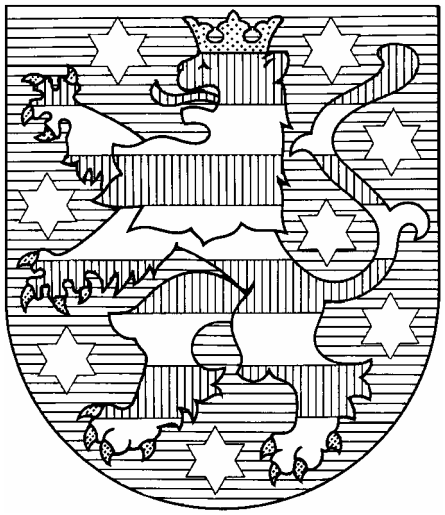

5. TÄTIGKEITSBERICHT DER AUFSICHTSBEHÖRDE FÜR DEN DATENSCHUTZ IM NICHT-ÖFFENTLICHEN BEREICH DES FREISTAATES THÜRINGEN

Berichtszeitraum

1.1.2009 - 31.12.2010

VORGELEGT VON

DER AUFSICHTSBEHÖRDE

FÜR DEN DATENSCHUTZ

IM NICHT-ÖFFENTLICHEN BEREICH

IM

THÜRINGER LANDESVERWALTUNGSAMT

Inhaltsverzeichnis

1. Vorbemerkungen zum fünften Tätigkeitsbericht

Im Berichtszeitraum 2009/2010 sind einige Veränderungen eingetreten, die die Arbeit in den meisten Aufsichtsbehörden beeinflussen werden, die aber auch Neuerungen für den Bürger, für jeden Einzelnen von uns, haben werden.

Der Europäische Gerichtshof hat eine wegweisende Entscheidung in Sachen Unabhängigkeit der Aufsichtsbehörden getroffen und der Deutsche Bundestag hat drei Änderungen des Bundesdatenschutzgesetzes in Kraft gesetzt. Dabei steht die grundsätzliche (Neu-)Regelung zum Beschäftigtendatenschutz noch aus.

Die Persönlichkeitsrechte der Bürgerinnen und Bürger sind zwar gestärkt worden. Dennoch gilt es darauf zu achten, dass mit den eigenen personenbezogenen Daten sparsamer als bisher umgegangen werden muss, um den „gläsernen Bürger“ zu verhindern. Die Daten, die von vielen – vornehmlich jüngeren – Bürgern ins weltweite Netz eingestellt werden, entwickeln schnell ein Eigenleben und die Verwendung durch Dritte ist nicht mehr beherrschbar.

Seit Mai 2001 sind die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich nach § 38 Abs. 1 Satz 7 BDSG verpflichtet, regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen. Der vorliegende Bericht umfasst die Zeit vom 1. Januar 2009 bis zum 31. Dezember 2010.

Er gibt einen Überblick über die im Berichtszeitraum wahrgenommenen Aufgaben der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich im Freistaat Thüringen. Er stellt Lösungen für datenschutzrechtliche Fallgestaltungen vor und gibt Empfehlungen für datenschutzgerechtes Verhalten insbesondere bei privaten Wirtschaftsunternehmen, Vereinen, Verbänden und freiberuflich Tätigen.

Das Thüringer Landesverwaltungsamt ist mit seiner Internetpräsentation als zuständige Aufsichtsbehörde für den Datenschutz bei den nicht-öffentlichen Stellen im Freistaat Thüringen erreichbar unter:

http://www.thueringen.de/de/tlvwa/fachabteilungen/inneres/hoheitsangelegenheiten_gefahrenabwehr/datenschutz/taetigkeitsberichte/content.html

Alle Tätigkeitsberichte stehen im Internet unter gleicher Adresse mit Links auf die entsprechenden Berichtszeiträume zur Verfügung.

Weiterhin finden Sie unter http://www.thm.de/zaftda/index.php alle bisher veröffentlichten Tätigkeitsberichte der Landesbeauftragten für den Datenschutz und der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich.

2. Allgemeines

2.1 Urteil des Europäischen Gerichtshofs zur Unabhängigkeit der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 09. März 2010

Der Europäische Gerichtshof hat in seinem Urteil vom 09. März 2010 festgestellt, dass die Bundesrepublik Deutschland gegen Artikel 28 Absatz 1 Unterabsatz 2 der EU-Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 verstoßen hat, indem sie die für die Überwachung der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt und damit das Erfordernis, dass diese Stellen ihre Aufgaben „in völliger Unabhängigkeit“ wahrnehmen, nicht europarechtskonform umgesetzt habe. Die Entscheidung zwingt dazu, die Datenschutzaufsicht über die Privatwirtschaft in einigen Bundesländern neu zu strukturieren. Um das Urteil des Gerichtes umzusetzen, müssen daher Änderungen bei der organisatorischen Stellung der Datenschutzaufsichtsbehörden vorgenommen werden. Eile scheint geboten, da das Gericht die Verhängung von Bußgeldern angekündigt hat, falls die Unabhängigkeit der Aufsichtsbehörden nicht zügig hergestellt werde.

Mit der Neuregelung des Datenschutzes im Freistaat Thüringen auf der Grundlage des Gesetzes zur Änderung des Thüringer Datenschutzgesetzes und anderer Vorschriften will die Thüringer Landesregierung die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich, die bislang beim Thüringer Landesverwaltungsamt angesiedelt ist, auf den Thüringer Landesbeauftragten für den Datenschutz übertragen. Die Aufsicht soll dort mit der Aufsicht über den öffentlichen Bereich im Freistaat Thüringen zusammengelegt werden. Die Zusammenlegung der Zuständigkeiten beseitigt die bisherigen Unsicherheiten der Bürgerinnen und Bürger im Freistaat Thüringen bei der Suche nach dem richtigen Ansprechpartner für datenschutzrechtliche Belange gleich welcher Art. Mit dem Thüringer Landesbeauftragten für den Datenschutz steht ihnen künftig ein Ansprechpartner für Anfragen, Eingaben und Beschwerden zur Verfügung. Die datenschutzrechtliche Fachkompetenz wird mit allen Befugnissen der Datenschutzaufsicht bei einer Stelle gebündelt. Problemlösungen im Umgang mit Daten erfolgen künftig aus einer Hand. Die bisherige

zweigleisige Bearbeitung je nach öffentlichem oder privatem Ausgangspunkt mit allen sich daraus ergebenden Abgrenzungsfragen entfällt. Dies vermag insbesondere auch dazu beizutragen, länderübergreifend den Informationsaustausch der Datenschutzaufsichtsbehörden zu optimieren und die Abstellung und Ahndung datenschutzrechtlicher Verstöße zu beschleunigen.

2.2 Neuregelungen im Bundesdatenschutzgesetz

Zum Ende der letzten Legislaturperiode wurden im Bundestag folgende Änderungen des Bundesdatenschutzgesetzes beschlossen:

- BDSG-Novelle I: Gesetz vom 29.07.2009, BGBl. I S. 2254; trat am 01.04.2010 in Kraft,
- BDSG-Novelle II: Gesetz vom 14.08.2009, BGBl. I S. 2814; trat weitestgehend am 01.09.2009 in Kraft mit Übergangsregelungen in § 47 (§ 34 Abs. 1a, Abs. 5 und § 43 Abs. 1 Nr. 8a BDSG neuer Fassung traten am 01.04.2010 in Kraft),
- BDSG-Novelle III: Gesetz vom 29.07.2009, BGBl. I S. 2355; trat am 11.06.2010 in Kraft.

2.2.1 BDSG-Novelle I

Die BDSG-Novelle I umfasst Neuregelungen, die die Datenübermittlung an Auskunfteien (§ 28 a BDSG), das sogenannte Scoring, d.h. die Berechnung und Verwendung mathematisch-statistischer Wahrscheinlichkeitswerte zur Erstellung von Verhaltensprognosen (§ 28 b BDSG) sowie Auskunfts- und Informationsrechte des Betroffenen gegenüber Auskunfteien und sonstigen verantwortlichen Stellen betreffen.

