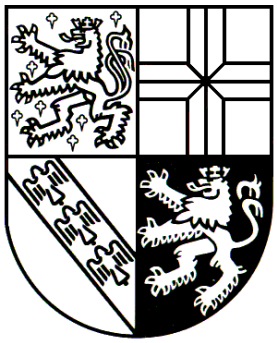


4. Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Saarlandes

Berichtszeitraum

2007/2008

Impressum

Herausgeber: Aufsichtsbehörde für den Datenschutz
im nicht-öffentlichen Bereich beim
Ministerium für Inneres und Sport
Franz-Josef-Röder-Straße 21
66119 Saarbrücken

Hausanschrift:
Mainzer Straße 136
66121 Saarbrücken
Telefon: 0681 501-00
Telefax: 0681 501-2699
E-Mail: datenschutz@innen.saarland.de
Internet: www.saarland.de

VORGELEGT VON

DER AUFSICHTSBEHÖRDE

FÜR DEN DATENSCHUTZ

IM NICHT-ÖFFENTLICHEN BEREICH

BEIM

MINISTERIUM FÜR INNERES UND SPORT

DES SAARLANDES

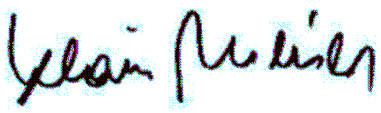
Liebe Bürgerinnen und Bürger,

unsere modernen Informations- und Kommunikationstechnologien haben sich in den letzten Jahren in beachtlichem Maße weiterentwickelt. Sie eröffnen heute ungeahnte Chancen der grenzüberschreitenden Kommunikation, der Meinungsbildung und des weltweiten Datenaustausches. Unser Leben, unsere Arbeit, das Handeln der Wirtschaft und der staatlichen Institutionen verlagern sich mehr und mehr in die virtuelle Welt hinein. Denn Daten, insbesondere personenbezogene Daten, sind Rohstoff für informiertes Handeln. Ihr Besitz kann zu einem Wettbewerbsvorteil von Unternehmen und zu wirtschaftlicher Stärke eines Landes beitragen.

Allerdings ist die gesellschaftliche Teilhabe an der Informations- und Wissensgesellschaft mit Risiken behaftet, die bis in den Kernbereich des privaten Lebens hineinreichen können. Die jüngsten Datenschutzskandale im privatwirtschaftlichen Bereich haben uns vor Augen geführt, dass der Schutz der Arbeitnehmer größerer Aufmerksamkeit bedarf und die seit langem geforderte gesetzliche Regelung des Arbeitnehmerdatenschutzes endlich realisiert werden muss.

Sie haben darüber hinaus zudem gezeigt, dass der Selbstdatenschutz unserer Bürgerinnen und Bürger, also die Kompetenz der oder des Einzelnen im eigenverantwortlichen Umgang mit ihren oder seinen Daten, in erheblichem Maße an gesellschaftlicher Bedeutung gewonnen hat. Es ist daher zu begrüßen, dass das Verhalten und das Selbstverständnis vieler Bürgerinnen und Bürger im Umgang mit ihren persönlichen Daten im Wandel begriffen ist.

Die Lektüre des vorliegenden Tätigkeitsberichts der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich kann für Sie eine Hilfe sein, Ihre Daten und damit sich selbst besser in der neuen Informationswelt zu schützen. Bei Beratungsbedarf oder Problemen zum Datenschutz steht Ihnen unsere Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich gerne zur Verfügung.



Klaus Meiser
Minister für Inneres und Sport

Inhaltsverzeichnis Seite

1. Allgemeines

1.1 Grundrecht des allgemeinen Persönlichkeitsrechts und Grundrecht auf informationelle Selbstbestimmung

Nach Artikel 2 Absatz 1 des Grundgesetzes hat jeder das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht Rechte anderer verletzt oder gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt. Ein Teilbereich dieser Norm erfährt als „Allgemeines Persönlichkeitsrecht“ einen besonderen Schutz und hat sich zu einem eigenen Grundrecht verselbstständigt. Es wird beeinflusst durch das Grundrecht des Artikels 1 Absatz 1 des Grundgesetzes, das einen uneinschränkbaren Kern des Rechts, nämlich die Würde des Menschen, festschreibt. Aus diesem in Artikel 2 Absatz 1 des Grundgesetzes verankerten Grundrecht des Allgemeinen Persönlichkeitsrechts hat das Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65, 1) das Grundrecht auf informationelle Selbstbestimmung hergeleitet. Grundlage dieses Grundrechts ist Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes. Dieses Grundrecht auf informationelle Selbstbestimmung schützt den Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten. Es gewährleistet dem Einzelnen als Herr der ihn betreffenden Daten die Befugnis, grundsätzlich über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.
Dieses Grundrecht ist dem Einzelnen aber nicht schrankenlos gewährt im Sinne einer absoluten uneingeschränkten Herrschaft über seine „Daten“:
Im Verhältnis zwischen Staat und Bürger sind Einschränkungen dieses Grundrechts durch den Staat im überwiegenden Allgemeininteresse zulässig. Sie bedürfen jedoch einer gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss, d. h. aus der gesetzlichen Regelung müssen sich die Voraussetzungen und der Umfang der Beschränkungen klar und für die Betroffenen erkennbar ergeben. Ferner wird staatliches Handeln durch den Grundsatz der Verhältnismäßigkeit mit Blick auf die Eingriffsintensität des Datenzugriffs begrenzt. Schließlich hat jedem staatlichen Datenzugriff eine klar definierte Zweckbestimmung voranzugehen.

Im Verhältnis der Bürger untereinander sind Datenerhebung und Datenverarbeitung unter bestimmten gesetzlichen Voraussetzungen grundsätzlich zulässig. Allerdings kann es dabei zu Konflikten zwischen dem allgemeinen Persönlichkeitsrecht bzw. dem Recht des datenschutzrechtlich Betroffenen auf informationelle Selbstbestimmung und den individuellen Informations- und Informationsverarbeitungsrechten der datenerhebenden bzw. datenverarbeitenden Dritten kommen.

In diesem Kontext kann staatliche Aufsicht über den Datenschutz gefragt sein.

1.2 Aufsichtsbehörde für den Datenschutz

Wenn es um staatliche Aufsicht über den Datenschutz im Saarland geht, ist zwischen der Aufsicht über den Datenschutz im öffentlichen Bereich und der Aufsicht über den Datenschutz im nicht-öffentlichen Bereich zu unterscheiden.
Während die Aufsicht über den Datenschutz im öffentlichen Bereich, also die datenschutzrechtliche Kontrolle öffentlicher Stellen, dem Landesbeauftragten für Datenschutz und Informationsfreiheit des Saarlandes obliegt, ist die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich einer gesonderten Aufsichtsbehörde übertragen, die beim Ministerium für Inneres und Sport angesiedelt ist. Da der Landesbeauftragte für Datenschutz und Informationsfreiheit des Saarlandes einen eigenen Tätigkeitsbericht veröffentlicht, wird im vorliegenden Tätigkeitsbericht nur über die Tätigkeit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich berichtet.

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich hat die Aufgabe, die Ausführung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz durch die nicht-öffentlichen Stellen zu überprüfen und zu überwachen. Nicht-öffentliche Stellen sind vor allem privatrechtliche Organisationsformen, wie beispielsweise Banken, Versicherungen, Industrie- und Dienstleistungsunternehmen sowie sonstige Gesellschaften, Vereine und Stiftungen. In Betracht kommen können aber auch freiberuflich Tätige, wie etwa Ärzte und Architekten, oder

ausnahmsweise Privatpersonen, wenn sie personenbezogene Daten in datenschutzrechtlich relevanter Form verarbeiten. Ob dabei die Datenverarbeitung hauptsächlich einem geschäftlichen Zweck der nicht-öffentlichen Stelle dient oder nur eine Hilfsfunktion hat, wie etwa bei der Personaldaten- oder Kundendatenverwaltung, ist unmaßgeblich. Vielmehr ist entscheidend, dass die Daten entweder in automatisierten Verfahren bzw. in oder aus nicht automatisierten Dateien (z. B. Karteikartensystemen) verarbeitet oder genutzt oder dafür erhoben werden.

Fragen nach dem Schutz personenbezogener Daten sind in der Regel nicht nur einem bestimmten Rechtsgebiet zuzuordnen. Weil Datenschutz eine Querschnittsmaterie ist, sind bei der Beurteilung datenschutzrechtlicher Sachverhalte immer auch bereichsspezifische Vorschriften zu beachten. Wenn es also um die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten geht, ist sich die Aufsichtsbehörde stets bewusst, dass der Datenschutz als Teilbereich in größeren Zusammenhängen zu sehen ist. Dies kann nicht nur für die Folgenabschätzung datenschutzrechtlicher Verstöße maßgeblich sein.

Die fehlende Zuordnung zu einer bestimmten Rechtsmaterie bedingt bereits, dass allgemeine datenschutzrechtliche Regelungen immer im jeweiligen Kontext, wie beispielsweise im Arbeitsrecht oder im Urheberrecht, zu betrachten und auch umzusetzen sind. Vorrangig ist dabei stets zu prüfen, ob und inwieweit die Erhebung, Verarbeitung und Nutzung bestimmter Daten überhaupt erforderlich ist. Nur so kann dem in § 3a BDSG normierten Prinzip der Datenvermeidung und Datensparsamkeit Genüge getan werden: Diesem datenschutzrechtlichen Prinzip zufolge haben sich Gestaltung und Auswahl der Datenverarbeitungssysteme an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Auch sind stets die Interessen der Betroffenen in unterschiedlicher Gewichtung zu berücksichtigen. Mit dieser gesetzgeberischen Entscheidung wird klargestellt, dass das Recht auf informationelle Selbstbestimmung, also das Recht auf Schutz der eigenen Daten, kein absolutes Recht ist. Es muss sich gerade im Spannungsfeld zwischen wirtschaftlichen und privaten Interessen immer wieder neu definieren, da auch die Ausübung eines Gewerbes grundrechtlich geschützt ist.

Mit der voranschreitenden Digitalisierung unserer Welt haben Daten und Informationen an enormer Bedeutung gewonnen. Im modernen Wirtschaftsleben sind Daten und Informationen selbst zur Ware geworden. In einem konstruktiven Dialog mit allen Beteiligten sind daher datenschutzrechtliche Vorschriften sachgerecht auszulegen und praktikable Lösungen zu entwickeln. Nur durch gegenseitige Akzeptanz der Datenverarbeiter und der Betroffenen kann ein Verständnis für das Grundanliegen des Datenschutzes gefunden werden: Einen möglichst weitgehenden Schutz personenbezogener Daten einerseits und gleichzeitig den jeweils notwendigen Informationsfluss andererseits zu sichern gehört zu den Aufgaben der Aufsichtsbehörden für den Datenschutz. Klassisch wird dies umgesetzt durch Kontrollen, rechtliche Bewertung der jeweiligen Datenverarbeitungen und dem Erarbeiten von Lösungswegen.
Jedoch ist in diesem Zusammenhang zu sehen, dass zunächst die Eigenverantwortung und Selbstkontrolle wirtschaftlicher Unternehmen gefordert ist. Nach unserem Staats- und Bürgerverständnis ist zunächst jeder selbst für sich und sein rechtmäßiges Handeln verantwortlich. Der Gesetzgeber hat daher das Instrument des betrieblichen Datenschutzbeauftragten geschaffen. Der betriebliche Datenschutzbeauftragte hat im Binnenverhältnis auf die Einhaltung datenschutzrechtlicher Vorschriften hinzuwirken und die Datenverarbeitung zu überwachen. Er ist sozusagen für eine betriebsinterne Datenschutzrevision zuständig. Darüber hinaus schult der betriebliche Datenschutzbeauftragte die Mitarbeiter in der praktischen Anwendung datenschutzrechtlicher Vorschriften. Betriebsextern ist er Schnittstelle zu von Unternehmensentscheidungen datenschutzrechtlich Betroffenen und zur Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich.
Nicht-öffentliche Stellen haben einen betrieblichen Datenschutzbeauftragten zu bestellen, wenn sie in der Regel mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen haben nicht-öffentliche Stellen einen betrieblichen Datenschutzbeauftragten zu bestellen, wenn sie automatisierte Verarbeitungen vornehmen, die einer Vorab-

kontrolle unterliegen oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung automatisiert verarbeiten.
Flankiert wird diese betriebliche Selbstkontrolle durch die Kontrolle der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich. Es besteht insoweit ein Kontrolldualismus zwischen der betriebsinternen Datenschutzrevision und der externen staatlichen Kontrolle durch die Aufsichtsbehörde.
Bei dieser aufsichtsrechtlichen Kontrolle handelt es sich nicht um eine dauerhafte Überwachung. Vielmehr werden aufsichtsrechtliche Kontrollen anlassbezogen oder anlassunabhängig durchgeführt. Die Aufsichtsbehörde kann jedes Unternehmen, das personenbezogene Daten erhebt, verarbeitet oder nutzt, jederzeit um die erforderlichen Auskünfte bitten. Die Mitarbeiter der Aufsichtsbehörde haben ferner das Recht, die Geschäftsräume zu betreten und alle mit der Datenverarbeitung in Zusammenhang stehenden Unterlagen einzusehen. Dies gilt auch für personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Die Erkenntnisse und Erfahrungen im Berichtszeitraum haben die Aufsichtsbehörde veranlasst, künftig in verstärktem Maße anlassunabhängige Kontrollen in verschiedenen Wirtschaftszweigen durchzuführen.
Darüber hinaus bietet die Aufsichtsbehörde ihre Hilfe und Beratung vor Beginn einer geplanten Datenverarbeitung an. Risiken für das informationelle Selbstbestimmungsrecht können dadurch frühzeitig erkannt und vermieden werden und so - als weiteres Resultat - auch Rechtssicherheit für die jeweils Verantwortlichen geschaffen werden.

1.3 Aufgaben und Kompetenzen der Aufsichtsbehörde

Aufgaben und Kompetenzen der Aufsichtsbehörden lassen sich im Wesentlichen in drei Bereiche gliedern:

a) Kontrolle

- Kontrolle der Rechtmäßigkeit der Datenverarbeitung, auch ohne konkreten Anlass (§ 38 Absatz 1 Satz 1 BDSG),

- Führung des Registers meldepflichtiger Verarbeitungen im Rahmen der vorgelagerten Kontrolle (§ 38 Absatz 2 BDSG),
- Betretungs-, Informations- und Einsichtsrechte (§ 38 Absatz 3 und 4 BDSG),
- Genehmigung von Datenübermittlungen in Dritt-Staaten (Nicht-EU-Staaten) ohne angemessenes Datenschutzniveau (§ 4c Absatz 2 BDSG,
- die Herausgabe von Tätigkeitsberichten (§ 38 Absatz 1 Satz 6 BDSG) als Ausfluss der Kontrolle im weitesten Sinne.

b) Beratung

- Beratung von Unternehmen bei der Erstellung von Unternehmensrichtlinien zum Schutz personenbezogener Daten,
- Mitwirkung bei der Vorabkontrolle (§ 4d Absatz 6 Satz 3 BDSG),
- Unterstützung der betrieblichen Datenschutzbeauftragten (§ 4g Absatz 1 Satz 2 BDSG),
- Prüfung von Unternehmensregelungen zur Verarbeitung personenbezogener Daten (§ 38a BDSG)

c) Sanktionen

- Unterrichtung der Betroffenen, Anzeige bei Verfolgungsbehörden, bei schwerwiegenden Mängeln auch bei der Gewerbeaufsicht (§ 38 Absatz 1 Satz 4 BDSG),
- Anordnung zur Beseitigung technischer und organisatorischer Mängel (§ 38 Absatz 5 Satz 1 BDSG),
- Zwangsgeld bei unterlassener Mängelbeseitigung (§ 38 Absatz 5 Satz 2 BDSG),
- Durchführung von Bußgeldverfahren (§ 43 BDSG),
- Strafantragsrecht bei Verstößen gegen Vorschriften des Bundesdatenschutzgesetzes (§ 44 Absatz 2 BDSG).

In der Praxis machen Anfragen und Eingaben von Bürgerinnen und Bürgern (auch „Petentinnen/Petenten“ genannt), die telefonisch, schriftlich und verstärkt auch per E-Mail an die Aufsichtsbehörde für den Datenschutz herangetragen werden, den Hauptteil der praktischen Arbeit aus. Ein großer Teil der telefonischen Anfragen bezieht sich auf die generelle Zulässigkeit der Datenverarbeitung und kann in der Regel unmittelbar beantwortet werden.

Konkret geschilderte Fälle hingegen erfordern eine sog. „Sachverhaltsaufklärung“: Die Aufsichtsbehörde wendet sich in solchen Fällen an die verantwortliche Stelle, die in der Eingabe genannt wurde und bittet um Stellungnahme. Diese darf nur dann verweigert werden, wenn die Gefahr eines Bußgeld- oder Strafverfahrens bestünde. Ist der Sachverhalt geklärt, erfolgt die datenschutzrechtliche Bewertung, die den Petentinnen/Petenten mitgeteilt wird. In der Regel werden im Saarland die verantwortlichen Stellen nur dann informiert, wenn die Datenverarbeitung zu beanstanden ist.

Die Aufsichtsbehörde für den Datenschutz hat für sich das Leitbild einer Verwaltung formuliert, die im Interesse aller Bürgerinnen und Bürger arbeitet. Ziel ist es, Eingaben und Anfragen möglichst umfassend, zeitnah und letztendlich unbürokratisch zu beantworten, soweit dies einer an Recht und Gesetz und damit auch Verfahrensvorschriften gebundenen Verwaltung möglich ist. Durch die Tätigkeit der Aufsichtsbehörde entstehen den Betroffenen keine Kosten, es werden keine Gebühren erhoben. Anwalt der Betroffenen zu sein und gleichzeitig eine objektive Interessenabwägung vorzunehmen, ist das Ziel aller Bemühungen der Aufsichtsbehörde für den Datenschutz.

1.4 Zusammenarbeit mit anderen Aufsichtsbehörden

„Düsseldorfer Kreis“

Bei dieser Einrichtung handelt es sich um ein Gremium der Vertreter der obersten Aufsichtsbehörden für den Datenschutz, in dem alle Bundesländer vertreten sind.

Benannt nach seinem ursprünglichen Tagungsort unter dem Vorsitz des Innenministeriums des Landes Nordrhein-Westfalen, wechselt der Vorsitz seit 2002 und damit auch das ausrichtende Bundesland. Aufgabe des Düsseldorfer Kreises ist es, eine – so weit wie möglich – bundeseinheitliche Behandlung datenschutzrechtlicher Probleme sicherzustellen. Eine weitere Aufgabe ist die Erörterung datenschutzrechtlicher Grundsatzfragen.

Die im Berichtszeitraum gefassten Beschlüsse des Düsseldorfer Kreises sind im Anhang aufgeführt.

2. Videoüberwachung

Über die rechtlichen Vorraussetzungen, unter denen eine Videoüberwachung grundsätzlich zulässig ist, wurde bereits im 3. Tätigkeitsbericht unter Ziffer 2.1 bis 2.10 ausführlich berichtet, so dass im Folgenden nur noch auf die Besonderheiten der Einzelfälle eingegangen wird.

