



Datenschutz
im nicht-öffentlichen Bereich
Thüringen
2007/2008

Vierter Tätigkeitsbericht nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) vom 18.05.2001 der für die Überwachung des Datenschutzes bei den nicht-öffentlichen Stellen Thüringens zuständigen Aufsichtsbehörde (Thüringer Landesverwaltungsamt)

Berichtszeitraum: 01.01.2007 bis 31.12.2008

Inhaltsverzeichnis

1.	Vorbemerkungen zum vierten Tätigkeitsbericht	4
2.	Überblick zu den Zuständigkeiten und Aufgaben der Aufsichtsbehörde im nicht-öffentlichen Bereich	4
2.1	Zuständigkeiten	4
2.1.1	Örtliche Zuständigkeit	5
2.1.2	Sachliche Zuständigkeit	5
2.2	Aufgaben	6
3.	Überwachung von Mitarbeitern eines Discounters unter Einsatz von Videotechnik und Detektiven	7
4.	Anlassfreie Kontrollen des Datenschutzes in Unternehmen und Einrichtungen	8
4.1	Kontrollen nach § 38 Abs. 1 BDSG als Vor-Ort-Kontrollen	8
4.2	Kontrollen nach § 38 Abs. 1 BDSG durch schriftliches Verfahren	12
5.	Beratungstätigkeit und Anfragen an die Behörde	12
6.	Anlasskontrollen nach Eingaben und Beschwerden	14
6.1	Allgemeine Übersicht	14
6.2	Darstellung ausgewählter Einzelbeispiele	15
6.2.1	Handyortung durch den Arbeitgeber	15
6.2.2	Bekanntgabe von Abfindungen	17

6.2.3	Einsatz als Inventuraushilfe	18
6.2.4	Weitergabe von Informationen durch eine Wirtschaftsauskunftei	19
6.2.5	Weitergabe von personenbezogenen Daten von Vereinsmitgliedern	21
6.3	Weitere Themen zu den Eingaben und Beschwerden	23
6.3.1	Unerwünschte Werbe – E-Mails	23
6.3.2	Entsorgung von Personal- und Bewerbungsunterlagen über den „normalen“ Papiermüll	24
6.3.3	„Standardschreiben“ der Auskunfteien zu Datenübermittlungen	25
7.	Register der meldepflichtigen Verarbeitungen nach § 4 d BDSG	26
8.	Außenwirkung der Aufsichtsbehörde	28
9.	Datenübermittlungen in Drittstaaten	29

1. Vorbemerkungen zum vierten Tätigkeitsbericht

Der Tätigkeitsbericht gibt einen Überblick über die im Berichtszeitraum Januar 2007 bis Dezember 2008 wahrgenommenen Aufgaben, stellt Lösungen für datenschutzrechtliche Fallgestaltungen vor und gibt Empfehlungen für datenschutzgerechtes Verhalten insbesondere bei privaten Wirtschaftsunternehmen, Vereinen, Verbänden und freiberuflich Tätigen.

Gemäß § 38 Abs. 1 Satz 6 BDSG hat die Aufsichtsbehörde spätestens alle zwei Jahre einen Tätigkeitsbericht zu veröffentlichen.

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

www.thueringen.de/de/tlvwa/inneres/hoheit/datenschutz/content.html

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

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

2.1 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.

Nach § 38 Abs. 1 BDSG kontrollieren die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich die Ausführungen 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, einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5 BDSG.

2.1.1 Örtliche Zuständigkeit

Die örtliche Zuständigkeit ist immer dann gegeben, wenn sich der Sitz des Unternehmens/der Einrichtung bzw. deren Niederlassung oder Betriebsstätte im Freistaat Thüringen befindet. Das bedeutet, dass durchaus mehrere Aufsichtsbehörden für ein Unternehmen oder eine Einrichtung zuständig sein können.

Dabei ist 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.

2.1.2 Sachliche Zuständigkeit

Die sachliche Zuständigkeit der Aufsichtsbehörde erstreckt sich auf die Überwachung der Einhaltung des BDSG und anderer datenschutzrechtlicher Vorschriften durch nicht öffentliche Stellen. Dies sind in erster Linie die privaten Wirtschaftsunternehmen, Vereine, Verbände und freiberuflich Tätigen.