2.2.2 BDSG-Novelle II

Die Novelle II beinhaltet vor allem Änderungen im Zusammenhang mit der Werbung und der Markt- und Meinungsforschung sowie zum Arbeitnehmerdatenschutz.

Für den betrieblichen Datenschutzbeauftragten wurde in § 4 f Abs. 3 BDSG ein Kündigungsschutz installiert, ebenso ein Recht auf Teilnahme an Fort- und Weiterbildungsveranstaltungen.

Mit § 28 Abs. 3 und 4 BDSG wurde die Datenverarbeitung zum Zwecke der Markt- und Meinungsforschung sowie der Werbung neu geregelt. Es gilt als Grundsatz das Einwilligungserfordernis der Betroffenen, wobei unter bestimmten Voraussetzungen von diesem Grundsatz abgewichen werden kann.

Mit dem § 32 BDSG ist eine Regelung zum Schutz von Arbeitnehmerdaten aufgenommen worden, ohne dass dadurch ein Arbeitnehmerdatenschutzgesetz entbehrlich geworden ist.

Eine Informationspflicht der Betroffenen und der Aufsichtsbehörde anlässlich von Datenpannen oder vorsätzlichem Datenmissbrauch ist in einem neuen § 42 a festgelegt worden.

Die Befugnisse der Aufsichtsbehörde sind durch die Erweiterung der Anordnungs- und Untersagungsrechte in § 38 Abs. 5 BDSG sowie der Ausdehnung des Bußgeldkatalogs und der Erhöhung des Bußgeldrahmens auf 50.000 EURO in § 43 Abs. 1 bzw. 300.000 EURO in § 43 Abs. 2 BDSG vergrößert worden.

2.2.3 BDSG-Novelle III

Mit dieser Novelle wurde Artikel 9 der Verbraucherkreditrichtlinie umgesetzt, wonach Betroffene unter bestimmten Voraussetzungen einen Anspruch auf Information über abgelehnte Datenbankabfragen (§ 29 Abs. 6 und 7 BDSG) haben. Der Anspruch besteht nur, wenn der Abschluss eines Verbraucherdarlehensvertrages (§ 491 Abs. 1 BGB) oder eines Vertrages über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft abgelehnt wird.

3. Überblick über die Zuständigkeiten und Aufgaben der Aufsichtsbehörde im nicht-öffentlichen Bereich

3.1 Zuständigkeiten

Nach § 38 Abs. 6 BDSG haben die Landesregierungen oder die von ihnen ermächtigten Stellen die für die Kontrolle der Durchführung des Datenschutzes im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden zu bestimmen.

Das Thüringer Innenministerium hat nach § 5 der Thüringer Verordnung zur Bestimmung von Zuständigkeiten im Geschäftsbereich des Thüringer Innenministeriums vom 15. April 2008 (GVBl. S. 102) das Thüringer Landesverwaltungsamt als zuständige Aufsichtsbehörde nach § 38 Abs. 6 BDSG bestimmt.

3.1.1 Örtliche Zuständigkeit

Die örtliche Zuständigkeit des Thüringer Landesverwaltungsamtes ist immer dann gegeben, wenn sich die nicht-öffentliche Stelle, d. h. der Sitz des Unternehmens/der Einrichtung bzw. deren Niederlassung oder Betriebsstätte im Freistaat Thüringen befinden.

Es ist aber zu beachten, dass bei Sachverhalten, die grundsätzlicher Art sind bzw. das Gesamtunternehmen betreffen, die für den Hauptsitz des Unternehmens zuständige Aufsichtsbehörde tätig werden muss. Bezieht sich eine Maßnahme auf eine Verwendung oder Verarbeitung von Daten, die lediglich eine Niederlassung berühren, so ist die Aufsichtsbehörde zuständig, in deren Bereich diese Niederlassung liegt.

Wird eine Beschwerde bei einer unzuständigen Behörde eingereicht, wird sie von dort an die zuständige Behörde weitergereicht und der Beschwerdeführer wird über die Weiterleitung seines Schreibens informiert.

Ergibt sich erst im Laufe des Verfahrens, dass eine andere Aufsichtsbehörde zuständig ist, wird der Vorgang von der bisher tätigen Behörde an die tatsächlich zuständige Behörde abgegeben.

3.1.2 Sachliche Zuständigkeit

Nach § 38 Abs. 1 BDSG überprüfen und überwachen die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich die Ausführungen des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz durch die nicht-öffentlichen Stellen. Nicht-öffentliche Stellen sind vor allem privatrechtliche Einrichtungen, wie beispielsweise Banken, Versicherungen, Industrie- und Dienstleistungsunternehmen aber auch sonstige Gesellschaften, Vereine und Stiftungen. Ebenfalls davon betroffen sind freiberuflich Tätige, wie etwa Ärzte, Apotheker und Architekten.

Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen diese Vorschriften denen des BDSG vor. Das heißt, sofern es Regelungen gibt, die den Datenschutz in Spezialgesetzen betreffen, sind auch die dort genannten Stellen/Behörden für deren Einhaltung zuständig.

Der Datenschutz bei den staatlichen Stellen, also Behörden, öffentlichen Einrichtungen und Kommunalverwaltungen in Thüringen wird hier nicht angesprochen. Die datenschutzrechtliche Kontrolle für diesen Bereich obliegt dem Thüringer Landesbeauftragten für den Datenschutz.

3.2 Aufgaben

Die Tätigkeit der Aufsichtsbehörde wird im Wesentlichen durch folgende Aufgaben bestimmt:

- Beantwortung allgemeiner Anfragen zum Datenschutz
- Bearbeitung von Eingaben und Beschwerden
- Beratung und Unterstützung von betrieblichen Datenschutzbeauftragten (§ 4 g Abs. 1 S. 2 BDSG)
- Beratung von nicht-öffentlichen Stellen bei geplanten Vorhaben, die den Datenschutz berühren
- Durchführung von Vor-Ort-Kontrollen nach Eingaben und Beschwerden
- Kontrolle der Rechtmäßigkeit der Datenverarbeitung, auch ohne konkreten Anlass (§ 38 Abs. 1 S. 1 BDSG)
- Anordnung von Maßnahmen bei festgestellten Datenschutzverstößen in den Unternehmen und Einrichtungen und Kontrolle der Umsetzung
- Durchführung von Ordnungswidrigkeitenverfahren
- Stellung von Strafanträgen
- Führung des öffentlichen Registers der meldepflichtigen Verarbeitungen mit personenbezogenen Daten (§ 38 Abs. 2 BDSG)

4. Anlassfreie Kontrollen des Datenschutzes in Unternehmen und Einrichtungen

Nach § 38 Abs. 1 Satz 1 BDSG kontrolliert die Aufsichtsbehörde die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln.

Somit hat die Aufsichtsbehörde eine Rechtsgrundlage, auf die sie Kontrollen zum Datenschutz ohne konkreten Anlass bei allen nicht-öffentlichen Stellen, die personenbezogene Daten

- für ihre eigenen geschäftlichen Zwecke
- als Auftragnehmer in Dienstleistung
- zum Zwecke der Übermittlung
- zum Zwecke der anonymisierten Übermittlung

verarbeiten oder nutzen, stützen kann.

Es handelt sich hierbei um Kontrollen, bei denen die Belange des Datenschutzes und der Datensicherheit in einem Unternehmen oder Betrieb auf den Prüfstand gestellt werden. Diese Kontrollen können auf schriftlichem Weg, online oder vor Ort durchgeführt werden.

Dabei ist eine flächendeckende Durchführung von Kontrollen durch die Aufsichtsbehörde weder vom BDSG gewollt noch möglich. Vielmehr wird davon ausgegangen, dass bereits eine interne Kontrolle durch die betrieblichen Datenschutzbeauftragten in den einzelnen Unternehmen einen nicht unerheblichen Beitrag zum Schutz des informationellen Selbstbestimmungsrechtes leistet. Dadurch nehmen die Daten verarbeitenden Stellen die ihnen im Datenschutzrecht zukommende Selbstverantwortung wahr.

