.

Eine Zulässigkeit ergibt sich auch nicht aus § 28 Abs. 1 Nr. 2 BDSG. Es ist schon zweifelhaft, ob die Veröffentlichung des Bildes eines Mitarbeiters im Intranet zur Wahrung eines berechtigten Interesses des Unternehmens erforderlich ist und ob die Argumentation des Unternehmens, man wolle letztlich das Zusammengehörigkeitsgefühl der Belegschaft stärken, dafür ausreicht. Auf jeden Fall überwiegt jedoch das schutzwürdige Interesse vieler Mitarbeiter daran, dass sehr persönliche Merkmale, wie sie auf einem Foto verzeichnet sind, einem größeren, dem Betroffenen wohl weitgehend unbekannten Personenkreis nicht übermittelt werden.

Als Rechtfertigung für die Bildveröffentlichung kommt somit nur eine Einwilligung der Arbeitnehmer in Betracht. Allerdings ist die Wirksamkeit von Einwilligungen im Rahmen von Arbeitsverhältnissen problematisch, weil es dort oft an der erforderlichen freien Entscheidung eines Arbeitnehmers fehlt. Die Autorität des Arbeitgebers und der Gruppendruck innerhalb der Belegschaft können die Freiwilligkeit einer Einwilligung eines Arbeitnehmers beeinträchtigen.

Um diesen Bedenken zu begegnen, muss im vorliegenden Fall sichergestellt werden, dass die Einstellung der Bilder für die Mitarbeiter freiwillig ist, und dass ein Mitarbeiter, der dies nicht will, keine Nachteile zu befürchten hat. Die absolute Freiwilligkeit dieser Aktion muss den Mitarbeitern bekannt sein.

Es ist fraglich, ob die Bitte an alle Mitarbeiter, ein Foto für das Intranet einzureichen, diesen Erfordernissen entspricht. Die Freiwilligkeit könnte man nach unserer Auffassung etwas besser dadurch erreichen, dass man den Mitarbeitern statt der „Bitte“ lediglich die „Möglichkeit anbietet“, ihre Fotos für eine Plattform im Intranet zur Verfügung zu stellen, und sie ausdrücklich darauf hinweist, dass es ihnen überlassen ist, ob sie von diesem Angebot Gebrauch machen. Unter Zurückstellung von Bedenken würden wir in diesem Fall von einer rechtswirksamen, konkludent mit der Einstellung in das Intranet erteilten Einwilligung in die dortige Veröffentlichung der Bilder gemäß § 4a BDSG und § 22 KunstUrhG ausgehen.

*** * ***

11 Gesundheitswesen

11.1 Datenschutzgerechte Altpapierentsorgung in Apotheken

Wir waren mit mehreren Vorgängen befasst, in denen Apotheken Papierunterlagen nicht den Vorgaben der Datensicherheit entsprechend aufbewahrt und entsorgt hatten.

So sind in einem Fall Papierunterlagen aus einer Apotheke in einer offenen Feuerstelle auf öffentlichem Gelände verbrannt worden. Die alarmierten Polizeibeamten fanden an der Feuerstelle und im umliegenden Bereich noch eine Menge nicht verbrannter Rezepte, die dann von der Polizei ordnungsgemäß beseitigt wurden.

Die polizeiliche Kontrolle in der Apotheke ergab, dass dort Rezepte in eine für jedermann zugängliche Papiertonne eingeworfen wurden.

In einem weiteren Fall entdeckte ein Bürger Papierunterlagen aus einer Apotheke, u. a. Rezepte, Schriftverkehr mit Krankenkassen mit personenbezogenen Daten von Patienten, in einem öffentlichen Altpapiercontainer. Bei unseren Ermittlungen gab der Inhaber der Apotheke an, diese Materialien seien wohl versehentlich nicht geschreddert und so als ganze Schriftstücke im öffentlichen Altpapiercontainer gelandet. Eigentlich gebe es in der Apotheke genaue Vorgaben, dass solche Papiere im Aktenvernichter entsprechend zu zerkleinern sind.

Die geschilderten Vorfälle stellen Verstöße gegen die sich aus § 9 BDSG einschließlich der dazugehörigen Anlage ergebenden Verpflichtungen zur Wahrung der Datensicherheit dar. Danach muss eine Apotheke gerade im Hinblick auf die Gesundheitsdaten ihrer Kunden alles tun, dass diese sicher vor dem Zugriff von Unbefugten sind. Dies war weder bei den Rezepten in der für jedermann zugänglichen Papiertonne noch bei der Entsorgung im öffentlichen Altpapiercontainer und schon gar nicht bei der schlampigen Verbrennung auf einem öffentlichen Gelände der Fall.

Soweit in derartigen Fällen bei den Verantwortlichen in der Apotheke bedingter Vorsatz, d. h. billigende Inkaufnahme bezüglich des Offenbarens eines Apothekergeheimnisses nachgewiesen werden kann, ist sogar der Straftatbestand des § 203 Abs. 1 Nr. 1 StGB erfüllt. Ein derartiger Nachweis war in den uns vorgetragenen Fällen nicht möglich.

Da ein Verstoß gegen Datensicherheitsvorschriften nicht bußgeldbewehrt ist, konnten wir jeweils nur eine Beanstandung gegenüber den verantwortlichen Apothekern aussprechen.

Eine Apotheke hat inzwischen eine Reihe von Sicherheitsmaßnahmen getroffen, insbesondere die Aufbewahrung der Papiertonne in den Apothekenräumen und das vorherige Schreddern der Papiere, die personenbezogene Daten enthalten, um solche Vorfälle künftig zu vermeiden.

Wir werden dies gelegentlich ebenso überprüfen wie die Zusagen der anderen Apotheker, künftig die ordnungsgemäße Altpapierentsorgung besonders im Auge zu haben.

11.2 Wahlwerbung durch Ärzte

Nutzt ein Arzt die Adressen seiner Patienten ohne deren Einwilligung zur Wahlwerbung, ist dies unzulässig.

In mehreren Fällen hatten Ärzte vor den Kommunalwahlen die in Ihrer Praxis gespeicherten Adressen ihrer Patienten dazu genutzt, diese anzuschreiben und darum zu werben, Ihnen bzw. einer bestimmten Partei oder Wählergruppe ihre Stimme zu geben.

Diese Datennutzungen waren unzulässig. Es lag weder eine Einwilligung der Patienten vor noch können die Vorschriften des § 28 Abs. 6 Nr. 3 und Abs. 7 Satz 2 BDSG die Nutzung einer Patientenadresse durch den Arzt für Wahlwerbezwecke rechtfertigen.

*** * ***

12 Vereine und Verbände

Heranziehung von Mitgliederadressen für Wahlwerbeschreiben

Das Datenschutzrecht steht einer Heranziehung von Mitgliederadressen für persönliche Wahlwerbeschreiben in aller Regel entgegen.