2.1 Videoüberwachung in einem Schwimmbad

Durch einen Besucher eines saarländischen Schwimmbades wurde die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich darauf aufmerksam, dass in der Gemeinschaftsumkleide der Sauna des Schwimmbades Videokameras angebracht seien. Entsprechende Hinweisschilder befänden sich im Kassenbereich. Dieser Hinweis war für die Aufsichtsbehörde Anlass, eine Kontrolle in dem betreffenden Schwimmbad vor Ort vorzunehmen. Die Kontrolle ergab, dass sowohl im Umkleidebereich der Sauna als auch im Umkleidebereich des Schwimmbades Videokameras installiert waren. Darüber hinaus wurden im Eingangs-/Kassenbereich sowie im Shop Videokameras festgestellt, von denen eine so ausgerichtet war, dass der Kassenbereich samt Mitarbeiter und Badegästen permanent aufgenommen wurde. An verschiedenen Stellen des Bades waren zudem drei Hinweisschilder mit unterschiedlichen Aufschriften, die jedoch nicht die Voraussetzungen des § 6b BDSG erfüllten, angebracht.
Was die Videokameras im Kassenbereich bzw. Shop, mit denen u. a. Mitarbeiter aufgenommen werden konnten, angeht, ist wegen des permanenten Überwachungsdruckes und der damit einhergehenden Beeinträchtigung des Persönlichkeitsrechts der Angestellten eine solche Videoüberwachung nur zulässig, wenn überwiegende Sicherheitsbedürfnisse des Arbeitgebers diese erfordern. Im Rahmen der Abwägung ist darauf zu achten, dass kein unverhältnismäßiger Überwachungsdruck auf die davon quasi ständig miterfassten Mitarbeiter entsteht. Dabei ist auch die Intensität der Beobachtung zu berücksichtigen. Eine permanente Überwachung von Mitarbeitern, der sich diese nicht oder nicht ausreichend entziehen können, ist daher

unzulässig. Auf Veranlassung der Aufsichtsbehörde hat die Betreibergesellschaft die Kameras im Kassenbereich bzw. im Shop so eingerichtet, dass der Arbeitsbereich der Angestellten im Kassenbereich nur noch zu einem kleinen Teil, im Shop dagegen nicht mehr erfasst wird.
Hinsichtlich der Frage der Kameras im Umkleidebereich der Sauna und im Umkleidebereich des Schwimmbades will die verantwortliche Stelle ggf. ein neues Konzept vorlegen.
Die Betreibergesellschaft des Schwimmbades wurde auch auf die nach § 6b Absatz 2 BDSG gebotene Hinweispflicht, der nur unzureichend nachgekommen wurde, hingewiesen. Danach ist der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen deutlich erkennbar zu machen. Im übrigen bleibt festzuhalten, dass selbst zum Zwecke der Diebstahlprävention installierte Kameras in keinem Fall die Überwachung von Toiletten bzw. Umkleidekabinen rechtfertigen, da hier über die normale Beobachtung hinaus in einem solchen Maße in die Privat- und Intimsphäre eingegriffen wird, dass dies außerhalb jeder Verhältnismäßigkeit liegt. Auf Verlangen der Aufsichtsbehörde hat die Betreibergesellschaft die entsprechenden Hinweisschilder angebracht.

2.2 Videoüberwachung eines privaten Hauseinganges

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich wurde von einem Petenten darüber informiert, dass am Carport auf dem Nachbargrundstück eine Videokamera installiert sei, mit der sowohl ein Teil seines eigenen Grundstücks als auch ein Teil des öffentlichen Straßenraumes überwacht werden könne. Zumindest gebe dies die Bedienungsanleitung der installierten Kamera, die er sich im Internet angesehen habe, her.
In seiner Stellungnahme erklärte der betroffene Grundstückseigentümer, dass er nicht gegen Datenschutzbestimmungen verstoßen habe. Die installierte Videokamera diene ausschließlich der Kontrolle der 15 m langen Zufahrt sowie des Zugangs zum Haus. Die Kamera sei so eingerichtet, dass weder das Nachbargrundstück, noch die öffentliche Straße im Blickwinkel der Kamera liegen. Die Kamera diene dem

privaten Zweck, nicht bei jedem Klingeln den langen Weg vom Haus bis zum Hoftor zurücklegen zu müssen.
Der Hauseigentümer wurde von der Aufsichtsbehörde darüber informiert, dass auch die Beobachtung eines öffentlich zugänglichen Eingangsbereiches in den Anwendungsbereich des § 6b Bundesdatenschutzgesetz (BDSG), welcher die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen regelt, fällt. Auch wenn die Zugangskontrolle für den privaten Zweck erfolge, sich der Identität oder Lauterkeit eines Besuchers zu vergewissern, so überschreite die Beobachtung mit der Videokamera sowie eine gegebenenfalls erfolgende Aufzeichnung der erfassten Daten jedoch den Kreis einer ausschließlich privaten Tätigkeit, soweit sie auf die Beobachtung eines öffentlich zugänglichen Raumes gerichtet ist. Hierzu zählt mit Rücksicht auf den Schutz der beobachteten Personen auch der jedermann zugängliche Eingangsbereich einer privaten Haus- oder Wohnungstür (vgl. Simitis, Bundesdatenschutzgesetz, 6. Auflage, Randnummer 34). Dies gelte im vorliegenden Fall umso mehr, als die Klingel außerhalb des Hoftores liege.
In Folge dessen bestehe eine Hinweispflicht nach § 6b Absatz 2 BDSG. Diese Vorschrift besagt, dass der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind. Das Gesetz mache keine speziellen Vorgaben zur Gestaltung dieses Hinweises. Empfehlenswert sei ein Schild mit einem entsprechenden Text bzw. Piktogramm, das den Umstand der Überwachung darstellt, verbunden mit einem Hinweis auf die verantwortliche Stelle. Das Schild sei deutlich sichtbar anzubringen und müsse vor Betreten des überwachten Bereiches problemlos wahrnehmbar sein, damit die freie Entscheidung für oder gegen das Betreten möglich sei.

2.3 Videoüberwachung in einem Eiscafé

Aufgrund der Eingabe eines Betroffenen hat die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich eine Vor-Ort-Kontrolle in einem Eiscafé durchgeführt. Dabei wurde festgestellt, dass zwei Videokameras im Eiscafé angebracht waren, die den Innenraum überwachten. Ein entsprechendes Hinweisschild auf die Vi-

deoüberwachung gemäß § 6b Absatz 2 BDSG war nicht vorhanden. In seiner Stellungnahme hierzu gab der Inhaber des Cafés als Begründung für die Erforderlichkeit der Maßnahme ein allgemeines Sicherheitsbedürfnis an. Außerdem könne so ein hohes Kundenaufkommen schneller erkannt und entsprechend reagiert werden. Eine Aufzeichnung erfolge nicht.
Er wurde von der Aufsichtsbehörde darauf hingewiesen, dass nach § 6b BDSG die Beobachtung öffentlich zugänglicher Räume nur zulässig ist, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Die Überwachung beeinträchtige die Gäste in ihrem Recht auf informationelle Selbstbestimmung, was das Recht des Einzelnen, sich in der Öffentlichkeit frei und ungezwungen bewegen zu können, ohne befürchten zu müssen überwacht zu werden, beinhalte. Was das allgemeine Sicherheitsbedürfnis betrifft, so könne dies grundsätzlich als berechtigtes Interesse anerkannt werden. Allerdings sei eine besondere Gefahrensituation bzw. ein konkreter Anlass für die Videoüberwachung weder vorgetragen worden, noch erkennbar. Der allgemeine Hinweis auf das Sicherheitsbedürfnis reiche aber nicht aus, um Videoüberwachung zu begründen.
Darüber hinaus seien auch die Interessen der Mitarbeiter zu beachten. Durch die auf den Tresen und Kassenbereich gerichtete Kamera seien die Mitarbeiter einem dauerhaften Überwachungsdruck ausgesetzt, dem sie sich nicht entziehen könnten. Somit überwiegen die Interessen der Mitarbeiter, nicht ständig beobachtet zu werden, den geringer einzustufenden Interessen des Inhabers.
Vor diesem Hintergrund wurde der Inhaber von der Aufsichtsbehörde aufgefordert, die Videokameras im Innenbereich des Eiscafés abzubauen bzw. den Erfassungsbereich der Kameras so zu ändern, dass der Gastraum sowie der Tresen und der Kassenbereich nicht erfasst werden, wobei in letzterem Fall ein entsprechendes Hinweisschild auf die Videoüberwachung anzubringen sei. Daraufhin hat der Inhaber des Eiscafés die Videoüberwachungsanlage abgebaut.

2.4 Videoüberwachung eines Grundstücks

Im Berichtszeitraum wurden weitere Fälle der Videoüberwachung von privaten Grundstücken an die Aufsichtsbehörde herangetragen. In einem Fall bat ein Grundstückseigentümer, der eine Videoanlage auf seinem Grundstück aufgebaut hatte, im Rahmen eines Schiedsverfahrens mit seinem Grundstücksnachbarn um datenschutzrechtliche Überprüfung der Anlage.
Bereits im Vorfeld hatte die Aufsichtsbehörde beide Parteien darauf hingewiesen, dass ihre Zuständigkeit sich nur auf den öffentlich zugänglichen Bereich erstreckt. Wo dagegen ausschließlich private Grundstücke betroffen seien, komme möglicherweise ein zivilrechtlicher Unterlassungsanspruch in Betracht.

Vor dem Hintergrund, dass eine Erfassung des öffentlichen Raumes zumindest nicht von vornherein ausgeschlossen werden konnte, wurde die Aufsichtsbehörde in Abstimmung mit den beiden Parteien um ihre Beurteilung gebeten.
Von den drei auf dem Grundstück installierten Kameras war eine so angebracht, dass ein kleiner Teil des Nachbargrundstückes mit aufgenommen wurde. Die beiden übrigen Kameras waren unproblematisch.
Da die Vor-Ort-Besichtigung ergab, dass kein öffentlich zugänglicher Raum überwacht wurde, ist die Aufsichtsbehörde für die Beurteilung der Zulässigkeit der Videokamerainstallationen nicht zuständig. Da sie jedoch von beiden Parteien um Äußerung gebeten wurde, gab die Aufsichtsbehörde zu bedenken, ob vor dem Hintergrund, dass nur ein sehr schmaler Teil des Nachbargrundstücks von einer Kamera erfasst wird und in diesem Bereich Personen nur schwer zu erkennen sind, die in dem Abwehranspruch des § 1004 BGB geforderte Beeinträchtigung des Eigentums tatsächlich vorliegt, oder die Eigentumsrechte des Grundstückseigentümers, der die Überwachung betreibt, vorgehen.
Die Beteiligten einigten sich dahingehend, dass in Absprache mit der Installationsfirma der Bereich des Nachbargrundstücks, der von einer Kamera erfasst wird, durch eine entsprechende Kameraeinstellung ausgeblendet wird.

2.5 Videoüberwachung von Wohnanlagen

An die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich wurden auch Fälle der Videoüberwachung von Wohnanlagen herangetragen. In einem Fall monierte ein Bewohner einer Seniorenwohnanlage die von der Hausverwaltung mit Hilfe eines Informationsschreibens angekündigte Videoüberwachung des Aufzuges der Wohnanlage. Die angekündigte Maßnahme wurde von der Hausverwaltung mit der wiederholt festgestellten extremen Verschmutzung des Aufzuges durch Urinieren, die letztlich zur Nutzungsbeeinträchtigung und zu Schäden führe, begründet.
In einem weiteren Fall waren im Treppenhaus einer Appartementwohnanlage, im Bereich der Zählerkästen sowie im Kellerbereich (Waschküche, Heizung) Überwachungskameras installiert. Die Installation war auf Veranlassung der Eigentümergemeinschaft durchgeführt worden. Zur Begründung wurden nachgewiesene Vorfälle wie Anpöbeln junger Frauen im Kellerbereich, Manipulationen an Zählerschränken und Waschmaschinen, Diebstahl von Wäsche, Öffnen von Wasserhähnen ohne diese wieder zu schließen, Feuer legen etc. angeführt.

Hierzu ist grundsätzlich anzumerken, dass gemäß § 6b Absatz 1 des Bundesdatenschutzgesetzes (BDSG) die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen durch Private nur zulässig ist, soweit sie

- zur Wahrnehmung des Hausrechts oder
- zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Nach Absatz 2 dieser Vorschrift sind dabei der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen (Hinweisschild) erkennbar zu machen.
Sollten Videobilder aufgezeichnet werden, sind die Aufzeichnungen zu löschen, wenn kein Schaden eingetreten ist, der Anlass für eine weitere Aufbewahrung zu Beweiszwecken gäbe. Die Löschung sollte nach einem gewissen zeitlichen Ablauf automatisch erfolgen, in der Regel nach 24 bis 72 Stunden.

Da es sich bei den vorgenannten Beispielen um öffentlich zugängliche Räume handelte – es gelten im voraus bestimmbare und von jedermann erfüllbare Zugangsvoraussetzungen (Bewohner, Besucher etc.) – kommen die Bestimmungen des § 6b des BDSG zur Anwendung. Aufgrund der geschilderten Sachverhalte wurden die für die Zulässigkeit der Überwachung geforderten Voraussetzungen als gegeben erachtet. Die für die Videoüberwachung bzw. die beabsichtigte Videoüberwachung verantwortlichen Stellen wurden entsprechend unterrichtet.

3. Versicherungen

3.1 Speicherung von Kundendaten ohne Zustandekommen eines Versicherungsvertrages

Im Berichtszeitraum haben sich mehrere Petenten an die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich gewandt und um Überprüfung einer möglicherweise unzulässigen Speicherung bzw. einer Weigerung zur Löschung ihrer personenbezogenen Daten durch das betreffende Versicherungsunternehmen gebeten, obwohl letztlich kein Versicherungsvertrag zustande gekommen sei. Das jeweilige Versicherungsunternehmen habe sich bei der Speicherung bzw. der Weigerung zur Löschung der Daten auf gesetzliche Aufbewahrungsfristen berufen.
Hierzu ist folgendes anzumerken:
Die Rechtsgrundlagen für die Aufbewahrung von Antragsunterlagen sind in § 257 Absatz 1 Nummer 2 Handelsgesetzbuch in Verbindung mit Absatz 4 der Vorschrift sowie in § 147 Absatz 1 Nummer 2 Abgabenordnung in Verbindung mit Absatz 3 zu sehen. Danach sind empfangene Handelsbriefe für die Dauer von 6 Jahren aufzubewahren. Diese Vorschriften gehen – deklaratorisch bestätigt durch § 35 Absatz 3 Nummer 1 Bundesdatenschutzgesetz (BDSG) – der Regelung des § 35 Absatz 2 Nummer 3 BDSG vor, wonach personenbezogene Daten zu löschen sind, wenn sie nicht mehr benötigt werden. Die Tatsache, dass ein Vertrag letztlich nicht zustande gekommen ist, ändert an der Beurteilung nichts, da auch die Antragsunterlagen zu den empfangenen Handelsbriefen zählen. Insofern können die Ausführungen der Versicherungsunternehmen bestätigt werden. Die Aufbewahrungsfristen wurden den Datenschutzaufsichtsbehörden zuletzt im Januar 2005 seitens des Gesamtverbandes der Deutschen Versicherungswirtschaft bestätigt und von der Datenschutzseite anerkannt. Im Einzelnen betragen die Aufbewahrungsfristen für Abrechnungsunterlagen 10 Jahre, für Geschäftsbriefe, Antragsunterlagen, Schriftwechsel, Versicherungspolicen und Verträge jeweils 6 Jahre. Nach § 35 Absatz 3 Nummer 1 BDSG sind die Daten in jedem dieser Fälle zwingend zu sperren und ausschließlich für

Zwecke der externen Kontrolle durch Behörden, etwa die Finanzbehörden, zu verwenden. Nach Ablauf der Aufbewahrungsfrist müssen sie gelöscht werden.

3.2 Weitergabe von personenbezogenen Daten an das Hinweissystem des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV)

Über die Aufbewahrungsfristen hinaus wurde von Versicherungsnehmern moniert, dass ihre personenbezogenen Daten von Versicherungsunternehmen an den Gesamtverband der Deutschen Versicherungswirtschaft (GDV) weitergegeben werden. Die Versicherungsunternehmen berufen sich dabei auf die sog. „Einwilligungserklärung“, wonach die Kunden auf dem Antragsformular im Rahmen der Schlusserklärung die Versicherungsunternehmen zur Weitergabe ihrer Daten legitimiert hätten.

Tatsächlich haben die Kunden in der von Ihnen unterschriebenen „Schlusserklärung des Versicherungsnehmers und der zu versichernden Person“ eingewilligt, dass der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung ergeben, an den GDV zur Weitergabe dieser Daten an andere Versicherer übermittelt. Diese Einwilligung gilt auch unabhängig vom Zustandekommen des Vertrags.

Dies bedeutet aber nicht, wie vielfach befürchtet, dass die Gesundheitsdaten an Tochterunternehmen oder andere Versicherungen weitergegeben werden. Der GDV unterhält ein zentrales Hinweis- und Informationssystem (HIS). Mit diesem Hinweissystem wollen sich die Versicherer vor Missbrauch (Versicherungsbetrug) schützen und eine Risikoprüfung betreffend Neuabschlüsse durchführen. Wird nun ein Antrag auf Abschluss beispielsweise einer Lebensversicherung und/oder Zusatzversicherung abgelehnt oder kann ein solcher nur unter Leistungseinschränkungen oder gegen Zahlung eines Mehrbetrages angenommen werden, erfolgt von den Versicherungsgesellschaften, die an dem System partizipieren, eine Kurzmitteilung an das HIS. Diese Meldung umfasst lediglich die Mitgliedsnummer des Versicherers, das Meldedatum, den Familien- und Rufnamen sowie das Geburtsdatum des Antragstellers und einen kennzeichnenden Vermerk, der darauf hinweist, dass es sich um eine Lebensversicherung oder Berufsunfähigkeits-Zusatzversicherung gehandelt hat.

Die Daten werden dabei codiert übermittelt. Die Hinweismeldung stellt daher eine reine Tatsachenmitteilung dar und enthält keine Wertung über die generelle Versicherbarkeit des Antragstellers. Jeder Lebensversicherer nimmt eine eigene Risikoprüfung vor und verfügt über unternehmensspezifische Aufnahmerichtlinien. Insofern werden keine spezifischen Gesundheitsdaten weitergeleitet, sondern nur der beschriebene Kurzvermerk. Aus diesem Wagniseintrag können keine Aussagen über den Gesundheitszustand abgeleitet werden.

Diese Verfahrensweise ist in der Vergangenheit von den Aufsichtsbehörden nicht beanstandet worden. Der Text der verwendeten Standardeinwilligungserklärung wurde ursprünglich mit den Datenschutzaufsichtsbehörden abgestimmt. Zwischenzeitlich haben die Aufsichtsbehörden jedoch Bedenken gegen die von der Versicherungswirtschaft verwendeten Einwilligungserklärungen wegen mangelnder Transparenz erhoben. Anhand der Formulierung der Einwilligungserklärung ist für die Betroffenen nicht ersichtlich, welche konkreten Datenübermittlungen wann, an welches Unternehmen und mit welchen Konsequenzen erfolgen.
Von der Meldung an das HIS können neben Versicherungsnehmern auch andere Personen wie Zeugen, Geschädigte etc., die in keinem Vertragsverhältnis mit dem Versicherer stehen, betroffen sein, die nicht durch Erklärung in die Übermittlung ihrer Daten eingewilligt haben.
Ein weiterer Kritikpunkt der Aufsichtsbehörden ist die nach § 4a BDSG geforderte Freiwilligkeit der Einwilligungserklärung. Die Freiwilligkeit der Einwilligungserklärung beruht u. a. darauf, dass der Betroffene ohne Zwang selbstständig über die Abgabe der Erklärung entscheiden kann. Die im Antragsformular der Versicherungsunternehmen verwendete Einwilligungserklärung ist jedoch für die Antragsteller obligatorisch, d. h. es kommt kein Vertrag zustande, falls ein Antragsteller die Erklärung verweigert. Da aber bei nahezu allen Versicherungsunternehmen gleichermaßen verfahren wird, ist der potentielle Versicherungsnehmer gezwungen, die Erklärung abzugeben, wenn er einen Vertrag mit dem jeweiligen Versicherungsunternehmen abschließen will. Nach Ansicht der Aufsichtsbehörden verstößt diesen Verfahrensweise gegen die Regelung des § 4a BDSG.

Vor diesem Hintergrund haben die Aufsichtsbehörden den GDV aufgefordert, ein überarbeitetes Konzept vorzulegen, im Rahmen dessen den Betroffenen besser als bisher bewusst wird, welche Daten über sie zu welchen Zwecken erhoben und übermittelt werden.