4.1 Kontrollen nach § 38 Abs. 1 BDSG als Vor-Ort-Kontrollen

Vor-Ort-Kontrollen stellen eine Überprüfung der Einhaltung des Datenschutzes in größerem Umfange dar. Dabei ist die Möglichkeit des Kontrollumfanges breit gefächert und umfasst die Überprüfung der Verpflichtungen der Einrichtung zur Durchsetzung des Datenschutzes von der

- formal-rechtlichen Seite des BDSG (Meldepflicht nach § 4 d, Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten nach § 4 f und § 4 g, Verpflichtung der Mitarbeiter auf das Datengeheimnis nach § 5, Einhaltung des Prinzips von Datenvermeidung und Datensparsamkeit nach § 3 a)

und

- von der Seite der EDV-technischen Ausstattung (Hardware und Software) sowie der technisch-organisatorischen Maßnahmen nach § 9 BDSG (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Eingabekontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungsgebot).

Die Durchführung anlassfreier Kontrollen bei den verantwortlichen Stellen vor Ort war im Berichtszeitraum aufgrund des hohen Arbeitsanfalles insbesondere im Bereich der Videoüberwachung nicht möglich.

4.2 Kontrollen nach § 38 Abs. 1 BDSG durch schriftliches Verfahren

Neben der Vor-Ort-Kontrolle kann eine Kontrolle über die Ausführung des Datenschutzgesetzes auch durch ein schriftliches Verfahren erfolgen. Der Arbeitsaufwand für eine Kontrolle durch schriftliches Verfahren ist geringer als bei den Vor-Ort-Kontrollen, da die Vorbereitung, die Durchführung und die Auswertung gleichzeitig für eine größere Anzahl von Einrichtungen gestaltet werden können.

Erfahrungen bei diesen Kontrollen im vorangegangenen Berichtsraum haben auch gezeigt, dass eine solche komplexe Aktion recht schnell in der gesamten Branche zur Kenntnis genommen wird und damit zur Sensibilisierung des Problemkreises Datenschutz beiträgt.

Es ist daher zweckmäßig ein solches Kontrollverfahren regelmäßig durchzuführen.

5. Beratungstätigkeit und Anfragen an die Behörde

Im Nachgang zu den öffentlich gewordenen Datenschutzskandalen, die sich in der verschiedenartigen Überwachung von Mitarbeitern sowie den bekannt gewordenen Datendiebstählen durch Hacker dokumentierten, hat in weiten Teilen der Bevölkerung eine Sensibilisierung für den Datenschutz eingesetzt, obwohl für viele Bürger das Thema Datenschutz immer noch nur mit dem Computer in Verbindung gebracht wird.

Das Interesse für den Datenschutz dokumentiert sich in der gestiegenen Anzahl der eingegangenen Anfragen. Waren es im Berichtszeitraum 2005/2006 63 Anfragen, die schriftlich an die Aufsichtsbehörde gestellt wurden, so ist diese Zahl im Zeitraum 2007/2008 zwar auf 52 gesunken. Aber in den darauffolgenden Jahren 2009/2010 ist sie dann auf 90 gestiegen.

Davon wurden die meisten Anfragen von Bürgern gestellt. Die Anfragen, die von betrieblichen Datenschutzbeauftragten gestellt wurden, machen demgegenüber nur einen geringen Teil aus. Aber auch der Austausch mit den anderen Aufsichtsbehörden findet teilweise auf diesem Wege statt.

Im Einzelnen haben sich dabei die folgenden Schwerpunkte ergeben, die kaum von denen der vorhergehenden Berichtszeiträume abweichen:

a) Anfragen von Bürgern

- Umgang mit Beschäftigtendaten
- Fragebogen mit persönlichen Daten von Pflegebedürftigen
- Ärztliche Schweigepflicht
- Betriebsvereinbarung zu Personalbeurteilungsbögen
- Anfrage zur Herkunft von persönlichen Daten, die zu Werbezwecken genutzt werden
- Meldung von Datenpannen nach § 42 a BDSG

b) Beratungstätigkeit für Einrichtungen und Unternehmen:

- Externer Datenschutzbeauftragter für eine Arztpraxis
- Ausbildung zum externen Datenschutzbeauftragten
- Anfragen zu Formularen und Fragebögen im Bereich des Datenschutzes
- Anfragen zu Merkblättern und Personalbögen

6. Anlasskontrollen nach Eingaben und Beschwerden

6.1 Allgemeine Übersicht

Neben allgemeinen Anfragen zum Datenschutz sind Eingaben und Beschwerden ein Indiz dafür, dass die Bürgerinnen und Bürger für das Problem des Umganges mit ihren eigenen personenbezogenen Daten und deren Schutz sensibilisiert sind. Hierzu wird eingeschätzt, dass sich dieses Bewusstsein in Thüringen auch in diesem Berichtszeitraum weiterentwickelt hat.

Im Berichtszeitraum 2009 / 2010 wurden insgesamt 128 schriftliche Eingaben und Beschwerden registriert und bearbeitet, bzw. an die zuständigen Behörden weitergeleitet, wenn unsere Zuständigkeit nicht gegeben war.

Vergleichend mit den Zahlen der zurückliegenden Jahre ist eine weitere Zunahme um 19 Vorgänge zu verzeichnen.

In 27 Fällen war eine Zuständigkeit der Aufsichtsbehörde Thüringens letztlich nicht gegeben. Vielmehr waren entweder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der Thüringer Landesbeauftragte für den Datenschutz oder Aufsichtsbehörden anderer Bundesländer zuständig.

Von den 101 Eingaben und Beschwerden im Berichtszeitraum, die zuständigkeitshalber bearbeitet worden sind, wurde in 45 Fällen ein Datenschutzverstoß festgestellt.

Der Umstand, dass trotz größerer Zahl von Beschwerden im Vergleich zum vorherigen Berichtszeitraum die Zahl der festgestellten Datenschutzverstöße von 52 auf 45 gesunken ist, veranschaulicht eine zunehmende Sensibilisierung sowohl der Bürger als auch der verantwortlichen Stellen beim Thema Datenschutz.

Auf die festgestellten Verstöße wurde in angemessener Weise und in kurzer Zeit durch die verursachenden Stellen reagiert und diese dann auch abgestellt.

Bei den berechtigten Eingaben und Beschwerden handelte es sich u.a. um folgende Problemkreise:

- Umgang mit Bewerbungsunterlagen
- Unverlangte E-Mail-Werbung
- Unzulässige Datenübermittlungen
- Erhebung von Kundendaten durch Kopieren des Personalausweises
- Fehlende Hinweise auf Widerspruchsrechte
- Umgang mit Vereinsdaten
- Videoüberwachung öffentlich zugänglicher Bereiche
- Videoüberwachung im persönlichen Bereich
- Umgang mit Patientendaten
- Info-Schreiben von Kabelnetzbetreibern

Im Verlauf der Berichtszeiträume hat es sich herausgestellt, dass sich die Problemkreise, zu denen schwerpunktmäßig Eingaben und Beschwerden eingehen, kaum verändern.

6.2 Bußgeld- und Strafverfahren

6.2.1 Bußgeldverfahren

Im Berichtszeitraum wurden 2 Bußgeldverfahren jeweils mit dem Erlass eines Bußgeldbescheides abgeschlossen.

6.2.1.1 Einem Bußgeldverfahren, das nach Rücknahme des Einspruches nach Verhängung eines Bußgeldes in Höhe von 500 € bestandskräftig abgeschlossen wurde, lag folgender Sachverhalt zugrunde:

Eine Mitarbeiterin eines Unternehmens aus dem Gesundheitsbereich teilte uns mit, dass auf einer Personalversammlung eine Liste ausgelegt worden sei, aus der die Anzahl der Krankentage der einzelnen Mitarbeiter einzusehen war. Jede an der

Versammlung teilnehmende Person habe die Anzahl der Krankentage der Mitarbeiter nachlesen können.

Bei den Daten zur Dauer einer Krankheit handelt es sich um personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG der Beschäftigten nach § 3 Abs. 11 BDSG. Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten der Beschäftigten sind nach § 32 BDSG nur zulässig, wenn dies zur Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach dessen Begründung für dessen Durchführung oder Beendigung erforderlich ist.

