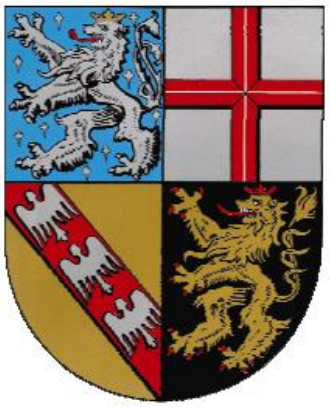


5. TÄTIGKEITSBERICHT DER AUFSICHTSBEHÖRDE FÜR DEN DATENSCHUTZ IM NICHT-ÖFFENTLICHEN BEREICH DES SAARLANDES

Berichtszeitraum

2009/2010

Impressum

Herausgeber: Aufsichtsbehörde für den Datenschutz
im nicht-öffentlichen Bereich beim
Ministerium für Inneres und Europaangelegenheiten
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 EUROPAANGELEGENHEITEN

DES SAARLANDES

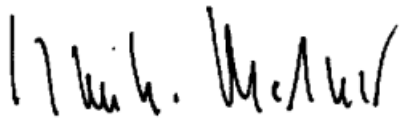
Vorwort Mai 2011

Liebe Bürgerinnen und Bürger,

Datenschutz schützt unsere Menschenwürde und gehört zu den grundlegenden Regelungen unserer Informationsgesellschaft; er ist von nachhaltiger Bedeutung für unsere Zukunft.
Auch im Berichtszeitraum 2009/2010 konnte die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich feststellen, dass immer mehr Datenquellen öffentlich zugänglich werden und die Kommunikation sich zunehmend in soziale Netzwerke verlagert. Durch die allgegenwärtige Verarbeitung und Veröffentlichung digital abrufbarer Daten von Menschen entsteht eine neue digitale Öffentlichkeit. Sie ermöglicht die Bildung von Persönlichkeits-, Verhaltens- und Bewegungsprofilen. Dies kann dazu führen, dass unser Verhalten für andere nicht nur merkantil kalkulierbar, sondern auch in sonstiger Weise berechenbar wird.
Zwar sind im Berichtszeitraum drei Novellierungen des Bundesdatenschutzgesetzes durchgeführt und damit die Persönlichkeitsrechte der Bürgerinnen und Bürger gestärkt worden. Dennoch geht der Weg zu mehr Datenschutz auch weiterhin über mehr Datensparsamkeit.
Die Lektüre des vorliegenden Tätigkeitsberichts der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich kann für die Bürgerinnen und Bürger eine Hilfe sein, ihre Daten und damit sich selbst besser in unserer Informationsgesellschaft zu schützen.

Mit dem Gesetz zur Änderung des Saarländischen Datenschutzgesetzes vom 18. Mai 2011 wird die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich, die bislang beim Ministerium für Inneres und Europaangelegenheiten angesiedelt war, auf die Landesbeauftragte für Datenschutz und Informationsfreiheit übertragen. Sie wird dort mit der Datenschutzaufsicht über den öffentlichen Bereich im Unabhängigen Datenschutzzentrum Saarland zusammengelegt.
Datenschutz wird es also künftig aus einer Hand geben: Die Bürgerinnen und Bürger brauchen sich nur noch an eine Datenschutzkontrollstelle zu wenden, wenn es um

Fragen rund um den Datenschutz geht. Das Unabhängige Datenschutzzentrum Saarland unter Leitung der Landesbeauftragten für Datenschutz und Informationsfreiheit wird Sie gerne beraten und unterstützen.
Der nächste Tätigkeitsbericht über die Datenschutzaufsicht im nicht-öffentlichen Bereich wird zusammen mit dem Bericht über die Datenschutzaufsicht im öffentlichen Bereich von der Landesbeauftragten für Datenschutz und Informationsfreiheit erstellt.



Karin Schmitz-Meßner
Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich
im Ministerium für Inneres und Europaangelegenheiten

Inhaltsverzeichnis

1. Allgemeines

1.1 Grundrecht des Allgemeinen Persönlichkeitsrechts, Grundrecht auf informationelle Selbstbestimmung und Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

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 dem Grundrecht des Allgemeinen Persönlichkeitsrechts hat das Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. Dezember 1983 (Az.: 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83; 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 Verhältnismäßig-

keit mit Blick auf die Eingriffsintensität des Datenzugriffs begrenzt. Schließlich hat jedem staatlichen Datenzugriff eine klar definierte Zweckbestimmung voranzugehen.

Ferner hat das Bundesverfassungsgericht in richterlicher Rechtsfortbildung aus dem Allgemeinen Persönlichkeitsrecht des Artikels 2 Absatz 1 des Grundgesetzes in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hergeleitet (vgl. Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 zur Online-Durchsuchung – Az.: 1 BvR 370/07, 1 BvR 595/07; NJW 2008, S. 822 ff.). Den Leitsätzen der Entscheidung zufolge ist danach die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems staatlich überwacht und seine Speichermedien ausgelesen werden können, verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen. Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen. Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff an Artikel 10 Absatz 1 des Grundgesetzes zu messen. Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Artikel 10 Absatz 1 des Grundgesetzes, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Nimmt der Staat im Internet öffentlich zugängliche

Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.

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.
Im Berichtszeitraum oblag nur die Aufsicht über den Datenschutz im öffentlichen Bereich, also die datenschutzrechtliche Kontrolle öffentlicher Stellen, der Landesbeauftragten für Datenschutz und Informationsfreiheit des Saarlandes, während die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich einer gesonderten Aufsichtsbehörde übertragen war, die beim Ministerium für Inneres und Europaangelegenheiten angesiedelt war. Mit dem Gesetz zur Änderung des Saarländischen Datenschutzgesetzes (Landtagsdrucksache 14/443), das vom Landtag des Saarlandes am 18. Mai 2011 erlassen worden ist, wird der Landesbeauftragten für Datenschutz und Informationsfreiheit des Saarlandes die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich übertragen und bei ihr das Unabhängige Datenschutzzentrum Saarland errichtet. Da die Landesbeauftragte für Datenschutz und Informationsfreiheit des Saarlandes einen eigenen Tätigkeitsbericht für den Berichtszeitraum bereits veröffentlicht hat, 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 kann er Schnittstelle zu von Unternehmensentscheidungen datenschutzrechtlich Betroffenen und zur Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich sein.

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 Vorabkontrolle 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 Aufsichtsbehörde 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),
- 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 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 Aufsichtsbe-

hörde 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 unter Nr. 7 aufgeführt.

2. Gesundheitswesen

2.1 Übergabe einer Arztpraxis

Im Rahmen des Schutzes der Gesundheitsdaten wurde die Aufsichtsbehörde auch mit einem Fall der Übergabe einer Arztpraxis befasst.
Ein Patient, der nach längerer Zeit wieder die Praxis seines Arztes aufsuchte, stellte bei der Anmeldung fest, dass der Arzt, bei dem er bisher in Behandlung war, die Praxis an einen Nachfolger übergeben hatte. Da der Patient vermutete, dass der Praxisnachfolger ohne seine Einwilligung Einsicht in seine Patientenunterlagen genommen hatte, beklagte er sich bei der Aufsichtsbehörde. Nach den von der Aufsichtsbehörde durchgeführten Ermittlungen stellte sich der Fall folgendermaßen dar:

Zur Übernahme der Arztpraxis wurde zwischen dem übergebenden sowie dem übernehmenden Arzt ein Praxiskaufvertrag abgeschlossen. Darin wurde u. a. vereinbart, dass der Erwerber der Praxis über die Patientendaten, die EDV-mäßig erfasst sind, nur verfügen darf, soweit sich die betreffenden Patienten hiermit ausdrücklich oder durch schlüssiges Verhalten einverstanden erklärt haben. Die übrigen Daten bleiben gesperrt und sind nur über ein Passwort zugänglich. Der Zugriff mittels Passwort darf durch den Erwerber nur dann erfolgen, wenn der Patient hierzu ausdrücklich oder durch schlüssiges Verhalten seine Einwilligung erteilt hat, oder die Daten durch einen nachbehandelnden Arzt des Patienten schriftlich angefordert wurden. Bezüglich der auf Papier erfassten Patientenkartei hat der Übernehmende die Karteikarten in einem besonders gekennzeichneten, abgeschlossenen Stahlschrank zu verwahren. Der Zugriff, der zu dokumentieren ist, ist nur nach den oben dargelegten Kriterien möglich.

Hierzu ist anzumerken, dass für ärztliche Patientenunterlagen verschiedene gesetzliche Aufbewahrungspflichten (aus Behandlungsvertrag, aus der Röntgenverordnung, aus dem Transfusionsgesetz usw.), die bis zu 30 Jahre andauern können, gelten. Entsprechend ist auch die Aufbewahrung der Patientenunterlagen für die deutschen

Ärztinnen und Ärzte in § 10 Absatz 4 der Musterberufsordnung der Bundesärztekammer geregelt:

> *„(4) Nach Aufgabe der Praxis haben Ärztinnen und Ärzte ihre ärztlichen Aufzeichnungen und Untersuchungsbefunde gemäß Absatz 3 aufzubewahren und dafür Sorge zu tragen, dass sie in gehörige Obhut gegeben werden. Ärztinnen und Ärzte, denen bei einer Praxisaufgabe oder Praxisübergabe ärztliche Aufzeichnungen über Patientinnen oder Patienten in Obhut gegeben werden, müssen diese Aufzeichnungen unter Verschluss halten und dürfen sie nur mit Einwilligung der Patientin oder des Patienten einsehen oder weitergeben.“*

Die Verfahrensweise, dem Praxisnachfolger die Aufbewahrungspflicht der Patientendokumentation zu übertragen, erscheint auch vor dem Hintergrund sinnvoll, dass ein Arzt, der aus Altersgründen seine Praxis aufgibt, oftmals wegen seines fortgeschrittenen Lebensalters nicht in der Lage ist, die gesetzlich vorgegebenen sehr langen Aufbewahrungsfristen zu gewährleisten.