3.3 Schweigepflichtentbindungserklärung

Im Berichtszeitraum wurden der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich auch Fälle vorgetragen, in denen der Versicherer im Rahmen der Leistungsgewährung bei einer Kranken- bzw. Krankenzusatzversicherung Einblick in umfangreiche Gesundheitsunterlagen begehrte, was für die Betroffenen nicht nachvollziehbar war.
Die Versicherer begründen dies mit ihrer Verpflichtung, im Interesse der Solidargemeinschaft die Anspruchsvoraussetzungen für den Erhalt einer Leistung zu prüfen und berufen sich dabei u. a. auf entsprechende Regelungen der Allgemeinen Versicherungsbedingungen für die Krankheitskosten- und Krankenhaustagegeldversicherung, die Bestandteil des Vertrages zwischen ihnen und den Versicherungsnehmern sind, wonach Versicherungsnehmer auf Verlangen des Versicherers jede Auskunft, die zur Feststellung des Versicherungsfalles oder der Leistungspflicht des Versicherers und ihres Umfanges erforderlich ist, zu erteilen haben. Des Weiteren hätten die Versicherungsnehmer mit dem Antragsformular bei Abschluss der Versicherung eine Entbindung von der Schweigepflicht unterzeichnet. Diese grundsätzliche Mitwirkungspflicht begegnete bisher keinen datenschutzrechtlichen Bedenken der Aufsichtsbehörde.
Was die Schweigepflichtentbindungserklärung angeht, die bei allen Versicherungsarten, bei denen Gesundheitsdaten erhoben und verarbeitet werden, von den Betroffenen schon bei der Antragstellung abgegeben werden muss, berufen sich die Versicherer auf eine allgemeine Form der Erklärung, die vor Jahren mit den Aufsichtsbehörden abgestimmt worden war. Zwischenzeitlich, nicht zuletzt auch wegen entsprechender Änderungen des BDSG, wird diese Schweigepflichtentbindungserklärung von den Aufsichtbehörden als nicht mehr gesetzeskonform angesehen, weil es ihr an

Bestimmtheit fehlt. So werden beispielsweise Versicherte, deren Schweigepflichtentbindungserklärung oftmals viele Jahre vor Eintritt des Leistungsfalles abgegeben wurde, im Unklaren gelassen, in welchem Umfang, bei welchen Institutionen, Personen, Firmen etc. der Versicherer Gesundheitsdaten abfragt. Wie bei der „Einwilligungserklärung“ (vgl. oben) haben auch in diesen Fällen die Aufsichtsbehörden den GDV aufgefordert, eine überarbeitete Form der Erklärung vorzulegen, die den Interessen der Versicherungsnehmer gerecht wird. Ein Lösungsansatz könnte dabei die Regelung im Bereich der privaten Krankenversicherung sein, wo der Entwurf des § 211 Versicherungsvertragsgesetz (VVG) vorsieht, dass die Erhebung personenbezogener Gesundheitsdaten durch den Versicherer bei Dritten nur zulässig ist, soweit die Kenntnis der Daten für die Beurteilung des zu versichernden Risikos bzw. der Leistungspflicht erforderlich sind, die Daten bei einer der in § 203 (1) Nummer 1, 2 und 6 Strafgesetzbuch (StGB) genannten Personen erhoben werden und die betroffene Person eine Einwilligung nach § 4a BDSG erteilt hat.

4. Ärzte

4.1 Herausgabe bzw. Aufbewahrungspflicht der ärztlichen Behandlungsunterlagen

Vielfach wurde die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich von Patienten mit der Frage befasst, ob die Herausgabe der im Rahmen der ärztlichen Behandlung angefallenen Patientenunterlagen von den Patienten verlangt werden könne bzw. wie lange diese Unterlagen gegebenenfalls aufbewahrt werden müssen.

Die Petenten wurden darauf hingewiesen, dass ein Anspruch auf Herausgabe der Originalakte, insbesondere vor Ablauf der unten genannten Fristen, nicht besteht. Nach Ablauf der Fristen kann der Arzt die Unterlagen an den Patienten abtreten. Vor Ablauf der Fristen kann der Arzt gegen eine angemessene Gebühr Kopien an den Patienten herausgeben.

Die Pflicht des Arztes zur Dokumentation ist im ärztlichen Standesrecht (vgl. § 10 der Musterberufsordnung) und, für den vertragsärztlichen Bereich, in den Bundesmantelverträgen für Ärzte und Zahnärzte geregelt. Die Aufbewahrungsfrist für Krankenunterlagen beträgt nach § 10 Absatz 3 der Musterberufsordnung zehn Jahre nach Abschluss der Behandlung. Andere gesetzliche Bestimmungen enthalten jedoch längere Fristen, wie etwa 30 Jahre für Aufzeichnungen über die Behandlung mit radioaktiven Stoffen bzw. Strahlen, 15 Jahre für Unterlagen und Röntgenbilder beim Durchgangsarzt sowie 20 Jahre für Aufzeichnungen für berufsgenossenschaftliche Verletzungsverfahren im stationären Bereich. Nach Ablauf der genannten Fristen werden die Unterlagen vernichtet oder an den Patienten abgetreten. Im Interesse der Beweissicherung kann eine Vernichtung vor Ablauf der Fristen nicht verlangt werden.

4.2 Zugriff von Ärzten bzw. Krankenhäusern auf eine bei einem Facharzt einzurichtende Labordatenbank

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich wurde von einem Facharzt, der beabsichtigte, eine Laborbefunddatenbank einzurichten, um datenschutzrechtliche Bewertung gebeten. Auf die beim Facharzt einzurichtende Labordatenbank sollen andere Ärzte und Krankenhäuser Zugriff erhalten. Hintergrund sei, dass Patienten oftmals stationär behandelt würden, weil keine Laborbefunde vorlägen. Ein zentraler Zugriff aus diese Datenbank könne dies vermeiden und so Zeit und Kosten sparen.
Seitens der Aufsichtsbehörde wurde dargelegt, dass für den Zugriff von Dritten wie Ärzten oder Krankenhäuser auf in einer Datenbank gespeicherte Laborbefunddaten eines Patienten eine Einwilligung des datenschutzrechtlich betroffenen Patienten benötigt wird. Die Einwilligung ist gemäß § 4a Bundesdatenschutzgesetz (BDSG) nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Der Betroffene ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit dies nach den Umständen des Einzelfalles erforderlich ist oder vom Betroffenen verlangt wird, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, sofern nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

Da besondere Arten personenbezogener Daten (dazu gehören Gesundheitsdaten) erhoben, verarbeitet oder genutzt werden sollen, muss sich die Einwilligung nach § 4a Absatz 3 BDSG ausdrücklich auf diese Daten beziehen.
Die Einwilligung muss also grundsätzlich schriftlich erklärt werden und den in § 126 BGB näher geregelten Voraussetzungen entsprechen. Die Betroffenen müssen ihr Einverständnis nicht nur schriftlich erklären, sondern auch eigenhändig unterzeichnen. Diese Formbindung ist eine Schutzvorkehrung zugunsten der Betroffenen. Weder eine konkludente, noch eine stillschweigende oder gar mutmaßliche Einwilligung reichen infolgedessen aus. Auch „prophylaktische“ Einwilligungserklärungen in All-

gemeinen Geschäftsbedingungen (AGB) müssen sich am Maßstab des § 4a BDSG messen lassen. Als Wirksamkeitsvoraussetzung für eine Einwilligungserklärung, die als AGB-Teil anzufügen ist, wird verlangt, dass der Betroffene über die Erteilung oder Ablehnung seiner Einwilligung frei entscheiden kann, ohne den Vertrag dadurch zu gefährden (vgl. Menzel, „Datenschutzrechtliche Einwilligung“, DuD 2008, S. 400 [406]).
Auch werden aus datenschutzrechtlicher Sicht hohe Anforderungen an die technische und organisatorische Ausgestaltung gestellt, wenn personenbezogene Gesundheitsdaten automatisiert in einer Datenbank verarbeitet oder genutzt werden sollen. Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben nach § 9 BDSG die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation gemäß der Anlage zu § 9 BDSG so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Was die in dem künftigen Geschäftsbetrieb beschäftigten Personen anbelangt, die mit der Verarbeitung personenbezogener Daten befasst sein werden, ist darauf hinzuweisen, dass es nach § 5 BDSG den bei der Datenverarbeitung beschäftigten Personen untersagt ist, personenbezogene Daten unbefugt zu erheben, zu verarbei-

ten oder zu nutzen (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.
Zur Frage, ob eventuell ein betrieblicher Beauftragten für den Datenschutz zu bestellen ist, ist Folgendes zu beachten:
Soweit nach § 4f Absatz 1 BDSG nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen. Eine Vorabkontrolle nach § 4d Absatz 5 Nummer 1 BDSG ist bei der Verarbeitung personenbezogener Daten über die Gesundheit eines Menschen stets erforderlich, es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

4.3 Weitergabe von Patientendaten an ärztliche Abrechnungsstellen

Eine häufig wiederkehrende Problematik wirft die Frage auf, unter welchen Voraussetzungen Patientendaten von Ärzten an ärztliche Abrechnungsstellen weitergeben werden dürfen. So wurde, zumindest nach Angabe von Petenten, von einigen Ärzten die Ansicht vertreten, eine Weitergabe der Daten an die Abrechnungsstellen sei auch ohne Zustimmung der Patienten möglich.
Diese Auffassung, wonach die Behandlungsdaten auch ohne Einwilligung der Betroffenen zur Abrechnung weitergegeben werden, widerspricht datenschutzrechtlichen wie auch strafrechtlichen Vorschriften (zur Einwilligung nach § 4a BDSG vgl. die Ausführungen unter Ziffer 4.2).
Was die Tätigkeit der ärztlichen Abrechnungsstellen selbst betrifft, so äußern Petenten Bedenken hinsichtlich der Weitergabe Ihrer Daten an die Abrechnungsstelle sowie hinsichtlich der Entbindung des Arztes von der Schweigepflicht. Hier ist darauf

hinzuweisen, dass sich die Schweigepflichtentbindung des Arztes nur auf die für Abrechnung und Geltendmachung der Forderung erforderlichen Daten bezieht. Ohne diese Schweigepflichtentbindung wäre die Weitergabe der Daten und damit die Übernahme der Forderung durch die Abrechnungsstellen insgesamt überhaupt nicht möglich.

4.4 Abrechnung und Bereitstellung von Servicedienstleistungen für Heilberufe durch eine GmbH

Im Zusammenhang mit der privatärztlichen Liquidation von Behandlungskosten wurden verstärkt Anfragen von Privatpatienten an die Aufsichtsbehörde betreffend die Tätigkeit einer GmbH, die sich mit der Abrechnung von Patientendaten und Servicedienstleistungen für Heilberufe befasst, gerichtet. Dabei ging es um die Frage, ob das Geschäftsmodell der GmbH mit den datenschutzrechtlichen Regelungen konform ist, insbesondere um die Einwilligungserklärung der Patienten zur Datenübermittlung sowie um das von der GmbH im Internet bereitgestellte Patientenportal.
Nach ihrem Geschäftsmodell kauft die betroffenen Gesellschaft privatärztliche Honorarforderungen von Ärzten, Zahnärzten, Dentallabors und Kliniken auf, um in eigener Zuständigkeit die Honorarforderungen bei den Patienten einzutreiben. Der Vorteil für die Kunden (Ärzte etc.) der GmbH liegt neben einer einfacheren und kostengünstigen Abwicklung vor allem darin, dass die GmbH auch das Risiko übernimmt. Die Ärzte müssen sich nicht mehr um Rechnungen, Zahlungseingänge und eventuelle Mahnverfahren kümmern. Auch die Vereinbarung von Ratenzahlungen mit Patienten ist durch die GmbH möglich. Außerdem können die Patienten online Teilzahlungen vereinbaren, Zahlungseingangsbestätigungen ausdrucken oder Rechnungskopien anfordern.
Aufgrund verschiedener Stellungnahmen der betreffenden GmbH sowie Gesprächen mit der Aufsichtsbehörde ist hierzu folgendes anzumerken:

Was die Risikoprüfung angeht, wird die Einholung einer Information bei einer Auskunftei zur Prüfung der Zahlungsfähigkeit auf eine entsprechende Einverständniser-

klärung der Patienten gestützt. Nach § 4 Absatz 1 des Bundesdatenschutzgesetzes ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Soweit demnach eine wirksame Einwilligung vorliegt, kann die Datenverarbeitung auf diese gestützt werden. Insofern bestehen auch keine durchgreifenden Bedenken gegen eine derartige Einwilligung, die letztendlich dem von der Verrechnungsstelle zu tragenden finanziellen Ausfallrisiko geschuldet ist. Eine ganz ähnliche Klausel für Anfragen einer Verrechnungsstelle verwendet beispielsweise auch die Schufa. Die Formulierung in der Einverständniserklärung muss jedoch so präzise sein, als die GmbH als Auskunftsempfangsberechtigter explizit genannt ist. In einer transparenten Einverständniserklärung müssen die Betroffenen die möglichen Beeinträchtigungen ihres informationellen Selbstbestimmungsrechts klar erkennen können.

Das Patientenportal soll nach Darstellung der GmbH einer vereinfachten, internetbasierten Kommunikation zwischen GmbH und dem Patienten dienen. Die Daten werden der Öffentlichkeit nicht zugänglich gemacht. Allein der Patient kann mit Hilfe der nur ihm bekannten Rechnungsnummer sowie zusätzlich mit einem gesondert erhaltenen Passwort Zugriff auf verschiedene Servicefunktionen des SSL-verschlüsselten Portals nehmen.
Neben der Implementierung eines Passwortschutzes werden über die Internetverbindung auch keine Gesundheitsdaten selbst übertragen. Zur jeweiligen Rechnungsnummer werden lediglich der Rechnungsbetrag sowie die Kontaktanschrift des behandelnden Arztes ohne weiteren Bezug zur Person des Patienten oder etwaigen Behandlungsdaten zugänglich gemacht.
Die Verarbeitung personenbezogener Daten im Internet ist auch nicht generell unzulässig. Ebenso wie in Bereichen außerhalb des Internets haben nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, nach § 9 BDSG nebst Anlage zu dieser Vorschrift die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der

Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten.
Zu diesen Maßnahmen zählen laut Nummern 1 – 3 der Anlage zu § 9 BDSG u. a. Zutritts-, Zugangs- und Zugriffskontrollen. Ist die Einhaltung dieser Anforderungen und der sonstigen datenschutzrechtlichen Vorschriften gewährleistet, so hat die Aufsichtsbehörde keine Möglichkeit, weitergehende Maßnahmen zu fordern oder das Verfahren gar ganz zu untersagen.
Im vorliegenden Fall hat die betroffene GmbH die Einhaltung bzw. Umsetzung der vorgenannter Regelungen zugesagt.

5. Datenschutz in Vereinen

5.1 Der Sponsoringvertrag

Ein Bürger hatte sich an die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich gewandt mit der Bitte um Prüfung der datenschutzrechtlichen Zulässigkeit der Weitergabe von Mitgliederdaten eines Sportvereins an die örtlich ansässige Geschäftsstelle einer Versicherungsgesellschaft im Rahmen eines Sponsoringvertrages.

Der Sportverein hatte mit der Versicherung einen Sponsoringvertrag geschlossen, wonach die Versicherung die Vereinsmitglieder zwecks Angebotes einer KFZ-Versicherung anschreibt und dafür den Verein finanziell unterstützt. Konkret hatte der Sportverein die Adressdaten seiner Mitglieder weitergegeben, woraufhin die Versicherung die Mitglieder angeschrieben hat. Der Petent äußerte insbesondere die Befürchtung, dass die einmal übermittelten Daten von der Versicherung an weitere Stellen weitergegeben werden könnten.
Nach § 4 Absatz 1 Bundesdatenschutzgesetz (BDSG) sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.
Eine vorherige Einwilligung lag hier nicht vor. Eine gesetzliche Befugnis könnte sich möglicherweise ergeben aus § 28 Absatz 1 bis 3 BDSG. Dabei sind die „berechtigten Interessen“ – auch finanzieller Art – der verantwortlichen Stelle bei der Interessenabwägung genauso zu berücksichtigen wie eventuell entgegenstehende schutzwürdige Interessen Betroffener. In der konkreten Fallbetrachtung sind diese Interessen gegeneinander abzuwägen.

So ist vorliegend festzustellen, dass es bei den übermittelten Mitgliederdaten um Adressdaten ging, die so auch größtenteils öffentlich zugänglich in Telefonbüchern

u. ä. stehen. Andere, nicht öffentlich zugängliche Daten, wie Geburtsdaten o. ä., wurden nicht übermittelt.

Auch ist in die Betrachtung mit einzubeziehen, ob den Verein möglicherweise über das Normalmaß hinausgehende Schutzpflichten treffen, wie dies beispielsweise bei einer Suchtselbsthilfegruppe der Fall wäre. Da es hier um einen Sportverein geht, kann dies verneint werden, da die Sensibilität der dort verarbeiteten Adressdaten als vergleichsweise niedrig eingestuft werden kann.

Trotzdem bleibt festzuhalten, dass die Bekanntgabe von Mitgliederdaten für Werbezwecke in der Regel vom Vereinszweck nicht gedeckt ist. Die Mitglieder vertrauen üblicherweise darauf, dass ihre Daten nicht an Dritte weitergegeben werden.
In diesem Sinne war der Verein auch hier zur Rücksichtnahme gegenüber seinen Mitgliedern verpflichtet.

Das richtige Verfahren wäre letztlich gewesen, schon im Vorfeld die Bekanntgabe der fraglichen Mitgliederdaten an Sponsoren für Werbezwecke in der Vereinssatzung oder durch Mitgliederbeschluss festzulegen, bzw. vor der Datenübermittlung die Einwilligung der Mitglieder einzuholen. Den Vereinsmitgliedern wurde im Anschreiben der Versicherung zwar ein Widerspruchsrecht eingeräumt, allerdings zu einem Zeitpunkt, als die Daten schon übermittelt waren.
Die Aufsichtsbehörde hat dies gegenüber den Sportvereinsvorsitzenden beanstandet.

Um nun künftig denkbare Beeinträchtigungen schutzwürdiger Interessen der Betroffenen soweit wie möglich zu vermeiden, hat die Aufsichtsbehörde die Vorsitzenden des Sportvereins zu einem Gesprächstermin eingeladen, um das weitere Vorgehen zu erörtern.

Als Ergebnis dieser Besprechung wurde festgehalten, dass eine Zusatzvereinbarung zu dem Sponsoringvertrag geschlossen werden soll, worin sich die Vertragspartner wie folgt verpflichten:

1. Die Versicherung verpflichtet sich, die ihr zur Verfügung gestellten Mitgliederadressen ausschließlich in ihrem Organisationsbereich für Zwecke im Sinne der abgeschlossenen Werbevereinbarung zu verwenden.

2. Eine Weitergabe an andere Unternehmen und Organisationen oder andere Organisationseinheiten auch innerhalb der Versicherung ist nicht zulässig.

3. Zwischen den Vertragspartnern besteht Einvernehmen, dass bei einem Verstoß gegen dieses Weitergabeverbot die Werbevereinbarung insgesamt mit sofortiger Wirkung hinfällig wird.

4. Die Versicherung verpflichtet sich ferner, ihr zur Verfügung gestellte Mitgliederadressen aus ihrem Datenbestand zu löschen, wenn Vereinsmitglieder dies zukünftig nachträglich wünschen sollten. Zudem verpflichtet sich die Versicherung, die fraglichen Daten zu löschen, sobald die Kenntnis der Daten für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, spätestens jedoch zum Ende der fraglichen Werbesaison.

5.2 Die Kleingärtner

Eine örtlich ansässige Bezirksgruppe von Kleingärtnervereinen war von der Stadt als Verpächterin zur Mitteilung der Einzelpächter aufgefordert worden. Hintergrund dieser Aufforderung war, dass die Stadt ihrerseits selbst um eine Stellungnahme hinsichtlich des sozialen Aspekts des Kleingartenwesens gebeten worden war. In diesem Zusammenhang forderte die Stadt darüber hinaus von den Kleingärtnervereinen auch die Namen weiterer Interessenten.

Der Vorsitzende der Bezirksgruppe wandte sich daraufhin an die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich mit der Bitte um Auskunft zu der Frage, ob die Namen und Anschriften der Einzelpächter sowie weiterer Interessenten seinerseits herausgegeben werden dürften bzw. müssten.

Die Aufsichtsbehörde hat sich zur Beurteilung dieser Frage den Pachtvertrag vorlegen lassen. Aus diesem Pachtvertrag ergab sich die Verpflichtung der Pächter, der Verpächterin jedes Jahr ein Verzeichnis der Garteninhaber mit Angabe der Flächengröße einzureichen. Die fraglichen Daten in Bezug auf die Einzelpächter mussten der Stadt daher ohnehin vorgelegt werden. Insofern bestand eine Übermittlungspflicht der Kleingärtnervereine, die einen eventuellen Rückgriff auf das Bundesdatenschutzgesetz insofern unnötig machten. Sollte dieser vertraglichen Verpflichtung bisher nicht hinreichend nachgekommen worden sein, so war das kein datenschutzrechtliches Problem.