Die Mitgliederdateien der Vereine werden im Vorfeld von politischen Wahlen immer wieder von Kandidaten, die sich zur Wahl stellen, für die Versendung von Wahlwerbeschreiben genutzt. Die zahlreichen Eingaben und Beschwerden zu diesem Thema über mehrere Jahre hinweg zeigen uns, dass viele Vereinsmitglieder die Heranziehung ihrer Mitgliederadressen für persönliche Wahlwerbeschreiben missbilligen.

Folgende Fallkonstellationen wurden uns vorgetragen:

a) Der erste Vorsitzende eines Vereins kandidiert für den Stadtrat und sendet ein Werbeschreiben an die Vereinsmitglieder mit der Bitte, ihn zu wählen.

b) Ein Mitglied der Geschäftsführung eines Vereins sendet ein Wahlwerbeschreiben an die Eltern der Kinder des Kindergartens, dessen Träger der Verein ist.

c) Ein Funktionär eines Vereins, der einen berechtigten Zugang zu den Mitgliederadressen hat, übermittelt den Adressbestand an eine bei einer Wahl kandidierende Person außerhalb des Vereins.

In den Fällen a) und b) handelt es sich um Nutzungen der Mitglieder- bzw. Elternadressen. Im Fall c) hat ein Vertreter des Vereins die Mitgliederadressen an einen Wahlkandidaten außerhalb des Vereins übermittelt.

Alle genannten Datenverwendungen waren nicht zulässig. Es lag weder eine Einwilligung der Vereinsmitglieder bzw. der Eltern der Kindergartenkinder noch eine die Verwendungen rechtfertigende Rechtsvorschrift vor. Insbesondere sind die Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 bzw. des Abs. 3 Satz 1 Nr. 3 BDSG nicht gegeben.

Man muss annehmen, dass die Vereinsmitglieder ein schutzwürdiges Interesse an dem Ausschluss der Nutzung bzw. Übermittlung zum Zweck der Wahlwerbung haben. Sie vertrauen darauf, dass ihre Mitgliederdaten nur für satzungsmäßige Ver-

einszwecke verwendet werden. In aller Regel rechnen sie nicht damit, dass die Daten vom Verein für Wahlwerbung genutzt oder an Dritte zur politischen Wahlwerbung übermittelt werden. Deshalb überwiegen die entgegenstehenden schutzwürdigen Interessen der Mitglieder die berechtigten Interessen der Wahlkandidaten.

Diese Abwägung entspricht auch der Interessenlage der Eltern der Kindergartenkinder im Fall b).

Im Fall c) ist auf Seiten des Empfängers der unzulässiger Weise übermittelten Adressen die Speicherung und Nutzung dieser Daten für Wahlwerbezwecke in gleicher Weise unzulässig. Auch dort überwiegen die entgegenstehenden schutzwürdigen Interessen der Vereinsmitglieder die berechtigten Interessen des Kandidaten an einer Wahlwerbung (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG).

Hinweis:

Zur **Veröffentlichung von Sportgerichtsurteilen und Spielersperren** durch Vereine im Internet bzw. Intranet vgl. bei Nr. 14.4 sowie

zur **Veröffentlichung von Fotos auf der Homepage eines Sportvereins** vgl. bei Nr. 14.5.

*** * ***

13 Videoüberwachung

13.1 Videoüberwachung in öffentlich zugänglichen Räumen

13.1.1 Videoüberwachung vor einer Bankfiliale

Der auf Grund der Interessenabwägung festgelegte Umfang des überwachten Bereiches wurde vom städtischen Ordnungsamt und der Polizei für ausreichend erachtet.

Eine Bank überwachte mit zwei Videokameras den Gebäudeeingang und die Außenfassade einschließlich der davor liegenden Straßenkreuzung bis hin zu dem gegenüberliegenden Gehweg, auf dem sich Tische und Stühle eines Cafes befinden. Dagegen richtete sich eine Beschwerde. In ihr wurde die Zulässigkeit einer derart weit reichenden Überwachung von öffentlichem Straßenraum bezweifelt.

Banken haben unbestritten ein hohes Sicherheitsbedürfnis. Eine Videoüberwachung der Straßenfront des Bankgebäudes leistet einen Beitrag zur Gewährleistung der Sicherheit. Sie ist zur Wahrnehmung des daran bestehenden berechtigten Interesses einer Bank erforderlich. Auf der anderen Seite haben die Passanten, Gäste des Cafes und Kunden der Bank ein schutzwürdiges Interesse daran, dass keine Videoaufzeichnungen von ihnen gefertigt werden, mit denen ihr Verhalten - zumindest für eine gewisse Zeit - rekonstruierbar ist.

Um beiden Interessenlagen gerecht zu werden, muss einerseits die Videoüberwachung geeignete Aufnahmen für die Gewährleistung der Sicherheit liefern können. Mit zunehmendem Abstand von der Außenfassade fällt aber die Interessenabwägung gemäß § 6 b Abs. 1 BDSG zugunsten derjenigen aus, die sich ohne böse Absichten auf öffentlichem Grund aufhalten.

Ausgehend von diesen Überlegungen schätzten wir die entgegenstehenden schutzwürdigen Interessen der Passanten auf dem gegenüberliegenden Gehsteig und der Gäste des Cafes höher ein als die Sicherheitsinteressen der Bank und forderten, diesen Bereich aus der Videoüberwachung herauszunehmen.

Das auf unsere Anregung hin von der Bank eingeschaltete städtische Ordnungsamt und die Polizei bestätigten, dass die von uns geforderte Einschränkung des überwachten Bereiches auch aus dortiger Sicht vertretbar ist.

13.1.2 Videoüberwachung und -aufzeichnung der Kassenbereiche in Einkaufsmärkten

Für bestimmte Zwecke ist eine Zulässigkeit gegeben.

In zahlreichen Einkaufsmärkten werden die Kassen videoüberwacht. Es ist anzuerkennen, dass die Videoüberwachung zur Wahrnehmung berechtigter Interessen im Sinne von § 6 b Abs. 1 Nr. 3 BDSG für folgende Zwecke erforderlich ist:

- Schutz des Eigentums
- Sicherung von Beweismaterial bei Straftaten, insbesondere bei Diebstahl und bei Überfällen
- Aufklärung von Kassendifferenzen und Streitigkeiten oder Unklarheiten beim Zahlungsvorgang

Diese einzelnen berechtigten Interessen eines Einkaufsmarktes überwiegen das schutzwürdige Interesse der Kunden daran, dass keine Videoaufnahmen von ihnen gefertigt werden, die für eine spätere Auswertung zur Verfügung stehen und ihr Verhalten im Nachhinein nachvollziehen lassen. Der Kunde befindet sich in einem Einkaufsmarkt in der Öffentlichkeit und damit in einem Bereich, in dem er von anderen Personen, insbesondere von Mitarbeitern des Marktes, gesehen wird. Das Zahlen an der Kasse stellt einen "neutralen" Vorgang dar, bei dem eine Videoüberwachung bzw. -aufzeichnung die Persönlichkeit eines Kunden nur unerheblich tangiert. Etwas anderes gilt allerdings für die Erfassung der PIN-Eingabe. Sie ist stets unzulässig. Es sind deshalb entsprechende technische Vorkehrungen zu treffen (vgl. Kapitel 14.1.3.6 unseres Tätigkeitsberichts 2006).