Aus datenschutzrechtlicher Sicht ist bezüglich der Einwilligungserklärung allerdings Folgendes zu beachten:

Nach § 4 Absatz 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Da im vorliegenden Fall weder das BDSG noch eine andere Rechtsvorschrift die Datenverarbeitung erlaubt, bleibt als Zulässigkeitsvoraussetzung nur die Einwilligung des Betroffenen. Die Einwilligung des Betroffenen als Grundlage für die Verarbeitung personenbezogener Daten bedarf gem. § 4a Absatz 1 Satz 3 BDSG grundsätzlich der Schriftform. Ausnahmen davon sind nur zulässig, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Werden be-

sondere Arten personenbezogener Daten (§ 3 Absatz 9 BDSG), wie zum Beispiel Gesundheitsdaten, erhoben, verarbeitet oder genutzt, so muss sich gem. § 4a Absatz 3 BDSG die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen. Im vorliegenden Fall sind keine Anhaltspunkte dafür zu erkennen, dass wegen besonderer Umstände eine andere Form als die Schriftform angemessen ist. Ebenso verlangt § 10 Absatz 4 der Berufsordnung für die Ärztinnen und Ärzte des Saarlandes eine schriftliche Einwilligungserklärung der Patienten bei Praxisübergang.

Vor diesem Hintergrund ist vor dem Zugriff auf die Patientendaten des Praxisvorgängers die schriftliche Einwilligung der Patienten, die zu den übrigen Patientenunterlagen zu nehmen ist, von dem Praxisnachfolger einzuholen. Das „schlüssige Verhalten“ des Patienten, wie es im vorgenannten Praxisübernahmevertrag festgelegt wurde, reicht nicht aus. Dies gilt auch dann, wenn zwischen dem Praxisnachfolger und den Patienten des Praxisvorgängers ein neuer Behandlungsvertrag zu Stande kommt. Der betreffende Arzt wurde zur Einhaltung dieser Regelungen aufgefordert.

2.2 Diskretion in Arztpraxen

Im Berichtszeitraum hat sich eine Patientin über mangelnde Diskretion in einer Arztpraxis beklagt. Die Anmeldung der Patienten in der Praxis erfolgte an einem Tresen bei den Mitarbeiterinnen der Praxis. Die Petentin monierte, dass dieser Tresen sich unmittelbar im Wartezimmer befindet. Weder eine akustische noch eine visuelle Abschirmung ist dort vorhanden. Jeder Patient, der sich im Wartezimmer befindet, kann die bei der Anmeldung geführten Gespräche mithören. Es können sogar Gespräche über Patientendaten, die zwischen den Helferinnen bei der Anmeldung und den Ärzten geführt werden von den wartenden Patienten mitgehört werden.
Hierzu ist Folgendes anzumerken: Der Anmelde- bzw. Empfangsbereich einer Arztpraxis ist sehr häufig anfällig für Indiskretionen. Deshalb ist der beste Schutz vor Indiskretionen eine bauliche/räumliche Trennung von Warte- und Anmeldebereich. Dies ist jedoch aufgrund der Verhältnisse vor Ort bzw. wegen zu hoher Kosten nicht

immer möglich. Um dennoch den Patientenschutz zu gewährleisten sind folgende Maßnahmen geeignet:

- Der Arzt hat darauf zu achten und dies gegebenenfalls in einer Dienstanweisung, die dem gesamten Personal zur Kenntnis gegeben werden muss, festzulegen, dass keine mündlichen Therapie- oder sonstige Anweisungen gegeben werden, wenn Umstehende daraus auf Patienten schließen können.

- Die Verpflichtung der Mitarbeiter auf das Datengeheimnis ist vorzunehmen und gegebenenfalls sind die Mitarbeiter öfter daran erinnern.

- Notwendige Behandlungsanweisungen durch den Arzt an die Helferinnen sollten nur im Behandlungszimmer oder schriftlich gegeben werden.

- Auch wenn keine gesetzliche Verpflichtung dazu besteht, kann ein Datenschutzbeauftragter bestellt werden, der auf die Einhaltung der Datenschutzbestimmungen achtet.

- Auf dem Tresen sollen keine Patientenakten oder sonstige Unterlagen mit Patientendaten abgelegt werden. Es kommt nicht darauf an, dass Umstehende tatsächlich die Angaben lesen, sondern nur ob die Möglichkeit dazu besteht.

- Die Computerbildschirme sind so aufzustellen, dass Umstehende keinen Einblick in Patientendaten nehmen können.

Im vorliegenden Fall hat der betroffene Arzt solche Maßnahmen umgesetzt, und gegenüber der Aufsichtsbehörde zugesichert, darauf zu achten, dass das Recht der Patienten auf Diskretion künftig beachtet wird.

2.3 Hausarztzentrierte Versorgung

Die Hausarztzentrierte Versorgung (HzV), die im fünften Buch des Sozialgesetzbuches (SGB V) geregelt ist, besagt, dass die Hausärzte und Hausärztinnen bei der Behandlung und Zuweisung der an der Hausarztzentrierten Versorgung teilnehmenden Patientinnen und Patienten zu den einzelnen Fachärzten als Lotsen fungieren. Darüber hinaus müssen sich die Hausärzte und Hausärztinnen bei der Behandlung und Verschreibung von Medikamenten an bestimmte Vorgaben halten. Dadurch sollen die Qualität der Behandlung verbessert und Kosten gesenkt werden.
Die Abrechnung der hierbei erbrachten Leistungen soll ohne Beteiligung der Kassenärztlichen Vereinigung durch private Stellen erfolgen. Hierzu werden zwischen den Hausarztverbänden und den Krankenkassen Verträge geschlossen, die u. a. die Abrechnung der Hausärzte und Hausärztinnen mit den privaten Stellen regeln. Die Krankenkassen stehen der Hausarztzentrierten Versorgung bisher skeptisch gegenüber. Können sich die Hausarztverbände und die Krankenkassen nicht über den Inhalt der Verträge einigen, wird eine Schiedsstelle eingerichtet. Im Rahmen dieser Verträge sollen die Patientendaten zu Abrechnungszwecken von den Hausärzten und Hausärztinnen an die jeweiligen, mit der Abrechnung betrauten privaten Stellen übermittelt werden. Aus datenschutzrechtlicher Sicht kann dies, solange keine andere gesetzliche Regelung existiert, nur im Rahmen der Auftragsdatenverarbeitung nach den Vorgaben des § 80 Sozialgesetzbuches X erfolgen. Danach fungieren die Hausärzte und Hausärztinnen als Auftraggeber, die privaten Abrechnungsstellen als Auftragnehmer. Neben den einzelnen Maßnahmen, die nach § 80 SGB X im Auftrag im Einzelnen schriftlich festzulegen sind, sind die Auftraggeber (Hausärzte) unter anderem verpflichtet, erforderlichenfalls Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zu erteilen. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.
Die Prüfung der Aufsichtsbehörden hat in den meisten Bundesländern ergeben, dass bei den bisher abgeschlossenen Verträgen zur Hausarztzentrierten Versorgung kei-

ne echte Auftragsdatenverarbeitung vorliegt und insofern eine Übermittlung der Patientendaten von den Hausärzten und Hausärztinnen an die privaten Abrechnungsstellen unzulässig ist. Hauptkritikpunkt ist dabei der Einsatz eines sogenannten gekapselten Kerns, d. h. in die Praxisverwaltungssysteme bei den Hausärzten und Hausärztinnen soll ein Softwaremodul eingebaut werden, wobei die Hausärzte und Hausärztinnen nicht feststellen können, welche Funktionen dieses Softwaremodul genau erfüllt. Es ist ihnen sogar untersagt, Einfluss auf diese Software zu nehmen. Dadurch sind die Hausärzte und Hausärztinnen nicht mehr in der Lage zu kontrollieren, welche Patientendaten überhaupt an die privaten Abrechnungsstellen übermittelt werden. Genau dies wird jedoch in der Auftragsdatenverarbeitung vorausgesetzt.
Das Oberverwaltungsgericht Schleswig-Holstein, das mit dieser Sache in Schleswig-Holstein befasst war, hat in seinem Beschluss festgestellt, dass der HzV-Vertrag gegen materielles Datenschutzrecht verstößt und darauf hingewiesen, dass wegen der Verantwortlichkeit des Auftraggebers diesem die vollständige Aufsichts- und Kontrollmöglichkeit über die Datenverarbeitung gewahrt bleiben muss, was den Hausärzten und Hausärztinnen jedoch verwehrt wird.
Im Saarland wurde im Berichtszeitraum kein Vertrag zur Hausarztzentrierten Versorgung abgeschlossen.

3. Kreditinstitute

Erstmals wurden im Berichtszeitraum auch anlassunabhängige Prüfungen durch die Aufsichtsbehörde durchgeführt. Hierfür wurden zehn Kreditinstitute mit Sitz im Saarland nach dem Zufallsprinzip ausgewählt. Dabei mussten die betroffenen Institute unter anderem Auskunft zu folgenden Themenbereichen erteilen:

- Zweckbestimmungen der Datenerhebung, -verarbeitung oder –nutzung,

- Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,

- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,

- Regelfristen für die Löschung der Daten,

- Datenübermittlung in Drittstaaten, d. h. an Stellen außerhalb der Europäischen Union oder anderer Vertragsstaaten des Europäischen Wirtschaftsraums,

- Anzahl der mit der Datenerhebung, -verarbeitung oder –nutzung befassten Personen,

- Verfahren, in denen personenbezogene Daten verarbeitet werden (z. B. Kundenstammdatenverwaltung, Personalverwaltung),

- Betrieblicher Datenschutzbeauftragter (§§ 4f, 4g BDSG), falls erforderlich

- Verpflichtung der Mitarbeiter auf das Datengeheimnis,

- Bei Einsatz von Videoüberwachungskameras: Anzahl und Art der Kameras.

- Bei Verarbeitung personenbezogener Daten im Auftrag: Art der Daten und beauftragtes Unternehmen.

- Rechte der Betroffenen (§§ 33 bis 35 BDSG),

- Stelle im Betrieb, die Anfragen Betroffener bearbeitet,

- Bei Verwendung der Daten zu Werbungszwecken: Hinweis auf das Widerspruchsrecht Betroffener (§ 28 Abs. 4 BDSG),

- Sicherstellung, dass eingegangene Widersprüche gegen Werbung beachtet werden,

- Arbeitnehmerdatenschutz,

- Technisch-organisatorischer Datenschutz (§ 9 BDSG und Anlage) Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungsgebot.