Die eigentliche Frage, um die es in dem vorliegenden Fall ging, war demnach, ob die Stadt die bei ihr bereits potentiell vorhandenen Daten auch zu anderen als den in dem Pachtvertrag vorgesehenen Zwecken verwenden durfte.
Da die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Saarlandes für die datenschutzrechtliche Kontrolle der Stadt als öffentlicher Stelle jedoch nicht zuständig ist, musste diese Frage offen bleiben.

Was allerdings die von der Stadt geforderte Datenübermittlung, auch soweit es Interessenten betrifft, angeht, so wurde hier keine Verpflichtung der Vereine zur Übermittlung nach dem Pachtvertrag gesehen, da mit der Interessebekundung an einer Pacht noch kein Vertrag vorliegt.

Es ist zwar durchaus vorstellbar, dass gerade zur Beurteilung der gegenwärtigen Situation des Kleingartenwesens sowie zur Vorhersage künftiger Entwicklungen in diesem Bereich insbesondere die Anzahl der Interessenten von großem Interesse sowohl für den Verein als auch für die Interessenten sein kann. Ohne nähere Infor-

mationen zu Hintergrund und Ziel der zu erstellenden Stellungnahme zum Kleingartenwesen konnte dies aber nicht abschließend bewertet werden.

6. Datenschutz bei Auskunfteien

6.1 Das Mahnschreiben

Ein Bürger wandte sich an die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Saarlandes wegen eines Mahnschreibens, das er aufgrund einer angeblich noch offenen Forderung von einem Inkassounternehmen erhalten hatte. Das Inkassounternehmen betreibt neben diesem Bereich auch die Bereiche Wirtschaftsauskünfte sowie Marketing.

Das Mahnschreiben enthielt eine „Benachrichtigung gemäß BDSG“, wonach die den Petenten betreffenden Daten auch bei einer außerhalb des Saarlandes ansässigen Wirtschaftsauskunftei desselben Verbandes gespeichert seien.

Der Petent bat um Auskunft, was es mit dieser Benachrichtigung genau auf sich habe, da er sich hierdurch unter Druck gesetzt sah. Er befürchtete, dass nun hinsichtlich seiner Person beauskunftet werden könnte, dass er seine Rechnungen nicht zahle. Er habe jedenfalls gewichtige Gründe geltend gemacht, die Zahlung zu verweigern.

Eine Nachfrage der Aufsichtsbehörde bei dem Inkassounternehmen ergab, dass die in Rede stehende Benachrichtigung die der Auskunft erteilenden Stelle obliegende Benachrichtigungspflicht nach § 33 des Bundesdatenschutzgesetzes erfüllen solle.

Diese Benachrichtigungspflicht besagt, dass der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen ist, wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert werden. Dies ist bei Auskunfteien der Fall.

Die Pflicht zur Benachrichtigung besteht nach § 33 Absatz 2 Nummer 1 BDSG aber dann nicht, wenn der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat.

Vor dem Hintergrund dieser Ausnahmeregelung vertrat das Unternehmen die Auffassung, dass die Benachrichtigungspflicht für die Auskunftei entfalle, wenn der Betroffene bereits in dem Mahnschreiben auf die Speicherung hingewiesen wurde.

Die Aufsichtsbehörde hat dem entgegen gehalten, dass der fragliche Hinweis in der Funktion als Inkassounternehmen angebracht worden war, nicht in Funktion als Auskunftei. Inkassounternehmen speichern Daten jedoch nicht zum Zwecke der geschäftsmäßigen Übermittlung.

Diese beiden Tatbestände sind zu trennen, d. h. die Norm ist nicht so zu verstehen, dass die Kenntnis von der Speicherung die Kenntnis von der Übermittlung (oder umgekehrt) ersetzen könnte. Danach macht also der Hinweis auf eine Speicherung gerade nicht den Hinweis auf eine erstmalige Übermittlung entbehrlich, so dass demnach die Auskunftei bei erstmaliger Beauskunftung weiter zur Benachrichtigung verpflichtet bleibt.

Konsequenterweise hat die Aufsichtsbehörde die Änderung des Hinweises gefordert, soweit dieser „Benachrichtigung gemäß Bundesdatenschutzgesetz“ genannt wird. Dies liegt darin begründet, dass der Hinweis eine eigenständige, BDSG-konforme Benachrichtigung der für die Auskunftserteilung örtlich zuständigen Stelle nicht ersetzen kann.

Für die Betroffenen wäre dies ansonsten auch irreführend, wenn der Hinweis – wie hier unter ausdrücklichem Verweis auf das BDSG – den Eindruck erweckt, eine Bestimmung des Bundesdatenschutzgesetzes zu erfüllen. Der rein informatorische Charakter des Hinweises muss dabei zum Ausdruck kommen.

Das Unternehmen hat daraufhin mitgeteilt, den Hinweis künftig nicht mehr „Benachrichtigung gemäß Bundesdatenschutzgesetz“, sondern nur noch „Hinweis“ zu nennen.

Was die eigentliche Forderung betrifft, so konnte aufgeklärt werden, dass diese tatsächlich strittig war. In dem Datensatz wurde daher sichergestellt, dass dem Petenten hierdurch keine Nachteile erwachsen können.

7. Fälle von überregionaler Bedeutung

7.1 Mitarbeiterüberwachung in Lebensmitteldiscountern eines Unternehmens unter Einsatz von Detektiven und Überwachungskameras

Jedes Jahr verschwinden im Einzelhandel Waren im Wert von etwa 4 Milliarden Euro durch Diebstähle von Kunden, Mitarbeitern oder Fremdpersonal. Experten schätzen, dass von diesem Schaden etwa 1 Milliarde Euro auf Mitarbeiterdiebstähle zurückzuführen ist. Vor diesem Hintergrund ist es nicht verwunderlich, wenn im Einzelhandel Detektive und Videokameras eingesetzt werden. Allerdings sollte dabei der Datenschutz beachtet werden.

Nach Medienberichten im Jahre 2008 zufolge soll ein Unternehmen der Lebensmittelbranche in den Jahren 2006 und 2007 Detekteien und andere Sicherheitsunternehmen (im Folgenden Sicherheitsunternehmen genannt) beauftragt haben, Geschäftsräume in ihren Filialen durch Videoüberwachungsanlagen zu beobachten und dabei das Verhalten von Mitarbeitern festzustellen. Als Belege wurden Auszüge aus Einsatzberichten veröffentlicht. Darin waren unter anderem Informationen aus dem Privatleben, zum Beispiel über Beziehungsprobleme oder finanzielle Schwierigkeiten, sowie über das Verhalten der Kolleginnen und Kollegen bei der Arbeit und im Umgang miteinander protokolliert.

Auftraggeber der Sicherheitsunternehmen, die diese Einsatzberichte angefertigt hatten, waren rechtlich verselbständigte Vertriebsgesellschaften des Unternehmens. Während sich der Hauptsitz des Unternehmens in Baden-Württemberg befindet, sind die Vertriebsgesellschaften in verschiedenen Bundesländern angesiedelt. Die für die Unternehmenssitze zuständigen Datenschutzaufsichtsbehörden der Länder leiteten daher die zur Aufklärung der Geschehnisse erforderlichen datenschutzrechtlichen Überprüfungsverfahren ein. Dabei übernahm die baden-württembergische Aufsichtsbehörde dankenswerterweise die Koordination der Datenschutzüberprüfungen.

Im Zuständigkeitsbereich der Datenschutzaufsichtsbehörde des Saarlandes befindet sich nur eine Vertriebsgesellschaft. Diese verwaltet Filialen nicht nur im Saarland, sondern auch in angrenzenden Gebietsteilen von Rheinland-Pfalz.

Die von der Aufsichtsbehörde des Saarlandes durchgeführten Ermittlungen, in deren Rahmen auch Arbeitnehmerverbände miteinbezogen wurden, ergaben keine Anhaltspunkte, dass in den dem Zuständigkeitsbereich der Aufsichtsbehörde des Saarlandes unterfallenden Filialen sich datenschutzrechtliche Vorfälle gemäß der Medienberichterstattung ereignet haben. Zwar sind in einer Filiale Überwachungsmaßnahmen von einer Detektei mit zwei Kameras durchgeführt worden. Dabei handelt es sich in Bezug auf den Zuständigkeitsbereich der hiesigen Aufsichtsbehörde um den einzigen Ladendetektiveinsatz in einer Filiale, bei dem offen sichtbare Überwachungskameras verwendet wurden. Eine verdeckte Observation durch Kameras hat dabei also nicht stattgefunden. Nach dem Ermittlungsergebnis der hiesigen Aufsichtsbehörde sind aber seitens des Lebensmittelunternehmens keine Mitarbeiterinnen oder Mitarbeiter durch Einsatz von Detekteien und Kameras beobachtet oder sonst wie bespitzelt worden.

In anderen Bundesländern haben sich hingegen einige Vorwürfe in den Medien bestätigt. In einer von der baden-württembergischen Aufsichtsbehörde im Jahre 2008 im Einvernehmen mit den an den Ermittlungen beteiligten Datenschutzaufsichtsbehörden der Länder veröffentlichten Pressemitteilung, die für diesen Tätigkeitsbericht entsprechend anonymisiert wurde und auszugsweise wiedergegeben wird, ist festgehalten:

„1. (Video-) Beobachtung von Mitarbeitern durch einen Ladendetektiv mit Kamera (sog. LDK-Einsätze)

Rund 30 Vertriebsgesellschaften haben im Untersuchungszeitraum 1. Januar 2006 bis Ende März 2008 vor allem „zur Verringerung inventurrelevanter Verluste“ Sicherheitsunternehmen in mehr als 900 Fällen meist mündlich und zumeist ohne exakte Formulierung des Auftrags

mit der Durchführung kameragestützter Einsätze in Filialen beauftragt (sogenannter „Ladendetektiv mit Kamera“). In der Regel erfolgte der Einsatz so, dass ein Mitarbeiter des Sicherheitsunternehmens (nachfolgend: Detektiv) für die Mitarbeiter erkennbar für eine Woche in eine Filiale kam.

Der Detektiv nutzte in dieser Zeit teilweise die im öffentlichen Verkaufsraum vorhandenen Kameras mit Monitor. Sofern keine Kameras vorhanden waren oder diese ungeeignet erschienen, installierte das Sicherheitsunternehmen eigene, in der Regel versteckt angebrachte Miniaturkameras. Die Videodaten wurden in der Regel nicht aufgezeichnet, vielmehr verfolgte der Detektiv das Geschehen aus einem im Aufenthaltsraum befindlichen Kontrollmonitor.

Insbesondere drei der bei den Vertriebsgesellschaften seit 2006 für die unterschiedlichsten Aufgaben eingesetzten Sicherheitsunternehmen erstellten im Rahmen ihrer Aufträge umfassende Revisionsberichte. Die Detektive achteten sowohl auf Kundendiebstahl als auch auf das Verhalten der Mitarbeiter. Die Videobeobachtung spielt dabei wohl nur eine geringe Rolle. Die Detektive beobachteten die Mitarbeiter vor allem ohne Videogeräte, die Mitarbeiterbeobachtung wurde heimlich durchgeführt.
Gegenüber den Filialmitarbeitern wurde der Einsatz mit der Aufklärung von inventurrelevanten Verlusten bzw. der Aufdeckung von Kundendiebstählen begründet. Auf Nachfrage von Mitarbeitern bestritten die Detektive, wie einzelne Einsatzberichte belegen, dass sie Informationen über Mitarbeiter erheben und in einem Bericht verarbeiten, hörten deren Gespräche und (privaten) Telefonate mit, führten mit Ihnen Gespräche über sich und Dritte (Vorgesetzte und Kollegen) und legten alles in schriftlichen Einsatzberichten nieder. Die Einsatzberichte enthielten neben nicht personenbezogenen Angaben zur jeweiligen Filiale unter anderem folgende mitarbeiterbezogenen Feststellungen und Bewertungen:

- *Mitteilungen mit Bezug zu Inventurdifferenzen,*
- *Einschätzungen der Arbeitsleistung, -fähigkeit und –motivation der Mitarbeiter,*
- *Informationen zum Mitarbeiterverhalten gegenüber Kunden,*
- *Informationen, die sich auf die Einhaltung organisatorischer oder arbeitsvertraglicher Pflichten beziehen,*
- *Informationen zum Führungsverhalten und zu den Führungsqualitäten der Vorgesetzten in den Filialen,*

- *Informationen über das Pausenverhalten einzelner Mitarbeiter,*
- *Informationen über persönliche Problemlagen einzelner Mitarbeiter,*
- *Informationen über Zwischenmenschliches und daran anknüpfende Beurteilungen,*
- *Informationen zum Gesundheitszustand sowie zu (möglichen) Schwangerschaften,*
- *Informationen über die finanzielle Situation der Mitarbeiter und ihrer Familien,*
- *Informationen über Ereignisse, die aus Sicht des Detektivs einen wie auch immer gearteten Verdacht gegen einen oder mehrer Mitarbeiter begründen,*
- *Informationen über die (vermutete) Stimmungslage und Wesensart der Mitarbeiter,*
- *sonstige sehr persönliche Informationen."*

Weiter heißt es: *„In einem Fall führte der Protokollinhalt nachweisbar zur Kündigung einer Mitarbeiterin. Ob Protokollinhalte darüber hinaus Konsequenzen für einzelne Mitarbeiter hatten, ließ sich im Nachhinein nicht mehr feststellen."*

Datenschutzrechtlich ist das Vorgehen der Vertriebsgesellschaften des Lebensmittelsunternehmens in Bezug auf die Beobachtung von Mitarbeitern durch einen Ladendetektiv mit Kamera wie folgt bewertet worden:

„Die Datenschutzaufsichtsbehörden sind der Auffassung, dass bei etwa der Hälfte der noch vorhandenen Protokolle die Grenzen des rechtlich Zulässigen überschritten wurden. Die Vertriebsgesellschaften, die immer wieder die drei Sicherheitsunternehmen beauftragten, von denen sie wussten, dass sie Berichte mit solchen unzulässigen Inhalten anfertigen, tragen dafür die datenschutzrechtliche Verantwortung. Indem die Vertriebsgesellschaften die von den Detektiven verfassten Berichte entgegennahmen, lasen und aufbewahrten, verstießen sie gegen § 28 Absatz 1 des Bundesdatenschutzgesetzes. Die mit den datenschutzwidrigen Einsatzberichten verbundenen Datenschutzverstöße waren vielfach schwerwiegend und wurden von den Datenschutzaufsichtsbehörden der Länder, die solche Verstöße feststellten, gegenüber zwölf Vertriebsgesellschaften mit einem Bußgeld zwischen 3.000 und 15.000 Euro je Protokoll geahndet."

Zur heimlichen Beobachtung von Mitarbeitern durch Kameraeinsatz ist in der Pressemitteilung Folgendes ausgeführt worden:

„2. <u>Heimliche Beobachtung von Mitarbeitern durch Kameraeinsatz (sog. OBK)</u>

In rund 80 Fällen haben Vertriebsgesellschaften in nahezu allen Bundesländern im Wesentlichen die bereits oben angesprochenen drei Sicherheitsunternehmen damit beauftragt, in den Verkaufsräumen von Filialen zumeist oberhalb der Kassen, mitunter aber auch in den Mitarbeitern vorbehaltenen Nebenräumen, beispielsweise im Bereich der Mitarbeiterspinde oder von Türen und Fenstern oder im Pausenraum eine verdeckte Observation mit Kamera (OBK) durchzuführen. Dabei wurden ohne Kenntnis der Filialmitarbeiter meist mehrere Minikameras so in der Filiale angebracht, dass sie von diesen in der Regel nicht entdeckt wurden. Die von den Kameras erfassten Daten wurden – da während des Einsatzes kein Detektiv in der Filiale vor Ort war – für den Zeitraum des gesamten, in der Regel eine Woche dauernden Einsatzes aufgezeichnet. Anschließend wurden die Videodaten von den Sicherheitsunternehmen nach Auffälligkeiten, zum Beispiel aufgezeichneten Diebstählen oder anderen Straftaten durch Kunden oder Mitarbeiter oder Verstößen gegenüber betrieblichen Vorschriften ausgewertet. Für die auftraggebende Vertriebsgesellschaft wurde sodann ein Bericht gefertigt, dem belegende Videosequenzen beigefügt waren. 29 derartiger Berichte sowie eine größere Zahl von Videoaufzeichnungen lagen den Datenschutzaufsichtsbehörden vor.
Begründet wurden diese Maßnahmen von den Vertriebsgesellschaften vor allem mit „permanent schlechten Inventurergebnissen“, deren Gründe durch andere Maßnahmen nicht geklärt werden konnten, zum Teil auch mit einem Diebstahlsverdacht gegen einen oder mehrere Mitarbeiter. Nach Einschätzung der Aufsichtsbehörden wurde die Maßnahme vor allem eingesetzt, wenn eine Vertriebsgesellschaft Mitarbeiter verdächtigte, eine (Mit-)Schuld an zu hohen Inventurverlusten zu tragen.
Nach Auffassung der Datenschutzaufsichtsbehörden ließ sich die heimliche Videoüberwachung der Mitarbeiter nur in einem Teil der Fälle rechtfertigen. In anderen Fällen fehlte dafür eindeutig die Rechtsgrundlage oder es konnte nicht der Nachweis erbracht werden, dass die rechtlichen Voraussetzungen für die heimliche Mitarbeiterüberwachung vorlagen. In diesen Fällen wurden Daten von Mitarbeitern unbefugt erhoben, verarbeitet oder genutzt. Die Datenschutzaufsichtsbehörden haben dies gerügt und in Einzelfällen auch mit einem Bußgeld geahndet.“

Von allen zuständigen Datenschutzaufsichtsbehörden, also auch von der Aufsichtsbehörde des Saarlandes, wurde die Nichtbestellung betrieblicher Datenschutzbeauftragter bemängelt:

„Alle Vertriebsgesellschaften hatten bis Anfang Juni 2008 keinen betrieblichen Datenschutzbeauftragten bestellt, obwohl sie nach § 4 f des Bundesdatenschutzgesetzes hierzu verpflichtet gewesen wären. Die Datenschutzaufsichtsbehörden haben dies beanstandet. Es handelt sich insoweit nicht um einen Formalverstoß. Betriebliche Datenschutzbeauftragte haben die Aufgabe, in den Unternehmen auf die Einhaltung des Datenschutzes hinzuwirken. Angesichts des Umfangs und der Art der Erhebung, Verarbeitung und Nutzung personenbezogener Daten wäre es bei den Vertriebsgesellschaften besonderes dringlich gewesen, über betriebliche Datenschutzbeauftragte zu verfügen. Durch deren Einsatz hätte es möglicherweise vermieden werden können, dass es zu so schwerwiegenden Verstößen kam. Die Datenschutzaufsichtsbehörden haben daher jede der Vertriebsgesellschaften mit einem Bußgeld in Höhe von 10.000 Euro belegt."

7.2 Internetveröffentlichungen von personenbezogenen Bewertungen über Professoren und Lehrer

Während dienstleistungs- oder produktbezogene Bewertungen auf kommerziellen Internetportalen sich in den letzten Jahren etabliert haben, sind personenbezogene Bewertungen auf Internetforen nach wie vor umstritten. Im Fokus der Diskussion stehen insbesondere das Lehrerbewertungsportal www.spickmich.de und das Hochschullehrerportal www.meinprof.de. Portalnutzer können dort anonyme Bewertungen über Lehrpersonen abgeben.

So eröffnet der Portalbetreiber der Website „spickmich.de" die Möglichkeit zur Leistungsbewertung von Lehrern in den Kriterien „guter Unterricht", „leichte Prüfungen" und „faire Noten". Ferner können dort Zensuren vergeben werden, ob ein Lehrer sexy, cool, witzig oder beliebt ist.

Die internetbasierte Meinungsplattform „meinprof.de" erlaubt es, Dozenten in verschiedenen Kategorien wie „Fairness", „Verständlichkeit" oder „Spaß" zu bewerten.