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

2.2 Aufgaben:

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

- Beantwortung allgemeiner Anfragen zum Datenschutz
- Bearbeitung von Eingaben/Beschwerden
- Beratung und Unterstützung von betrieblichen Datenschutzbeauftragten
- Beratung von Unternehmen und Einrichtungen bei geplanten Vorhaben, die den Datenschutz berühren
- Durchführung von Anlasskontrollen nach Eingaben und Beschwerden
- Durchführung von anlassfreien Kontrollen in den Unternehmen und Einrichtungen
- Anordnung von Maßnahmen bei festgestellten Datenschutzverstößen in den Unternehmen und Einrichtungen und Kontrolle der Umsetzung
- Durchführung von Ordnungswidrigkeitsverfahren
- Stellung von Strafanträgen
- Führung des öffentlichen Registers der meldepflichtigen Verarbeitungen mit personenbezogenen Daten

3. Überwachung von Mitarbeitern eines Discounters unter Einsatz von Videotechnik und Detektiven

Im März 2008 wurde in den Medien berichtet, dass ein bundesweit tätiger Discounter seine Mitarbeiter in den Filialen monatelang durch Detektive und zahlreiche Überwachungskameras ausspioniert und intime Details aus deren Privatleben protokolliert habe. Dabei soll z. B. festgehalten worden sein, jeweils mit Tag und Uhrzeit, wann und wie häufig Mitarbeiter auf die Toilette gehen, wer mit wem möglicherweise ein Liebesverhältnis hat, wer nach Ansicht der Überwacher unfähig ist oder einfach nur "introvertiert und naiv wirkt."

Aufgrund dieser Informationen wurden von uns neun Filialen der Discounterkette in sechs Thüringer Städten aufgesucht.

In sechs Filialen wurden unsere Fragen von den Marktleiter/innen bereitwillig beantwortet. Dabei wurde uns mitgeteilt, dass in allen sechs Filialen keine stationäre Videoanlage installiert sei. Eine von uns durchgeführte Sichtkontrolle hat ebenfalls keine stationären Kameras im Verkaufs- und Kassenbereich erkennen lassen. In vier Filialen würden keine Detektiveinsätze stattfinden und in einer Filiale habe es vor ca. zwei bis drei Jahren einen Detektiveinsatz ohne Kamerabnutzung gegeben. In einer weiteren Filiale habe es vor ca. einem halben Jahr einen Detektiveinsatz mit Kamerabnutzung gegeben. Dies sei allerdings der einzige Einsatz in den letzten zehn Jahren gewesen. Ob die Kamera vorwiegend zur Überwachung der Angestellten eingesetzt war oder ob damit Diebstähle durch Kunden verhindert werden sollten, wurde nicht angegeben.

In den restlichen drei Filialen erhielten wir keine Auskunft. Es wurde uns lediglich mitgeteilt, wir mögen uns schriftlich mit unseren Fragen an die zuständige Bezirksdirektion wenden.

Da sich die für Thüringen zuständige Bezirksdirektion außerhalb unseres Zuständigkeitsbereiches befindet, haben wir die bei den Vor-Ort-Kontrollen erhaltenen Informationen an die für die zuständige Bezirksdirektion des Discounters zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich weitergegeben und das Verfahren wurde von dort weiterverfolgt.

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 anlassfreie Kontrollen zum Datenschutz bei allen nicht-öffentlichen Einrichtungen, 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 Umfang dar. Dabei ist die Möglichkeit des Kontrollumfangs 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).

Im Berichtszeitraum 2007 / 2008 wurden 33 Einzelhandelsgeschäfte einer anlassfreien Vor-Ort-Kontrolle unterzogen.

Die Aufsichtsbehörde hat sich bei den Kontrollen auf ein Thema konzentriert, welches sich kontinuierlich zu einem Schwerpunkt entwickelt hat, nämlich die Videoüberwachung.