Die Auswertung der Fragebögen hat im Wesentlichen keine Beanstandungen ergeben. Dies mag dem Umstand geschuldet sein, dass in Kreditinstituten in der Regel betriebliche Datenschutzbeauftragte bestellt sind. Lediglich bei der Speicherdauer der Videoüberwachung hatte sich im Einzelfall Nachfragebedarf ergeben. Aus diesem Grunde wurde die Videoüberwachung von drei Banken im Rahmen einer Vor-Ort-Kontrolle überprüft. Als Ergebnis dieser Prüfung hat die Aufsichtsbehörde folgende Rechtsauffassung über die Videoüberwachung in Banken den Kreditinstituten zur Beachtung mitgeteilt:

Die an der Prüfung beteiligten Banken haben sowohl bei der Beantwortung der von der Aufsichtsbehörde versandten Fragebögen, als auch bei der jeweiligen Vor-Ort-Kontrolle im Wesentlichen folgende Gründe für die Videoüberwachung angeführt:

- Wahrnehmung des Hausrechts,
- Verhinderung und Verfolgung von Straftaten,
- Vollzug der Unfallverhütungsvorschrift Kassen und
- Überprüfung von Kundeneinsprüchen aus Vertragsrecht.

Dagegen bestehen von Seiten der Aufsichtsbehörde keine grundsätzlichen Bedenken. Allerdings ist Folgendes anzumerken:
Nach § 6b Bundesdatenschutzgesetz dürfen private Stellen öffentlich zugängliche Räume dann mit Videokameras überwachen, wenn dies

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

erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Wenn die Überwachung nicht ausschließlich der Wahrung des Hausrechts dient, muss sie berechtigten Interessen für konkret festgelegte Zwecke dienen. „Berechtigt“ sind alle von der Rechtsordnung anerkannten Interessen. Dies können sowohl wirtschaftliche wie ideelle Interessen sein. Diese Zwecke müssen konkret festgelegt werden. Um eine Nachprüfung zu ermöglichen, wird empfohlen, die Zwecke schriftlich zu dokumentieren. Nach § 6b BDSG sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Dies bedeutet, dass sich der Zeitpunkt der Löschung danach richtet, ob die Daten für den ursprünglichen Erhebungszweck noch erforderlich sind bzw. schutzwürdige Interessen der Betroffenen entgegenstehen.

Hinsichtlich der Speicherdauer ist zwischen den einzelnen Überwachungskameras zu unterscheiden, je nach dem zu welchem Zweck die jeweilige Kamera Daten erfasst. So ist eine längere Speicherdauer, die mit der Einspruchsfrist nach der zwischen Bank und Kunden vertraglich vereinbarten AGB begründet wird, für die Kameras, die die Geldausgabeautomaten sowie deren Umfeld überwachen, nachvollziehbar und berechtigt. Denn gemäß dieser vertraglichen Regelung können die Kunden bis zu sechs Wochen nach Quartalsabschluss den durchgeführten Buchungen widersprechen. Die Videoüberwachungsdaten werden für den entsprechenden Zeitraum einschließlich einer Bearbeitungszeit von einer Woche benötigt, um Einwendungen der Kunden überprüfen zu können.

Bei reinen „Überfallkameras“, d. h. Kameras, die nur bei einem Überfall vom Personal ausgelöst werden, genügt eine erheblich kürzere Speicherdauer. Bei den Kameras, die zur Wahrung des Hausrechts eingesetzt werden, wird unter Berücksichtigung der arbeitsfreien Wochenenden ebenfalls eine kürzere Speicherdauer der Bilddaten als angemessen angesehen. Die Speicherdauer einer Videoüberwachung darf keinesfalls mit der zur Verfügung stehenden Kapazität des Speichermediums begründet werden.

Der Zugriff auf gespeicherte Videodaten muss in Anwendung der Anlage zu § 9 BDSG protokolliert werden, da bei einer Prüfung nachvollziehbar sein muss, wer, wann, auf welche Daten und aus welchem berechtigten Grund zugegriffen hat. Ebenso ist der Personenkreis, der Zugriff auf die gespeicherten Daten hat, konkret festzulegen. Maßnahmen, die einen unbefugten Zugriff verhindern sollen, sind festzulegen.

Nach § 6b Absatz 4 BDSG hat eine Benachrichtigung von identifizierten Betroffenen zu erfolgen. Dies betrifft insbesondre die Kameras, die die Geldausgabeautomaten sowie deren Umfeld überwachen, wenn die Bilddaten mit weiteren Daten, z. B. den Transaktionsdaten der Betroffenen, verknüpft werden.

4. Ahnen-/Familienforschung

An die Aufsichtsbehörde wurde auch ein Fall von einem Interessenten, der sich mit der Ahnen-/Familienforschung befasst, herangetragen. Anlässlich einer bevorstehenden Jahrhundert-Jubiläums-Feier eines Dorfes wollte eine Gruppe interessierter Genealogen ein Familienbuch mit den Namen der lebenden und verstorbenen Einwohner der letzten 100 Jahre dieses Dorfes veröffentlichen.

Zu diesem Fall und auch zu anderen Vorhaben, die sich mit der Familienforschung befassen, ist aus datenschutzrechtlicher Sicht auf Folgendes hinzuweisen:

Datenschutzrechtliche Regelungen als Ausdruck des Grundrechtes auf informationelle Selbstbestimmung beziehen sich - von wenigen Ausnahmen abgesehen, in denen auch die Daten Verstorbener besonders geschützt werden - ausschließlich auf lebende Personen. Ein besonderes Schutzbedürfnis für die Daten Verstorbener kann sich aus Spezialvorschriften, u. a. Archivgesetze und Personenstandsregister sowie aus der Art der Daten, wie zum Beispiel Gesundheitsdaten, ergeben. Sofern kein derartiger Ausnahmetatbestand vorliegt, ist es aus datenschutzrechtlicher Sicht unbedenklich, die personenbezogenen Daten von Verstorbenen, wie beispielweise Namen, Geburts- Eheschließungs- und Sterbedaten, zu verarbeiten, wozu auch die Veröffentlichung dieser Daten zählt.

Anders ist die Rechtslage, wenn die Angaben sich auf lebende Personen beziehen. Für diese Fälle gilt grundsätzlich, dass die Verarbeitung personenbezogener Daten nur dann zulässig ist, wenn sie durch Rechtsvorschrift erlaubt ist oder die Betroffenen gemäß § 4a Bundesdatenschutzgesetz schriftlich eingewilligt haben. Zwar findet nach § 1 Abs. 2 Nr. 3 BDSG sowie nach § 27 Abs. 1 Satz 2 BDSG das Bundesdatenschutzgesetz keine Anwendung, wenn die Erhebung, Verarbeitung oder Nutzung ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Dies greift jedoch nicht mehr, wenn die Daten in irgendeiner Form (z. B. Buch, Broschüre, Zeitung, Internet) veröffentlicht werden, weil die Daten dadurch einem unbeschränkten Perso-

nenkreis zugänglich gemacht werden und insofern keine ausschließliche persönliche bzw. familiäre Nutzung vorliegt. Neben der Einwilligung der Betroffenen als Voraussetzung für die Veröffentlichung dürfen die Daten noch lebender Personen gem. § 28 Abs. 1 Satz 1 Nr. 3 BDSG auch dann veröffentlicht werden, wenn sie allgemein zugänglich sind, es sei denn, dass das schutzwürdige Interesse Betroffener an der Veröffentlichung offensichtlich überwiegt. Weitere Voraussetzung für diesen Fall ist, dass die Daten bei der ersten Bekanntgabe in den allgemein zugänglichen Quellen rechtmäßig erhoben wurden. Zu den allgemein zugänglichen Quellen zählen beispielweise Zeitungsanzeigen (etwa über Geburt, Heirat, Tod), Amtsblätter, Stadtanzeiger, Gemeindebriefe der Kirchengemeinden, Grabinschriften, Familienbücher etc. Bei der Nutzung der Bestände anderer Genealogen kommt es entscheidend darauf an, ob es sich bereits um rechtmäßig veröffentlichte Daten handelt. Ist dies nicht der Fall, bedarf es auch hier der Einwilligung der Betroffenen in die Veröffentlichung.

Falls bei der Familienforschung auf die Personenstandsbücher zurückgegriffen werden soll, kann es unabhängig von der datenschutzrechtlichen Bewertung Kollisionen mit dem Personenstandsrecht geben. Dies gilt sowohl für die Daten von Lebenden, als auch von Verstorben. Nach § 61 des Personenstandsgesetzes ist die Einsicht in die Personenstandsbücher, die Durchsicht dieser Bücher und die Erteilung von Personenstandsurkunden nur für die Personen möglich, auf die sich der Eintrag bezieht sowie für deren Ehegatten, Vorfahren und Abkömmlingen. Andere Personen, zu denen auch Verwandte in der Seitenlinie zählen, haben dieses Recht nur, wenn sie ein rechtliches Interesse glaubhaft machen. Das heißt, dass die Nutzung der Register durch spezielle Rechtsvorschrift erlaubt sein muss, oder die andere Person muss auf die Kenntnis der Daten zur Verfolgung eines ihr zustehenden Rechtes angewiesen sein. Das Forschungsinteresse der Genealogen allein reicht für diese Voraussetzung nicht aus. Die Rechtsprechung hat in der Vergangenheit mehrfach bestätigt, dass die Genealogie kein rechtliches Interesse begründet. Soll dennoch auf die Personenstandsbücher zurückgegriffen werden, bleibt den Genealogen nur der Weg über eine Vollmacht der nach § 61 des Personenstandsgesetzes Berechtigten.

5. Videoüberwachung

Auch im Berichtszeitraum waren die Eingaben und Anfragen zu dem Themenkomplex Videoüberwachung wieder ein Schwerpunkt der aufsichtsbehördlichen Tätigkeit. Oftmals zeigt sich, dass die Betreiber von Videokameras diese vorschnell installieren, ohne sich über die rechtlichen Voraussetzungen oder Alternativen ausreichend Gedanken zu machen. Nicht zuletzt verursacht dies den Betreibern auch unnötige Kosten, wenn sie die Kameras – spätestens auf Betreiben der Aufsichtsbehörde – wieder entfernen müssen.