Grundlage der Bewertung sollen Lehrveranstaltungen an den jeweiligen Hochschulen sein, die von den Portalnutzern besucht worden sind.
Personenbezogene Bewertungen auf diesen Portalen gaben daher Anlass, Rechtsschutz wegen eines Unterlassungsbegehrens aus einer möglichen Verletzung des allgemeinen Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung vor den Zivilgerichten zu suchen (vgl. Urteil des OLG Köln vom 27.11.2007, Az.: 15 U 142/07; Urteil des LG Köln vom 30.01.2008, Az.: 28 O 319/07; Urteil des LG Duisburg vom 18.04.2008, Az.: 10 O 350/07; Urteil des OLG Köln vom 03.07.2008, Az.: 15 U 43/08). Insbesondere durch die Möglichkeit von Freitexteingaben auf solchen Meinungs- und Diskussionsforen kann der Ehrenschutz der bewerteten Personen erheblich gefährdet werden. Im Zusammenhang mit Bewertungsportalen stellte sich auch die Frage nach der Haftung eines Forenbetreibers (vgl. Urteil des LG Düsseldorf vom 27.6.2007, Az.: 12 O 343/06; Urteil des LG Berlin vom 31.05.2007, Az.: 27 S 2/07).
Seitens der Zivilgerichte ist bislang zugunsten der Portalbetreiber entschieden worden.
Das allgemeine Persönlichkeitsrecht wurde beispielsweise wie folgt gewichtet:
Die Bewertung eines Lehrers auf einer Internetseite mittels vordefinierter Bewertungsskalen, die sich auf die konkrete Ausübung seiner beruflichen Tätigkeit – und somit seine Sozialsphäre – beziehe, verletze nicht dessen allgemeines Persönlichkeitsrecht, da es sich insoweit um grundrechtlich geschützte Meinungsäußerungen bzw. Werturteile handele (vgl. Urteil des OLG Köln vom 3.07.2008, Az.: 15 U 43/08 – juris-Dokument - Orientierungssatz 1). Das Bewertungsforum eines internetbasierten Schülerportals könne zwar in den Schutzbereich des Grundrechts auf Meinungsfreiheit gemäß Artikel 5 Absatz 1 des Grundgesetzes fallen. Aber auch Meinungen, die lediglich unter einer E-Mail-Adresse oder anonym im Internet abgegeben werden, würden den verfassungsrechtlich verankerten Schutz der Meinungsfreiheit genießen. Kollidiere das allgemeine Persönlichkeitsrecht nach Artikel 2 Absatz 1 des Grundgesetzes bzw. ein auf dieser Grundlage in Betracht kommendes Unterlassungsbegehren nach den §§ 823, 1004 BGB mit dem Recht zur Freiheit der Meinungsäußerung nach Artikel 5 Absatz 1 des Grundgesetzes, sei tatrichterlich eine Abwägung zwi-

schen den beiderseitigen Grundrechtspositionen im Rahmen der Tatbestandsmerkmale der einschlägigen zivilrechtlichen Normen vorzunehmen (vgl. Urteil des OLG Köln vom 27.11.2007, Az.: 15 U 142/07 – juris-Dokument – Leitsätze 1 bis 3). Dabei finde eine wertende Kritik ihre Grenze dort, wo es sich um eine reine Schmähkritik oder Formalbeleidigung handele oder sich die Äußerung als Angriff auf die Menschenwürde darstelle (vgl. Urteil des OLG Köln vom 27.11.2007, Az.: 15 U 142/07 – juris-Dokument – Seite 8). Der Schutz des allgemeinen Persönlichkeitsrechts reiche aber nicht so weit, dass er einem Einzelnen einen Anspruch darauf verleihe, in der Öffentlichkeit nur so dargestellt zu werden, wie er sich selber sehe oder von anderen gesehen werden möchte. In der Bewertung einer Lehrperson in einem Internetportal für Schüler liege auch dann keine Verletzung ihres allgemeinen Persönlichkeitsrechts, wenn die in fachlicher Form organisierte Bewertung unter Angabe des Zunamens der betroffenen Person, der Schule, an der sie unterrichte, und deren Lehrfächer erfolge (vgl. Urteil des OLG Köln vom 27.11.2007, Az.: 15 U 142/07 – juris-Dokument – Leitsätze 4 und 5).

Gemäß einer Pressemitteilung hat der Bundesgerichtshof in seiner Entscheidung vom 23. Juni 2009 das Urteil des OLG Köln vom 3. Juli 2008 (Az.: 15 U 43/08) bestätigt. Auch die Bundesrichter befanden, dass das Recht der Schüler auf Meinungsaustausch und freie Kommunikation das Recht der Lehrer auf informationelle Selbstbestimmung überwiege.

In datenschutzrechtlicher Hinsicht wurde das Recht auf informationelle Selbstbestimmung etwa wie folgt berücksichtigt:

Nach § 4 Absatz 1 in Verbindung mit § 28 Absatz 1 Satz 1 Nummer 3 des Bundesdatenschutzgesetzes ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten des Betroffenen auch ohne seine Einwilligung nach § 4a des Bundesdatenschutzgesetzes zulässig, wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Das Vorliegen dieser Voraussetzungen wurde für personenbezogene Daten

eines Lehrers, die auf der Website einer Schule veröffentlicht waren, bejaht (vgl. Urteil des OLG Köln vom 27.11.2007, Az.: 15 U 142/07 – juris-Dokument – Leitsatz 6).
Zur Haftung eines Forenbetreibers wurde ausgeführt:
Die Annahme einer Pflicht eines Betreibers eines Meinungsportals im Internet (Onlineportal) zur inhaltlichen Überprüfung aller eingestellten Beiträge scheide aus. Sie wäre wegen der Fülle der Beiträge praktisch nicht durchführbar. Allein der Umstand, dass sich der Forumbetreiber in seinen Nutzungsbedingungen die Löschung rechtswidriger Äußerungen vorbehalten habe, führe nicht zu einer generellen Prüfpflicht. Sei ein Professor von Studenten auf einer Online-Bewertungsplattform für Hochschullehrer als „Psychopath“ und „echt das Letzte“ bezeichnet worden und habe der Betreiber der Plattform die Bewertungen nach erfolgter Abmahnung gelöscht, stehe dem Betroffenen gegen den Plattformbetreiber kein Unterlassungsanspruch zu. Denn der Plattformbetreiber sei jedenfalls nicht passivlegitimiert (vgl. Urteil des LG Berlin vom 31.05.2007, Az.: 27 S 2/07 – juris-Dokument – Orientierungssatz 1 und 2).

Nach Ansicht der Aufsichtsbehörde des Saarlandes für den nicht-öffentlichen Bereich haben die zivilgerichtlichen Entscheidungen bislang das Recht auf informationelle Selbstbestimmung nicht hinreichend berücksichtigt. Gemeinsam mit den Datenschutzaufsichtsbehörden der anderen Länder drängt sie daher auf die Einhaltung des Datenschutzes bei Bewertungsportalen. Die Datenschutzaufsichtsbehörden weisen in einem im Anhang dieses Tätigkeitsberichts abgedruckten Beschluss, der auf einer Sitzung ihres Koordinierungsgremiums „Düsseldorfer Kreis“ am 17./18. April 2008 gefasst wurde, darauf hin, dass es sich bei Beurteilungen und Bewertungen von Lehrerinnen und Lehrern sowie von vergleichbaren Einzelpersonen in internetbasierten Bewertungsportalen vielfach um sensible Informationen und subjektive Werturteile handelt, die in das Portal eingestellt werden, ohne dass die Urheber erkennbar sind. Hinzu kommt, dass sensible personenbezogene Daten veröffentlicht werden und diese Veröffentlichung nicht etwa auf den Kreis einer Schülerzeitung beschränkt bleibt, wie dies die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen auf Seite 25 in ihrem 19. Datenschutzbericht (2009) zu

Recht bemerkt. Diese Informationen und Werturteile können jederzeit von jedermann abgerufen werden. Anbieter entsprechender Portale haben daher in der Rechtspraxis der Datenschutzaufsichtsbehörden die Vorschriften des Bundesdatenschutzgesetzes mit seinen Schutzvorkehrungen für die bewerteten Personen zu beachten. 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 (vgl. insoweit auch die kritische Würdigung des Urteils des OLG Köln vom 27.11.2007 durch Günther Dorn, „Lehrerbenotung im Internet“, in DuD 2008, S. 98 ff.).
In datenschutzrechtlicher Hinsicht sollten sich Portalbetreiber solcher Internetforen fragen, ob sie nicht geschäftsmäßig nicht allgemein zugängliche personenbezogene Daten an Dritte übermittelt haben, ohne die betroffenen Personen hierüber zu unterrichten, vgl. § 33 Absatz 1 des Bundesdatenschutzgesetzes. Ferner sollten sie sich mit der Frage befassen, ob sie im Rahmen des Betriebs des Internetportals nicht allgemein zugängliche personenbezogene Daten an Dritte weitergegeben haben, ohne die Gründe oder die Art und Weise der glaubhaften Darlegung eines berechtigten Interesses abzufragen und mindestens stichprobenartig zu überprüfen, vgl. § 29 Absatz 2 Satz 3 des Bundesdatenschutzgesetzes. Verstöße gegen diese Vorschriften stellen jeweils eine Ordnungswidrigkeit dar und können mit Bußgeldern geahndet werden, vgl. § 43 Absatz 1 Nummern 5 und 8, Absatz 3 des Bundesdatenschutzgesetzes.

Die Aufsichtsbehörde des Saarlandes für den Datenschutz im nicht-öffentlichen Bereich empfiehlt datenschutzrechtlich Betroffenen, sich an die jeweilige, für das Bewertungsportal zuständige Datenschutzaufsichtsbehörde zu wenden. Dies ist für das Bewertungsportal „spickmich.de“ die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, für das Bewertungsportal „meinprof.de“ der Berliner Landesbeauftragte für Datenschutz und Informationsfreiheit.
Die Adressen dieser Aufsichtsbehörden können aus dem Anhang dieses Tätigkeitsberichts entnommen werden.

7.3 Soziale Netzwerke im Internet und aktuelle Gefahren für ihre Nutzer

Bestimmte Internetdienste bieten Internetnutzern die Mitgliedschaft in einem Online-Kontaktnetzwerk, einem sozialen Netzwerk im Internet, an. In diesem Online-Kontaktnetzwerk haben Internetnutzer die Möglichkeit, von ihrer Person ein Persönlichkeitsprofil samt Interessen und Aktivitäten zu generieren und ihre Beziehungen zu anderen Menschen abzubilden, um diese Daten für weitere, vom Internetdienst zur Verfügung gestellte Anwendungsfunktionen in dieser Netzgemeinschaft zu verwenden. Diese Anwendungsfunktionen können zum Beispiel sein: die Festlegung der Zugehörigkeit zu einer Interessengruppe innerhalb der Netzgemeinschaft, die Ablage persönlicher Fotos oder Videodateien in sogenannten Fotoalben auf der Plattform des Internetdienstes, die Verwendung sogenannter Suchfunktionen zum gezielten Auffinden von Nutzerprofilen anderer Mitglieder der Netzgemeinschaft, die Veröffentlichung von sozialen Kontakten (sogenannte Kontaktlisten) zu anderen Mitgliedern, die Veröffentlichung von Kurzmeldungen des Mitglieds (sogenannte News-Feeds) über aktuelle Ereignisse aus seinem Privatleben, das Führen und Veröffentlichen eines digitalen Tagebuchs (sogenannte Blogs) sowie das Führen eines sogenannten Gästebuchs, in das andere Nutzer des Online-Kontaktnetzwerkes Kommentare insbesondere zum dargestellten Persönlichkeitsprofil eintragen dürfen. Online-Kontaktnetzwerke dieser Art dienen in der Regel als Privatplattformen für den Einsatz im privaten Bereich (z.B. myspace, facebook, studiVZ, wer-kennt-wen, lokalisten) oder als Geschäftsplattform zur Pflege von geschäftlichen Kontakten (z.B. XING, Linkedln).

Finanzquellen sozialer Netzwerke im Internet können Mitgliedsbeiträge und zielgruppengerichtete Werbung sein. Für Letzteres sind der sogenannte soziale Graph eines Mitglieds, also dessen innerhalb der Netzgemeinschaft abgebildete Beziehungen zu anderen Mitgliedern und Interessengruppen, sowie seine sonstigen, von ihm auf der Plattform eingetragenen personenbezogenen Daten von kommerziellem Interesse.

Vor diesem Hintergrund können soziale Netzwerke im Internet erhebliche Gefahren für deren Mitglieder aufweisen:

Viele Nutzer sind sich offenbar nicht bewusst, dass auf die von Ihnen im Internet preisgegebenen Daten eine Vielzahl anderer Nutzer der Netzgemeinschaft weltweit zugreifen können. Es besteht die Gefahr, dass diese personenbezogenen Daten unbefugt kopiert und etwa für merkantile Interessen von Adresshändlern missbraucht werden. Auch ist in den Medien vielfach berichtet worden, dass Personalberater Personensuchmaschinen einsetzen, um sich Informationen über Bewerber zu verschaffen. Im Internet recherchierte Informationen, wie freizügige Angaben über die eigene Person oder unvorteilhafte Partybilder, können dann der Karriere abträglich sein. Preisgegebene Daten über die eigene Person können aber auch für Angriffe auf die Privatsphäre bis hin zur Vorbereitung von Straftaten missbraucht werden. Denn für die Nutzung eines solchen Netzwerks kann häufig bereits eine Registrierung unter einem Pseudonym, einem sogenannten nickname, genügen. Die wahre Identität des Nutzers bleibt dann verborgen. Zudem besteht eine besonders hohe Gefährdung für die Mitglieder, wenn auf solchen Internetplattformen Sicherheitsschwachstellen existieren und Schutzmechanismen fehlen. Auf solche Sicherheitsrisiken hat das Frauenhofer Institut für Sichere Informationstechnologie in seiner Studie „Privatsphärenschutz in Soziale-Netzwerke-Plattformen“ hingewiesen.

Gerade in virtuellen Netzgemeinschaften ist daher Selbstdatenschutz aktueller denn je. Es gilt, die eigene Privatsphäre möglichst umfassend zu schützen. Aber auch die Anbieter von sozialen Netzwerken im Internet bleiben aufgefordert, ihre Internetdienste datenschutzkonform auszugestalten. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben deshalb am 17./18. April 2008 in Wiesbaden einen Beschluss zur datenschutzkonformen Ausgestaltung sozialer Netzwerke gefasst. Dieser Beschluss ist im Anhang abgedruckt.

8. Ausblick – Prävention: Google Street-View

Die US-Firma Google betreibt den Dienst “Google Maps”, in den ein Zusatzdienst mit dem Namen “Google Street-View“ eingebunden ist. Dieser Zusatzdienst „Google Street-View“ ist eine Funktion, die es dem Internetnutzer erlaubt, am Computerbildschirm bei einem virtuellen Spaziergang einen Straßenzug aus der Perspektive des Fußgängers zu betrachten. Um den Zusatzdienst Google Street-View anbieten zu können, fahren tagsüber Autos der Firma Google Germany GmbH, welche mit speziellen Kameras ausgestattet sind, öffentliche Straßen entlang und machen dabei Aufnahmen. Die Autos sind mit dem Google-Logo gekennzeichnet und auch aufgrund der Dachaufbauten erkennbar. Laut Google werden die so angefertigten Bilder in dieser Form nicht veröffentlicht. Vor der Veröffentlichung würden die Bilder dergestalt nachbearbeitet, dass Gesichter von Passanten und Autokennzeichen automatisch erkannt und unkenntlich gemacht werden.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben hierzu bereits im November 2008 festgestellt, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. (vgl. insoweit den im Anhang dieses Tätigkeitsberichts aufgeführten Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 13./14. November 2008 in Wiesbaden – Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet) .

Google hat daraufhin den Datenschutzaufsichtsbehörden zugesichert, eine Technologie zur Verschleierung von Gesichtern und von Kraftfahrzeugkennzeichen vor der Veröffentlichung von derartigen Aufnahmen einzusetzen.

Darüber hinaus können Grundstückseigentümer und Bewohner von Häusern der Veröffentlichung aufgezeichneter Haus- bzw. Grundstücksansichten widersprechen. Google hat verbindlich zugesichert, Widerspruchsmöglichkeiten zur Entfernung bzw. Unkenntlichmachung eines Gebäudes durch einen Bewohner oder Eigentümer vorzuhalten und derartige Widersprüche zu bearbeiten.

Ferner hat Google verbindlich zugesichert, dass Widersprüche zu Personen, Kennzeichen und Gebäuden bzw. Grundstücken bereits vor der Veröffentlichung von Bildern in einer einfachen Form berücksichtigt werden mit der Folge, dass die entsprechenden Bilder vor der Veröffentlichung unkenntlich gemacht werden. Voraussetzung ist eine Identifizierung des Grundstücks, der Person oder des Fahrzeugs.

Google hat verbindlich zugesagt, dass die Widerspruchsmöglichkeit auch nach der Veröffentlichung noch besteht.

Die Aufsichtsbehörde des Saarlandes für den nicht-öffentlichen Bereich ist nach § 38 des Bundesdatenschutzgesetzes für die Kontrolle der Verarbeitung von personenbezogenen Daten durch Unternehmen zuständig, die ihren Sitz im Saarland haben. Die Google Germany GmbH hat ihren Sitz in Hamburg. Für die datenschutzrechtliche Kontrolle der Google Germany GmbH ist daher die Zuständigkeit des Hamburgischen Datenschutzbeauftragten gegeben.
Im Mai 2009 hat die Google Germany GmbH angekündigt, digitale Straßenbilder für seinen Dienst „Google Street-View“ in Saarbrücken aufzunehmen. Daraufhin wurde auf Veranlassung des Ministeriums für Inneres und Sport des Saarlandes die Öffentlichkeit über die Medien informiert. Zwischenzeitlich hat Google verbindlich zugesichert, die geplanten Befahrungen mit einem Hinweis auf die Widerspruchsmöglichkeit im Internet rechtzeitig vorher bekannt zu geben. Die vorhandenen Befahrungspläne werden bis zu 2 Monate im Voraus veröffentlicht und ständig aktualisiert. Google hat die verbindliche Zusage gemacht, die Liste genauer zu gestalten und auf Landkreise und kreisfreie Städte zu erstrecken.

Betroffene können sich per E-Mail an streetview-deutschland@google.com oder postalisch an „Google Germany GmbH, Betr. Street View, ABC-Straße 19, 20353 Hamburg“ wenden. Widerspruch kann eingelegt werden im Internet unter http://maps.google.de/intl/de/help/maps/streetview/faq.html#q7 oder schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg. Der Link mit dem Text: "FAQ Street View (inkl. Widerspruchsmöglichkeiten)" ist di-

rekt auf der ersten Seite der Hilfeseiten für Google Maps Deutschland erreichbar. Diese Hilfeseiten erreicht jeder Nutzer direkt aus dem Produkt Google Maps Deutschland, wenn er oben rechts den Link "Hilfe" klickt.

Anhang

Beschlussfassungen des Düsseldorfer Kreises im Berichtszeitraum 2007/2008

Im Berichtszeitraum hat sich der Düsseldorfer Kreis mit folgenden Schwerpunktthemen befasst:

A. Beschlussfassungen der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 19./20. April 2007 in Hamburg:

Weitergabe von Kundendaten durch Versandhandelsunternehmen an Auskunfteien

Die Übermittlung von personenbezogenen Daten über das vertragsgemäße Zahlungs- und Geschäftsabwicklungsverhalten ihrer Kunden sowie die Übermittlung von Scorewerten, die auf der Grundlage dieses Verhaltens berechnet wurden, durch Versandhandelsunternehmen an Auskunfteien zur Nutzung für deren eigene Geschäftszwecke ist unzulässig, es sei denn, die Kunden haben ausdrücklich in die Weitergabe dieser Daten eingewilligt.
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 Zulässigkeit einer Weitergabe von Kundendaten in dem genannten Umfang kann nicht auf § 28 BDSG gestützt werden, da sie nicht der Zweckbestimmung des Vertragsverhältnisses des Versandhandelsunternehmens mit dem Kunden dient (§ 28 Absatz 1 Satz 1 Nummer 1 BDSG) und die schutzwürdigen Interessen der Kunden an dem Ausschluss der Weitergabe ihrer Daten an Auskunfteien überwiegen (§ 28 Absatz 1 Satz 1 Nummer 2 BDSG).
Die Kunden, die im Versandhandel bestellen, müssen nicht damit rechnen, dass ihr bisheriges Kundenverhalten gegenüber einem Versandhaus entscheidend dafür sein kann, ob sie Lieferungen von anderen Unternehmen erhalten, die bei einer Auskunftei Bonitätsauskünfte einholen.
Die Kunden dürfen nicht zum Objekt wirtschaftlichen Handelns dadurch gemacht werden, dass der Handel selbst definiert, was für die Kunden bzw. ihre Daten gut ist. Sie haben daher ein überwiegendes schutzwürdiges Interesse an dem Ausschluss der Vermarktung ihrer positiven Bonitätsdaten.