Die Interessenabwägung ergibt somit die Zulässigkeit einer derartigen Videoüberwachung bzw. -aufzeichnung zu den oben genannten Zwecken. Dies gilt auch für die entsprechenden Auswertungen (Datennutzungen).

Soweit kein konkreter Verdacht vorliegt, darf die Videoüberwachung jedoch nicht für eine ständige Verhaltens- und Leistungskontrolle des Kassenpersonals genutzt werden. Insoweit überwiegen die schutzwürdigen Interessen des Personals.

Durch entsprechende Regelungen für die Auswertung, z. B. durch ein Vier-Augen-Prinzip mit dem Datenschutzbeauftragten und dem Betriebsrat, ist sicherzustellen,

dass eine unbefugte Beobachtung oder eine unbefugte Auswertung der Videoaufnahmen nicht erfolgt.

13.1.3 Klingelkameras

Videokameras, die im Klingeltableau neben einer Haustür angebracht sind und die Person erkennen lassen, die gerade geklingelt hat, sind grundsätzlich zulässig.

Die Prüfung, wer geklingelt hat und ob man dieser Person Zutritt gewähren will, stellt ein berechtigtes Interesse der Bewohner dar (§ 6b Abs. 1 Nr. 3 BDSG), wenn sie die Außenseite der Haustür nicht einsehen können. Die Personen, die Einlass begehren, haben kein überwiegendes schutzwürdiges Interesse daran, dass eine solche Zutrittskontrolle nicht stattfindet.

Allerdings ist zu beachten, dass keine schutzwürdigen Interessen Dritter berührt werden. Daher ist die Kamera so einzurichten, dass nur kurze Zeit nach dem Klingeln ein Bild in die Wohnung, bei der geklingelt wurde, übertragen wird und dass nur der unmittelbare Umgriff der Haustür erkennbar ist. Eine Dauerbeobachtung des Bürgersteiges vor dem Grundstück wäre unzulässig.

Am Klingeltableau ist ein Hinweis auf die Videoüberwachung anzubringen.

13.1.4 Erfassung von Kfz-Kennzeichen

a) Kennzeichenerfassung zur monatlichen Abrechnung der Parkgebühren der Dauerkunden eines Parkhauses

Der Vertrag zwischen dem Parkhausbetreiber und dem Dauerkunden sieht vor, dass die Gebühr für die Parkhausbenutzung monatlich auf Grund der tatsächlich angefallenen Parkzeiten abgerechnet wird. Die Parkzeiten werden dadurch ermittelt, dass beim jeweiligen Ein- und Ausfahren das Kfz-Kennzeichen von einer Videokamera erfasst und protokolliert wird.

Dabei ist darauf zu achten, dass der Kunde im Vertrag deutlich über den Umstand der videogestützten Kennzeichenerfassung und -speicherung informiert wird. Nur bei ausreichender Transparenz und besonderer Hervorhebung kann dies wirksamer Vertragsbestandteil werden.

Unter diesen Umständen dient die Erhebung und Speicherung des Kennzeichens der Zweckbestimmung des Parkvertrages und ist daher gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig.

b) Speicherung und Nutzung der „verkürzten" Kennzeichen aller in das Parkhaus einfahrenden Autos zur statistischen Auswertung (Herkunftsgebiet, Parkdauer)

Bei der nach § 6 b Abs. 1 BDSG vorzunehmenden Interessenabwägung kommen wir zu dem Ergebnis, dass für eine statistische Auswertung die vollständige Erfassung der Kfz-Kennzeichen (z. B. M - XY - 1234) nicht erforderlich und daher unzulässig ist.

Vertretbar ist jedoch die Speicherung eines Teils des Kfz-Kennzeichens (z. B. M - XY - 1). Dies kann durch entsprechende technische Maßnahmen erreicht werden. Auf diese Weise wird die Erkennbarkeit des konkreten Fahrzeuges wesentlich erschwert. Damit werden die schutzwürdigen Interessen der Betroffenen ausreichend gewahrt.

c) Verkehrszählung durch eine Bürgerinitiative.

Eine Bürgerinitiative hatte zur Begründung ihrer Forderungen eine videokameragestützte Verkehrszählung durchgeführt. Im Hinblick auf die Frage, ob eine Ortsumgehung erforderlich ist, sollte ermittelt werden, wie viele Verkehrsteilnehmer in der Ortschaft für Einkäufe etc. einen Zwischenstopp einlegen. An der Ortsein- und ausfahrt war jeweils in jede Fahrtrichtung eine Kamera installiert, so dass gemessen werden konnte, wie lange der Fahrer für die Ortsdurchfahrt benötigt. Dabei waren die Kameras so eingestellt, dass jeweils das vollständige Fahrzeug einschließlich des Kfz-Kennzeichens und des Fahrers erfasst wurde.

Eine so weit gehende Datenerfassung war zum Erreichen des durchaus berechtigten Verkehrszählungszweckes nicht erforderlich und damit unzulässig.

Es hätte vielmehr ausgereicht, wie unter b) dargestellt, einen Teil des Kfz-Kennzeichens der vorbeifahrenden Fahrzeuge zu speichern und deren Durchfahrtszeit zu messen. Unter diesen Umständen wäre die Verkehrszählung datenschutzrechtlich zulässig.

13.2 Aufzeichnung von Videoaufnahmen in nicht öffentlich zugänglichen Räumen

13.2.1 Videoaufzeichnung in der Sammelumkleidekabine

Im überprüften Fall war die Videoüberwachung zur Wahrung berechtigter Interessen der verantwortlichen Stelle nicht erforderlich und das schutzwürdige Interesse der betroffenen Schüler stand entgegen.

Uns wurde folgender Fall vorgetragen:
In einem Hallenbad dürfen sich während des Schulschwimmens außer den Schülern keine anderen Personen in der Sammelumkleidekabine aufhalten. Da es immer wieder vorkam, dass gegen dieses Verbot verstoßen wurde, sollten Videoaufzeichnungen gefertigt werden, um auf diese Weise andere Badegäste von den Sammelumkleidekabinen fern zu halten und mögliche Störer identifizieren zu können.

Da es sich hier nicht um einen öffentlich zugänglichen Raum handelt, ist die Zulässigkeit einer Aufzeichnung am Maßstab der Abwägungsvorschrift des § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu prüfen.