Das Auslegen einer Liste mit den Krankheitstagen der Mitarbeiter auf der Personalversammlung stellte ein unzulässiges Übermitteln personenbezogener Daten dar, da es an einer Rechtsgrundlage für das Offenlegen der Krankheitstage gefehlt hat. Dadurch wurde der Tatbestand des unbefugten Verschaffens von personenbezogenen Daten, die nicht allgemein zugänglich sind, i.S.d. § 43 Abs. 2 Nr. 3 BDSG verwirklicht.

Die verantwortliche Stelle ließ in der Anhörung durch ihre Rechtsanwältin mitteilen, dass mitnichten eine Liste mit Namen und genauer Anzahl der Krankheitstage der Mitarbeiter ausgelegt worden sei. Vielmehr sei innerhalb einer Präsentation mit einem Overheadprojektor versehentlich eine nicht anonymisierte Darstellung von Krankentagen der Mitarbeiter ersichtlich gewesen. Nachdem das Versehen bemerkt worden sei, sei die Liste sofort entfernt worden und die Teilnehmer der Personalversammlung hätten nicht die Möglichkeit gehabt, die Liste im Einzelnen durchzugehen.

Diese Schutzbehauptung wurde aber durch die ausführliche Darstellung einer ehemaligen Mitarbeiterin, die an dieser Personalversammlung teilgenommen hatte, widerlegt. Nach Akteneinsicht durch die beauftragte Rechtsanwältin wurde der Einspruch gegen den Bußgeldbescheid zurückgenommen.

6.2.1.2 In einem weiteren Verfahren wurde gegen eine verantwortliche Stelle ein Bußgeld verhängt, weil sie weder eine von uns abgeforderte Stellungnahme abgegeben hatte noch auf unsere folgenden Mahnschreiben reagiert hatte. Nachdem aufgrund des

eingelegten Einspruches der Vorgang an die Staatsanwaltschaft abgegeben worden war, blieb die verantwortliche Stelle dem angesetzten Termin der mündlichen Verhandlung vor dem Amtsgericht ohne genügende Entschuldigung fern, so dass der Einspruch verworfen wurde und unser Bußgeldbescheid in Höhe von 200 € bestätigt wurde.

6.2.2 Strafverfahren

Im Berichtszeitraum wurden 2 Strafanträge nach § 44 Abs. 2 Satz 2 BDSG gestellt und die Akten an die Staatsanwaltschaft weitergeleitet.

6.2.2.1 Das erste Verfahren betraf einen Partnervermittler, der sich in der Wohnung einer Kundin einen entsprechenden Vertrag und drei nicht ausgefüllte Überweisungsträger unterschreiben ließ. Während der kurzzeitigen Abwesenheit der Kundin hat sich der Partnervermittler unbefugt Zugang zu deren Kontodaten verschafft, die Daten in die Überweisungsträger eingetragen und anschließend größere Geldbeträge vom Konto der Kundin abgehoben.

6.2.2.2 Der zweite Vorgang betraf eine Internetseite, auf der eine Vielzahl von Adressdaten (Vor- und Nachname, Straße, Hausnummer sowie Postleitzahl und Wohnort) aufgelistet waren. Die Daten stammten aus der Kundendatei eines Bekleidungsgeschäftes und waren durch einen Hackerangriff in die Hände der verantwortlichen Stelle gelangt. Die Zusatzinformationen waren zweifellos in der Absicht auf der Internetseite platziert worden, um die Betroffenen, deren Adressdaten veröffentlicht worden waren, zu schädigen.

Da der Betreiber der Internetseite nicht ermittelt werden konnte – der Server stand im Ausland – wurde das Verfahren schließlich durch die Staatsanwaltschaft ergebnislos eingestellt.

6.3 Darstellung ausgewählter Einzelbeispiele

6.3.1. Werbung von einem Geldinstitut

Ein ehemaliger Kunde eines Geldinstitutes beschwerte sich darüber, dass er immer noch Werbebriefe von dieser Bank erhalten würde, obwohl er dort kein Kunde mehr sei und obwohl er der Bank bereits mehrfach mitgeteilt habe, dass sie seine Daten löschen sollte.

Dem Geldinstitut wurde von uns mitgeteilt, dass der Wunsch des Petenten, keine Werbeschreiben mehr zu erhalten, als Widerspruch gegen die Nutzung seiner Daten für Zwecke der Werbung anzusehen sei. Daher sei eine weitere Nutzung der Daten nach § 28 Abs. 4 Satz 1 BDSG für diese Zwecke unzulässig. Es habe somit eine Löschung der Daten nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG zu erfolgen. Die Bank wurde auch darauf hingewiesen, dass auch dann eine weitere Nutzung zu Werbezwecken unzulässig sei, wenn gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungspflichten einer Löschung der Daten des Beschwerdeführers zum jetzigen Zeitpunkt entgegenstehen würden. Die Daten seien dann nach § 35 Abs. 3 Nr. 1 BDSG zu sperren.

Die Bank teilte uns daraufhin mit, dass der Beschwerdeführer noch Verträge mit ihren Kooperationspartnern abgeschlossen habe. In Zusammenhang mit dem Abschluss dieser Produkte seien die benötigten personenbezogenen Daten gespeichert worden und sie würden auch bis zur unmittelbaren Abwicklung der Produkte gespeichert bleiben. Ferner habe der Bank bis zum Erhalt unseres Schreibens kein ausdrücklicher Werbewiderspruch vorgelegen.

Sie habe aber mit sofortiger Wirkung eine Werbesperre veranlasst. Aber auf Grund der zum Teil recht langen Vorlaufzeit von bestimmten Werbeprodukten sei nicht auszuschließen, dass der Petent in der nächsten Zeit doch noch Werbung erhalten würde.

Nachdem wir dieses Ergebnis dem Beschwerdeführer mitgeteilt hatten, informierte er uns einige Zeit später darüber, dass er inzwischen alle Verträge mit der Bank bzw. deren Kooperationspartnern gekündigt habe und gleichzeitig verlangte er weiterhin die Löschung seiner Daten.

Die Bank hat dem Begehren auf unser Anschreiben hin dann auch umgehend entsprochen.

6.3.2 Datenverwendung bei Fahrzeugbewertung

Im Rahmen eines außergerichtlichen Verfahrens wurde einer Beschwerdeführerin das Bewertungsergebnis ihres Pkws per Post zugestellt, welche durch ein Autohaus ermittelt worden war. Die Bewertung habe alle relevanten Daten des Fahrzeuges wie Kennzeichen, Fahrzeugnummer, Fahrgestellnummer, km-Stand usw. erhalten. Die Beschwerdeführerin hatte dem Autohaus aber keinen Auftrag zur Fahrzeugbewertung erteilt. Die Bewertung war von ihrem getrennt lebenden Ehemann in Auftrag gegeben worden, der aber keine Vollmacht der Fahrzeughalterin für die Erstellung der Fahrzeugbewertung vorlegen konnte. Auch hatte er weder das Fahrzeug noch die Fahrzeugpapiere in seinem Besitz.

In seiner Stellungnahme führte der Geschäftsführer des Autohauses aus, dass keine Daten weitergegeben worden seien. Auch seien keine gespeicherten Kundendaten für die vom früheren Ehemann in Auftrag gegebene Bewertung des Fahrzeuges der Kundin herangezogen worden. Die Bewertung des Fahrzeuges sei nach den Angaben des früheren Ehemannes über das DAT-System (Deutsche Automobil Treuhand) durchgeführt worden.

Dieser Darstellung wurde aber von der Beschwerdeführerin ernsthaft widersprochen. Bei der Erstellung der Fahrzeugbewertung müsse auf Kundendaten zurückgegriffen worden sein. Bei einer „anonymen“ Bewertung nur über das DAT-System wären die genauen Angaben wie z. B. die Kfz-Ident.-Nr. nicht bekannt gewesen. Dass der von der Beschwerdeführerin seit 1 ½ Jahren getrennt lebende Ehemann die genauen

Fahrzeugdaten habe angeben können, sei nicht nachvollziehbar gewesen. Es müsse daher auf die gespeicherten Kundendaten zurückgegriffen worden sein.