Weitergabe von umzugsbedingten Adressänderungen durch Versandhandelsunternehmen (in der Fassung vom 26. Juni 2007)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest: 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 weitergeleitet werden sollen.

Kreditscoring / Basel II

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich beurteilen die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten beim Einsatz von Scoring-Verfahren im Bereich der Kreditwirtschaft wie folgt:
I. Welche personenbezogenen Merkmale dürfen für die Berechnung des Scores genutzt werden?
1. Es dürfen nur Parameter genutzt werden, deren Bonitätsrelevanz mittels eines den wissenschaftlichen Standards entsprechenden mathematisch-statistischen Verfahrens nachgewiesen wurde. Die statistische Relevanz eines Parameters ist für die Einstellung in das Scoring-Verfahren eine notwendige, aber noch keine hinreichende Bedingung.
2. Nach § 28 Absatz 1 Satz 1 Nummer 1 BDSG dürfen nur Daten erhoben und gespeichert werden, soweit dies zur Zweckbestimmung eines Vertragsverhältnisses erforderlich ist. Die Tatsache, dass ein Scoring-Verfahren durchgeführt wird, ändert daran nichts und erweitert nicht den Berechtigungsrahmen der Banken. Es dürfen daher nur Daten in ein Scoring-Verfahren eingestellt werden, die das Institut im Rahmen eines Kreditvertrages erheben darf (Erforderlichkeitsprinzip). Soweit Daten für andere Zwecke, etwa aufgrund von Vorgaben des KWG oder des WpHG erhoben und gespeichert wurden, dürfen diese Daten nur für diese Zwecke, nicht jedoch für Scoring-Verfahren verwendet werden. (Da sensitive Daten im Sinne des § 3 Absatz 9 BDSG nicht nach § 28 Absatz 1 Satz 1 Nummer 1 BDSG erhoben und verarbeitet werden, dürfen diese auch nicht in die Score-Berechnung einfließen.)
3. Das Scoring-Verfahren selbst stellt eine Datennutzung dar. Für diese gilt § 28 Absatz 1 Satz 1 Nummer 2 BDSG. Danach ist die Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ein berechtigtes Interesse der Banken an der Nutzung der für das Scoring-Verfahren verwendeten Parameter kann in der Regel angenommen werden. Wenn das Kreditinstitut die Möglichkeit hat, konkrete, unmittelbar boni-

tätsrelevante Daten zu erheben, darf es nicht auf Daten zurückgreifen, die nur Indizcharakter haben.
Soweit ein berechtigtes Interesse der Banken vorliegt, ist bei jedem einzelnen Parameter zu überprüfen, ob der Betroffene überwiegende schutzwürdige Interessen am Ausschluss der Datennutzung geltend machen kann. Die hier vorzunehmende Abwägung stellt einen normativen Prozess dar; die bloße statistische Relevanz eines Kriteriums führt noch nicht dazu, dass nicht von überwiegenden schutzwürdigen Interessen des Betroffenen auszugehen ist.
Bei der Abwägung können die gesetzgeberischen Wertungen aus § 10 Absatz 1 Satz 3 ff. KWG herangezogen werden. § 10 Absatz 1 KWG gilt zwar als bankenaufsichtsrechtliche Norm nur für die Erhebung und Verarbeitung personen- bezogener Daten zur internen Risikobemessung (Eigenkapitalausstattung), nicht jedoch für das Scoring im Außenverhältnis zu den (potentiellen) Kundinnen und Kunden.
Die Wertungen aus § 10 Absatz 1 Satz 3 ff. KWG können allerdings als gesetzgeberisches Leitbild in die Auslegung des BDSG einfließen. Das gilt insbesondere für die Anforderungen an Scoring-Merkmale. Die Merkmale müssen daher nicht nur mathematisch-statistisch erheblich sein, sondern eine ebenso hohe Stringenz aufweisen wie die im Merkmalskatalog des § 10 Absatz 1 Satz 6 KWG aufgeführten Regelbeispiele. So sind Angaben zur Staatsangehörigkeit bereits aufgrund des ausdrücklichen Verbots in § 10 Absatz 1 Satz 3 KWG als Score-Merkmale ausgeschlossen.
Bei der Abwägung sind darüber hinaus Wertungen des Grundgesetzes wie auch des einfachen Rechts daraufhin zu überprüfen, ob eine Benachteiligung der (potentiellen) Kundinnen und Kunden aufgrund eines bestimmten Kriteriums unzumutbar ist.
4. Auch wenn sich Basel II vornehmlich mit der Eigenkapitalhinterlegung der Institute befasst, wird der Einsatz von Scoring-Verfahren zunehmend dazu führen, jeden Kredit entsprechend dem individuellen Risiko zu bezinsen. Nur wenn in einer Gesamtschau der Kriterien sichergestellt ist, dass diesem Anliegen Rechnung getragen wurde, erfolgt die Datennutzung zur Wahrung berechtigter Interessen und sind keine überwiegenden schutzwürdigen Interessen der Betroffenen tangiert.
II. Wie transparent müssen die Bewertungen für die Betroffenen sein?
Für die Betroffenen (wie auch für die Aufsichtsbehörden) muss nachvollziehbar sein,
1. welche personenbezogenen Merkmale in die Berechnung des Score-Wertes einfließen;
2. welche konkreten personenbezogenen Daten der kreditsuchenden Person dafür genutzt wurden;
3. welches die maßgeblichen Merkmale sind, die den konkreten Score-Wert der betroffenen Person negativ beeinflusst haben. Diese maßgeblichen Merkmale sollen nach ihrer Bedeutung bzw. den Grad ihres Einflusses auf den konkreten Score-Wert aufgelistet werden, wobei sich die Auflistung auf die vier bedeutsamsten Merkmale beschränken soll.
Darüber hinaus ist bei der Anwendung von Scoring-Verfahren der § 6a BDSG zu beachten.

Internationaler Datenverkehr

1. Der Düsseldorfer Kreis beschließt das anliegende **Positionspapier** zum internationalen
Datenverkehr. Der BlnBDI wird gebeten, das Papier als Vorsitzender der AG „Internationaler Datenverkehr“ an die damals beteiligten Wirtschaftsvertreter zu versenden, die zugleich darauf hingewiesen werden sollen, dass weitere Fallkonstellationen in einer allgemein zugänglichen Handreichung näher dargestellt werden.
Die im Positionspapier genannten Auffassungen können von den Aufsichtsbehörden bei der Beratung auch anderer Wirtschaftsvertreter genutzt werden.
2. Der Düsseldorfer Kreis beschließt ferner die anliegende **Handreichung** zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung.
Sie beinhaltet die häufigsten Fallkonstellationen und soll den Unternehmen die rechtliche Bewertung erleichtern. Im Einzelfall kann eine abweichende Bewertung erforderlich sein. Deshalb verbieten sich schematische Lösungen. Den Aufsichtsbehörden wird anheim gestellt, die Handreichung im Internet zu veröffentlichen oder auf andere Weise interessierten Unternehmen zugänglich zu machen.

Abgestimmte Positionen der Aufsichtsbehörden in der AG "Internationaler Datenverkehr" am 12./13. Februar 2007 - Bezug: Protokoll der Sitzung mit Wirtschaftsvertretern am 23. Juni 2006 –

I. Bestimmung der "datenexportierenden Stelle" nach §§ 4 b, 4 c BDSG

1. Faustregel: Wer öffnet die Tür zum Datenexport?
Maßgebliches Entscheidungskriterium ist die Entscheidungsbefugnis über den Datenexport in das Drittland (z. B. Entscheidung über die Zuteilung/Vergabe von Zugriffsrechten). Die Befugnis verbleibt grundsätzlich beim Datenverarbeiter in Deutschland.
2. Rechtlich unselbständige Niederlassungen können übermittelnde Stellen im Sinne der §§ 4b, 4c BDSG sein.
3. Rechtlich unselbständige Niederlassungen sind nicht Antragsteller oder Adressat von Genehmigungsverfahren.
4. Ein Standardvertrag zwischen einem Unternehmen und seiner rechtlich unselbständigen Niederlassung ist nicht möglich, da dies ein In-Sich-Geschäft wäre. Eine (zugangs-, aber nicht empfangsbedürftige) Garantieerklärung (durch die ein Garantievertrag mit den betroffenen Personen zustande kommt) ist daher erforderlich.
5. Eine Zulässigkeitsprüfung in der 1. Stufe unabhängig von derjenigen in der 2. Stufe erfolgt in den Fällen, in denen deutsche Niederlassungen Daten an den europäischen Hauptsitz übermitteln (z.B. zum Abruf von dort durch den US-Konzernhauptsitz). Gleichwohl können Fragestellungen der 2. Stufe bei der Prüfung der 1. Stufe von Bedeutung sein.

II. Arbeitsbericht der Ad-hoc-Arbeitsgruppe "Konzerninterner Datentransfer" – Auswirkungen bzw. Bedeutung und Umsetzung der Ergebnisse beim Drittstaatentransfer

1. Die Verbindlichkeit von Betriebsvereinbarungen im Drittland wird durch "Unterwerfungserklärung" des Datenimporteurs hergestellt.
2. Der alternative Standardvertrag ist grundsätzlich für Arbeitnehmerdaten nicht geeignet (und evt. ergänzungsbedürftig), da die Haftung und Auskunftspflicht des Da-

tenexporteurs (des deutschen Arbeitgebers) eingeschränkt sind. Wertungswidersprüche zum deutschen Recht (1. Stufe) sind zu vermeiden.
3. Bei allen Standardverträgen sind auch die Anforderungen nach nationalem Recht (1. Stufe) zu erfüllen, ggf. durch eine Zusatzvereinbarung (z. B. des Einwilligungserfordernisses statt Widerspruchsrecht). Wertungswidersprüche zum deutschen Recht (1. Stufe) sind zu vermeiden (vgl. Artikel 2 der Kommissionsentscheidungen vom 15. Juni 2001 und 27. Dezember 2001).
4. Bei Änderung eines Standardvertrages, die eindeutig zugunsten des Betroffenen ausfällt, besteht u. U. keine Genehmigungspflicht nach § 4 c Absatz 2 BDSG, was durch Rückfrage bei der zuständigen Aufsichtsbehörde zu klären ist.
5. Die Antwort 4 zu FAQ 9 / Safe Harbor-Entscheidung hat nur deklaratorische Wirkung, kann also Rechte der betroffenen Arbeitnehmer gegen den Arbeitgeber in Deutschland / EU weder begründen noch beschränken, sondern gibt nur das Verständnis der US-Seite bezüglich des EU-(Arbeits-)Rechts wieder. Die Unternehmen tragen die Darlegungslast für die Arbeitnehmerrechte, die sicherzustellen sind.
III. Gelten bei der Datenweitergabe von einem in Deutschland befindlichen Datenverarbeitungsdienstleister an seinen im Drittstaat befindlichen Auftraggeber die Anforderungen der §§ 4 b, 4 c BDSG?
1. Der Auftraggeber (AG) im Drittland muss das BDSG nach § 1 Absatz 5 Satz 2 bei der Datenverarbeitung durch den deutschen Auftragnehmer (AN) berücksichtigen, wenn der AG auf automatisierte Mittel zur Datenverarbeitung in Deutschland zurückgreift.
2. Bei der (Rück-)Übermittlung durch den AN an den AG gelten die §§ 4 b, 4 c BDSG nicht (insofern neue Ansicht), unter anderem weil nach § 3 Absatz 8 Satz 3 BDSG der Auftragnehmer in Deutschland nicht Dritter im Verhältnis zur verantwortlichen Stelle ist und somit keine Übermittlung im Sinne von § 3 Absatz 4 Nummer 3 BDSG stattfindet. Die Rückausnahme, die § 3 Absatz 8 Satz 3 BDSG selbst impliziert, nämlich dass Auftragnehmer außerhalb des EWR Dritte sind, greift nicht für den Auftraggeber im Drittstaat.
3. Für die Verarbeitung in Europa und die Rückübermittlung durch deutsche AN an AG im Drittland gelten die technisch-organisatorischen sowie bestimmte materiellrechtliche Regelungen des BDSG (d.h. nur §§ 28 ff, nicht §§ 4 b, 4 c BDSG). Adressat der Aufsichtsbehörde zur Durchsetzung der materiell-rechtlichen Vorschriften ist weiterhin nur der Auftraggeber. Den AN trifft gegenüber dem AG eine "qualifizierte Remonstrationspflicht" bei Kenntniserlangung von Umständen im Sinne von § 11 Absatz 3 Satz 2 BDSG.
4. Wegen § 1 Absatz 5 BDSG gilt materielles Datenschutzrecht, wenn die Daten in Deutschland erarbeitet werden (siehe 1.). Bei der Anwendung insbesondere des § 28 BDSG ist aber der besonderen Sachlage der Auftragsdatenverarbeitung Rechnung zu tragen. Einerseits ist das berechtigte Interesse des Auftraggebers, im Rahmen seiner Organisationsentscheidungen auch Datenverarbeitungsschritte auf Auftragnehmer (AN) zu verlagern, bei § 28 Absatz 1 Satz 1 Nummer 2 BDSG zu betrachten. Die schutzwürdigen Interessen der Betroffenen sind andererseits entsprechend der jeweiligen Fallkonstellation zu gewichten. In diesem Zusammenhang sind grundsätzlich auch die Wertungen der Rechtsordnungen im Drittstaat von Bedeutung, sofern sie nicht gegen den "ordre public" in Deutschland (z.B. bei Menschenrechtsverletzungen) verstoßen.

5. Deutsches materielles Recht gilt nicht, wenn der deutsche AN nicht auf die vom AG übermittelten Daten zugreifen kann (weil die Datenverarbeitung im geschlossenen System / Black Box oder verschlüsselt erfolgt).

Fallgruppen zur internationalen Auftragsdatenverarbeitung
Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung
Einleitung
Die folgende Darstellung beinhaltet die häufigsten Fallkonstellationen der internationalen Auftragsdatenverarbeitung und soll den Unternehmen die rechtliche Bewertung erleichtern. Im Einzelfall kann eine abweichende Bewertung erforderlich sein. Deshalb verbieten sich schematische Lösungen. Alle Grafiken stammen vom Regierungspräsidium Darmstadt, Dezernat Datenschutz.

Fallgruppe A
Konstellation:
Der Auftraggeber ist in der EU/EWR ansässig, während der Auftragnehmer und der von ihm beauftragte Unterauftragnehmer im Drittland ansässig sind.
Besonderheit:
Die Pflichten des Auftragnehmers sind an den Unterauftragnehmer "weiterzuleiten".
Bewertung:
Der Auftraggeber hat einen weiteren "Drittstaatenvertrag" mit dem Unterauftragnehmer zu schließen, oder der Unterauftragnehmer muss dem Vertrag zwischen dem Auftraggeber und dem Auftragnehmer beitreten.

Fallgruppe B
Konstellation:
Der Auftraggeber und der Auftragnehmer sind in der EU/EWR ansässig. Es wird ein Unterauftragnehmer im Drittland eingeschaltet, der die Daten vom Auftragnehmer erhält.
Besonderheit:
Der Abschluss eines Standardvertrags zwischen Auftragnehmer in der EU/EWR und dem Unterauftragnehmer im Drittland ist nicht sachgerecht, weil der Auftragnehmer (anders als der Datenexporteur in den Standardverträgen) nicht verantwortliche Stelle ist. Der Auftragnehmer hat dann selbst keine vertraglichen Rechte oder Pflichten.
Bewertung:
Der Auftraggeber ist als Datenexporteur im Sinne der §§ 4b, 4c einzustufen, der Unterauftragnehmer als Datenimporteur. Beide müssen daher Vertragsparteien des Standardvertrages vom Dez. 2001 sein. Ein Beitritt des Auftragnehmers in der EU/EWR zum Vertrag ist jedenfalls sinnvoll.
Näheres hierzu: s. Erläuterungen.

Erläuterung der Bewertung zur Fallgruppe B:
Da u.U. wegen der möglichen Vielzahl von Auftraggebern entsprechend viele Standardverträge mit den Unterauftragnehmern abgeschlossen werden müssten, ist es praktikabel und akzeptierbar, dass der Auftragnehmer im Auftrag (oder besser: in Vertretung) der Auftraggeber einen Standardvertrag (Auftragsdatenverarbeitung) mit dem Unterauftragnehmer abschließt. Dass auch der EU/EWR-Auftragnehmer dem

Vertrag zwischen Auftraggeber und Drittstaaten-Unterauftragnehmer beitritt, ist jedenfalls sinnvoll. Bei einem Beitritt besteht keine Genehmigungspflicht nach § 4 c Absatz 2 BDSG, und zwar unabhängig davon, ob er durch eine gesonderte Vereinbarung erfolgt oder als Vertragsergänzung in den "Drittstaatenvertrag" integriert wird.
Folgender Text kann für einen derartigen Beitritt verwendet werden:
"Die vorstehenden Regelungen gelten mit folgender Maßgabe auch für den DV-Dienstleister in Europa [Name, Sitz], der insoweit dem Vertrag beitritt. Da der Datenexporteur einen Datenverarbeitungsdienstleistungsvertrag mit [Name des DV-Dienstleisters in Europa] geschlossen hat (als Auftragsdatenverarbeitung gemäß § 11 BDSG / Artikel 2e, 17 Absatz 3 EGDatenschutzrichtlinie 95/46/EG und den hierzu erlassenen nationalen Vorschriften) und der Datenimporteur als "Unterauftragnehmer" (oder: Subunternehmer) für [Name des DVDienstleisters in Europa] fungiert, ist der/die [Name des DV-Dienstleisters in Europa] gegenüber dem Datenexporteur primär verantwortlich, dass der Datenimporteur die Pflichten gemäß diesem Vertrag erfüllt. Der [Name des DV-Dienstleisters in Europa] hat zu diesem Zweck entsprechende abgeleitete Kontrollpflichten gegenüber dem Datenimporteur und kann hierfür die in diesem Vertrag beschriebenen Kontrollbefugnisse des Datenexporteurs wahrnehmen. Dieser bleibt verpflichtet, die Ausübung der Kontrollbefugnisse zu überwachen, und kann jederzeit auch selbst diese Kontrolle gegenüber dem Unterauftragnehmer ausüben."

Fallgruppe C
Konstellation:
Ein in der EU/EWR ansässiges Unternehmen beauftragt einen im Drittstaat ansässigen DV-Dienstleister mit der Verarbeitung personenbezogener Daten und schließt mit diesem den Standardvertrag vom Dezember 2001 (Controller - Processor) oder einen entsprechenden individuellen Vertrag. Der DV-Dienstleister im Drittstaat schaltet einen DV-Dienstleister in der EU/EWR ein, welcher die Daten nach Erledigung des Auftrags an das Unternehmen im Drittstaat (rück-) transferiert.
Besonderheit:
Der Dienstleister in der EU (DV-Dienstleister 2) erhält Daten vom DV-Dienstleister im Drittland (DV-Dienstleister 1). Ein Vertrag besteht nur zwischen dem Unternehmen und dem DVDienstleister 1.
Bewertung:
Es besteht keine Notwendigkeit einer eigenständigen vertraglichen Regelung nach § 4 c Absatz 2 BDSG zwischen dem EU-/EWR-Dienstleister und dem Drittland-Unternehmen. Ein Beitritt des EU-/EWR-Dienstleisters zum "Drittstaatenvertrag" ist jedenfalls sinnvoll.
Näheres hierzu: s. Erläuterungen.

Fallgruppe D
Konstellation:
Ein in der EU/EWR ansässiges Unternehmen übermittelt Daten an ein Unternehmen im Drittstaat und schließt mit diesem den Standardvertrag vom Juni 2001 oder Dezember 2004 (Controller - Controller) oder einen entsprechenden, individuellen Vertrag. Das Unternehmen im Drittstaat schaltet einen DV-Dienstleister in der EU/EWR

ein, welcher die Daten nach Erledigung des Auftrags an das Unternehmen im Drittstaat (rück-)transferiert.