Wir kamen zu dem Ergebnis, dass in dem vorgetragenen Fall die Videoüberwachung zur Wahrung berechtigter Interessen der verantwortlichen Stelle nicht erforderlich war und dass darüber hinaus das schutzwürdige Interesse der betroffenen Schüler entgegenstand.

Erforderlich ist eine Maßnahme nur dann, wenn keine anderen, weniger beeinträchtigenden Mittel zum Erreichen des festgelegten Zweckes zur Verfügung stehen. Dass bisher alle anderen Mittel zum Schutz der Kinder beim Umkleiden erfolglos ausgeschöpft wurden, konnten wir nicht feststellen:

- Es war im vorliegenden Fall im Bad nicht für jedermann ausreichend kenntlich gemacht, dass die Sammelumkleideräume während des Schulschwimmens von anderen Badegästen nicht genutzt werden dürfen.

- Es waren bereits vor den Umkleidekabinen (zulässigerweise) Videokameras installiert. Ist den Badegästen bekannt, dass ein Aufenthalt in den Sammelumkleidekabinen verboten und die Bereiche davor mit Kameras überwacht werden, dürf-

te dies zur Abschreckung genügen und gegenüber einem Störer ein unbefugtes Betreten der Sammelumkleidekabine nachweisbar sein.

- Eine zusätzliche Kamera in den Umkleidekabinen kann nicht als ein geeignetes Mittel zum Erreichen dieses Zweckes angesehen werden. Es ist vielmehr Aufgabe des Personals des Bades sowie der Aufsicht führenden Lehrkräfte, Unbefugte von den Sammelumkleidekabinen fern zu halten.

Unter diesen Umständen haben die Schüler ein schutzwürdiges Interesse daran, dass sie beim Umkleiden nicht beobachtet oder aufgezeichnet werden, zumal besondere Umstände, die eine Videoaufzeichnung in der Sammelumkleidekabine rechtfertigen könnten, im vorgetragenen Fall nicht erkennbar waren.

Die Videoaufzeichnung in der Sammelumkleidekabine war deshalb hier unzulässig.

13.2.2 Videoüberwachung in der Wohnanlage

Wir haben die Videoüberwachung von gefährdeten Bereichen innerhalb der Wohnanlage für zulässig erachtet.

Die Eigentümerversammlung einer großen Wohnanlage beschloss mehrheitlich, sämtliche Eingänge, den Kellervorraum und den Aufzugsbereich im Keller mit Videokameras zu überwachen, weil in der Vergangenheit Keller aufgebrochen wurden und fremde Personen in den Kellerräumen übernachtet haben.

Eine Videoaufzeichnung ist gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG nur dann zulässig, wenn dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Der Schutz der Bewohner und des Eigentums stellen berechtigte Interessen der Eigentümer dar. Dabei reicht allerdings eine allgemeine Gefahrenvorsorge nicht aus. Vielmehr müssen belegbare Tatsachen die Annahme rechtfertigen, dass es zu Belästigungen oder Schäden kommen kann.

Bei den schutzwürdigen Interessen der Betroffenen am Ausschluss einer Videoüberwachung war im vorgetragenen Fall wie folgt zu differenzieren:

1. Die Aufnahmen im Kellervorraum und im Aufzugsbereich im Keller können zur Aufklärung etwaiger Taten beitragen, weil damit feststellbar ist, welche hausfremden Personen sich zur Zeit bestimmter Vorfälle dort aufgehalten haben. Es handelte sich dabei um gefährdete Bereiche. Schutzwürdige Interessen der Betroffenen sind hier weniger tangiert. Sie überwiegen deshalb die berechtigten Interessen an einer Videoaufzeichnung nicht.

   Im Ergebnis hielten wir die Videoüberwachung der Kellervorräume und des Aufzugbereichs im Keller unter der Voraussetzung für zulässig, dass nur wenige autorisierte Personen die Aufzeichnungen zum Zweck der Aufdeckung von Straftaten einsehen können.

2. Bei den Eingängen handelt es sich zum Einen nicht um gefährdete Bereiche. Zum Anderen wird lückenlos aufgezeichnet, wer zu welcher Zeit das Haus betritt oder verlässt, so dass ein umfassendes Bewegungsprofil erstellt werden könnte. Eine derartige Überwachung greift erheblich in das Persönlichkeitsrecht der Betroffenen ein. (vgl. LG Berlin, Urteil vom 31.10.2000, Az. 65 S 279/00; OLG Köln, Urteil vom 13.10.1988, Az. 18 U 37/88).

   Insgesamt gesehen überwiegen die schutzwürdigen Interessen der Betroffenen daran, dass hier keine Videoüberwachung stattfindet. Die Videoüberwachung an den Eingängen war deshalb nicht zulässig.

*** * ***

14 Veröffentlichung personenbezogener Daten im Internet

14.1 Allgemeines

Es ist geradezu ein Volkssport geworden, Tatsachen, Meinungen und Bewertungen, die sich auf andere Personen beziehen, sowie Bilder und Videoaufnahmen, auf denen andere Personen erkannt werden können, im Internet weltweit zu veröffentlichen. Dies geschieht vor allem auf den eigenen Homepages, auf Bewertungsplattformen, wie spickmich.de, meinprof.de, und bei sozialen Netzwerken, wie z. B. StudiVZ, SchülerVZ, MySpace oder Facebook.

Die Anwendbarkeit des BDSG auf die Bewertungen und sonstigen Angaben über Dritte im Internet ergibt sich daraus, dass diese Veröffentlichungen Einzelangaben über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren Personen und damit personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG enthalten.

Der Begriff des personenbezogenen Datums ist viel weiter als landläufig immer angenommen wird. Es gehören deshalb nicht nur die „klassischen“ Daten, wie Name, Vorname, Adresse, Geburtsdatum und Personenstand dazu. Der Gesetzgeber wollte vielmehr alle Informationen erfassen, die über eine Bezugsperson etwas aussagen. Somit umfasst dieser Begriff u. a. auch

- Meinungsäußerungen, Beurteilungen und Werturteile, die sich auf eine bestimmte oder bestimmbare Person beziehen,

- die Wiedergabe von mündlichen und schriftlichen Aussagen einer Person,

- die Darstellung des privaten oder des dienstlichen Verhaltens einer Person,

- vereinsrechtliche Entscheidungen, wie Spielersperren und Sportgerichtsurteile.

Bei der Veröffentlichung personenbezogener Daten im Internet handelt es sich um Datenübermittlungen an Dritte im Sinne des § 3 Abs. 4 Nr. 3 BDSG in der Form, dass die Dritten die zur Einsicht oder zum Abruf bereitgehaltenen Daten einsehen oder abrufen.