Auf diesem Sektor ist eine sich ständig erhöhende Sensibilität der Bürger zu beobachten. Das ist sicherlich vor allem den sich immer mehr sichtbar werdenden Überwachungseinrichtungen in allen Bereichen geschuldet.

In § 6 b BDSG – „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen“ – ist die Videoüberwachung im nicht-öffentlichen Bereich geregelt.

"(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zweckes erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19 a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen."

Die 33 überprüften Geschäfte gehörten folgenden Branchen an:

- 1 Apotheke
- 1 Geldinstitut
- 1 Optikerfachgeschäft
- 1 Lederwarenfachgeschäft
- 1 Reisebüro
- 1 Tabak-/Zeitschriftenladen
- 1 Drogeriemarkt
- 1 Blumenfachgeschäft
- 1 Reinigung
- 1 Telefonanbieter
- 2 Allgemeine Fachgeschäfte
- 2 Discounter
- 2 Elektronikfachgeschäfte
- 3 Schuhfachgeschäfte
- 12 Bekleidungsfachgeschäfte

Bei der Kontrolle wurde überprüft, ob eine Videoüberwachung durchgeführt wurde. Wenn dies der Fall war, wurden die überwachten Bereiche überprüft und es wurde untersucht, ob entsprechende Hinweisschilder angebracht waren.

Die Kontrolle erbrachte folgende Ergebnisse:

In 18 der 33 überprüften Geschäfte sind keine Videoüberwachungsanlagen installiert. Es ist auch nicht vorgesehen, dort kurzfristig Kameras einzubauen.

Bei den 15 Geschäften, in denen eine Videoüberwachung stattfindet, wurde als Grund für die Überwachung der Schutz des Eigentums vor Beschädigung und Diebstahl (§ 6 b Abs. 1 Nr. 3) angegeben sowie die Wahrnehmung des Hausrechts (§ 6 b Abs. 1 Nr. 2).

Lediglich bei 4 Geschäften wurden keine Mängel festgestellt, d.h. die Kameras waren an zulässigen Stellen im Geschäftslokal installiert, es wurden zulässige Bereiche überwacht, die Videobilder wurden nur für einen kurzen Zeitraum gespeichert und es wurde für jeden den Laden betretenden Kunden gut sichtbar auf die Videoüberwachung hingewiesen.

Bei den übrigen 11 gab es nur geringfügige leicht und kurzfristig zu behebbende Beanstandungen, die letztlich nicht die Einleitung von Ordnungswidrigkeitsverfahren gerechtfertigt hätten. Entweder waren keine Hinweise auf die vorhandene Überwachung angebracht oder sie waren an einer Stelle angebracht, an der sie die Kunden nicht oder nur unter Schwierigkeiten erkennen konnten.

In zwei Geschäften konnten sofort die Hinweisschilder in die richtige Position gebracht werden.

Bei den restlichen neun Geschäften wurde mit einem Schreiben an die Geschäftsleitung auf die Mängel hingewiesen. Bei den anschließenden Kontrollbesuchen konnte festgestellt werden, dass nunmehr in allen Geschäften gesetzmäßige Zustände herrschten.

Die Geschäftsinhaber bzw. Geschäftsführer der Filialgeschäfte wurden darauf hingewiesen, dass nur sie Zugriff auf die Überwachungsdaten haben dürfen, wenn diese gespeichert werden würden; dass die Datenträger vor Zugriffen unberechtigter Dritter aufbewahrt werden müssen, dass die Daten umgehend gelöscht werden müssen, wenn sie nicht mehr benötigt werden. Dies habe im Normalfall spätestens nach drei Tagen zu erfolgen. In Ausnahmefällen hat bei

entsprechenden Vorkommissionen die Übergabe der gespeicherten Daten an die Strafverfolgungsbehörden zu erfolgen.

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 immer wieder durchzuführen.

5. Beratungstätigkeit und Anfragen an die Behörde

Die Beantwortung von Anfragen betrieblicher Datenschutzbeauftragter und von verantwortlichen Stellen war schon immer ein wichtiges Mittel, um die Verantwortlichen für die Einhaltung der datenschutzrechtlichen Regelungen zu sensibilisieren.