5.1 Videoüberwachung eines Parkplatzes

Die Aufsichtsbehörde wurde auf eine an einem Haus angebrachte Videokamera hingewiesen, die auf einen Parkplatz gerichtet ist. Der hierzu angehörte Betreiber nahm dahingehend Stellung, dass die Kamera auf vier ihm gehörende Stellflächen ausgerichtet sei. Anlass hierfür sei, dass die Begrenzungspfosten der Stellflächen durch Parkplatzbenutzer regelmäßig stark beschädigt worden seien, ohne dass sich die für die Schäden Verantwortlichen gemeldet hätten. Durch die Videoüberwachung sollten zukünftige Schädiger ermittelt werden.
Anlässlich einer Vor-Ort-Kontrolle durch Vertreter der Aufsichtsbehörde wurde festgestellt, dass die Kamera zumindest von der Anbringung her nicht nur auf die vier Stellflächen, sondern auf den gesamten Parkplatz ausgerichtet war. Ein Hinweis auf die Videoüberwachung war nicht vorhanden.
Die Aufsichtsbehörde hat dem Betreiber daraufhin mitgeteilt, dass die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) gemäß § 6b Absatz 1 BDSG nur zulässig ist, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Zwar ist allgemein anerkannt, dass die Ermittlung von Schädigern bzw. die Verhinderung von Sachbeschädigungen zur

Wahrung des Hausrechts sowie zu den berechtigten Interessen der verantwortlichen Stelle im Rahmen des § 6b BDSG zu rechnen sind. Im Rahmen der Erforderlichkeitsprüfung und Interessenabwägung des § 6b Absatz 1 BDSG darf dies jedoch nicht dazu führen, dass der gesamte öffentliche Parkraum überwacht wird. Eine solche Überwachung greift unzulässigerweise in das informationelle Selbstbestimmungsrecht der übrigen Parkplatzbenutzer ein. Das verfassungsmäßige Recht auf informationelle Selbstbestimmung beinhaltet das Recht des Einzelnen, sich in der Öffentlichkeit frei und ungezwungen bewegen zu können, ohne befürchten zu müssen, ungewollt einer Beobachtung durch eine Videoanlage ausgesetzt zu sein
Vor diesem Hintergrund hat der Betreiber die Videokamera abgebaut.

5.2 Videoüberwachung in einem Sport- und Freizeitzentrum

Von einem Kunden eines Sport- und Freizeitzentrums wurde die Aufsichtsbehörde darüber unterrichtet, dass im Herren-Umkleideraum eine Videokamera angebracht worden sei. Daraufhin erfolgte durch die Aufsichtbehörde eine Vor-Ort-Kontrolle in dem Betrieb, bei der festgestellt wurde, dass sowohl im Herren-Umkleideraum als auch im Flur davor jeweils eine Videoüberwachungskamera angebracht waren.
Bei der Kontrolle wurde außerdem festgestellt, dass neben diesen Kameras im gemeinsam genutzten Umkleidebereich auch im sonstigen Betrieb noch mehrere Überwachungskameras angebracht und zum Teil auch angeschlossen waren. Die Kameras im Bereich des Herren-Umkleideraumes sowie im Flur davor waren jedoch noch nicht angeschlossen und somit nicht betriebsbereit. Der Betreiber äußerte sich hierzu dahingehend, dass er im Begriff sei, eine umfassende Videoüberwachungsanlage installieren zu lassen.
Die Aufsichtsbehörde hat dem Betreiber daraufhin die datenschutzrechtlichen Voraussetzungen für eine Videoüberwachung erläutert. In diesem Zusammenhang wurde von Seiten der Aufsichtsbehörde empfohlen, die Überwachungskamera im Herren-Umkleideraum – auch wenn sie nicht funktionsfähig war – bis zur Klärung des Sachverhaltes zu demontieren, da auch bei einer nicht funktionsfähigen Überwa-

chungskamera (Attrappe) ein zivilrechtlicher Unterlassungsanspruch in Betracht kommen kann. Zu der geplanten Videoüberwachungsanlage hat die Aufsichtsbehörde angeboten, ein von dem Betreiber vorzulegendes Konzept über die beabsichtigte Videoüberwachung in datenschutzrechtlicher Sicht zu prüfen.
Der Betreiber hat der Aufsichtsbehörde in der Folgezeit ein Konzept vorgelegt, wonach die künftige Anlage sowohl Videokameras als auch Bewegungsmelder umfassen und auch als Alarmanlage nach Betriebsende dienen soll. Kameras waren dabei in fast allen Bereichen des Betriebes vorgesehen, auch in sensiblen Bereichen der Freizeitgestaltung oder der Rezeption.
Die Aufsichtsbehörde hat dem Betreiber nach Prüfung des Konzeptes mitgeteilt, dass die geplanten Videokameras nur unter den folgenden Voraussetzungen zulässig sind:
Bei den Kameras, die nur der Überwachung eines geordneten Betriebsablaufes dienen, muss durch entsprechende Maßnahmen sichergestellt werden, dass keine Personen identifizierbar sind.
Die auf die Ruhe- und Verweilbereiche gerichteten Kameras sind ausschließlich Bestandteil der Alarmanlage und müssen während der Betriebszeiten abgeschaltet sein. Dieser Umstand ist durch entsprechende, für die Gäste gut sichtbare Hinweisschilder erkennbar zu machen.
Soweit bei den Kameras eine Aufzeichnung stattfinden soll, darf eine Speicherdauer von drei Tagen nicht überschritten werden.
Die Zutrittskontrolle ist durch einen verschlossenen Raum, die Zugriffskontrolle durch ein geschütztes Passwort sicherzustellen; sollte ein Zugriff auf die gespeicherten Daten erfolgen, so ist dieser zu protokollieren.
Der Betreiber hat diese Auflagen akzeptiert.

5.3 Videoüberwachung in der Gastronomie

Die Aufsichtsbehörde wurde auf eine Videokamera im gastronomischen Bereich einer Buchhandlung aufmerksam gemacht. Eine Vor-Ort-Kontrolle zeigte, dass es sich

dabei nicht um eine Kamera handelte, sondern dass nach Umbauarbeiten und der Einrichtung des Gastronomiebereiches lediglich die Außenhülle einer Dome-Kamera verblieben war, mit der eine Beobachtung demnach tatsächlich nicht erfolgen konnte. Grundsätzlich wäre eine Videobeobachtung dieses Bereiches aber auch nicht zulässig.

Die Aufsichtsbehörde hat in den letzten Jahren einen nicht unerheblichen Anstieg der Videoüberwachung in Gastronomiebetrieben festgestellt. Dort wurden die datenschutzrechtlichen Bestimmungen oft nicht eingehalten. Von daher ist es geboten, diesen datenschutzrechtlichen Rahmen im Tätigkeitsbericht näher zu erläutern.

Häufig berücksichtigt die Videoüberwachungsinfrastruktur in Gastronomiebetrieben nicht die unterschiedliche Eingriffsintensität in das Recht auf informationelle Selbstbestimmung der Betroffenen. Die Beobachtung erfolgt nicht nur in kurzzeitig verweilenden Durchgangszonen, sondern auch in zeitintensiven Wartebereichen, in denen Aktivitäten wie Kommunikation, Essen, Trinken, Lesen oder Erholung im Vordergrund stehen können (vgl. hierzu Weichert, „Rechtsfragen der Videoüberwachung“, DuD 2000, S. 664 [667]), wie etwa in den Gästebereichen. Die Betroffenen sind in diesen Gästebereichen einer dauerhaften und flächendeckenden Videoüberwachung ausgesetzt, der sie sich nicht entziehen können (vgl. hierzu die Ausführungen im gemeinsamen Informationsblatt des Berliner Beauftragten für Datenschutz und Informationsfreiheit/des Landesbeauftragten für den Datenschutz Niedersachen/des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, „Achtung Kamera! Videoüberwachung durch private Stellen“, Stand: 07/09, S. 5). Es wird ihnen zugemutet, ohne selbst einen Anlass gegeben zu haben, die Erfassung ihres Bildes und ihrer Kontaktpersonen für die nicht unerhebliche Dauer ihres Aufenthalts im überwachten Gästebereich hinzunehmen (vgl. Bizer, „Überwachung durch Bilder!“, DuD 2000, S. 190). Fraglich ist dann, inwieweit es dem Einzelnen bewusst bleibt, selbst darüber bestimmen zu können, ob er mit optisch-elektronischen Einrichtungen aufgenommen werden darf und was mit den Aufnahmen geschehen soll (vgl. Saeltzer, „Vorsicht, Videoüberwachung“, DUD 1997, S. 462). Die Wahr-

nehmung seines ihm zustehenden Grundrechts auf informationelle Selbstbestimmung kann ihm so erschwert werden. Die Gäste können zudem nicht erkennen, welches Überwachungspotenzial die einzelne Videokamera beinhaltet (vgl. Bäumler, „Datenschutzrechtliche Grenzen der Videoüberwachung“, RVD 2001, S. 67 [70]). Eine Überwachung in solchen Bereichen greift besonders intensiv in das Allgemeine Persönlichkeitsrecht der Betroffenen ein (vgl. Duhr/Naujok/Peter/Seiffert, „Neues Datenschutzrecht für die Wirtschaft“, DuD 2002, S. 5 [28]).

In der Rechtsprechung ist anerkannt, dass bei Videoüberwachungen von zeitintensiven Wartebereichen die Abwägung zu Gunsten der Betroffenen mit Rücksicht auf deren Grundrecht auf informationelle Selbstbestimmung vorzunehmen ist. In dem Urteil des Amtsgerichts Hamburg vom 22.04.2008, Az.: 4 C 134/08, ist hierzu Folgendes ausgeführt:

„Bezüglich der Videoüberwachung des Kundenbereichs […] fällt die Abwägung zu Gunsten des Klägers aus. Das Recht auf informationelle Selbstbestimmung verbürgt das Recht des Einzelnen, sich in der Öffentlichkeit frei und ungezwungen bewegen zu können, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden. Ob dieses Recht bei der Videoüberwachung im öffentlich zugänglichen Raum überwiegt, ist einzelfallabhängig und situationsbezogen zu beurteilen. (Bizer in: Simitis, BDSG-Kommentar, 5. Auflage, § 6 b Rn. 60). Regelmäßig ist die Schutzbedürftigkeit in öffentlich zugänglichen Räumen, in denen sich Menschen typischerweise länger aufhalten und/oder miteinander kommunizieren besonders hoch einzustufen (Bizer in: Simitis, BDSG-Kommentar, 5. Auflage, § 6b Rn. 60). Dies trifft auf die für Kunden eingerichteten Sitzbereiche, durch die ein längerer Aufenthalt […] ermöglicht werden soll in besonderem Maße zu. Anders als in den Bereichen des Tresens oder der Regale, an denen sich die Kunden in der Regel nur kurzfristig zur Besorgung der gewünschten Produkte aufhalten, werden die Persönlichkeitsrechte der sich in den Sitzbereichen länger aufhaltenden Kunden durch eine ständige Videoüberwachung erheblich beeinträchtigt. Diese Rechtsverletzungen wiegen schwerer als die Interessen der Beklagten an einer effektiven Strafverfolgung […]. Ferner bleibt zu beachten, dass der Waren- und Geldzahlungsverkehr sich […] auf die Bereiche der Warenregale sowie insbesondere des Waren- und Kassentre-

sens beschränkt. Dort ist die Gefahr von Diebstählen oder Unterschlagungen durch Kunden oder Mitarbeiter besonders hoch. Hingegen bestehen in den Kundenbereichen keine besonderen Anhaltspunkte für eine Gefahr der Begehung von Straftaten. Insofern kommt in diesen Bereichen dem Interesse der Beklagten an einer effektiven Strafverfolgung auch eine geringere Bedeutung zu. Während also in den Tresen- und Regalbereichen eine Videoüberwachung durchaus gerechtfertigt erscheint, ist die Beobachtung der Kundenbereiche unzulässig im Sinne des § 6b Abs. 1 S. 1 BDSG."