Der Geschäftsführer des Autohauses blieb allerdings bei seiner Darstellung, dass keine Daten des Fahrzeuges der Beschwerdeführerin beim Autohaus gespeichert seien. Vielmehr habe der Ehemann der Petentin dem Verkäufer gegenüber diese Angaben gemacht.

Da das Gegenteil letztlich nicht nachgewiesen werden konnte, wurde der Geschäftsführer des Autohauses eindringlich auf seine Pflichten nach dem Bundesdatenschutzgesetz hingewiesen, insbesondere darauf, dass (auch) künftig keinesfalls auf die beim Autohaus vorhandenen Kundendaten zurückgegriffen werden dürfe, wenn der Auftraggeber des Gutachtens nicht selbst der Eigentümer des zu bewertenden Fahrzeuges sei.

6.3.3 Bewerbungsunterlagen in der blauen Papiertonne

Unserer Behörde wurde schriftlich mitgeteilt, dass in der blauen Papiertonne einer Wohnanlage, die auch von einer unter der gleichen Adresse firmierenden Arbeitsvermittlung mitgenutzt wird, nicht mehr benötigte Bewerbungsunterlagen entsorgt würden. Diese Unterlagen seien von jedem einzusehen, der ebenfalls Papier in diese Tonne einfülle. Da die Tonne nur alle vier Wochen geleert würde, seien die Unterlagen längere Zeit für Jedermann zugänglich.

In seiner Stellungnahme über ein Rechtsanwaltsbüro ließ der Betreiber der privaten Arbeitsvermittlung mitteilen, dass er die anfallenden Kosten innerhalb seines Unternehmens so gering wie möglich halten wolle und daher zur Reinigung der Büroräume familiäre Hilfe in Anspruch nehme. Er habe daher seine Schwester beauftragt, die Räumlichkeiten einmal wöchentlich zu säubern, wobei er sie darauf hingewiesen habe, Unterlagen mit personenbezogenen Daten nicht im normalen Papiermüll zu entsorgen. Dabei sei es jedoch einmalig vorgekommen, dass Unterlagen, die zu entsorgen gewesen seien, versehentlich von seiner Schwester in den normalen Papiermüll gegeben worden seien.

Um dies zukünftig auszuschließen, habe der Arbeitsvermittler einen verschließbaren Aktenschrank erworben, in dem nunmehr sämtliche Unterlagen, welche personenbezogene Daten von Arbeitsuchenden enthalten, aufbewahrt würden.

Sofern Unterlagen nicht mehr benötigt würden, würden diese durch den Arbeitsvermittler persönlich im Reißwolf vernichtet und nur die nach dem Reißwolf verbleibenden Papierschnipsel der Altpapierverwertung zugeführt werden. Ferner sei auch nur der Arbeitsvermittler im Besitz eines Schlüssels für den Aktenschrank.

Der verantwortlichen Stelle ist von der Aufsichtsbehörde der richtige Weg zur Einhaltung der Bestimmungen des Bundesdatenschutzgesetzes aufgezeigt worden. Da weitere Vorkommnisse nicht angezeigt worden sind, ist von der Einleitung eines Bußgeldverfahrens abgesehen worden.

6.3.4 Aufnahme von Personaldaten beim Kauf eines Geschenkgutscheins

Der Aufsichtsbehörde wurde mitgeteilt, dass ein Kunde, der bei einer Tankstelle zwei Geschenkgutscheine erwerben wollte, aufgefordert worden sei, die persönlichen Daten der Gutscheinempfänger wie Name, Adresse und Geburtsdatum anzugeben. Auf seinen Einwand, die Daten aus datenschutzrechtlichen Gründen nicht angeben zu wollen, wurde ihm mitgeteilt, dass ein Erwerb von Geschenkgutscheinen ohne Angabe dieser Daten nicht möglich sei.

Auf unsere Nachfrage, warum beim Kauf von Gutscheinen die Angabe der persönlichen Daten der Gutscheinempfänger erforderlich sei, wurde uns mitgeteilt, dass die von der Betreiberfirma der Tankstellen herausgegebenen Gutscheine ausschließlich an der Tankstelle eingelöst werden können, an der sie auch erworben wurden. Ferner erfülle das Vermerken von Daten des Begünstigten den Zweck einer Personalisierung des Geschenkes. Auch liege der Ausgabe und der Einlösung der betreffenden Gutscheine ein ausschließlich manuelles Verfahren zugrunde. Dementsprechend erfolge bei der Ausgabe keinerlei elektronische Erfassung und bei der Einlösung auch keine elektronische Prüfung.

Die persönlichen Daten des Begünstigten würden in Form des an der Tankstelle verbleibenden Gutscheinabschnittes aufbewahrt. Mit der buchhalterischen Verarbeitung des Gutscheines am Einlösetag würden beide Gutscheinabschnitte vernichtet. Eine darüber hinaus gehende Speicherung erfolge nicht. Es würden auch keine Daten an Dritte weitergegeben. Bei der Einlösung des Gutscheines würde auch keine Kontrolle der Übereinstimmung der Daten mit dem Gutscheininhaber erfolgen. Es fände lediglich ein Abgleich der beiden Gutscheinabschnitte statt. Es seien daher auch keine Konsequenzen zu befürchten, falls der Einlöser des Gutscheines nicht mit dem vom Erwerber angegebenen Empfänger übereinstimmen würde.

Da die in den Gutscheinen eingetragenen persönlichen Daten durch die Mitarbeiter der Tankstelle nicht mittels Datenverarbeitungsanlagen weiterverarbeitet worden sind und die sofortige Vernichtung der Gutscheine nach der Einlösung erfolgt ist, stellte die Eintragung der persönlichen Daten keinen Verstoß gegen datenschutzrechtliche Vorschriften dar.

Der die Gutscheine herausgebende Tankstellenbetreiber wurde von uns aufgefordert, die persönlichen Daten in die Gutscheine nur dann einzutragen, wenn dies vom Kunden ausdrücklich gewünscht werde. Ein Abhängigmachen des Erwerbs eines Gutscheines von der Angabe der persönlichen Daten des Beschenkten wird nicht für zweckmäßig erachtet, zumal bei der Einlösung der Gutscheine keine Personalienfeststellung der einlösenden Person erfolgt. Die Zuordnung des Gutscheines zu dem bei der Tankstelle verbleibenden Abschnitt kann auch anhand der Gutscheinnummer erfolgen. Hierzu werden keine personenbezogenen Daten des Gutscheinempfängers benötigt.

6.3.5 Überwachung der Arbeitnehmer bei einer Autovermietungsfirma

a) durch GPS im Firmenwagen

Ein Außendienstmitarbeiter einer Mietwagenfirma, der den zur Verfügung gestellten Dienstwagen zum Teil auch privat nutzen kann, teilte der Aufsichtsbehörde mit, dass er zufällig erfahren habe, dass der neue Dienstwagen, den er seit kurzem habe, mit einem GPS (Global Positioning System = ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung) -Gerät ausgestattet sei. Sein Arbeitgeber könne ihn damit jederzeit überwachen. Von seinem Arbeitgeber sei er nicht über den Einbau des GPS-Gerätes informiert worden. Er habe inzwischen das Arbeitsverhältnis gekündigt, da er das Vorgehen der Firma als großen Vertrauensverstoß empfinde.

Er bat die Aufsichtsbehörde, den Vorgang datenschutzrechtlich zu überprüfen.

Der nunmehr frühere Arbeitgeber teilte in seiner Stellungnahme mit, dass bei dem betreffenden Mitarbeiter der dringende Verdacht eines Betruges vorgelegen habe. Er sei von anderen Mitarbeitern seiner Firma informiert worden, dass der betreffende Außendienstmitarbeiter entgegen seiner Darstellung und den Nachweisen für Privatfahrten und Dienstfahrten erheblich mehr Privatfahrten mit dem Dienstwagen unternehmen würde als er angegeben habe. Auch habe der Verdacht bestanden, dass dieser Mitarbeiter während seiner Arbeitszeit nicht seinen vorgegebenen Verpflichtungen nachkomme sondern auch während dieser Zeit noch private Wege erledigen würde. Aus diesem Grund habe man sich entschlossen, für die begrenzte Dauer von fünf Tagen die dienstlichen Aktivitäten nachzuverfolgen. Nach diesen fünf Tagen sei der Zugriff auf das Auswertungsportal für alle Personen gesperrt worden. Die Auswertung der Fahrzeugortung habe ergeben, dass der Anfangsverdacht begründet war.