Die Zulässigkeit dieser Datenübermittlungen bestimmt sich nach den Vorschriften des BDSG. Als Rechtfertigungen für die Veröffentlichung personenbezogener Daten anderer Personen im Internet kommen gemäß § 4 Abs. 1 BDSG in Betracht:

a) Die Einwilligung der betroffenen Person (§ 4a BDSG)

Die Person muss vorher – in der Regel schriftlich – ihre Einwilligung in die konkrete Veröffentlichung erklärt haben.

b) Allgemeine Zugänglichkeit der Daten oder Veröffentlichungsbefugnis (§ 28 Abs. 1 Satz 1 Nr. 3 BDSG)

Die Voraussetzungen dieser Bestimmung liegen zum Beispiel vor, wenn die in das Internet eingestellte Information bereits in der Zeitung veröffentlicht ist oder wenn es um die Ergebnisse einzelner Personen bei öffentlichen Sportveranstaltungen geht.

Derartige Veröffentlichungen sind in der Regel zulässig, es sei denn das entgegenstehende schutzwürdige Interesse der Betroffenen überwiegt im Einzelfall offensichtlich.

c) Zweckbestimmung eines Vertrages (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG)

Die Mitarbeiter eines Unternehmens, die Kunden oder Vertragspartnern bekannt sein sollten, müssen es in der Regel hinnehmen, dass ihre dienstlichen Kontaktdaten, jedoch ohne Foto, auf der Homepage des Unternehmens präsentiert werden. Rechtsgrundlage ist hier der Arbeitsvertrag.

Dagegen entspricht es nicht der Zweckbestimmung eines Kaufvertrages, wenn der Gläubiger den säumigen Schuldner im Internet auf einer Art „Schuldnerpranger“ einer weltweiten Öffentlichkeit vorstellt.

d) Interessenabwägung (§ 28 Abs. 1 Satz 1 Nr. 2, § 29 Abs. 2 BDSG)

Eine Internetveröffentlichung ist nach 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig, wenn sie zur Wahrung berechtigter Interessen dessen, der personenbezogene Daten im Internet veröffentlicht, erforderlich ist und wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss einer derartigen Veröffentlichung überwiegt.

In gleicher Weise ist diese Interessenabwägung bei der Bestimmung des schutzwürdigen Interesses in den Fällen durchzuführen, die in den Anwendungsbereich des § 29 Abs. 2 BDSG fallen.

Nach unserer Auffassung ist in diesen Fällen das entgegenstehende schutzwürdige Interesse des Betroffenen in aller Regel höher einzuschätzen, was zur Unzulässigkeit dieser Internetveröffentlichungen führt. Schließlich wird mit einer mehr oder weniger öffentlichen und weltweiten Vorführung im Internet in erheblicher Weise in das Persönlichkeitsrecht der Betroffenen eingegriffen.

Dies gilt insbesondere für Leistungsbewertungen, für Anprangerungen und Warnhinweise sowie für die Darstellung von Verhaltensweisen und Äußerungen von Personen. Auf unsere Tätigkeitsberichte 2002/2003 (Kap. 14.1) und 2006 (Kap. 15.2) wird hingewiesen. Im Folgenden werden weitere Einzelfälle von Interessenabwägungen dargestellt.

14.2 Bewertungsplattformen

Bewertungen von Personen im Internet sind nur mit deren Einwilligung zulässig.

Im Internet existieren Bewertungsportale für berufliche Leistungen zahlreicher Berufssparten, z. B. für Hochschulprofessoren, Lehrer, Ärzte, Handwerker, Finanzberater usw.

Das Oberlandesgericht Köln vertrat in seinem noch nicht rechtskräftigen Urteil vom 03.07.08 - 5 U 43/08 - zur Lehrerbewertungsplattform spickmich.de die Auffassung, dass im Rahmen der Interessenabwägung der Meinungsfreiheit der Vorrang vor dem informationellen Selbstbestimmungsrecht der Lehrer einzuräumen ist und somit die Bewertungen zulässig sind. Etwas anderes gelte lediglich dann, wenn es sich um eine reine Schmähkritik oder eine Formalbeleidigung handele oder sich die Äußerung als Angriff auf die Menschenwürde darstelle. Dieses Urteil steht derzeit auf dem Prüfstand des Bundesgerichtshofs.

Im Gegensatz zu dieser Rechtsprechung hat der Düsseldorfer Kreis, die Konferenz der Datenschutzaufsichtsbehörden der Bundesländer, zu den Bewertungsportalen im Internet im April 2008 folgenden einstimmigen Beschluss gefasst:

"1. Die Datenschutzaufsichtsbehörden weisen darauf hin, dass es sich bei Beurteilungen und Bewertungen von Lehrerinnen und Lehrern sowie von vergleichbaren Einzelpersonen in Internet-Portalen vielfach um sensible Informationen und subjektive Werturteile über Betroffene handelt, die in das Portal eingestellt werden, ohne dass die Urheber erkennbar sind und die jederzeit von jedermann abgerufen werden können.

2. Anbieter entsprechender Portale haben die Vorschriften des Bundesdatenschutzgesetzes über die geschäftsmäßige Verarbeitung personenbezogener Daten einzuhalten.

3. Bei der danach gesetzlich vorgeschriebenen Abwägung ist den schutzwürdigen Interessen der bewerteten Personen Rechnung zu tragen. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen."

Soweit wir die Zulässigkeit von Bewertungen in Internetportalen zu beurteilen hatten, schätzten wir das entgegenstehende schutzwürdige Interesse der im Internet bewerteten Personen regelmäßig höher ein als die Meinungsfreiheit der Bewertenden. Dies gilt nicht nur für den Bereich der Privatsphäre, sondern auch im Bereich der Sozialsphäre, zu der die berufliche Tätigkeit der Betroffenen gehört. Schließlich wird mit einer öffentlichen und weltweiten Vorführung im Internet in erheblicher Weise in das Persönlichkeitsrecht einer bewerteten Person eingegriffen. Sie wird gerade auf diese Weise zum gläsernen Bürger! In Anwendung der Grundsätze des Volkszählungsurteils des Bundesverfassungsgerichts aus dem Jahr 1983 muss vielmehr jeder Mensch im Rahmen des ihm zustehenden informationellen Selbstbestimmungsrechts selbst darüber entscheiden können, ob er im Internet bewertet wird, d. h. ihm muss das Recht zur Entscheidung verbleiben, ob er weltweit "ausgetragen", "ausgestellt" und "vorgeführt" wird.

Dabei spielt es auch keine Rolle, zu welchem Ergebnis die Bewertung einzelner Personen kommt. Wie Eingaben deutlich machen, fühlen sich Personen auch dann in ihrem Persönlichkeitsrecht verletzt, wenn das Ergebnis ihrer Bewertung positiv ausgefallen ist.

Im Ergebnis sehen wir somit Bewertungen im Internet als unzulässig an, sofern nicht eine wirksame Einwilligung der Betroffenen vorliegt.