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits im Jahr 2000 auf den zunehmenden Einsatz von Videokameras insbesondere auch im nicht-öffentlichen Bereich hingewiesen. Diese Entwicklung kann die Gefahr einer Überwachungsinfrastruktur begründen (vgl. die Entschließung „Risiken und Grenzen der Videoüberwachung" der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 200 in Hannover; DuD 2000, S. 304f.).

In ständiger Verwaltungspraxis achten daher die Datenschutzaufsichtsbehörden auf die ordnungsgemäße Einhaltung der gesetzlichen Vorgaben zur Videoüberwachung gerade im Gastronomiebereich. Beispielhaft zeigen die Tätigkeitsberichte verschiedener Datenschutzaufsichtsbehörden, dass Videoüberwachungen im Gästebereich von Gastronomiebetrieben in der datenschutzaufsichtsrechtlichen Verwaltungspraxis nicht geduldet werden: so auf Seite 32f. des 17. Tätigkeitsberichts (Berichtszeitraum 2003/2004) des Landesbeauftragten für Datenschutz Niedersachen, Seite 74 des zweiten Tätigkeitsberichts aus dem Jahr 2006 der Bayerischen Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich, Seite 94 ff. des vierten Tätigkeitsberichts aus dem Jahr 2007 des Innenministeriums Baden-Württemberg, Seite 22 ff. des 19. Tätigkeitsberichts (Berichtszeitraum 2007/2008) des Landesbeauftragten für Datenschutz Niedersachen und Seite 96 f. des 32. Tätigkeitsberichts (Berichtszeitraum 2009) des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.

6. Novellierungen des Bundesdatenschutzgesetzes im Jahre 2009

Der Deutsche Bundestag hat im Jahr 2009 das Bundesdatenschutzgesetz durch drei Novellen (im Folgenden BDSG-Novelle I bis III) geändert (vgl. in der Fachliteratur etwa: Gola, Die BDSG-Novellen 2009 – Ein Kurzüberblick, RDV 2009 S. 1 ff.; Abel, Die neuen BDSG-Regelungen, RVD 2009 S. 147 ff.; Eckhardt, BDSG: Neuregelungen seit 01.09.2009, DuD 2009 S. 587 ff.; Weichert, Dauerbrenner BDSG-Novellierung, DuD 2010 S. 7 ff.). Mit den Änderungen ist der Datenschutz erheblich gestärkt worden. Hierzu in der Kürze im Einzelnen:

BDSG-Novelle I:

Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 29. Juli 2009 (BGBl. I S. 2254) - Inkrafttreten am 1. April 2010:

Insbesondere die Kritik von Verbraucherschützern und Datenschutzaufsichtsbehörden an mangelnder Transparenz und unzureichender Rechtssicherheit im Auskunfteiwesen und speziell beim sogenannten (Kredit-)Scoring haben den Gesetzgeber bewogen, spezifische Erlaubnistatbestände für die Datenübermittlung an Auskunfteien (vgl. § 28a BDSG n.F.) und für die Nutzung mathematisch-statistischer Wahrscheinlichkeitswerte zur Ermittlung der Zahlungswilligkeit und –fähigkeit ihrer Kunden im Rahmen von Kreditgeschäften (sogenanntes Scoring - vgl. § 28b BDSG n.F.) sowie Auskunfts- und Informationsrechte des Betroffenen gegenüber verantwortlichen Stellen und Auskunfteien (vgl. Neufassung des § 34 Abs. 1 bis 9 BDSG n.F.) zu schaffen. Infolgedessen erhöht das Änderungsgesetz die Rechtssicherheit sowohl für die Betroffenen als auch für die Unternehmen, indem zum Beispiel einheitlich festgelegt wird, wann ein Scoring durchgeführt werden darf und wann Unternehmen fällige, nicht beglichene Forderungen an Auskunfteien melden dürfen. Den Betroffenen wird es erleichtert oder teilweise erst ermöglicht, fehlerhafte Daten zu korrigieren, Missverständnisse aufzuklären und ihre Interessen sachgerecht zu vertreten. Sollten die Auskunfteien die Auskünfte verweigern, drohen Bußgelder (vgl. § 43 Abs. 1 Nrn 4a, 8b und 8c BDSG n.F.).

BDSG-Novelle II:

Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009 (BGBl. I S. 2814) – Inkrafttreten am 1. September 2009; für bestimmte Regelungen bestehen Übergangsfristen bis zum 31. August 2010 und 31. August 2012:

Die BDSG-Novelle II ist maßgeblich durch „Datenschutzskandale“ motiviert, die insbesondere durch illegalen Datenhandel und Fälle ausufernder Mitarbeiterkontrolle gekennzeichnet waren. Über die Einschränkung der Erlaubnis zur Verwendung personenbezogener Daten zu Zwecken des Adresshandels und der Werbung sowie neue Klarstellungsvorschriften zum Beschäftigtendatenschutz hinaus, hat der Gesetzgeber weitere Neuregelungen verabschiedet, die eine Anpassung der betrieblichen Datenschutzorganisation erforderlich machen, zumal parallel auch Vorschriften zur Effektivierung der Datenschutzkontrolle geschaffen worden sind. Hierzu im Einzelnen:

Gemäß der BDSG-Novelle II sollen personenbezogene Daten wie Adressen künftig weitergegeben werden dürfen, wenn der Kunde darin einwilligt (vgl. § 28 Abs. 3 BDSG n.F.): Die entsprechende Textpassage etwa in Vertragstexten soll dabei optisch deutlich hervorgehoben sein müssen. Listenmäßig erfasste Daten wie etwa Name, Beruf, Adresse, Geburtsjahr oder Titel sollen auch ohne Einwilligung weitergegeben werden dürfen, sofern die Betroffenen über die Herkunft der Angaben informiert werden. Damit soll ihnen ermöglicht werden, einer solchen Weitergabe und Nutzung ihrer Daten wirksam zu widersprechen. Weiterhin möglich soll dagegen die Eigenwerbung mit eigenen Kundendaten sein, die im Rahmen einer Vertragsbeziehung erhoben wurden (vgl. § 28 Abs. 3 Satz 4 BDSG n.F.). Ausgenommen von dieser Neuregelung des § 28 Abs. 3 BDSG n.F. ist der Bereich der Markt- und Meinungsforschung (vgl. § 30a BDSG n.F.). Der Regierungsentwurf hatte ursprünglich vorgesehen, dass die Verwendung personenbezogener Daten zu Werbezwecken oder zur Markt- und Meinungsforschung künftig grundsätzlich nur noch mit ausdrücklicher Einwilligung der Betroffenen zulässig sein soll. Das beschlossene Änderungsgesetz räumt den betroffenen Wirtschaftszweigen für die Verarbeitung personenbezogener Daten, die vor dem 1. September 2009 erhoben worden sind, mit Rücksicht auf Markt- und Meinungsforschung eine Übergangsfrist von zwei Jahren und mit

Blick auf Werbung eine Übergangsfrist von drei Jahren ein (vgl. § 47 BDSG n.F.). Neu ist ferner, dass künftig vor allem marktbeherrschende Unternehmen den Vertragsabschluss nicht mehr von der Einwilligung in die Datenweitergabe an Dritte und zu Werbezwecken abhängig machen dürfen. Es besteht ein sogenanntes Koppelungsverbot (vgl. § 28 Abs. 3b BDSG n.F.). Ferner soll die Sicherheit von Daten durch Vorschriften zur Verschlüsselung durch Anonymisierung und Pseudonymisierung erhöht werden (vgl. § 3a BDSG n.F.). Außerdem dürfen Unternehmen schwere Datenschutzpannen nicht mehr verheimlichen. Sie unterliegen nun einer Informationspflicht (vgl. § 42a BDSG n.F.). Gestärkt werden soll zudem die Stellung der betrieblichen Datenschutzbeauftragten, für die weitreichende Kündigungsschutzvorschriften vorgesehen sind (vgl. § 4f Abs. 3 Satz 5 bis 7 BDSG n.F.). Daneben sollen die Aufsichtsbehörden künftig bei Verstößen gegen Datenschutzregelungen nicht nur Bußgeldverfahren einleiten (vgl. § 43 Abs. 1 Nrn 2a, 2b, 3a, 8a sowie Abs. 2 Nrn 5a bis 7 BDSG n.F.), sondern auch anordnen können, dass der entsprechende Verstoß eingestellt wird (vgl. § 38 Abs. 5 BDSG n.F.). Auch sollen die Bußgelder für Verstöße gegen Datenschutzbestimmungen deutlich angehoben werden, wobei der Bußgeldrahmen bei formellen Verstößen auf bis zu 50.000 Euro verdoppelt und der für materielle Verstöße auf bis zu 300.000 Euro ausgeweitet wurde. Dabei ist für solche Fälle auch die Möglichkeit der Gewinnabschöpfung vorgesehen (vgl. § 43 Abs. 3 BDSG n.F.). Aus Anlass der bekanntgewordenen Überwachungen von Mitarbeitern in großen Unternehmen wie der Deutschen Telekom, der Deutschen Bahn oder bei Lidl wird durch die BDSG-Novelle II erstmalig eine Grundsatzregelung zum Arbeitnehmerdatenschutz in das Bundesdatenschutzgesetz integriert (vgl. § 32 BDSG n.F.). Sie entspricht den von der Rechtsprechung erarbeiteten Grundsätzen und ist ein erster Schritt zu einer besseren gesetzlichen Ausgestaltung des Arbeitnehmerdatenschutzes.