Die Erhebung der Daten des Mitarbeiters durch die zeitweise Überwachung des Firmenfahrzeuges mittels GPS wurde von uns als datenschutzrechtlich zulässig erachtet, da sie nach den Ausführungen des Arbeitgebers auf Grund eines vorliegenden Verdachts einer Arbeitspflichtverletzung erfolgte. Jedoch wurde dem

Arbeitgeber empfohlen, zukünftig eine eventuell zugelassene private Nutzung eines Firmenfahrzeuges durch vertragliche Regelungen genau festzulegen. Erst dann lässt sich eine unzulässige private Nutzung eines Firmenfahrzeuges feststellen.

6.3.5 Überwachung der Arbeitnehmer bei einer Autovermietungsfirma
b) durch Videokameras in den Büroräumen

In gleichem Schreiben wurde uns mitgeteilt, dass in den Büroräumen Videokameras installiert seien. Angeblich seien die Kameras nicht in Betrieb. Dies sei aber nicht genau bekannt. Jedenfalls seien keine Hinweisschilder auf eine mögliche Videoüberwachung in den Büroräumen angebracht.

Auch in diesem Fall wurde um eine datenschutzrechtliche Überprüfung gebeten.

Der Geschäftsführer der angeschriebenen Firma teilte uns in der angeforderten Stellungnahme mit, dass sich die Kameras in den öffentlich – auch von den Kunden – zugänglichen Räumen befinden würden. Die Kameras seien aufgrund von internen Kassendiebstählen durch Mitarbeiter installiert worden. Anzeigen wegen der Diebstähle seien bei der Polizei erfolgt. Weiterhin würden die Kameras dazu dienen, Zahlungen von Kunden an Mitarbeiter nachzuweisen, da hier des öfteren Unregelmäßigkeiten vorgekommen seien. Die Aufzeichnungen würden nach ca. einem Monat automatisch gelöscht bzw. überschrieben.

In unserer Antwort haben wir darauf hingewiesen, dass es ausnahmsweise zulässig sei, Daten von Beschäftigten mittels einer Videoüberwachungsanlage zu erheben, wenn dies zur Aufdeckung von Straftaten erforderlich sei. Jedoch sind vor dem Einsatz einer solchen Anlage alle anderen arbeitsorganisatorischen Maßnahmen wie z.B. Zutrittsbeschränkungen zu bestimmten Bereichen, Bestimmung von Zuständigkeiten und eventuell eine neue Kassenorganisation zu prüfen. Erst wenn diese arbeitsorganisatorischen Maßnahmen ausgeschöpft seien und trotzdem noch gravierende Kassendifferenzen bestehen, die den Verdacht einer Straftat begründen, ist eine Videoüberwachung für einen begrenzten Zeitraum zur Klärung dieser Angelegenheit erlaubt. Die Überwachung setzt aber voraus, dass alle Mitarbeiter

über den Grund des Einsatzes und den Standort der Kamera informiert sind. Eine heimliche Überwachung der Mitarbeiter ist unzulässig. Da sich die Kamera in einem auch für Kunden zugänglichen Raum befinden würde, hätte für diese ein sichtbarer Hinweis auf die Videoüberwachung angebracht werden müssen.

Die Videoüberwachung war einzustellen und die Kameras mussten entfernt werden.

6.3.6 Aushang privater Handy-Nummern im Betrieb

Ein Mitarbeiter eines mittelständischen Unternehmens (ohne Betriebsrat) mit ca. 250 Beschäftigten, das Teile für die Automobilindustrie liefert, wandte sich mit folgendem Anliegen an uns:

Seit die Firma einen neuen Geschäftsführer hat, werden die privaten Telefonnummern von einigen Mitarbeitern aus verschiedenen Abteilungen, auch vom Beschwerdeführer, an Aushängetafeln in der Firma jedermann, der an den Tafeln vorbeikommt, kundgetan. Es wurde weder in der Firma über den Aushang allgemein informiert noch wurde die Zustimmung der betroffenen Mitarbeiter zur Veröffentlichung der Telefonnummern eingeholt. Da es in der Firma eine Bereitschaftsnummer gebe, die bei Bedarf angerufen werden könne, sei überhaupt nicht nachzuvollziehen, warum die privaten Telefonnummern veröffentlicht werden mussten.

Der Beschwerdeführer wollte wissen, ob diese Verfahrensweise rechtlich zulässig sei.

Für die Verwendung von personenbezogenen Daten der Arbeitnehmer im Betrieb ist § 32 BDSG einschlägig. Danach darf der Arbeitgeber personenbezogene Daten eines Arbeitnehmers nur nutzen, soweit dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses, für dessen Durchführung oder für die Beendigung des Beschäftigungsverhältnisses erforderlich ist.

Ob die Bekanntgabe von privaten Telefonnummern bestimmter Mitarbeiter an einer Anschlagtafel von dieser Zweckbestimmung erfasst ist, kann ohne detaillierte

datenschutzrechtliche Prüfung nicht festgestellt werden. Hierzu müsste der Arbeitgeber seine betrieblichen Gründe darlegen, die es erforderlich machen, dass die Telefonnummern einzelner Mitarbeiter allen Kollegen bekannt sein müssen. Diese betrieblichen Gründe müssten dann die schutzwürdigen Interessen der Mitarbeiter an der Geheimhaltung ihrer privaten Telefonnummer überwiegen.

Es konnte allerdings dieser interessanten Frage nicht weiter nachgegangen werden, weil der Beschwerdeführer nicht bereit war, uns seinen Arbeitgeber zu nennen, so, dass es für die Aufsichtsbehörde nicht möglich war, die Gründe für die Veröffentlichung der privaten Telefonnummern zu erfragen.

6.3.7 Beschwerde wegen ganz persönlicher Fragen im Fragebogen eines Pflegeheimes

In zwei gleich gelagerten Fällen haben sich Angehörige von pflegebedürftigen Personen an die Aufsichtsbehörde gewandt, weil sie der Meinung waren, die Biographiebögen, die sie von den Pflegediensten zum Ausfüllen erhalten haben, würden zu sehr in die Persönlichkeitsrechte der pflegebedürftigen Person eingreifen, da letztlich sehr persönliche, intime Lebensbereiche und –gewohnheiten abgefragt wurden.

Solche Fragebögen sind in der heutigen Zeit ein fester Bestandteil in der ambulanten und stationären Pflege. Mit der Beantwortung der dort gestellten Fragen soll erreicht werden, dass den pflegebedürftigen Personen eine größtmögliche individuelle Pflege und Betreuung zuteil werden kann. Ohne Zweifel ist die so durchgeführte Frageaktion von Nutzen für den Pflegebedürftigen. Dennoch ist festzustellen, dass eine Vielzahl personenbezogener – teilweise sehr sensibler – Daten (§ 3 Abs. 9 BDSG) erhoben und verarbeitet wird.

Für die Angehörigen besteht keine Pflicht, diese Fragebögen auszufüllen, weder eine gesetzliche noch eine vertragliche. Von daher bedarf es der Einwilligung der pflegebedürftigen Person oder seiner Betreuungsperson.

Nach Rücksprache mit den beiden Pflegediensten haben diese ihren jeweiligen Fragebogen geändert. Dabei wurden Fragen gestrichen, die für die Pflege und Betreuung der Kranken nicht erforderlich waren. Ferner wurde die Freiwilligkeit der Angaben wesentlich stärker hervorgehoben. Auch wurden auf einem Informationsblatt, das dem Fragebogen beigefügt wurde, Hinweise zum Aufbewahrungsort, zur Aufbewahrungsdauer sowie zu den zugriffsberechtigten Personen gegeben. Dabei wurde auch ausdrücklich auf die Möglichkeit hingewiesen, dass einzelne Fragen unbeantwortet bleiben können.