14.3 Aussagen über andere Personen im Internet

Derartige Äußerungen sind im Internet nur mit der Einwilligung der betroffenen Personen zulässig.

Im Internet sind in Foren, Gästebüchern, Blogs usw. immer wieder meist kritische Äußerungen über Einzelpersonen zu finden. Die Palette der Anmerkungen ist breit gefächert. Viele Autoren machen dadurch ihrem Ärger, ihrer Enttäuschung oder ihrem Unverständnis über das Verhalten bestimmter oder bestimmbarer Personen Luft.

Immer wieder erreichten uns Eingaben, in denen die Betroffenen die Löschung der über sie eingestellten Beiträge anstrebten.

Mit der gleichen datenschutzrechtlichen Einschätzung wie unter 14.2 haben wir solche Äußerungen über andere Personen als unzulässig beurteilt

14.4 Sportgerichtsurteile und Sperrlisten

Sportgerichtsurteile dürfen, soweit keine Einwilligung der Betroffenen vorliegt, im Internet nur anonymisiert veröffentlicht werden.

Personenbezogene Sperrlisten dürfen ohne Einwilligung der Betroffenen nicht im Internet veröffentlicht werden. Eine Veröffentlichung im Intranet des Verbandes ist zulässig, wenn gewährleistet ist, dass in den Vereinen nur zuständige Personen zugreifen können.

Veröffentlicht ein Sportverband Sportgerichtsurteile und sog. Sperrlisten jeweils mit den Namen der betroffenen Sportler im offenen Internet, ist festzustellen, dass für derartige Datenübermittlungen eine rechtfertigende Rechtsvorschrift nicht vorhanden ist.

Gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG wäre diese Datenübermittlung dann zulässig, wenn sie der Zweckbestimmung eines vertragsähnlichen Vertrauensverhältnisses dient. Die Beziehung eines Vereinsmitgliedes zu dem jeweiligen Landessportverband kann als vertragsähnliches Vertrauensverhältnis im Sinne dieser Vorschrift qualifiziert werden. Es wird ausgefüllt von der Vereinssatzung und den Ordnungen des Landesverbandes. Bei manchen Verbänden sehen diese internen Ordnungen die Veröffentlichung von Sportgerichtsurteilen und Sperren im offenen Internet ausdrücklich vor.

Derartige Veröffentlichungen dienen zwar dem Ablauf und der Ordnung des Spielbetriebs auf Verbandsebene. Sportgerichtsurteile und angeordnete Sperren wirken nicht nur gegenüber dem betroffenen Sportler, sondern ihre Kenntnis ist auch für seinen Verein und für zahlreiche andere Vereine und Mannschaften von Bedeutung. So erfolgt anhand der Internetveröffentlichungen eine gegenseitige Kontrolle der am Spielbetrieb teilnehmenden Mannschaften, ob Sportler der gegnerischen Mannschaft auch tatsächlich spielberechtigt sind. Die Veröffentlichung im offenen Internet ist eine kostengünstige Möglichkeit, alle Vereine schnell und gleichberechtigt zu informieren.

Den weltweiten Veröffentlichungen im Internet steht jedoch entgegen, dass sie objektiv nicht erforderlich sind. Sie entsprechen nicht dem Grundsatz der Verhältnismäßigkeit. In diesem Rahmen sind auch die schutzwürdigen Interessen der betroffenen Sportler zu berücksichtigen. Es stellt eine erhebliche Beeinträchtigung deren Persönlichkeit dar, wenn sich Arbeitgeber, Mitarbeiter, Freunde oder Nachbarn über das Verhalten einer Person beim Sport im Internet informieren können.

Die Veröffentlichungen von Sportgerichts- und Sperrlistendaten erfüllen den damit verfolgten Zweck, wenn sie nur an Personen und Stellen übermittelt werden, die an dem Sportgerichtsverfahren beteiligt waren oder die die in den Sperrlisten enthaltenen Informationen für einen reibungslosen Ablauf des Spielbetriebes benötigen. Um diesen Zweck zu erreichen, ist eine weltweite Veröffentlichung der Sportgerichtsurteile und Sperrlisten im Internet objektiv nicht erforderlich. Sie schießt weit über dieses Ziel hinaus und kann somit nicht auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG gestützt werden.

Eine Zulässigkeit dieser Internetveröffentlichungen ergibt sich im Hinblick auf die im Rahmen der Interessenabwägung schwerer wiegenden schutzwürdigen Interessen der Sportler auch nicht aus § 28 Abs. 1 Satz Nr. 2 BDSG (vgl. oben 14.1 d). Darüber hinaus liegen die Zulässigkeitsvoraussetzungen des § 28 Abs. 1 Satz 1 Nr. 3 BDSG ebenfalls nicht vor.

Da eine Rechtsvorschrift somit für die Veröffentlichung von Sportgerichtsurteilen mit Namensnennungen und Sperren von Sportlern im offenen Internet nicht zur Verfügung steht, wäre sie nur mit der Einwilligung der betroffenen Sportler zulässig.

Nach unserer Auffassung sind jedoch mit dem Datenschutzrecht vereinbar:

1. die Veröffentlichung von gemäß § 3 Abs. 6 BDSG anonymisierten Sportgerichtsurteilen im Internet,

2. die personenbezogene Veröffentlichung der Sperrlisten im Intranet eines Verbandes. Hierbei ist jedoch zu beachten, dass in den einzelnen Vereinen nur diejenigen Personen darauf zugreifen können, die diese Informationen für die Abwicklung des Spielbetriebes benötigen.

14.5 Fotos auf der Homepage eines Sportvereins

Bilder von offiziellen Wettkämpfen sind kraft gesetzlicher Vorschriften zulässig.

Dagegen bedürfen Bilder vom Training und Portraitaufnahmen der Einwilligung.

Aus datenschutzrechtlicher Sicht stellt die Veröffentlichung von Fotos vom Training oder von Wettkämpfen und Mannschaftsspielen auf der Homepage eines Sportvereins eine Übermittlung personenbezogener Daten der abgebildeten Personen dar. Sie ist zulässig, wenn eine Rechtsvorschrift sie erlaubt oder die abgebildeten Personen eingewilligt haben.

Daneben sind die Vorschriften der §§ 22 ff. KunstUrhG zum "Recht am eigenen Bild" zu beachten. Danach dürfen Bildnisse grundsätzlich nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden (§ 22 Satz 1 KunstUrhG). Abweichend davon sieht u. a. § 23 Abs. 1 Nr. 3 KunstUrhG vor, dass Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben, ohne Einwilligung verbreitet werden dürfen.

Man muss bei der Veröffentlichung von Bildern auf der Homepage eines Sportvereins wie folgt unterscheiden:

1. Die Veröffentlichung von Bildern, die während öffentlicher Wettkämpfe oder Spiele aufgenommen worden sind, ist zulässig.