<u>BDSG-Novelle III:</u>

Artikel 5 des Gesetzes zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften

über das Widerrufs- und Rückgaberecht vom 29. Juli 2009 (BGBl. I S. 2355 [2384]) – Inkrafttreten am 11. Juni 2010:

Die BDSG-Novelle III dient der Umsetzung von Artikel 9 der Europäischen Verbraucherkreditrichtlinie 2008/48/EG vom 23. April 2008 (ABl. EG Nr. L 133/66), wonach Kreditgebern aus sämtlichen Mitgliedstaaten bei grenzüberschreitenden Krediten ein diskriminierungsfreier Zugang zu den zur Bewertung der Kreditwürdigkeit des Verbrauchers verwendeten Auskunftssystemen zu gewähren ist. Die Novelle schafft daher Auskunftspflichten aus Kreditdatenbanken sowie bei der Ablehnung von Verbraucherdarlehensverträgen und Verträgen über eine entgeltliche Finanzierungshilfe. Aus diesem Grunde wurden in § 29 Abs. 6 und 7 BDSG Auskunftspflichten bei Bonitätsanfragen innerhalb der EU/ des EWR verankert.

7. Beschlussfassungen des Düsseldorfer Kreises

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

7.1. Beschlussfassungen der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 23./24. April 2009 in Schwerin

7.1.1 Datenschutzrechtliche Aspekte des Mitarbeiter-Screenings in international tätigen Unternehmen

Viele Unternehmen sind dazu übergegangen, ihre Mitarbeiter gegenüber Listen abzugleichen, die terrorverdächtige Personen und Organisationen enthalten. Insbesondere Unternehmen, die internationalen Konzernen angehören, werden von ihren teilweise in Drittländern ansässigen Muttergesellschaften hierzu aufgefordert. Letztere stellen auch darüber hinaus gehende Listen z.B. mit gesuchten Personen zur Verfügung, die aufgrund nationaler Vorschriften in den Drittländern einzusetzen sind. Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Zwar kann § 28 Abs. 1 BDSG eine Rechtsgrundlage im Sinne des BDSG sein, diese Vorschrift kann jedoch für ein Screening nicht herangezogen werden. Der Abgleich mit den Listen dient nicht dem Vertragsverhältnis. Eine Abwägung der Unternehmens- und Betroffeneninteressen führt zu überwiegenden schutzwürdigen Interessen der Betroffenen. Dies gilt insbesondere vor dem Hintergrund, dass die Rechtsstaatlichkeit des Zustandekommens der Listen nachvollziehbar und gesichert sein muss, sowie Rechtsschutzmöglichkeiten bestehen müssen. Angesichts der fehlenden Freiwilligkeit einer solchen Erklärung im Arbeitsverhältnis kann auch das Vorliegen einer Einwilligung eine konkrete Rechtsgrundlage nicht ersetzen. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen daher fest, dass im Geltungsbereich des Bundesdatenschutzgesetzes lediglich solche Listen verwendet werden dür-

fen, für die eine spezielle Rechtsgrundlage im Sinne des § 4 Abs. 1 BDSG vorliegt. In diesem Zusammenhang weisen die obersten Aufsichtsbehörden für den Datenschutz im nicht- öffentlichen Bereich auch auf die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 in Magdeburg hin.

7.1.2 Telemarketing bei NGOs

Auch die so genannten NGOs (non governmental organization), also nichtstaatliche Organisationen die gemeinnützig oder auch als Interessenverbände tätig sind, haben in den letzten Jahren zunehmend damit begonnen, Telefonmarketing zu betreiben. Beworben werden insbesondere Personen, die schon einmal für die jeweilige NGO gespendet haben. Wenn der Spender seine Telefonnummer in den früheren Kontakten nicht angegeben hat, wird dieses Datum mit Hilfe des Telefonbuches oder einer Telefon-CD ermittelt. Die Aufsichtsbehörden erklären, dass auch NGOs ohne Einwilligung der Betroffenen nicht zu telefonischer Werbung berechtigt sind. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu diesem Zweck ist ohne Einwilligung rechtswidrig.

7.2 Beschlussfassung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 13. Juli 2009

7.2.1 Unzulässige Übermittlungen von Passagierdaten an britische Behörden verhindern!

Der Düsseldorfer Kreis stellt fest, dass die Übermittlung von Passagierdaten (Ausweis- und Reservierungsdaten) durch Fluggesellschaften in Deutschland an die britischen Zoll- und Sicherheitsbehörden für innereuropäische Flüge unzulässig ist. Die Bundesregierung wird gebeten, entsprechenden Forderungen der britischen Behörden entgegenzutreten.

Großbritannien verlangt im Rahmen des sog. eBorders-Projekts die Erhebung und Übermittlung von Ausweisdaten der Reisenden für innereuropäische Flüge von und nach Großbritannien und die Übermittlung von Daten aus den Reservierungsdatenbanken der Fluggesellschaften. Die britischen Behörden berufen sich bei ihrer Forderung auf die britische Gesetzgebung für Grenzkontrollen. Diese durch das eBorders-Projekt konkretisierte Gesetzgebung berührt einerseits den freien Reiseverkehr in der Europäischen Union. Andererseits bezieht sie sich auf Sachverhalte, die nicht alleine in der Regelungskompetenz des britischen Gesetzgebers liegen, weil sie Datenerhebungen in anderen Mitgliedstaaten der Europäischen Union vorschreibt und Übermittlungen aus Datenbanken verlangt, die sich in anderen Mitgliedstaaten befinden.

Die Übermittlung von Reservierungsdaten der Passagiere an britische Grenzkontrollbehörden, die sich in Datenbanken der verantwortlichen Fluggesellschaften in Deutschland befinden, ist nach deutschem Recht nicht erlaubt. Insbesondere enthält das Bundesdatenschutzgesetz (BDSG) keine Rechtsgrundlage, auf die die Fluggesellschaften die geforderte Übermittlung stützen könnten.

Bereits bei entsprechenden Forderungen der USA, Kanadas und Australiens bestand in Europa Konsens, dass die Übermittlung nicht zur Erfüllung der Flugreiseverträge erfolgt (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) und wegen der Zwangslage nicht auf eine Einwilligung (§ 4a BDSG) der Reisenden gestützt werden kann. Sie dient auch nicht den berechtigten Interessen der Fluggesellschaften, die selbst den Forderungen der britischen Behörden entgegentreten, weil sie sich als Reiseunternehmen und nicht als Gehilfen der Grenzkontrollbehörden verstehen. Außerdem besteht ein überwiegendes Interesse der Flugreisenden daran, dass eine Übermittlung ihrer Daten unterbleibt, solange die Vereinbarkeit der britischen Forderung mit vorrangigem europäischen Recht nicht geklärt ist (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Schließlich kann eine solche verdachts- oder gefahrunabhängige Übermittlung der Daten aller Reisenden für Sicherheitszwecke nicht auf § 28 Abs. 3 Satz 1 Nr. 2 BDSG gestützt werden, da diese Vorschrift das Vorliegen einer konkreten Gefahr oder Straftat voraussetzt. Die

Übermittlung der Reservierungsdaten ist außerdem verfassungsrechtlich bedenklich und auch fraglich im Hinblick auf die Vereinbarkeit mit der Europäischen Menschenrechtskonvention.

Was die Erhebung von Ausweisdaten anbelangt, gehen die britischen Behörden über die Europäische Richtlinie 2004/82/EG über die Verpflichtung von Beförderungsunternehmen, Angaben über beförderte Personen zu übermitteln, insoweit hinaus, als Daten auch für innereuropäische Flüge erhoben werden sollen. Die Europäische Kommission prüft zurzeit, ob diese einseitige Regelung eine Verletzung der Richtlinie 2004/82/EG darstellt. Jedenfalls dürfte eine solche Maßnahme im Hinblick auf die Freizügigkeit in der Europäischen Union kontraproduktiv sein. Der Düsseldorfer Kreis erwartet, dass die Erhebung und Übermittlung von Pass- und Ausweisdaten für innereuropäische Flüge bis zu einer Bewertung durch die Europäische Kommission unterbleiben.

7.3 Beschlussfassung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 22. Oktober 2009

7.3.1 Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig

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

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

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

Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen; sonstige Daten über negatives Zahlungsverhalten, bei denen

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

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

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

Hintergrund:

Nach § 29 Absatz 2 Nr. 1a Bundesdatenschutzgesetz ist die Erteilung von Bonitätsauskünften nur zulässig, wenn der Vermieter ein berechtigtes Interesse hieran hat und wenn kein Grund zu der Annahme besteht, dass der betroffene Mietinteressent ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Da Vermieter mit dem Abschluss eines Mietvertrages das Risiko eingehen, dass ein Mieter aufgrund von Zahlungsunfähigkeit oder –unwilligkeit den Mietzins oder Nebenkosten nicht begleicht, erkennen die Aufsichtsbehörden an, dass Vermieter aufgrund dieses finanziellen Ausfallrisikos grundsätzlich ein berechtigtes Interesse an einer Bonitätsauskunft über einen Mietinteressenten haben.

Bei der erforderlichen Abwägung sind allerdings auch die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensge-

staltung zu berücksichtigen. Ferner ist zu beachten, dass Mietkautionen in Höhe von bis zu drei Monatsmieten, das Vermieterpfandrecht und die bei nachträglicher Zahlungsunfähigkeit vielfach in die Zahlungspflicht eintretenden Sozialbehörden das finanzielle Risiko der Vermieter teilweise reduzieren.

Schließlich ist zu berücksichtigen, dass Auskunfteien an Vermieter nur Bonitätsdaten übermitteln dürfen, die eindeutig Rückschlüsse auf Mietausfallrisiken zulassen. Da das Zahlungsverhalten je nach Vertragsverhältnis unterschiedlich sein kann und teilweise auch ist, lassen zu spät oder nicht gezahlte Kleinbeträge etwa aus Handyverträgen und Internetgeschäften nicht unbedingt einen spezifischen Rückschluss auf die Zahlungsmoral bei Mietverträgen zu.

Aufgrund dieser Erwägungen haben die Aufsichtsbehörden nach Gesprächen mit den Auskunfteien und der Wohnungswirtschaft bereits im Jahr 2004 festgestellt, dass Auskunfteien keine uneingeschränkten Bonitätsauskünfte über Mietinteressenten erteilen dürfen. Vorzuziehen – so der damalige Beschluss – seien branchenspezifische Auskunftssysteme, die auf gesicherte Daten zu negativem Zahlungsverhalten aus öffentlichen Schuldnerverzeichnissen und dem Mietbereich beschränkt sind.