6.3.8 Heimliche Tonaufnahmen bei Verkaufsgesprächen in Elektromarkt

Ein Mitarbeiter eines Fachmarktes hat durch eine Betriebsübernahme einen neuen Arbeitgeber erhalten. Bei diesem Arbeitgeber sei es gängige Praxis, dass Verkaufsgespräche mit Kunden mit einem digitalen Diktiergerät aufgezeichnet würden, ohne die Kunden darüber zu informieren. Er hielt dieses Vorgehen für rechtwidrig und hat daher keine heimlichen Aufnahmen erstellt und dies auch seinem Vorgesetzten mitgeteilt. Dieser habe erwidert, dass der Fachmarkt ein öffentlicher Bereich sei und die Kunden damit rechnen müssten, dass jemand mithört. Im Übrigen sei am Eingang ein Hinweisschild angebracht, dass dieses Objekt „ton– und videoüberwacht“ werde. Deshalb müssten die Kunden nicht noch weiter informiert bzw. gar um Erlaubnis gefragt werden.

Der Mitarbeiter wollte wissen, ob die Aussage der Geschäftleitung zutreffen würde oder ob er richtig gehandelt habe.

Da der Mitarbeiter weder nähere Details noch seinen Arbeitgeber nennen wollte, war nur eine allgemein gehaltene Antwort möglich.

Wer unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt, wird nach § 201 Abs. 1 Satz 1 Strafgesetzbuch (StGB) mit einer Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. Dies stellt einen Straftat dar. Die in einem Verkaufsgespräch angegebenen Daten sind in jedem Fall

nicht für die Öffentlichkeit bestimmt, so dass die Aufzeichnung der Verkaufsgespräche diesen Straftatbestand erfüllt. An der Unzulässigkeit der Aufzeichnung ändert auch ein eventuell am Eingang angebrachtes Schild auf eine Video- und Tonaufzeichnung nichts.

Ob daneben auch ein Verstoß gegen das BDSG vorliegt, lässt sich allerdings nicht pauschal beurteilen. Das BDSG richtet sich gegen die unerlaubte Nutzung personenbezogener Daten eines Betroffenen. Es ist davon auszugehen, dass auch in den Verkaufsgesprächen solche personenbezogenen Daten mit erfasst werden. Die Videoüberwachung ist nach § 6 b BDSG in einem Geschäft zum Beispiel dann zulässig, soweit sie zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

In dem geschilderten Fall war nicht zu erkennen, dass der Arbeitgeber einen Grund hatte, seine Geschäftsräume videoüberwachen zu lassen. Auf jeden Fall waren die Gesprächsaufzeichnungen von keiner Rechtsnorm gedeckt.

Wir haben den Mitarbeiter aufgefordert, unsere Ausführungen seinem Arbeitgeber mitzuteilen und darauf hinzuwirken, dass die Praxis der Gesprächsaufzeichnung umgehend eingestellt wird.

6.3.9 Beschwerde wegen nichtgewährter Akteneinsicht in Patientenakte

Ein ehemaliger Patient, der mehrfach in einem privaten Krankenhaus stationär behandelt worden war, hatte bereits während seiner Aufenthalte in der Klinik um Einsichtnahme in seine Krankenakte gebeten, was ihm allerdings jedes Mal versagt worden war, zum Teil mit Begründungen, die der Petent nicht nachvollziehen konnte.

Auf seine neuerliche Bitte um Auskunft zu bestimmten Untersuchungen aus seiner Patientenakte, wurde er aufgefordert eine Vorauszahlung von knapp 10 EURO für die anfallenden Kopierkosten zu überweisen.

Das Recht der Einsichtnahme in die Patientenakte als besondere Form der Auskunftserteilung nach § 34 BDSG beruht nicht nur auf dem Datenschutzrecht bzw. dem „Recht auf Selbstbestimmung und der personalen Würde des Patienten“ (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG) sondern besteht auch als Nebenrecht aus dem Behandlungsvertrag und zivilrechtlich zur Durchsetzung von Rechtsansprüchen.

Eine weitere Rechtsgrundlage für das Recht auf Einsichtnahme in die Krankenhausakte bzw. auf Auskunftserteilung findet sich in § 27 Abs. 8 Thüringer Krankenhausgesetz. Danach steht dem Patienten auf Antrag ein kostenfreies Auskunftsrecht über die zu seiner Person gespeicherten Daten sowie über die Personen und Stellen zu, an die personenbezogene Daten weitergegeben wurden. Eine Beschränkung der Auskunft ist nur hinsichtlich ärztlicher Beurteilungen oder Wertungen zulässig. Die Einsichtnahme darf nicht komplett verweigert werden. Ist die Einsichtnahme nur teilweise möglich, so muss dem Patienten durch Abdecken oder Schwärzen der vorzuenthaltenden Teile Einsicht gewährt werden.

Ort, Zeitpunkt und Umstände der Einsichtsgewährung liegen zwar im Ermessen des Arztes, jedoch bedeutet dies nicht, dass die Einsichtnahme durch die Versendung kostenpflichtiger Kopien aus der Patientenakte ersetzt werden darf. Auch § 34 Abs. 1 sieht – wie § 27 Abs. 8 Thüringer Krankenhausgesetz – die Unentgeltlichkeit der Auskunftserteilung vor.

Im Antwortschreiben der Klinik auf unser Ersuchen um Stellungnahme zeigte sich diese allerdings etwas verwundert über die Einschaltung unserer Behörde. Der Patient habe gegenüber der Klinik die vollständige Kopie seiner Patientenakte gewünscht, was diese aus medizinischen Gründen ablehnen musste. Sie habe daher angeboten, die zur Einsichtnahme zur Verfügung stehenden Teile der Akte zu fotokopieren und ihm zukommen zu lassen. Sie teilte aber auch mit, dass eine Einsichtnahme in der Klinik jederzeit möglich sei. Es bedürfe lediglich einer Terminvereinbarung mit der Klinik, an der es aber nach deren Aussage nicht scheitern würde.

So kam eine Einsichtnahme in die eigene Patientenakte doch noch zustande. Allerdings hätte man dies auch einfacher und ohne Einschalten der Aufsichtsbehörde haben können, wenn die handelnden Personen besser miteinander kommuniziert

hätten und nicht den Kontakt abgebrochen hätten, sobald dem eigenen Ansinnen nicht vollumfänglich entsprochen wurde.

6.3.10 Beschwerde wegen Personalausweiskopie bei Schrottverkauf

Der Aufsichtsbehörde wurde mitgeteilt, dass ein Bürger, der eine kleine Menge Schrott (Wert ca. 20 EURO) an eine Recyclingfirma verkaufen wollte, vor Auszahlung des Kaufpreises seinen Personalausweis vorlegen musste. Dieser sei dann ohne seine Zustimmung beidseitig kopiert worden und die Kopie sei dann für jedermann sichtbar in ein Ablagefach gelegt worden. Auf seine Beschwerde über die Anfertigung der Personalausweiskopie habe die Mitarbeiterin unwirsch reagiert und mitgeteilt, dass sie zur Herstellung der Kopie verpflichtet sei. Dies sei eine Anordnung der Geschäftsleitung.

Die von der Recyclingfirma beauftragten Rechtsanwälte wiesen in ihrem Antwortschreiben an uns darauf hin, dass es sich bei der metall- und schrottverarbeitenden Branche um eine Branche mit zahlreichen Besonderheiten und auch mit einigen „schwarzen Schafen“ handele. Dies habe durch die Finanzbehörden zu einer deutlichen Verschärfung im Hinblick auf gesetzliche Nachweis- und Dokumentationserfordernisse geführt, die u. a. den Grund für die Fertigung von Ausweiskopien beim Ankauf von Metallschrott darstellt. In der Vergangenheit sei es regelmäßig zur Nichtanerkennung von Betriebsausgaben durch die Finanzbehörden gekommen, wenn der Ankäufer (die Recyclingfirma) zur vollständigen Benennung des Verkäufers gemäß § 160 Abgabenordnung (AO) nicht in der Lage gewesen sei. Der Ankäufer müsse nach § 160 AO auf Verlangen der Finanzbehörden den Empfänger von Zahlungen beim Ankauf von Schrott einwandfrei benennen können. Bei unvollständigem Benennungsverlangen durch den Ankäufer werde dieser nicht nur wie ein Haftender für fremde Steuerschulden in Anspruch genommen, sondern es komme zudem zur Aberkennung von Betriebsausgaben. Aus diesem Grunde sei die in Rede stehende Praxis zur Kopie der Personalausweise bei Ankauf von Metallschrott mit der Bundesvereinigung Deutscher Stahlrecycling- und Entsorgungsunternehmen e.V. sowie dem Verband Deutscher Metallhändler abgestimmt und ausdrücklich empfohlen worden. Dabei wurde auch ein Schreiben der o.g. Bundesvereinigung an ihre Mitglieder der

Aufsichtsbehörde vorgelegt, in dem darauf hingewiesen wird, dass der Unternehmer sich im Rahmen der Identitätsfeststellung über Namen und Adressen der Anlieferer anhand von Ausweispapieren zu vergewissern habe. Diese Registrierung könne auf verschiedene Weise erfolgen. Es kommen Kopien, Abschriften und/oder Scanner zum Einsatz.