   Aus datenschutzrechtlicher Sicht handelt es sich um allgemein zugängliche Daten im Sinne des § 28 Abs. 1 Nr. 3 BDSG. Auf Grund dieser Vorschrift ist die Veröffentlichung der Fotos im Internet ohne Einwilligung der abgebildeten Personen zulässig. Man darf zumindest im Normalfall davon ausgehen, dass deren entge-

genstehendes schutzwürdiges Interesse das berechtigte Interesse des Vereins nicht offensichtlich überwiegt.

Auch nach der Ausnahmevorschrift des § 23 Abs. 1 Nr. 3 KunstUrhG ist eine Einwilligung nicht erforderlich, da die Bilder bei öffentlichen Veranstaltungen aufgenommen worden sind.

Die Praxis, dass derartige Bilder auf der Homepage bekannt gemacht werden, ist vereinsintern in geeigneter Weise bekannt zu machen.

2. Anders stellt sich die Rechtslage bei der Internetveröffentlichung von Bildern dar, die während eines nicht öffentlichen Trainings gefertigt wurden, oder wenn es sich um Portraitaufnahmen der Sportler handelt.

   Diese Internetveröffentlichungen sind sowohl in datenschutzrechtlicher Hinsicht als auch gemäß § 22 Satz 1 KunstUrhG nur zulässig, wenn eine vorher erteilte Einwilligung der abgebildeten Personen vorliegt. Gemäß § 4a BDSG bedarf sie der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

Bei Jugendlichen kommt es für die Frage, ob sie eine Einwilligung wirksam erteilen können, nicht auf die Geschäftsfähigkeit, sondern auf die Einsichtsfähigkeit an. Dabei gehen wir bezüglich der Bilderveröffentlichungen im Internet von der Faustregel aus, dass bis zur Vollendung des 16. Lebensjahres neben der Einwilligung der Jugendlichen auch die der Eltern erforderlich ist. Nach Vollendung des 16. Lebensjahres genügt allein die Einwilligung der Jugendlichen.

*** * ***

15 Datensicherheit

15.1 Unzulässige Übermittlung von Daten bei der Entsorgung von Datenträgern

Die Entsorgung nicht ordnungsgemäß gelöschter Datenträger stellt eine unzulässige Übermittlung von personenbezogenen Daten dar.

Ein Geschäftsinhaber entsorgte eine – vermeintlich nicht mehr funktionsfähige – externe Festplatte mit gespeicherten Kunden- und Personaldaten auf dem örtlichen Wertstoffhof. Entsprechend den abfallrechtlichen Bestimmungen wurde der Datenträger von dort aus zur Wiederverwendung weitergegeben. Der neue Eigentümer konnte den Defekt der Festplatte beheben und die gespeicherten Kunden- und Personaldaten rekonstruieren.

Die Weitergabe der Festplatte, auf der sich noch lesbare Daten befanden, stellt eine Übermittlung personenbezogener Daten dar. Sie erfüllt auch den Tatbestand einer Ordnungswidrigkeit im Sinne des § 43 Abs. 2 Nr. 1 BDSG. Der Geschäftsinhaber hat fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, übermittelt. Wir haben deshalb ein Bußgeldverfahren durchgeführt.

Zur Vermeidung derartiger Datenschutzverstöße muss vor der Entsorgung von Festplatten, Laptops, PC`s usw. darauf geachtet werden, dass sich keine personenbezogenen Daten mehr auf dem Datenträger befinden bzw. dass keine Rekonstruktion dieser Daten mehr möglich ist. Dies erreicht man nach den Empfehlungen des Bundesamtes für Informationssicherheit (vgl. im Internet unter http://www.bsi.de/) beispielsweise durch den Einsatz von Löschprogrammen, welche die Daten mit unterschiedlichen Datenmustern mehrmals überschreiben und nicht zuletzt auch durch eine mechanische Zerstörung des Datenträgers.

15.2 Entsorgung von Alt-Handys

Alt-Handys als "Datenschleudern"

Funktioniert ein Handy nicht mehr oder soll ein moderneres Handy angeschafft werden, machen sich viele Menschen keine Gedanken über eine Löschung der auf dem Alt-Handy gespeicherten personenbezogenen Daten oder Bilder (SIM-Karten, sonstige Datenspeicher auf dem Handy, zusätzliche Speicherkarten etc.). Die Auskünfte,

die der Fachhandel zur datenschutzgerechten Entsorgung von Alt-Handys gibt, sind meist unzureichend.

Wir empfehlen anfragenden Bürgern, die Alt-Handys im Fachhandel oder bei zuverlässigen Sammel-Organisationen für elektronische Artikel zurückzugeben und sich eine datenschutzgerechte Komplett-Löschung der auf dem Handy gespeicherten personenbezogenen Daten und Bilder schriftlich zusichern zu lassen. Eine andere Möglichkeit besteht darin, alle Daten auf dem Gerät zu löschen sowie die nicht mehr benötigten SIM-Karten herauszunehmen und die SIM-Karte mechanisch zu zerstören.

*** * ***

16 Überblick und Statistik

16.1 Bearbeitung von Anfragen und Beschwerden

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

Die Beschwerden richten sich vor allem gegen

Veröffentlichungen im Internet
Videoüberwachungen
Umgang mit Daten bei Versandhandelsunternehmen
Datenverwendungen bei Banken und Versicherungen
Direktwerbemaßnahmen, insbesondere Telefonwerbung
Datenschutzverletzungen gegenüber Arbeitnehmern

Statistik 2006

- Schriftliche Eingaben insgesamt 519

  Keine Verstöße 245
  Verstöße 274
  (davon 3 Bußgeldbescheide)

- Anfragen/Beratungen von Betroffenen per Telefon oder E-Mail: 580

Statistik 2007:

- Schriftliche Eingaben insgesamt 521

  Keine Verstöße 284
  Verstöße 237
  (davon 5 Bußgeldbescheide)

- Anfragen/Beratungen von Betroffenen per Telefon oder E-Mail: 757

Statistik 2008:

- Schriftliche Eingaben insgesamt 539

  Keine Verstöße 256

  Verstöße 283
  (davon 11 Bußgeldbescheide)

- Anfragen/Beratungen von Betroffenen per Telefon oder E-Mail: 1036

16.2 Beratung der betrieblichen Datenschutzbeauftragten und der verantwortlichen Stellen

Diese Tätigkeit stellt einen weiteren Schwerpunkt dar. Zur schnellen Beratung wird meist der telefonische Kontakt gesucht. Schwierigere Fallgestaltungen werden schriftlich (einschl. E-Mail) vorgetragen oder in Besprechungen bei uns bzw. in den Unternehmen erörtert.