Die eingangs dargelegten Anforderungen berücksichtigen wesentliche Kritikpunkte der Wohnungswirtschaft und der Auskunfteien. So enthält der nunmehr definierte Katalog weder eine Beschränkung auf Daten aus dem Mietbereich noch eine Beschränkung auf titulierte Negativmerkmale. Eine derartige Beschränkung hatten mehrere Aufsichtsbehörden bislang auf Grundlage des Beschlusses aus dem Jahr 2004 gefordert und gegenüber so genannten Mieterwarndateien auch durchgesetzt.

Selbstverständlich dürfen nur Daten, die zulässigerweise bei der Auskunftei eingemeldet wurden, von dieser an Vermieter übermittelt werden. Das heißt, die allgemeinen Einmeldevoraussetzungen, die der Gesetzgeber im neuen § 28a BDSG präzisiert hat und die bereits bisher von den Aufsichtsbehörden gefordert wurden, müssen eingehalten werden.

Die Bagatellgrenze von 1500 € errechnet sich aus drei Monatsmieten der durchschnittlichen Kaltmiete. Nach der jüngsten Einkommens- und Verbrauchsstichprobe des Statistischen Bundesamtes beträgt sie monatlich 515 €.

Auch wenn die Speicher- bzw. Überprüfungsfrist der Auskunfteien bei Forderungen, die nach der Einmeldung beglichen wurden, drei Jahre beträgt (§ 35 Abs. 2 Nr. 4, 2. Halbsatz BDSG neu), ist ein berechtigtes Interesse von Vermietern an der Kenntnis solcher Daten nur für ein Jahr anzuerkennen. Daher ist auch nur innerhalb dieses Zeitraums eine Übermittlung an Vermieter zulässig. Ansonsten wäre dem Schuldner die Eingehung eines Mietverhältnisses unvertretbar erschwert.

Die Unzulässigkeit der Übermittlung von Scorewerten an Vermieter ergibt sich daraus, dass abgesehen von der allgemeinen Problematik der Scoreberechnung im Mietbereich die besondere Problematik besteht, dass die spezifischen Einschränkungen unterlaufen würden, wenn eine Scoreberechnung mit Daten erfolgte, die über den unter Nummer 2 genannten Katalog hinausgehen.
Die Einforderung von unbegrenzten Selbstauskünften oder Einwilligungen zur Einholung weit gefasster Auskünfte vom Mietinteressenten würde eine Umgehung der sich aus der Abwägung nach § 29 BDSG ergebenden gesetzlichen Begrenzungen darstellen, was demzufolge nicht zulässig ist.

Die bisherige Praxis der Auskunfteien entsprach den hier gestellten Anforderungen nicht bzw. nicht in ausreichendem Maße. Obwohl den Auskunfteien ausdrücklich die Möglichkeit eingeräumt wurde, ggf. alternative Lösungen zu den im Beschluss genannten Anforderungen zu entwickeln, die auf das jeweilige Geschäftsmodell der Auskunfteien und deren speziellen Datenbestand zugeschnitten sind, haben die Auskunfteien diese Möglichkeit bislang nicht genutzt.

Die Aufsichtsbehörden haben in Gesprächen mit den Auskunfteien angekündigt, dass sie bei datenschutzwidrigen Übermittlungen ggf. aufsichtsrechtliche Maßnahmen ergreifen werden.

7.4 Beschlussfassungen der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27. November 2009 in Stralsund

7.4.1 Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes.

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.
Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.

Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.
Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen. Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP- Adressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist. Werden pseudonyme Nutzungsprofile durch einen Auftragnehmer erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten.

7.4.2 Keine Internetveröffentlichung sportgerichtlicher Entscheidungen

Entgegen der Auffassung des OLG Karlsruhe in seinem Urteil vom 30. Januar 2009 gehen die zuständigen Aufsichtsbehörden in Anwendung des BDSG davon aus, dass die uneingeschränkt zugängliche Veröffentlichung von sportgerichtlichen Entscheidungen im Internet unzulässig ist.
Entsprechendes gilt auch für die Veröffentlichung von personenbezogenen Sperrlisten.

Eine Veröffentlichung in geschlossenen Benutzergruppen ist zulässig, wenn gewährleistet ist, dass in den Vereinen nur zuständige Personen zugreifen können. Soweit der Personenbezug nicht erforderlich ist, sind sportgerichtliche Entscheidungen zu anonymisieren.

Bei der mit der Veröffentlichung im Internet verbundenen Datenübermittlung an Dritte wird der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffen meist deswegen als besonders gravierend empfunden, weil hierdurch nicht nur ein weltweiter Zugriff auf die Daten, sondern darüber hinaus vor allem eine elektronische Recherchierbarkeit ermöglicht wird, welche auch zur Erstellung eines Persönlichkeitsprofil genutzt werden kann.

Der beabsichtigten „Prangerwirkung“ mit Abschreckungsfunktion könnte bereits dadurch Genüge getan werden, dass entsprechende Ahndungen organisations-/verbandsintern in zugriffsgeschützten Internetforen „für die, die es angeht“, publizieren würden. Die intendierte Information der Öffentlichkeit über das Vorgehen gegen Rechtsverstöße könnte ohne Personenbezug im Rahmen einer Ahndungsstatistik erfolgen.

7.4.3 Gesetzesänderung bei der Datenverwendung für Werbezwecke

Vom 1. September 2009 an gelten nach § 28 Abs. 3 BDSG neue Datenschutzregelungen bei der Datenverwendung für Werbezwecke. Diese Regelungen gelten spätestens ab dem 31. August 2012, jedoch sofort für Daten, die nach dem 1. September 2009 erhoben oder von einer Stelle erstmalig gespeichert werden. Die Datenschutzaufsichtsbehörden weisen darauf hin, dass für Daten, deren erstmalige Speicherung nicht eindeutig erkennbar ist, die neuen Regelungen angewendet werden. Sie weisen weiterhin darauf hin, dass eine Übermittlung für Werbezwecke nur zulässig ist, wenn Herkunft der Daten und Empfänger gespeichert werden und eine Gruppenauswahl nach einem Merkmal erfolgt (Listenübermittlung). Bei der Werbemaßnahme muss die erstmalig erhebende Stelle den Adressaten mitgeteilt werden. Die bisher weit verbreitete Praxis der Übermittlung von nach mehr als einem Merkmal selektierten Adressen ist unzulässig, wenn keine Einwilligung vorliegt.

7.5 Beschlussfassung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover

7.5.1 Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen

Seit dem 26. Juli 2000 besteht eine Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA zu den Grundsätzen des sog. „sicheren Hafens“ (Safe Harbor) [1]. Diese Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (FTC) können sich die Unternehmen selbst zertifizieren. So zertifizierte US-Unternehmen schaffen damit grundsätzlich die Voraussetzungen, dass eine Übermittlung personenbezogener Daten aus Europa an sie unter denselben Bedingungen möglich ist, wie Übermittlungen innerhalb des europäischen Wirtschaftsraumes (EU/EWR). Das US-Handelsministerium veröffentlicht eine Safe Harbor-Liste aller zertifizierten Unternehmen im Internet.

Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

[1] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, S. 7.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Harbor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifizierungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, ob die Safe Habor-Zertifizierung des Importeurs noch gültig ist. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor [2] gegenüber den von der Datenverarbeitung Betroffenen nachkommt.

Dies ist auch nicht zuletzt deshalb wichtig, damit das importierende Unternehmen diese Information an die von der Übermittlung Betroffenen weitergeben kann.

Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können. Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen, empfehlen die Aufsichtsbehörden, der Verwendung von Standard-

[2] Informationspflicht: Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

Vertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteur den Vorzug zu geben.
Stellt ein Daten exportierendes Unternehmen bei seiner Prüfung fest, dass eine Zertifizierung des importierenden Unternehmens nicht mehr gültig ist oder die notwendigen Informationen für die Betroffenen nicht gegeben werden, oder treten andere Verstöße gegen die Safe Harbor-Grundsätze zu Tage, sollte außerdem die zuständige Datenschutzaufsichtsbehörde informiert werden.

Eine Schlüsselrolle im Hinblick auf die Verbesserung der Einhaltung der Grundsätze kommt dabei der Zusammenarbeit der FTC mit den europäischen Datenschutzbehörden zu. Hierfür ist es erforderlich, dass die FTC und die europäischen Datenschutzbehörden die Kontrolle der Einhaltung der Safe Harbor-Grundsätze intensivieren. Die mit der Safe Harbor-Vereinbarung beabsichtigte Rechtssicherheit für den transatlantischen Datenverkehr kann nur erreicht werden, wenn die Grundsätze auch in der Praxis effektiv durchgesetzt werden.

7.6 Beschlussfassung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 24./25. November 2010 in Düsseldorf

7.6.1 Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen

Bei sog. Gruppenversicherungsverträgen handelt es sich um Rahmenverträge zwischen Vereinen/Verbänden und Versicherungsunternehmen, die den Mitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen.
Werden für die Werbung zum Abschluss solcher Verträge personenbezogene Daten der Mitglieder an ein Versicherungsunternehmen übermittelt, setzt dies die Einwilligung der Betroffenen voraus.

In Bezug auf Altmitglieder wurde bisher eine Information mittels Avisschreibens mit der Möglichkeit des Widerspruchs für ausreichend gehalten. Die Aufsichtsbehörden stellen fest, dass auch für Altmitglieder die vorherige Einholung einer informierten Einwilligungserklärung erforderlich ist.

7.6.2 Minderjährige in sozialen Netzwerken wirksamer schützen

Soziale Netzwerke spielen in unserer Lebenswirklichkeit eine zunehmend wichtige Rolle. Minderjährige beteiligen sich in großer Zahl an solchen Netzen. Ihrer besonderen Schutzbedürftigkeit muss über die Anforderungen hinaus Rechnung getragen werden, die grundsätzlich an eine datenschutzgerechte Ausgestaltung solcher Angebote zu stellen sind (vgl. Beschluss des Düsseldorfer Kreises vom 18. April 2008). Hier besteht ein erheblicher Schutz-, Aufklärungs- und Informationsbedarf:

- Das Schutzniveau sozialer Netzwerke wird wesentlich dadurch bestimmt, dass die Betreiber Standardeinstellungen vorgeben, z. B. für die Verfügbarkeit von Profildaten für Dritte. Minderjährige Nutzer haben häufig weder die Kenntnisse noch das Problembewusstsein, um solche Voreinstellungen zu ändern. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, generell datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch welche die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Minderjährige richtet oder von ihnen genutzt wird.