In § 4 g Abs. 1 Satz 1 und 2 BDSG hat der Gesetzgeber dies gesetzlich festgelegt: "Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden."

Damit ist der gesetzliche Auftrag der Aufsichtsbehörde hinsichtlich ihrer Beratungstätigkeit für betriebliche Datenschutzbeauftragte umrissen. Darüber hinaus werden auch die Anfragen von betroffenen Bürgern entsprechend § 38 Abs. 1 Satz 7 BDSG in Verbindung mit § 21 Satz 1 BDSG durch die Aufsichtsbehörde bearbeitet.

Sowohl die Beratungen als auch die Anfragen werden telefonisch oder schriftlich durchgeführt bzw. beantwortet. Es finden auch persönliche Beratungen bei der Aufsichtsbehörde statt. Hier sind es besonders betriebliche Datenschutzbeauftragte bzw. Vertreter von Einrichtungen und Unternehmen, die für bestimmte Tätigkeiten oder im Vorfeld bestimmter Tätigkeiten Fragen zum Datenschutz und zur Datensicherheit haben.

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

a) Beratungstätigkeit für Einrichtungen und Unternehmen:

- Meldepflicht zum Register bei der Aufsichtsbehörde nach § 4 d BDSG
- Notwendigkeit der Bestellung eines betrieblichen Datenschutzbeauftragten
- Qualifizierungsmöglichkeiten für Datenschutzbeauftragte
- Bestellung externer Datenschutzbeauftragter
- Veränderungen zur Bestellung von Datenschutzbeauftragten durch die neuen gesetzlichen Grundlagen im Mittelstandsentlastungsgesetz
- Anfragen öffentlicher/nicht-öffentlicher Stellen nach Datenträger-Entsorgungsfirmen zwecks geplanter Auftragsvergabe
- Einstellen von sog. Warndateien ins Internet
- Datensicherheitsaspekte beim Videoeinsatz in der Planungsphase im Unternehmen

b) Anfragen von Bürgern

- Tätigkeit von Handels- und Wirtschaftsauskunfteien - hierbei standen im Mittelpunkt Fragen zu den gemäß § 33 BDSG versandten Benachrichtigungsschreiben an den Betroffenen bei erstmaliger Übermittlung seiner Daten. Dieses Thema ist nach wie vor ein "Dauerbrenner". Die Anfragen konnten in der Regel telefonisch beantwortet werden.
- Videoüberwachung im persönlichen Bereich
- Umgang mit Personalakten
- Personalausweisdaten im Kaufmarkt
- Werbewidersprüche und Datenlöschung
- Umgang mit E-Mails nach Betriebsausscheiden

Im Berichtszeitraum 2007 / 2008 waren es 52 (im vorherigen Zeitraum 63) Anfragen, die schriftlich beantwortet wurden oder im persönlichen Gespräch geklärt wurden. Die telefonisch erledigten Anfragen und Beratungen wurden statistisch nicht erfasst.

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 2007 / 2008 wurden insgesamt 109 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 10 Vorgänge zu verzeichnen.

In 24 Fällen war eine Zuständigkeit der Aufsichtsbehörde Thüringens letztlich nicht gegeben. Vielmehr waren entweder der Thüringer Landesbeauftragte für den Datenschutz oder Aufsichtsbehörden anderer Bundesländer zuständig.

Von den 85 Eingaben und Beschwerden im Berichtszeitraum, die zuständigkeitshalber bearbeitet worden sind, wurde in 52 Fällen ein Datenschutzverstoß festgestellt.

Ein Bußgeldverfahren, das aufgrund einer nicht rechtzeitigen Auskunftserteilung gegen eine nicht-öffentliche Einrichtung eingeleitet worden war, wurde nach Einspracheinlegung vor dem zuständigen Amtsgericht beendet, wobei das Amtsgericht das von uns verhängte Bußgeld halbierte.

Auf die festgestellten Verstöße wurde in angemessener Weise und in kurzer Zeit durch die verursachenden Stellen reagiert und durch die nach § 38 Abs. 5 Satz 1 BDSG angeordneten Maßnahmen die Mängel technischer oder organisatorischer Art beseitigt.