Es wurde auch vorgetragen, dass die Anfertigung von Personalausweiskopien gemäß § 28 Abs. 1 Nr. 2 BDSG aufgrund der eben dargestellten Sachlage und dem Vorliegen berechtigter Interessen seitens des Ankäufers nicht nur notwendig und aufgrund der Anforderungen der Finanzbehörden erforderlich sondern darüber hinaus auch selbstverständlich zulässig sei. Es stünden dem Interesse der Datenvermeidung und Datensparsamkeit und den Interessen der Verkäufer berechtigte Interessen des Ankäufers gegenüber.

Auf Nachfrage bestätigte die zuständige Landesfinanzdirektion zwar die Aussage, dass zur Benennung des Verkäufers grundsätzlich die Angabe des vollen Namens und der Wohn- bzw. Geschäftsadresse erforderlich sei. Allerdings war sie der gleichen Auffassung wie die Aufsichtsbehörde, dass eine Kopie des Personalausweises im Rahmen des § 160 Abs. 1 Satz 1 AO nicht gefordert werde, da eine Ermittlung des Empfängers bzw. Gläubigers ohne besondere Schwierigkeiten und ohne Zeitaufwand unabhängig von einer zusätzlichen Kopie eines Personalausweises möglich sei.

Diese Darstellung der Landesfinanzdirektion wurde den die Recyclingfirma vertretenden Rechtsanwälten mitgeteilt. Gleichzeitig wurde der für den Sitz der o. g. Bundesvereinigung zuständigen Aufsichtsbehörde deren Schreiben zur Kenntnis gegeben mit der Bitte, auf die Bundesvereinigung einzuwirken, um zu erreichen, dass diese ihren Mitgliedern nicht mehr die Anfertigung von Personalausweiskopien vorschreibt.

Weiterer Handlungsbedarf ist nicht entstanden, da keine weiteren Beschwerden eingegangen sind.

7. Zusammenarbeit mit anderen Aufsichtsbehörden

Die Aufsichtsbehörde stellt immer wieder fest, dass es Betroffenen – insbesondere aufgrund gegebener Unternehmensstrukturen – im Einzelfall kaum möglich ist, die örtlich zuständige Aufsichtsbehörde (die Zuständigkeit richtet sich grundsätzlich nach dem Ort der in Rede stehenden Datenverarbeitung bzw. dem Sitz der verantwortlichen Stelle) zu informieren. Deshalb wenden sich Betroffene oft an die Aufsichtsbehörde im eigenen Bundesland. Bei allgemeinen Anfragen kann die angefragte Aufsichtsbehörde die gewünschten Auskünfte erteilen. Sind jedoch Sachverhaltsermittlungen erforderlich, kann die Aufsichtsbehörde nur die Kontaktdaten der zuständigen Aufsichtsbehörde mitteilen oder gegebenenfalls mit Einverständnis des Betroffenen die Anfrage an die zuständige Aufsichtsbehörde weiterleiten. Niemand sollte bei Bedarf zögern, eine Aufsichtsbehörde – auch bei bestehenden Unsicherheiten über die örtliche Zuständigkeit – zu kontaktieren.

Die Aufsichtsbehörden stimmen sich auch in ihrer Vorgehensweise bei bundesweit auftretenden Problemstellungen ab.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich treffen sich seit 1995 einmal jährlich zu einem Erfahrungsaustausch (Workshop), um eine bundesweit einheitliche Vorgehensweise bei der Umsetzung und Anwendung datenschutzrechtlicher Regelungen abzustimmen und konkret aufgetretene Probleme bei der täglichen Arbeit und Fragestellungen zu besprechen. Diese bundesweite Veranstaltung wird im Wechsel jeweils von einer anderen Aufsichtsbehörde organisiert.

Im Berichtszeitraum erfolgte die Teilnahme an den Workshops 2009 beim damals noch für den nicht-öffentlichen Bereich zuständigen Innenministerium Baden-Württembergs in Stuttgart und 2010 bei dem damals ebenfalls noch zuständigen Innenministerium des Saarlandes in Saarbrücken.

Die im Berichtszeitraum unter Mitwirkung der Aufsichtsbehörde am 24./25. November 2010 gefassten Beschlüsse des „Düsseldorfer Kreises“ – dem Gremium der Vertreter der obersten Aufsichtsbehörden für den Datenschutz, in dem alle Bundesländer vertreten sind – sind unter 8. aufgeführt.

8. Beschlüsse des Düsseldorfer Kreises

8.1. 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 personen-bezogenen 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

§ 4 f 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 datenschutz-rechtliche 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 Betroffenen 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).

8.2. 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 Ange-

bote 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 Bezahlung 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 Nutzem 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

8.3. 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.

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

Baden-Württemberg

Der Landesbeauftragte für den Datenschutz
Baden-Württemberg
Königstraße 10 a
70173 Stuttgart
Telefon: 0711 615541-0
Telefax: 0711 615541-15
poststelle@lfd.bwl.de
http://www.baden-wuerttemberg.datenschutz.de

Bayern

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 (Schloss)
91522 Ansbach
Telefon: 0981 53-1300
Telefax: 0981 53-5300
poststelle@lda.bayern.de
http://www.lda.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

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/

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.datenschutz-hamburg.de/

Hessen

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 Datenschutz
und Informationsfreiheit Mecklenburg-Vorpommern
Schloß Schwerin
Johannes-Stelling-Straße 21
19053 Schwerin
Telefon: 0385 59494-0
Telefax: 0385 59494-58
datenschutz@mvnet.de
http://www.lfd.m-v.de/

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

Landesbeauftragter 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

Saarland

Unabhängiges Datenschutzzentrum Saarland
Fritz-Dobisch-Straße 12
66111 Saarbrücken
Telefon: 0681 94781-0
Telefax: 0681 94781-29
poststelle@datenschutz.saarland.de
http://www.datenschutz.saarland.de

Sachsen

Der Sächsische Datenschutzbeauftragte
Bernhard-von-Lindenau-Platz 1
01067 Dresden
Telefon: 0351 4935-401
Telefax: 0351 4935-490
saechsdsb@slt.sachsen.de
http://www.datenschutz.sachsen.de

Sachsen-Anhalt

Der Landesbeauftragte für den Datenschutz
Sachsen-Anhalt
Leiterstraße 9
39104 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 37-73 7258
Telefax: 0361 37-73 7346
datenschutz@tlvwa.thueringen.de
http://www.thueringen.de/de/tlvwa

Thüringer Landesbeauftragter für den Datenschutz
Jürgen-Fuchs-Straße 1
99096 Erfurt
Telefon: 0361 37 71 900
Telefax: 0361 37 71 904
poststelle@datenschutz.thueringen.de
http://www.thueringen.de/datenschutz/

Bund

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

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

Impressum

Herausgeber:

Aufsichtsbehörde für den Datenschutz
im nicht-öffentlichen Bereich im
Thüringer Landesverwaltungsamt
Weimarplatz 4
99423 Weimar

Postanschrift:
Postfach 22 49
99403 Weimar

Telefon: 0361 37-900
Telefax: 0361 37 73 71 90
E-Mail: datenschutz@tlvwa.thueringen.de
Internet: www.thueringen.de/de/tlvwa