- Es muss erreicht werden, dass die gesetzlich bzw. durch die Betreiber vorgegebenen Grenzen für das Mindestalter der Nutzer eingehalten und wirksam überprüft werden. Dies könnte durch die Entwicklung und den Einsatz von Altersverifikationssystemen oder Bestätigungslösungen gelingen. Solche Verifikationssysteme lösen zwar ihrerseits Datenverarbeitungsvorgänge aus und müssen berücksichtigen, dass die Nutzung von Telemedien und ihre Bezah-

lung anonym oder unter Pseudonym möglich bleiben muss (§ 13 Abs. 6 Telemediengesetz); dies begründet aber kein Hindernis für ihren Einsatz.

- Minderjährigen und ihren Eltern wird die Einschätzung, welche der angebotenen Dienste sozialer Netzwerke altersgerecht sind, wesentlich erleichtert, wenn die Betreiber eine freiwillige Alterskennzeichnung von Internetinhalten vornehmen. Denkbar ist auch der Einsatz von Jugendschutzprogrammen, die Alterskennzeichnungen automatisch auslesen und für Minderjährige ungeeignete Inhalte sperren. Die Möglichkeiten, die der Entwurf für einen neuen Jugendmedienschutz-Staatsvertrag hierzu anbietet, müssen intensiv genutzt werden.

- Ebenso wichtig ist die Bewusstseinsbildung bei den minderjährigen Nutzern sozialer Netzwerke für die Nutzungsrisiken und für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den respektvollen Umgang mit den Daten anderer. Die Betreiber sozialer Netzwerke, aber auch staatliche Behörden, Schulen und nicht zuletzt die Eltern stehen in der Pflicht, über bestehende datenschutzfreundliche Nutzungsmöglichkeiten aufzuklären.

7.6.3 Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bei der Kontrolle verantwortlicher Stellen festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Beauftragten für den Datenschutz (DSB) in den verantwortlichen Stellen angesichts zunehmender Komplexität automatisierter Verfahren zum Umgang mit personenbezogenen Daten nicht durchgängig den Anforderungen des BDSG genügen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass die Aus- und Belastung der DSB maßgeblich beeinflusst wird durch die Größe der verantwortlichen Stelle, die Anzahl der zu betreuenden verantwortlichen Stellen, Besonderheiten branchenspezifischer Datenverarbeitung und den Grad der Schutzbedürftigkeit der zu verarbeitenden personenbezogenen Daten. Veränderungen bei den vorgenannten Faktoren führen regelmäßig zu einer proportionalen Mehrbelastung der DSB.

Nachfolgende Mindestanforderungen sind zu gewährleisten:

I. Erforderliche Fachkunde gemäß § 4f Abs. 2 Satz 1 BDSG

§ 4f Abs. 2 Satz 1 BDSG legt fest, dass zum Beauftragten für den Datenschutz (DSB) nur bestellt werden darf, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Weitere Ausführungen dazu enthält das Gesetz nicht. Vor dem Hintergrund der gestiegenen Anforderungen an die Funktion des DSB müssen diese mindestens über folgende datenschutzrechtliche und technisch-organisatorische Kenntnisse verfügen:

1. Datenschutzrecht allgemein – unabhängig von der Branche und der Größe der verantwortlichen Stelle

- Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle und
- umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des BDSG, auch technischer und organisatorischer Art,
- Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG.

2. Branchenspezifisch – abhängig von der Branche, Größe oder IT-Infrastruktur der verantwortlichen Stelle und der Sensibilität der zu verarbeitenden Daten

- Umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,
- Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, etc.),
- betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),
- Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur bzw. Organisation der verantwortlichen Stelle) und
- Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

Grundsätzlich müssen die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse bereits zum Zeitpunkt der Bestellung zum DSB im ausreichenden Maße vorliegen. Sie können insbesondere auch durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen.

II. Anforderungen an die Unabhängigkeit der/des Beauftragten gem. § 4f Abs. 3 BDSG

Gemäß § 4f Abs. 3 Satz 2 BDSG sind DSB in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Um die Unabhängigkeit der DSB zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich:

1. DSB sind dem Leiter/der Leiterin der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen (§ 4f Abs. 3 Satz 1 BDSG). Sie müssen in der Lage sein, ihre Verpflichtungen ohne lnteressenkonflikte erfüllen zu können. Dieses ist durch entsprechende Regelungen innerhalb der verantwortlichen Stelle bzw. vertragliche Regelungen sicher zu stellen und sowohl innerhalb der verantwortlichen Stelle als auch nach außen hin publik zu machen. Den DSB ist ein unmittelbares Vortragsrecht beim Leiter der Stelle einzuräumen.
2. DSB dürfen wegen der Erfüllung ihrer Aufgaben in Hinblick auf ihr sonstiges Beschäftigungsverhältnis, auch für den Fall, dass die Bestellung zum DSB widerrufen wird, nicht benachteiligt werden (vgl. § 4f Abs. 3 Satz 3 ff BDSG). Analog muss bei der Bestellung von externen DSB der Dienstvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird. § 4f Abs. 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von 4 Jahren, bei Erstverträgen wird wegen der Notwendigkeit der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von 1 – 2 Jahren empfohlen.
3. Datenschutzbeauftragte sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit sie nicht davon durch die Betrof-

fenen befreit wurden. Dies gilt auch gegenüber der verantwortlichen Stelle und deren Leiter (§ 4f Abs. 4 BDSG).

III. Erforderliche Rahmenbedingungen innerhalb der verantwortlichen Stelle zur Fachkunde und Unabhängigkeit des DSB

1. Die Prüfpflichten der DSB (vgl. § 4g BDSG) setzen voraus, dass ihnen die zur Aufgabenerfüllung erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche eingeräumt werden.
2. DSB müssen in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden werden. Sie führen das Verfahrensverzeichnis (§ 4g Abs. 2 BSDG) und haben hierfür die erforderlichen Unterlagen zu erhalten.
3. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde haben die verantwortlichen Stellen den DSB die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Bei der Bestellung von externen DSB kann die Fortbildung Bestandteil der vereinbarten Vergütung sein und muss nicht zusätzlich erbracht werden.
4. Internen DSB muss die erforderliche Arbeitszeit zur Erfüllung ihrer Aufgaben und zur Erhaltung ihrer Fachkunde zur Verfügung stehen. Bei Bestellung eines externen DSB muss eine bedarfsgerechte Leistungserbringung gewährleistet sein. Sie muss in angemessenem Umfang auch in der beauftragenden verantwortlichen Stelle selbst erbracht werden. Ein angemessenes Zeitbudget sollte konkret vereinbart und vertraglich festgelegt sein.
5. Die verantwortlichen Stellen haben DSB bei der Erfüllung ihrer Aufgaben insbesondere durch die zur Verfügung Stellung von Personal, Räumen, Einrichtung, Geräten und Mitteln zu unterstützen (§ 4f Abs. 5 BDSG).

7.6.4 Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste

Gegenwärtig wird über die Umsetzung der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikationsdienste („ePrivacy Directive“) in nationales Recht beraten, die bis zum 24. Mai 2011 abgeschlossen sein muss. Die Richtlinie enthält in ihrem Artikel 5 Absatz 3 eine Regelung, die die datenschutzrechtlichen Voraussetzungen auch beim Umgang mit „cookies“ neu festlegt: Die bisherige Opt-Out-Lösung wird durch eine Opt-In-Lösung mit einer vorherigen umfassenden Information über die Zwecke der Verarbeitung ersetzt. Durch die Änderung der Richtlinie wird nun eine Anpassung des Telemediengesetzes hin zu einer informierten Einwilligung erforderlich, da im geltenden Telemediengesetz eine Widerspruchslösung umgesetzt ist (§ 15 Abs. 3 TMG).

Eine solche Änderung stößt auf erhebliche Widerstände auf Seiten des zuständigen Ministeriums, das eine Einwilligungslösung schon durch die in § 12 Abs. 1 und 2 TMG definierten allgemeinen Grundsätze realisiert sieht. Würde man dieser Auslegung folgen, müsste eine „alte“ Vorschrift zukünftig in „neuer“, zudem auch strengerer Weise ausgelegt und angewendet werden. Dies wäre nur schwer vermittelbar und möglicherweise kaum durchsetzbar.

Die Datenschutz-Aufsichtsbehörden betrachten bei ihrer Kontroll- und Aufsichtstätigkeit im Bereich der Telemedien § 15 Abs. 3 TMG als einschlägig für die Verwendung von „cookies“ in diesem Zusammenhang. Demnach sind Nutzungsprofile nur unter Verwendung eines Pseudonyms und vorbehaltlich eines Widerspruchs des Betroffenen zulässig. Nutzungsprofile werden in der Regel mit Hilfe von „cookies“ erstellt, die im „cookie“ gespeicherte eindeutige Identifikationsnummer (cookie-ID) wird entsprechend als Pseudonym angesehen. Diese Auslegung hat sich in der Praxis bewährt und wird allgemein anerkannt.

Die Umsetzung der „ePrivacy Directive“ erfordert daher eine gesetzliche Anpassung des TMG.

8. Adressen der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich und der Landesbeauftragten für den Datenschutz [3]

Bundesland	Aufsichtsbehörde	Landesbeauftragte/r für Datenschutz
Baden-Württemberg	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

[3] Die hier aufgeführten Links verweisen 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	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 Europaangelegenheiten Franz-Josef-Röder-Straße 21 66119 Saarbrücken Telefon: 0681 501-00 Telefax: 0681 501-2699 datenschutz@innen.saarland.de http://www.innen.saarland.de	Die Landesbeauftragte 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 **Hinweis:** Voraussichtlich ab 02.06.2011 als „Unabhängiges Datenschutzzentrum Saarland“ auch zuständige Aufsichtsbehörde
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	

Bundesland	Aufsichtsbehörde	Landesbeauftragte/r für Datenschutz
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
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

9. Links[4]

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

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

[4] Die Links verweisen mit Ausnahme desjenigen zum Angebot des Ministerium für Inneres und Europaangelegenheiten 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.

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

Datenschutzfreundliche Metasuchmaschinen für tracking-freies Suchen im Internet
www.ixquick.com
www.startpage.com
www.startingpage.com

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

Zentralarchiv für Tätigkeitsberichte des Bundes- und der Landesdatenschutzbeauftragten und der Aufsichtsbehörden für den Datenschutz
http://www.th-mittelhessen.de/zaftda/