Strafrechtlich relevante Handlungen im Sinne von § 44 BDSG wurden nicht festgestellt.

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 vom Personalausweis
- 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 Darstellung ausgewählter Einzelbeispiele

6.2.1. Handyortung durch den Arbeitgeber

Der Beschwerde eines Betroffenen lag folgender Sachverhalt zugrunde:

Im Rahmen seines Arbeitsvertrages erhielt der Beschwerdeführer von seinem Arbeitgeber ein Mobiltelefon, das er für dienstliche Zwecke nutzen konnte. Durch eine Information des Netzbetreibers erhielt er Kenntnis davon, dass die Erlaubnis erteilt worden war, den Standort des Handys zu orten. Sein Arbeitgeber, den er daraufhin angesprochen hat, sagte ihm, dass es mal ausprobiert worden sei. Der Beschwerdeführer hat darauf hingewiesen, dass seine Einwilligung nicht vorliege und auch nicht erteilt werde. Sein Arbeitgeber war allerdings der Meinung, dass die Handyortung sein gutes Recht sei, um die Mitarbeiter zu kontrollieren. Die Ortung wurde nicht nur einmalig durchgeführt.

Unsere Bewertung des Vorganges fiel wie folgt aus: Neben dem Arbeitnehmer als natürliche Person stand der durch die Handyortung ermittelte Aufenthaltsort als personenbezogenes Datum außer Frage.

Fraglich war allerdings, ob bei der Ermittlung des Aufenthaltsortes von einer Ausspionierung der Privatsphäre gesprochen werden konnte.

Das ausgegebene Handy ist ein Arbeitsmittel des Arbeitgebers und die Nutzung erfolgte zu dienstlichen Zwecken. Somit durfte das Handy auch nur während der Arbeitszeit benutzt werden. Das bedeutet, dass bei eingeschaltetem Handy nur der Aufenthaltsort des Benutzers während der Arbeitszeit durch den Arbeitgeber ermittelbar ist.

Nach § 28 Abs1. Nr. 1 BDSG alter Fassung ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

Danach wäre die Zulässigkeit nur dann gegeben, wenn die Handyortung arbeitsvertraglich oder durch eine entsprechende Betriebsvereinbarung schriftlich geregelt worden wäre.

Die Ermittlung des Aufenthaltsortes seiner Beschäftigten kann im berechtigten Interesse des Arbeitgebers liegen. Ein überwiegendes schutzwürdiges Interesse der Beschäftigten am Ausschluss der Handyortung vermochten wir nicht zu erkennen. Da es sich um ein dienstliches Handy handelte, war eine Ortung außerhalb der Arbeitszeit nicht vorgesehen. Die Privatsphäre der Arbeitnehmer war somit nicht betroffen.

Die Handyortung war daher zulässig. Allerdings hatte der Arbeitgeber gegen § 4 Abs. 3 BDSG verstoßen, weil er die Arbeitnehmer nicht vorher über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung der Daten unterrichtet hatte.

Der Arbeitgeber wurde von uns auf die künftige Einhaltung seiner Unterrichtungspflicht hingewiesen. Eine Ordnungswidrigkeit stellte dieses Verhalten allerdings nicht dar, so dass weitergehende Maßnahmen gegen das Unternehmen nicht erfolgten.

Später wurde uns dann mitgeteilt, dass eine Ortung der Diensthandys nicht mehr durchgeführt werde.

6.2.2 Bekanntgabe von Abfindungen

Ein Arbeitgeber (Geschäftsführer eines Hotels) wurde durch das zuständige Arbeitsgericht zu der Zahlung einer Abfindung an eine ausgeschiedene Mitarbeiterin verurteilt.

Der Anwalt der ausgeschiedenen Mitarbeiterin hat den Arbeitgeber durch ein Telefax, in dem der Name der ausgeschiedenen Mitarbeiterin und die Höhe der Abfindung genannt werden, zu Zahlung des Betrages aufgefordert. Dieses Telefax wurde, da das Faxgerät im Bereich der Rezeption für einen Teil der Mitarbeiter als Arbeitsmittel zur Verfügung stand, dem übrigen Personal und damit einem unbestimmten Kreis von weiteren Personen zugänglich gemacht. Das hatte zur Folge, dass dieser Personenkreis personenbezogene Informationen zur Kenntnis nehmen konnte, ohne dass diese Informationen für ihn bestimmt gewesen wären.