Folgende Themen standen im Berichtszeitraum im Vordergrund:

- Fragen des Arbeitnehmerdatenschutzes
- Videoüberwachung
- Datenschutzgerechte Gestaltung von Kundenkartensystemen
- Umgang mit personenbezogenen Daten bei Versicherungen

Statistik 2006:

Anfragen/Beratungen per Telefon, schriftlich oder per E-Mail:	689
Besprechungen	17

Statistik 2007:

Anfragen/Beratungen per Telefon, schriftlich oder per E-Mail:	725
Besprechungen	20

Statistik 2008:

Anfragen/Beratungen per Telefon, schriftlich oder per E-Mail:	817
Besprechungen	18

16.3 Kontrolltätigkeit

Es handelt sich hier um umfassende oder nur Einzelfragen betreffende Kontrollen, bei denen die Beachtung der datenschutzrechtlichen Vorschriften und der Datensicherheit in einem Unternehmen oder Betrieb auf den Prüfstand gestellt werden. Wir haben sowohl schriftlich als auch vor Ort folgende Prüfungen durchgeführt:

2006	15
2007	51
2008	11

Es ging dabei insbesondere um folgende Themen:

Videoüberwachung	(8)
Arbeitnehmerdatenschutz	(7)
Internet-Angebote	(4)
Wirtschaftsauskunfteien	(3)
Markt- bzw. Gesundheitsforschungsunternehmen	(3)
Werbeunternehmen und Callcenter	(3)
Industrieunternehmen	(2)
Kreditinstitut	(1)
Inkassounternehmen	(1)
Rabattkartenunternehmen	(1)
Auftragsdatenverarbeiter	(1)
Integrationsfachdienst	(1)
Bonitäts- und Scoringabfragen durch Versicherungen	(42)

Handlungsbedarf aus den Feststellungen der Datenschutzprüfungen hat sich insbesondere ergeben:

- zur Formulierung und Gestaltung von datenschutzrechtlichen Einwilligungserklärungen nach § 4a BDSG,
- im Hinblick auf die schriftlichen Vertragsregelungen bei der Auftragsdatenverarbeitung nach § 11 BDSG,

- bei den Regelungen zur Kontrolle der Nutzung von Telefon, Internet und E-Mail am Arbeitsplatz,
- für notwendige Sicherheitsmaßnahmen im Sinne von § 9 BDSG, und
- bei der Videoüberwachung.

Spezielle Beanstandungen aus der Kontrolltätigkeit sind in den vorstehenden Fachkapiteln dargestellt.

16.4 Meldepflicht

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

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

Uns liegen derzeit 127 Anmeldungen vor.

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

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

16.5 Zusammenarbeit der für den Datenschutz Verantwortlichen

16.5.1 Konferenzen der Datenschutzaufsichtsbehörden

Die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich arbeiten bundesweit in dem zwei Mal jährlich tagenden sog. „Düsseldorfer Kreis“ zusammen, um grundsätzliche Rechtsfragen und die Entscheidungen in länderübergreifenden Sach-

verhalten abzustimmen. In das Gesamtgremium des „Düsseldorfer Kreises“ sind wir ebenso eingebunden wie auch in die dazu gehörenden fünf Arbeitsgruppen Kreditwirtschaft, Auskunfteien/SCHUFA, Versicherungswirtschaft, Internationaler Datenverkehr und Telekommunikation/Tele- bzw. Mediendienste.

Wir beteiligen uns auch regelmäßig an gelegentlich eingerichteten sog. ad-hoc-Arbeitsgruppen für bestimmte Fachfragen. Für eine Arbeitsgruppe, die sich mit der datenschutzrechtlichen Beurteilung von Fahrzeugdatenspeichern befasst, ist uns 2008 der Vorsitz übertragen worden.

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

16.5.2 Arbeitskreise der Wirtschaftsunternehmen

Betriebliche Datenschutzbeauftragte treffen sich unter der Federführung der Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) zum Erfahrungsaustausch in sogenannten „Erfa-Kreisen“, um von- bzw. miteinander zu lernen und sich fortzubilden. Diese Arbeitskreise bestehen in München, Nürnberg, Würzburg und Coburg. Ihre Sitzungen finden jeweils zwei- bis dreimal im Jahr statt.

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

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

16.5.3 Kongresse und Fortbildungsveranstaltungen

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

Auf Wunsch und im Zusammenwirken mit Unternehmensverbänden und Datenschutzorganisationen haben wir bei Fortbildungsveranstaltungen und Seminaren Vor-

träge zu datenschutzrechtlichen Themen gehalten, um auch auf diesem Weg eine Breitenwirkung in der Datenschutzinformation zu erreichen:

2006 12 Vorträge
2007 5 Vorträge
2008 10 Vorträge

16.6 Öffentlichkeitsarbeit

Eine wichtige Aufgabe der Datenschutzaufsichtsbehörden ist die allgemeine Information der Öffentlichkeit zu Datenschutzthemen, um den Datenschutz sozusagen "unter die Leute zu bringen".

Der zentrale Kanal zur Streuung von Informationen ist in der heutigen Zeit das Internet. Wir haben deshalb auf unserer Homepage unter
http://www.regierung.mittelfranken.bayern.de/aufg_abt/abt1/abt1dsa10.htm eine Reihe von Dokumenten und Links zu anderen Datenschutzinformationen im Internet hinterlegt.

Gerade in den letzten Monaten hatten wir viele Anfragen der öffentlichen Medien zu beantworten. In Presse-, Rundfunk- und Fernsehbeiträgen haben wir zu verschiedenen aktuellen Datenschutzthemen Stellung genommen.

Europäischer Datenschutztag

Den jährlich stattfindenden Europäischen Datenschutztag, der vom Europarat auf den 28. Januar terminiert worden ist, haben wir in den Jahren 2007 und 2008 zu öffentlichkeitswirksamen Veranstaltungen genutzt.

- 2007 hielten wir eine Vortragsveranstaltung in unseren Räumen für das interessierte Fachpublikum und die Presse mit Beiträgen von Herrn Regierungspräsidenten Inhofer, Herrn Professor Gerling von der Max-Planck-Gesellschaft, München, sowie von Herrn Harmsen von der Industrie- und Handelskammer Nürnberg ab.

  Im Rahmen dieser Veranstaltung wurde der Öffentlichkeit eine themenbezogene Plakatausstellung zum Datenschutz in den Räumen der Regierung von Mittelfranken im Ansbacher Schloss vorgestellt. Die Ausstellung war mehrere Wochen lang

geöffnet. Einige Plakate wurden in der Folgezeit an interessierte Unternehmen und Verbände ausgeliehen.

- 2008 stellten wir im Rahmen einer Pressekonferenz in Nürnberg unsere datenschutzrechtliche Auffassung zu den Bewertungsportalen im Internet am Beispiel der Lehrerbewertungen bei "spickmich.de" vor.

Über diese Veranstaltungen wurde in Presse, Rundfunk und Fernsehen berichtet.