Besonderheit:

Es besteht nur ein Vertragsverhältnis zwischen dem Controller in der EU und dem Controller im Drittland.

Bewertung:

Es besteht (wie bei Fallgruppe C) keine Notwendigkeit einer eigenständigen vertraglichen Regelung nach § 4c Absatz 2 BDSG zwischen dem EU-/EWR-Dienstleister und dem Drittlandunternehmen. Ein Beitritt zum "Drittstaatenvertrag" ist jedenfalls sinnvoll.

Näheres hierzu: s. Erläuterungen.

Fallgruppe E

Konstellation:

Wie in Fallgruppe D, aber zwischen dem in der EU/EWR ansässigen Unternehmen und dem Unternehmen im Drittstaat wird kein "Drittstaaten-Vertrag" gemäß § 4c Absatz 2 BDSG abgeschlossen, weil eine der Katalogausnahmen des § 4c Absatz 1 BDSG gegeben ist.

Besonderheit:

Es besteht nur ein Vertragsverhältnis zwischen dem Controller in der EU und dem Controller im Drittland.

Bewertung:

Es besteht (wie bei Fallgruppen C und D) keine Notwendigkeit einer eigenständigen vertraglichen Regelung zwischen dem EU-/EWR-Dienstleister und dem Drittlandunternehmen.

Näheres hierzu: s. Erläuterungen.

Erläuterung der Bewertung zu den Fallgruppen C, D und E:

Die Fallgruppen C, D und E sind dadurch gekennzeichnet, dass die Daten von einer verantwortlichen Stelle, die quasi der "Primär-Exporteur" ist, in ein Drittland transferiert und hierbei die Voraussetzungen des § 4c BDSG erfüllt wurden.

Der DV-Dienstleister in der EU/EWR ist quasi der "Sekundär-Exporteur". Ungeachtet der grundsätzlichen Frage, inwieweit EU/EWR-Auftragnehmer überhaupt verantwortlich sind für das Vorliegen der Voraussetzungen der §§ 4b, 4c BDSG (s. hierzu Näheres zu den Fallgruppen F bis I), ist jedenfalls in den Fallgruppen C, D und E keine eigenständige vertragliche Regelung im Sinne des § 4c Absatz 2 BDSG zwischen dem EU/EWR-Dienstleister und dem Drittstaaten-Unternehmen erforderlich.

Offensichtlich ist dies bei der **Fallgruppe C**, bei der sich der eigentliche Auftraggeber in der EU/EWR befindet. Da Zweck und Umfang der zulässigen Datenverarbeitung, die einzuhaltenden Datensicherheitsmaßnahmen etc. bereits in dem Vertrag zwischen dem EU/EWRAuftraggeber und dem Drittstaaten-Auftragnehmer geregelt sind, besteht weder ein Erfordernis noch ein Spielraum für den EU/EWR-Unterauftragnehmer für eigenständige Vorgaben gegenüber dem Drittstaatenunternehmen bzgl. der dortigen Datenverarbeitung.

Würde man einen individuellen -genehmigungsbedürftigen- Vertrag mit dem EU/EWRUnterauftragnehmer für erforderlich halten (die Standardverträge passen hier nicht), dann würde dies sogar die Gefahr bergen, dass Regelungen getroffen

werden, die dem Vertrag zwischen dem EU-Auftraggeber und dem Drittstaaten-Unternehmen widersprechen.
Gleiches gilt für die **Fallgruppe D**. Wenngleich sich hier - im Unterschied zu C - der "Auftraggeber" im Drittstaat befindet, wurden doch auch hier bereits umfassende Regelungen zur Gewährleistung ausreichender Datenschutzgarantien im Drittstaat getroffen, sodass für den EU/EWR-Auftragnehmer kein Erfordernis und kein Spielraum für eigene Vorgaben bestehen. Ein Beitritt des EU/EWR-Auftragnehmers zu dem Vertrag zwischen dem "Primär- Datenexporteur" und dem Datenimporteur ist in den Fallgruppen C und D sinnvoll. Wenn kein DV-Dienstleistungsvertrag existiert, der den Vorgaben des § 11 BDSG entspricht, kann diese Lücke durch Beitritt zum Vertrag geschlossen werden.
In der **Fallgruppe E** besteht zwar kein Vertrag zwischen dem "Primär-Datenexporteur" und dem Datenimporteur zur Gewährleistung ausreichender Datenschutzgarantien (ein Beitritt scheidet daher aus), allerdings wäre es nicht gerechtfertigt, an den "Sekundär- Datenexporteur" strengere Anforderungen zu stellen als an den "Primär-Datenexporteur".
Der Abschluss eines -genehmigungsbedürftigen- Vertrags im Sinnes des § 4c Absatz 2 BDSG zwischen EU-Auftragnehmer und Drittstaatenunternehmen ist auch in der Fallgruppe E nicht erforderlich.

Fallgruppe F
Konstellation:
Ein in der EU/EWR ansässiger DV-Dienstleister wird von einem in einem Drittland ansässigen Unternehmen beauftragt, in der EU/EWR personenbezogene Daten zu erheben und zu verarbeiten und dann an den Auftraggeber im Drittstaat zu transferieren.
Besonderheit:
Der Auftraggeber im Drittland beauftragt den DV-Dienstleister in der EU/EWR auch zusätzlich mit Datenerhebungen in der EU/EWR. Der DV-Dienstleister bleibt zwar auch Datenverarbeiter, kennt die Daten aber selbst (im Unterschied zur Fallgruppe G).
Bewertung:
Der DV-Dienstleister ist für die von ihm durchgeführte Datenverarbeitung verantwortlich (§ 11 in Verbindung mit § 9 BDSG, Artikel 17 Europäische Datenschutzrichtlinie). Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich. Er ist Adressat der übrigen Vorschriften des BDSG. Der DV-Dienstleister hat selbst keine Verantwortung im Sinne der §§ 4b, 4c BDSG.
U.U. trifft ihn aber eine "Remonstrationspflicht". Bezüglich der selbst erhobenen Daten muss er eine summarische Plausibilitätsprüfung vornehmen.
Näheres hierzu: s. Erläuterungen.

Fallgruppe G
Konstellation:
Ein in der EU/EWR ansässiger DV-Dienstleister 1 wird von einem in einem Drittland ansässigen Unternehmen beauftragt, personenbezogene Daten zu verarbeiten und danach an den Auftraggeber zu transferieren. Die Daten stammen aus der EU/ dem

EWR. Sie wurden hier entweder vom Auftraggeber selbst oder in dessen Auftrag von einem DV-Dienstleister 2 erhoben.

Besonderheit:

Die Daten für den DV-Dienstleister 1 in der EU/EWR kommen vom Auftraggeber aus dem Drittland sowie vom europäischen DV-Dienstleister 2.

Bewertung:

Der DV-Dienstleister 1 ist für die von ihm durchgeführte Datenverarbeitung verantwortlich (§ 11 in Verbindung mit § 9 BDSG, Artikel 17 Europäische Datenschutzrichtlinie). Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich. Er ist Adressat der übrigen Vorschriften des BDSG. Der DV-Dienstleister 1 hat selbst keine Verantwortung im Sinne der §§ 4b, 4c BDSG. U.U. trifft ihn aber eine "Remonstrationspflicht".

Näheres hierzu: s. Erläuterungen.

Fallgruppe H

Konstellation:

wie Fallgruppe G, aber die Daten stammen nicht aus der EU/EWR, sondern aus dem Drittland. Sie werden in der EU/EWR nur verarbeitet und dann zurückübermittelt.

Besonderheit:

Die aus dem Drittland stammenden Daten wurden nach dortigem Recht zulässig erhoben. Nach deutschem Recht wäre die Erhebung unzulässig gewesen.

Bewertung:

Der DV-Dienstleister ist für die von ihm durchgeführte Datenverarbeitung verantwortlich (§ 11 in Verbindung mit § 9 BDSG, Artikel 17 Europäische Datenschutzrichtlinie). Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich. Er ist Adressat der übrigen Vorschriften des BDSG. Der DV-Dienstleister hat selbst keine Verantwortung im Sinne der §§ 4b, 4c BDSG. U.U. trifft ihn aber eine "Remonstrationspflicht".

Näheres hierzu: s. Erläuterungen.

Fallgruppe I

Konstellation:

Wie Fallgruppe G oder H, aber der EU/EWR-Dienstleister erhält die Daten in verschlüsselter Form und kann von dem Inhalt keine Kenntnis nehmen.

Besonderheit:

Der DV-Dienstleister in der EU/EWR kennt die Daten aus dem Drittland nicht (Black Box- Konstellation).

Bewertung:

Deutsches materielles Recht gilt weder für die DV-Dienstleister noch für den Auftraggeber, wenn der deutsche AN nicht auf die vom AG übermittelten Daten zugreifen kann (weil die Datenverarbeitung im geschlossenen System oder verschlüsselt erfolgt, ohne dass der AN über den Schlüssel verfügt).

Näheres hierzu: s. Erläuterungen.

Erläuterung der Bewertung zu den Fallgruppen F, G, H, I:

Nach § 1 Absatz 5 Satz 2 BDSG findet dieses Gesetz Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Für die Verarbeitung durch den DV-Dienstleister in Deutschland gilt somit das BDSG. Der DV-Dienstleister ist grundsätzlich nur für die Datensicherheit der von ihm durchgeführten Datenverarbeitung nach Maßgabe der Regelungen in § 11 in Verbindung mit § 9 BDSG, Artikel 17 Europäische Datenschutzrichtlinie verantwortlich. Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich. Bei den Fallgruppen F, G, H und I gibt es keine "Primär-Datenexporteure", die für das Vorliegen der Voraussetzungen des § 4c BDSG beim Drittstaaten-Auftraggeber zu sorgen haben. Die Frage der eigenen Verantwortlichkeit des EU/EWR-Auftragnehmers wird hier also besonders virulent. Fraglich ist, ob ihn weitere (über die vorgenannten hinausgehenden) Pflichten treffen.
Hinsichtlich der **Fallgruppen F bis I** ist zu fragen, ob sich für den Auftragnehmer aus § 1 Absatz 5 Satz 2 BDSG die Pflicht ergibt zu prüfen und sicherzustellen, dass beim (Rück-) Transfer der Daten die Voraussetzungen des § 4c BDSG (bzw. des § 4b BDSG) erfüllt werden. Würde man eine solche Pflicht annehmen, müsste der Auftragnehmer eine umfassende Prüfung der gesamten Datenverarbeitung vornehmen, also eine umfassende Prüfung des Zwecks der gesamten Datenverarbeitung sowie des Kontextes und der Umstände der Datenverarbeitung. Die bloße Vereinbarung mit dem Auftraggeber im Drittstaat, dass die Daten von jenem nur zu dem Zweck weiterverarbeitet werden dürfen, zu dem der Auftragnehmer die Daten erhalten hat, würde keinesfalls reichen. Eine Verantwortung gemäß §§ 4b, 4c BDSG würde vielmehr eine eigenständige umfassende Prüfung durch den Auftragnehmer erfordern. Dieser kennt aber höchstwahrscheinlich nur einen kleinen Ausschnitt der Datenverarbeitung und des Verwendungszusammenhanges. Die Rechtmäßigkeit der Verarbeitung von Daten im Konzernzusammenhang etwa wird er oft nur schwerlich beurteilen können. Er kann im Unterschied zu den Fallgruppen A - E gerade nicht auf einen vorhandenen Regelungsrahmen verweisen oder Bezug nehmen. Deshalb ist zu konstatieren, dass es in den meisten Fällen für den Auftragsverarbeiter in Deutschland (EU/EWR) unmöglich sein dürfte, eine umfassende Prüfung im Sinne der §§ 4b, 4c BDSG vorzunehmen, um beurteilen zu können, ob eine Katalogausnahme gegeben ist, oder um vertragliche Regelungen im Sinne des § 4 c Absatz 2 BDSG treffen zu können. Bezüglich etwaiger vertraglicher Regelungen im Sinne des § 4c Absatz 2 BDSG wäre im übrigen unklar, welche konkrete Rolle mit welchen Pflichten der Auftragsverarbeiter hierin übernehmen sollte (Einstandspflicht für Betroffenenrechte wie Auskunfts- und Haftungsanspruch?).
Aus alledem ergibt sich, dass der Auftragsverarbeiter in Deutschland (EU/EWR) keine Verantwortung im Sinne der §§ 4b, 4c BDSG hat. Der Gesetzgeber hat in § 1 Absatz 5 BDSG der Stelle im Drittstaat selbst die umfassende Verantwortung für die Vereinbarkeit der Datenverarbeitung mit dem BDSG zugewiesen, nicht dem Auftragsverarbeiter, dessen sich der Auftraggeber im Drittstaat bedient.
Den Auftragnehmer in Deutschland trifft aber eine qualifizierte Remonstrationspflicht entsprechend § 11 Absatz 3 Satz 2 BDSG sowie unter Umständen eine Pflicht zur materiellen Plausibilitätsprüfung bezüglich der von ihm selbst in Deutschland vorgenommenen Datenerhebungen, -verarbeitungen und -nutzungen.

Daraus ergeben sich folgende Konsequenzen:

a) **Fallgruppe F**
Wenn der DV-Dienstleister die Daten selbst zu erheben hat, so ist damit in aller Regel eine inhaltliche Kenntnisnahme der Daten verbunden. Daher hat der DV-Dienstleister summarisch auf Plausibilität zu prüfen, ob die Datenerhebung und -verarbeitung und die diesbezüglichen Weisungen des Auftraggebers mit dem BDSG vereinbar sind. Wenn nein, gelten die unter b)genannten Anforderungen.
b) **Fallgruppe G**
Die DV-Dienstleistung wird häufig in der Rechenzentrums-Dienstleistung bestehen, so dass eine inhaltliche Kenntnisnahme der Daten durch den Auftragsverarbeiter nicht vorgesehen ist. Der Auftragsverarbeiter hat lediglich für die Datensicherheit zu sorgen, er hat keine Prüfungspflicht bzgl. der Vereinbarkeit der Datenverarbeitung mit dem BDSG. Soweit ihm jedoch (aufgrund besonderer Hinweise Dritter o. ä.) bekannt wird, dass die Datenverarbeitung gegen das BDSG verstößt, hat er eine qualifizierte Remonstrationspflicht entsprechend § 11 Absatz 3 Satz 2 BDSG. Gleiches gilt in den Einzelfällen, bei denen dem Auftragsverarbeiter bekannt wird, dass offensichtlich (eindeutig) kein angemessenes Datenschutzniveau (ausreichende Datenschutzgarantien) beim Auftraggeber besteht und auch eindeutig kein Ausnahmetatbestand im Sinne des § 4c Absatz 1 BDSG gegeben ist. In diesen Fällen, in denen der Auftraggeber einen gravierenden Missstand trotz Hinweisen des Auftragsverarbeiters nicht abstellt, ist eine Hinweis-/Anzeigepflicht des Auftragsverarbeiters gegenüber der Datenschutzaufsichtsbehörde gegeben. Gegebenenfalls besteht somit unter Umständen die Pflicht des Auftragsverarbeiters, die weitere Ausführung des Auftrages einzustellen. Dann entscheidet die Aufsichtsbehörde, wie weiter zu verfahren ist.
c) Die **Fallgruppe H** bedarf besonderer Betrachtung:
In Drittstaaten können bestimmte Verarbeitungen personenbezogener Daten explizit vorgeschrieben sein, die in Deutschland unzulässig wären (z. B. die Verarbeitung der Sozialversicherungsnummern von Kunden, die die Funktion eines Personenkennzeichens haben). Zwar gilt das BDSG grundsätzlich unabhängig davon, ob die Betroffenen Personen in Deutschland ansässig sind oder nicht. Allerdings wird mit der Sondervorschrift des § 1 Absatz 5 Satz 2 BDSG der reguläre Anwendungsbereich des BDSG ohnehin ausgedehnt, so dass hier eine Relativierung möglich erscheint. Ob der Gesetzgeber bzw. die Europäische Datenschutzrichtlinie bei der Regelung des § 1 Absatz 5 Satz 2 BDSG (bzw. Artikel 4 Absatz 1 c) Richtlinie) einen "EU/EWR-Bezug" der Daten stillschweigend unterstellt hat, bleibt unklar.
Die Lösung besteht darin, dass zwar aus § 1 Absatz 5 Satz 2 BDSG keine umfassende Geltung des deutschen Datenschutzrechts abzuleiten wäre, aber Verarbeitungen, die eindeutig gegen unseren "ordre public" verstoßen (z. B. bei Menschenrechtsverletzungen), unzulässig sind, auch wenn die Daten keinerlei EU/EWR-Bezug aufweisen. Demzufolge besteht die qualifizierte Remonstrationspflicht des Auftragsverarbeiters (s. o. b)) nur bei derartigen Verstößen.
d) **Fallgruppe I**
Hier muss der Auftraggeber nicht die Regelungen des BDSG beachten, weil die Situation vergleichbar ist mit der Transitregelung des § 1 Absatz 5 Satz 4 BDSG. Es

besteht auch keine weitere (über die technisch-organisatorische hinausgehende) Verantwortlichkeit des EU/EWR-Auftragnehmers. Der Grundsatz lautet hier: Deutsches materielles Datenschutzrecht gilt nicht, wenn der deutsche Auftragnehmer nicht auf die vom Auftraggeber übermittelten Daten zugreifen kann (weil die Datenverarbeitung im geschlossenen System / Black Box oder verschlüsselt erfolgt).

Erhebung von Positivdaten zu Privatpersonen bei Auskunfteien

Nicht nur sog. Verbraucherauskunfteien wie beispielsweise die SCHUFA, sondern auch Handels- und Wirtschaftauskunfteien erheben und verarbeiten zunehmend Bonitätsdaten zu Privatpersonen, die nicht gewerblich tätig sind. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass die Handels- und Wirtschaftsauskunfteien insoweit die selben datenschutzrechtlichen Vorgaben zu beachten haben wie die "Verbraucherauskunfteien".
Handels- und Wirtschaftsauskunfteien können daher sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des § 29 Absatz 1 BDSG erheben. Denn bei Positivdaten - das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben - überwiegt das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten übermittelt, ist insoweit bereits die Übermittlung nach § 28 BDSG regelmäßig unzulässig.
Will eine Auskunftei Positivdaten zu Privatpersonen erheben, bedarf es dafür einer wirksamen Einwilligung der Betroffenen im Sinne des § 4a BDSG. Sofern die Auskunftei oder ihre Vertragspartner zu diesem Zweck eine für eine Vielzahl von Fällen vorformulierte Einwilligungsklausel verwenden, die als Allgemeine Geschäftsbedingung im Sinne des § 305 BGB zu werten ist, muss eine entsprechende Einwilligung darüber hinaus den Anforderungen des § 307 BGB genügen.

Mahnung durch Computeranruf

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest:
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.

Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring

Im modernen Wirtschaftsleben kommt Auskunfteien eine ständig wachsende Bedeutung zu. Diese sammeln eine Vielzahl von persönlichen Daten auch über Privatpersonen, um sie Dritten insbesondere für die Beurteilung der Kreditwürdigkeit ihrer Geschäftspartner gegen Entgelt zur Verfügung zu stellen.