Der Anwalt der ausgeschiedenen Mitarbeiterin zeigte sich anfangs uneinsichtig, nachdem er auf seinen Verstoß gegen § 9 BDSG in Verbindung mit Nr. 4 der Anlage zu § 9 Satz 1 hingewiesen wurde. Danach hat derjenige, der personenbezogene Daten automatisiert verarbeitet oder nutzt, seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen werden können. Der Anwalt war der Auffassung, wenn der Arbeitgeber für die Korrespondenz mit ihm Schreiben verwendet, wo neben der Adresse und Telefonnummer im Briefkopf auch die Faxnummer angegeben ist, könne er davon ausgehen, dass er auch über diese Medien mit dem Arbeitgeber kommunizieren könne. Seiner Ansicht nach hätte der Arbeitgeber speziell in dem Schreiben an ihn entweder inhaltlich einen entsprechenden Hinweis geben müssen oder er hätte entsprechende Streichungen im Briefkopf vornehmen müssen.

Später räumte er dann ein Organisationsversehen ein, da das Fax von einer erst kürzlich neu eingestellten Anwaltsgehilfin versendet worden sei. In seiner Kanzlei sei es üblich, dass wenn nicht von vornherein sichergestellt sei, dass keine Unbefugten ein per Telefax übersandtes Schreiben zur Kenntnis nehmen können vor der Absendung des Telefaxes mit dem Empfänger telefoniert werde, damit das Schreiben sofort vom richtigen Adressaten in Empfang genommen werden kann. Für Zukunft könne er solche Versehen ausschließen.

6.2.3 Einsatz als Inventuraushilfe

Eine Filiale einer großen Baumarktkette, die deutschlandweit tätig ist, suchte Inventuraushilfen für die zum Jahresende durchzuführende Inventur. Auf einem Informationsblatt waren alle wichtigen Angaben festgelegt. Danach wurden von allen Interessenten die Vorlage ihrer Originallohnsteuerkarte, ihrer Chipkarte der Krankenkasse und ihre Sozialversicherungsausweis erbeten. Von Rentnern wurden zusätzlich Kopien der ersten drei Seiten des Rentenbescheides verlangt.

Auf unseren Hinweis, dass wir diese spezielle Datenabforderung als unangemessen betrachten und dies nicht mit dem Grundsatz der Datenvermeidung und Datensparsamkeit des § 3 a BDSG vereinbar sei, wurde uns mitgeteilt, dass die vorzulegenden Unterlagen durch die Konzernzentrale festgelegt würden, so dass die geforderten Kopien der Rentenbescheinigung bundesweit bei allen Baumärkten der Kette vorzulegen seien.

Zufälligerweise lag uns auch das Informationsblatt eines anderen Marktes der gleichen Baumarktkette vor. Dort wurde von den Rentnern nur die Vorlage der Kopie des Rentenausweises verlangt. Mittlerweile hatte sich auch die Zentrale eingeschaltet und uns mitgeteilt, dass das selbst erstellte Informationsblatt des zweiten Marktes nicht ganz korrekt sei. Die Art der Rente müsse mitgeteilt werden. Je nach Höhe des Hinzuverdienstes (als Inventuraushilfe) könnte eventuell eine Versicherungspflicht für die Rentner entstehen. Um diese korrekt berechnen zu können, müsse die Art der Rente bekannt sein, da alle Rentenformen unterschiedliche Schlüssel in der Sozialversicherung hätten. Von daher müsse zwar die Art der Rente bekannt sein, dies könne aber auch auf andere Art geschehen als durch die Vorlage des Rentenbescheides. Im Übrigen werde von Personen, die im Arbeitsprozess stünden, die Vorlage der Lohnsteuerkarte nicht verlangt.