Während in der Vergangenheit vor allem Kreditinstitute, der Versandhandel und Telekommunikationsunternehmen Auskünfte abgefragt haben, werden Informationen zur Beurteilung der Kreditwürdigkeit zunehmend auch von Vermietern, Versicherungen und sonstigen Unternehmen eingeholt. Von den Auskunfteien wird dabei vielfach ein so genannter Scorewert übermittelt. Hierbei handelt es sich um einen Wert, der auf der Grundlage eines mathematisch-statistischen Verfahrens aus den bei der Auskunftei vorhandenen Angaben errechnet wird und eine Aussage über die Wahrscheinlichkeit des künftigen Zahlungsverhaltens der Betroffenen und damit über ihre Kreditwürdigkeit enthält.
Der Aufbau und die Erweiterung der zentralen Datenbestände über Betroffene bei Auskunfteien und die branchenübergreifende Bereitstellung dieser Informationen für eine Vielzahl von Unternehmen sowie der zunehmende Einsatz von Scoring- Verfahren gefährden nachhaltig das Recht auf informationelle Selbstbestimmung der Betroffenen. Vor diesem Hintergrund begrüßt der Düsseldorfer Kreis im Grundsatz den vom Bundesministerium des Innern vorgelegten Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, mit dem die Rechte der Betroffenen gestärkt und insbesondere auch die Transparenz beim Einsatz von Scoring-Verfahren verbessert werden sollen.
Nach Auffassung des Düsseldorfer Kreises bedarf der vorliegende Gesetzentwurf allerdings einer grundlegenden Überarbeitung, um das Ziel der Stärkung der Rechte der Betroffenen auch tatsächlich zu erreichen. Dabei muss insbesondere sichergestellt werden, dass die bei Auskunfteien gesammelten Daten die Erstellung umfassender Persönlichkeitsprofile von Betroffenen nicht zulassen. Darüber hinaus ist gesetzlich eindeutig zu regeln, dass die Einholung einer Bonitätsauskunft auch in Zukunft an das Vorliegen eines finanziellen Ausfallrisikos geknüpft bleibt. Die im Entwurf derzeit vorgesehene Regelung, wonach jedes rechtliche oder wirtschaftliche Interesse einschließlich der Vermeidung allgemeiner Vertragsrisiken ein berechtigtes Interesse darstellen kann, würde die Rechte der Betroffenen unverhältnismäßig beeinträchtigen.
Des Weiteren muss eindeutig klargestellt werden, dass nur vertragsrelevante Daten in die Berechnung eines Scorewerts einbezogen werden dürfen. Im Übrigen dürfen die Auskunftsrechte der Betroffenen nicht durch die pauschale Berufung auf ein Geschäftsgeheimnis vereitelt werden.

Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung in ihrer Stellungnahme zum 21. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erklärt hat, dass die Erhebung und Verwendung personenbezogener – auch mandatsbezogener – Daten durch Rechtsanwälte den Vorschriften des Bundesdatenschutzgesetzes unterliegt und dass die Aufsichtsbehörden der Länder zuständig sind, die Datenschutzkontrolle durchzuführen. Der Düsseldorfer Kreis sieht darin die Bestätigung seiner Auffassung, dass das Bundesdatenschutzgesetz (BDSG) – auch hinsichtlich mandatsbezogener Daten – auf Rechtsanwälte anwendbar ist. In der Bundesrechtsanwaltsordnung (BRAO) befinden sich aus datenschutzrechtlicher Hinsicht nur punktuelle Regelungen (§ 43a Absatz 2 BRAO Schweige-

pflicht, § 50 BRAO Handakten). Die Vorschriften des BDSG treten gemäß § 1 Absatz 3 BDSG lediglich insoweit zurück, als bereichsspezifische Datenschutzvorschriften bestehen. Durch das anwaltliche Berufsgeheimnis werden die Informationsrechte der Aufsichtsbehörden nach § 38 BDSG in Verbindung mit § 24 Absatz 6 und 2 BDSG nicht eingeschränkt.

B. Beschlussfassungen der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden

Internet-Portale zur Bewertung von Einzelpersonen

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.

Keine fortlaufenden Bonitätsauskünfte an den Versandhandel

Auskunfteien dürfen Bonitätsauskünfte gemäß § 29 Absatz 2 Nummer 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 gemäß § 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.
Hinweis: Die Vertreter des Versandhandels und der Auskunfteien haben sich bereit erklärt, ihre Verfahren entsprechend den vorgenannten gesetzlichen Anforderungen bis spätestens Ende September 2008 umzustellen.

Datenschutzkonforme Gestaltung sozialer Netzwerke

Der datenschutzgerechten Gestaltung sozialer Netzwerke im Internet kommt eine zentrale Bedeutung zu. Die Aufsichtsbehörden rufen in diesem Zusammenhang in Erinnerung, dass Anbieter in Deutschland zur Einhaltung des Regulierungsrahmen zum Datenschutz verpflichtet sind.
Insbesondere sind folgende rechtliche Rahmenbedingungen einzuhalten:
- Anbieter sozialer Netzwerke müssen ihre Nutzer umfassend gemäß den gesetzlichen Vorschriften über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Das betrifft auch Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.
- Die Aufsichtsbehörden weisen darauf hin, dass nach den Bestimmungen des Telemediengesetzes (TMG) eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke nur zulässig ist, soweit die Betroffenenwirksam darin eingewilligt haben. Bei Werbemaßnahmen aufgrund von Profildaten müssen die Betroffenen nach den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mindestens eine Widerspruchsmöglichkeit haben. Die Aufsichtsbehörden empfehlen, dass die Anbieter die Nutzer selbst darüber entscheiden lassen, ob – und wenn ja, welche – Profil- oder Nutzungsdaten zur zielgerichteten Werbung durch den Anbieter genutzt werden.
Die Aufsichtsbehörden erinnern weiterhin daran, dass eine Speicherung von personenbezogenen Nutzungsdaten über das Ende der Verbindung hinaus ohne Einwilligung der Nutzer nur gestattet ist, soweit die Daten zu Abrechnungszwecken gegenüber dem Nutzer erforderlich sind.
- Für eine vorauseilende Speicherung von Daten über die Nutzung sozialer Netzwerke (wie auch anderer Internet-Dienste) für eventuelle zukünftige Strafverfolgung besteht keine Rechtsgrundlage. Sie wird insbesondere auch nicht durch die Regelungen zur Vorratsdatenspeicherung vorgeschrieben.
- Schließlich weisen die Aufsichtsbehörden darauf hin, dass das TMG die Anbieter dazu verpflichtet, das Handeln in sozialen Netzwerken anonym oder unter Pseudo-

nym zu ermöglichen. Dies gilt unabhängig von der Frage, ob ein Nutzer sich gegenüber dem Anbieter des sozialen Netzwerks mit seinen Echtdaten identifizieren muss.
- Die Anbieter sind verpflichtet, die erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Sie müssen insbesondere einen systematischen oder massenhaften Export oder Download von Profildaten aus dem sozialen Netzwerk verhindern.
- Bei der datenschutzfreundlichen Gestaltung von sozialen Netzwerken kommt den Standardeinstellungen – z. B. für die Verfügbarkeit von Profildaten für Dritte – eine zentrale Bedeutung zu. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch die die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Kinderrichtet. Der Zugriff durch Suchmaschinen darf jedenfalls nur vorgesehen werden, soweit der Nutzer ausdrücklich eingewilligt hat.
- Der Nutzer muss die Möglichkeit erhalten, sein Profil auf einfache Weiseselbst zu löschen. Schließlich sollten die Anbieter sozialer Netzwerkdienste die Einführung von Verfallsdaten oder zumindest automatische Sperrungen erwägen, die von den Nutzern selbst festgelegt werden können.

Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet

Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessender Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückeigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessenbestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit mussselbstverständlich auch noch nach der Veröffentlichung bestehen.

Novellierung des Bundesdatenschutzgesetzes
in den Bereichen Adressenhandel, Werbung und Datenschutzaudit

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung durch eine Novellierung des Bundesdatenschutzgesetzes aus den jüngst bekannt gewordenen Datenschutzverstößen im Bereich der Privatwirtschaft Konsequenzen ziehen möchte. Die uneingeschränkte Streichung des Listenprivilegs und die Pflicht zur Einholung einer Einwilligung des Betroffenen bei der Übermittlung an Dritte oder bei der Nutzung für Werbezwecke für Dritte sind erforderlich, um das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger zu stärken. Hiervon wird künftig auch die Wirtschaft profitieren. Die geplanten Änderungen ermöglichen es, Werbung zielgerichteter und ohne Streuverluste vorzunehmen und unerwünschte Belästigungen zu vermeiden, so dass das Verbrauchervertrauen in die Datenverarbeitung der Wirtschaft gestärkt wird. Die vorgesehenen Regelungen zur Klarstellung, wann eine wirksame Einwilligung in die Werbenutzung vorliegt, und dass diese nicht mit wichtigen vertraglichen Gegenleistungen gekoppelt werden darf, verbessern die Transparenz und die Freiwilligkeit für den Betroffenen. Darüber hinaus hat die beim Datenschutzgipfel am 4. September 2008 eingesetzte Länderarbeitsgruppe weitere Vorschläge zur Verbesserung des Bundesdatenschutzgesetzes unterbreitet, die jedoch bisher nicht berücksichtigt wurden.
Die derzeit geplanten Vorschriften genügen nicht, um künftig im Bereich der privaten Wirtschaft ein ausreichendes Datenschutzniveau zu verwirklichen. Hierzu bedarf es zum einen einer angemessenen Ausstattung der Datenschutzaufsichtsbehörden. Es bedarf zum anderen gemäß den europarechtlichen Vorgaben wirksamer Einwirkungsbefugnisse. Hierzu gehört neben adäquaten Kontroll- und Sanktionsmitteln die Möglichkeit, bei schwerwiegenden Datenschutzverstößen die Erhebung und Verwendung personenbezogener Daten zu untersagen. Auch die Stellung der betrieblichen Datenschutzbeauftragten sollte gestärkt werden.
Die bisherigen Vorschläge des Bundesministeriums des Innern zur Einführung eines Datenschutzaudits sind nicht geeignet, den Datenschutz in der Wirtschaft zu verbessern.

Adressen der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich und der Landesbeauftragten für den Datenschutz [1]

Bundesland	Aufsichtsbehörde	Landesbeauftragte/r für Datenschutz
Baden-Württemberg	Innenministerium Baden-Württemberg Dorotheenstraße 6 70173 Stuttgart Telefon: 0711 231-4 Telefax: 0711 231-5000 Datenschutz@im.bwl.de http://www.im.baden-wuerttemberg.de/	Der Landesbeauftragte für den Datenschutz in Baden-Württemberg Urbanstraße 32 70182 Stuttgart Telefon: 0711 615541-0 Telefax: 0711 615541-15 poststelle@lfd.bwl.de http://www.baden-wuerttemberg.datenschutz.de
Bayern	Bayerisches Landesamt für Datenschutzaufsicht in der Regierung von Mittelfranken Promenade 27 (Schloss) 91522 Ansbach Telefon: 0981 53-1301 Telefax: 0981 53-5301 datenschutz@reg-mfr.bayern.de http://www.regierung.mittelfranken.bayern.de/	Der Bayerische Landesbeauftragte für den Datenschutz Wagmüllerstraße 18 80538 München Telefon: 089 212672-0 Telefax: 089 212672-50 poststelle@datenschutz-bayern.de http://www.datenschutz-bayern.de

[1] Die hier aufgeführten Links verweisen mit Ausnahme unserer eigenen Adresse (http://www.innen.saarland.de) auf externe Angebote. Für die Inhalte der verlinkten Seiten ist der jeweilige Anbieter verantwortlich. Die Aufsichtsbehörde für den Datenschutz übernimmt insoweit keine Haftung.

Bundesland	Aufsichtsbehörde	Landesbeauftragte/r für Datenschutz
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit An der Urania 4 – 10 10787 Berlin Telefon: 030 13889-0 Telefax: 030 215-5050 mailbox@datenschutz-berlin.de http://www.datenschutz-berlin.de/	
Brandenburg	Innenministerium des Landes Brandenburg Henning-von-Tresckow-Straße 9-13 14467 Potsdam Telefon: 0331 866-0 Telefax: 0331 866-2202 poststelle@mi.brandenburg.de http://www.mi.brandenburg.de	Die Landesbeauftragte für Datenschutz und das Recht auf Akteneinsicht Brandenburg Stahnsdorfer Damm 77 14532 Kleinmachnow Telefon: 033203 356-0 Telefax: 033203 356-49 poststelle@lda.brandenburg.de http://www.lda.brandenburg.de
Bremen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen Arndtstr. 1 27570 Bremerhaven Telefon: 0421 361-2010 Telefax: 0421 496-18495 office@datenschutz.bremen.de http://www.datenschutz-bremen.de/	

Bundesland	Aufsichtsbehörde	Landesbeauftragte/r für Datenschutz
Hamburg	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Klosterwall 6 (Block C) 20095 Hamburg Telefon: 040 42854-4040 Telefax: 040 42854-4000 mailbox@datenschutz.hamburg.de http://www.hamburg.datenschutz.de/	
Hessen	Regierungspräsidium Darmstadt Luisenplatz 2 64283 Darmstadt Telefon: 06151 12-0 Telefax: 06151 12-5794 Datenschutz@rpda.hessen.de http://www.rp-darmstadt.hessen.de	Der Hessische Datenschutzbeauftragte Gustav-Stresemann-Ring 1 65189 Wiesbaden Telefon: 0611 1408-0 Telefax: 0611 1408-900 poststelle@datenschutz.hessen.de http://www.datenschutz.hessen.de
Mecklenburg-Vorpommern	Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern Schloß Schwerin Johannes-Stelling-Straße 21 19053 Schwerin Telefon: 0385 59494-0 Telefax: 0385 59494-58 datenschutz@mvnet.de http://www.datenschutz.mvnet.de/	

Bundesland	Aufsichtsbehörde	Landesbeauftragte/r für Datenschutz
Niedersachsen	Der Landesbeauftragte für den Datenschutz Niedersachsen Brühlstraße 9 30169 Hannover Telefon: 0511 120-4500 Telefax: 0511 120-4599 poststelle@lfd.niedersachsen.de http://www.lfd.niedersachsen.de	
Nordrhein-Westfalen	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Kavalleriestraße 2-4 40213 Düsseldorf Telefon: 0211 38424-0 Telefax: 0211 38424-10 poststelle@ldi.nrw.de http://www.ldi.nrw.de/ http://www.lfd.nrw.de	
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz Hintere Bleiche 34 55116 Mainz Telefon: 06131 208-2449 Telefax: 06131 208-2497 poststelle@datenschutz.rlp.de http://www.datenschutz.rlp.de	

Bundesland	Aufsichtsbehörde	Landesbeauftragte/r für Datenschutz
Saarland	Ministerium für Inneres und Sport Franz-Josef-Röder-Straße 21 66119 Saarbrücken Telefon: 0681 501-00 Telefax: 0681 501-2699 datenschutz@innen.saarland.de http://www.innen.saarland.de	Landesbeauftragter für Datenschutz und Informationsfreiheit Saarland Fritz-Dobisch-Straße 12 66111 Saarbrücken Telefon: 0681 94781-0 Telefax: 0681 94781-29 poststelle@lfdi.saarland.de http://www.lfdi.saarland.de
Sachsen	Der Sächsische Datenschutzbeauftragte Bernhard-von-Lindenau-Platz 1 01067 Dresden Telefon: 0351 4935-401 Telefax: 0351 4935-490 saechsdsb@slt.sachsen.de http://www.datenschutz.sachsen.de	
Sachsen-Anhalt	Landesverwaltungsamt Sachsen-Anhalt Willy-Lohmann-Straße 7 06114 Halle Telefon: 0345 514-0 Telefax: 0345 514-144 poststelle@lvwa.sachsen-anhalt.de http://www.lvwa.sachsen-anhalt.de	Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt Berliner Chaussee 9 39114 Magdeburg Telefon: 0391 81803-0 Telefax: 0391 81803-33 poststelle@lfd.sachsen-anhalt.de http://www.datenschutz.sachsen-anhalt.de

Bundesland	Aufsichtsbehörde	Landesbeauftragte/r für Datenschutz
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Holstenstraße 98 24103 Kiel Telefon: 0431 988-1200 Telefax: 0431 988-1223 mail@datenschutzzentrum.de http://www.datenschutzzentrum.de	
Thüringen	Thüringer Landesverwaltungsamt Referat 200 Weimarplatz 4 99423 Weimar Telefon: 0361 37-737258 Telefax: 0361 37-737346 poststelle@tlvwa.thueringen.de http://www.thueringen.de/de/tlvwa	Der Thüringer Landesbeauftragte für den Datenschutz Jürgen-Fuchs-Straße 1 99096 Erfurt Telefon: 0361 377-1900 Telefax: 0361 377-1904 poststelle@datenschutz.thueringen.de http://www.thueringen.de/datenschutz/

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit	Der Bundesbeauftragte für den Datenschutz Husarenstraße 30 53117 Bonn Telefon: 0228 99-7799-0 Telefax: 0228 99-7799-550 poststelle@bfdi.bund.de http://www.bfdi.bund.de

Links[2]

Behörden:

Bundesamt für Sicherheit in der Informationstechnik:
http://www.bsi.de
http://www.bsi-fuer-buerger.de - „Ins Internet – mit Sicherheit“, ein Angebot des BSI nicht nur für Bürger/innen im statusrechtlichen Sinn

Bundesamt für Finanzdienstleistungsaufsicht:
http://www.bafin.de

Datenschutzseite der EU - deutschsprachiges Informationsportal der EU mit ausführlichen Informationen über die Entwicklung des Datenschutzes auf europäischer Ebene:
http://ec.europa.eu/justice_home/fsj/privacy/

Sonstige:

Virtuelles Datenschutzbüro, das gemeinsame Portal verschiedener Datenschutzinstitutionen:
http://www.datenschutz.de

Secorvo Security Consulting GmbH © - Datenschutzseminare und News
http://www.secorvo.de

heise online - Technik, Datenschutz, c’t, Newsletter
http://www.heise.de

DuD - Datenschutz und Datensicherheit, Fachzeitschrift
http://www.dud.de

Datenschutzberater Online - Fachzeitschrift
http://www.ad-on-line.de/portfolio_dsb.htm

GDD - Gesellschaft für Datenschutz und Datensicherheit
http://www.gdd.de

DATAKONTEXT-Gruppe - Fachverlag
http://www.datakontext.com

[2] Die Links verweisen mit Ausnahme desjenigen zum Angebot des Ministerium für Inneres und Sport auf externe Angebote, für deren Inhalt keine Haftung übernommen wird. Die Liste erhebt auch keinen Anspruch auf Vollständigkeit, ebenso wenig wie sie als Ausdruck einer Präferenz der Aufsichtsbehörde für den Datenschutz verstanden werden darf.

INTEREST – Verlag - Fachverlag
http://www.interest-verlag.de

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
http://www.bvdnet.de

COMPUTAS, Service und Konferenzen
http://www.computas.de

Deutsche Vereinigung für Datenschutz
http://www.datenschutzverein.de/

Informationen zum Datenschutz in der katholischen Kirche
http://www.datenschutz-kirche.de/

Informationen zum Datenschutz in der evangelischen Kirche in Deutschland
http://www.ekd.de/datenschutz/1618_4586.html

Datenschutz-Help - Datenschutzberatung für Unternehmen
http://www.datenschutz-help.de

Bundesverband der Verbraucherzentralen
http://www.vzbv.de

Teletrust Deutschland e.V. - Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik
http://www.teletrust.de

Schufa
http://www.schufa.de

SPAM, Viren, Dialer, Hoaxes etc.

Dialerinformationen des BSI
http://www.bsi.bund.de/dialer/index.htm

BSI für Bürger - Direktlink zu Dialerinformationen
http://www.bsi-fuer-buerger.de/abzocker/05_02.htm

Dialerschutz.de - Hinweise und Aufklärung über Dialer
http://www.dialerschutz.de

Vireninformationen auf SPIEGEL Online
http://www.spiegel.de/netzwelt/0,1518,k-1626,00.html

Vireninformationen des BSI
http://www.bsi.bund.de/av/HinweiseCV.htm

BSI für Bürger - Direktlink zu Vireninformationen
http://www.bsi-fuer-buerger.de/viren/

Verband der deutschen Internet-Wirtschaft - Informationen über SPAM
http://www.eco.de
http://www.internet-beschwerdestelle.de

Deutscher Direktmarketing Verband e.V. – Allgemeine Informationen zum Direktmarketing, nicht nur zu SPAM
http://www.direktmarketing-info.de/datenschutz/index.html

Beschwerdestelle der Wettbewerbszentrale
www.wettbewerbszentrale.de

Datenbanken:

Juris GmbH
http://www.bundesrecht.juris.de

de jure - Gesetze und Rechtsprechung zum europäischen, deutschen und baden-württembergischen Recht
http://www.dejure.org

Saar-Daten-Bank – Frisierte Gesetze (ab 1. Januar 2008 kostenpflichtig)
http://www.sadaba.de

Landesmedienanstalt Saarland
http://www.lmsaar.de

Rechtliches.de - Gesetze im WWW - Suchportal für Rechtsvorschriften
http://www.rechtliches.de

wikipedia.org – wikipedia, die freie Enzyklopädie im Internet
http://de.wikipedia.org/wiki/Hauptseite