Da der Rentenbescheid wesentlich mehr Informationen enthält als tatsächlich benötigt wurden, ist die Anforderung auf dem Informationsblatt wie folgt geändert worden: „Kopie des Rentenausweises, sowie einen Nachweis über die Art der Rentenbezüge (Altersrente, EU-Rente o.Ä.).“

6.2.4 Weitergabe von Informationen durch eine Wirtschaftsauskunftei

Einem Arbeitssuchenden wurde mitgeteilt, dass seine Bewerbung als Projektentwickler wegen „laufender Verfahren“ nicht berücksichtigt worden sei. Auf Nachfrage erfuhr er, dass eine negative Auskunft von einer Wirtschaftsauskunftei über ihn bei dem Arbeitgeber vorliegen würde. Der Arbeitgeber hat die ihm vorliegende Auskunft nicht an den Betroffenen weitergegeben sondern ihn allgemein an diese Wirtschaftsauskunftei verwiesen, noch dazu mit dem Hinweis, dass die Adresse im Internet stehe.

Der Betroffene wollte nun wissen,

1. ob die Firma berechtigt war, diese Auskünfte von seiner Person einzufordern, ohne dass er seine Einwilligung dazu in mündlicher oder schriftlicher Form erteilt hatte,
2. von welcher regionalen Betriebsgesellschaft dieser Auskünfte erteilt worden sind und
3. welche Informationen weitergegeben worden sind.

Die für den Arbeitgeber zuständige regionale Betriebsgesellschaft der Wirtschaftsauskunftei teilte dem Betroffenen mit, er möge sich an die für seinen Wohnsitz zuständige Betriebsgesellschaft wenden. Diese wiederum antwortete ihm, dass nicht bekannt sei, dass von ihr eine Auskunft über seine Person an den potentiellen Arbeitgeber erteilt worden sei.

Auf unsere Nachfrage bei der für den Arbeitgeber zuständigen regionalen Betriebsgesellschaft der Wirtschaftsauskunftei wurden uns vorab die Struktur und die Arbeitsweise erläutert, was sich wie folgt darstellt:

Die Unternehmensgruppe, der die Wirtschaftsauskunftei angehört, verfügt über regionale Strukturen, d.h. die Regionalgesellschaften haben einen genau definierten regionalen Bereich als sogenanntes Erledigungsgebiet. Die Firmen, die ihren Sitz innerhalb dieses Gebietes haben und die die Dienste – also den Auskunfts- wie auch den Inkassodienst - in Anspruch nehmen möchten, müssen eine Mitgliedschaft in der regionalen Betriebsgesellschaft begründen und werden auch von dieser Regionalstelle betreut.

Innerhalb des jeweiligen Erledigungsgebietes werden durch die zuständige Regionalgesellschaft zugleich die Datensätze zu Firmen und wirtschaftsrelevanten Privatpersonen erstellt und ständig aktualisiert. Zu den Quellen zählen die Register der Amtsgerichte sowie der Einwohnermelde- und Gewerbeämter, die Schuldnerlisten der Amtsgerichte, die eigenen Inkassovor-

gänge, Eigenangaben der Inhaber und auch der Geschäftsführer der Gesellschaften der jeweiligen Unternehmen. Datensätze zu Firmen oder Personen außerhalb des Erledigungsgebietes können nicht angelegt oder bearbeitet werden.

Die Daten aller Regionalgesellschaften in Deutschland werden mittels Datentransfer in die gemeinsame Datenbank eingespeist. Auf diese Datenbank können die Mitgliederfirmen auf der Grundlage entsprechender Zugangskennungen und unter Angabe des Anfragegrundes zugreifen und den entsprechenden Datensatz abrufen.

Weiter wurde uns mitgeteilt, dass die Regionalgesellschaft für den Wohnsitz des Betroffenen diesem die zu seiner Person gespeicherten Daten übermittelt habe.

Der Arbeitgeber habe aber seine Informationen nicht von dieser Regionalgesellschaft erhalten. Vielmehr sei der Auskunftsabruf über die Datenbank der angeschlossenen Privatauskunftei erfolgt. In diese spezielle Privatpersonendatenbank, die von einer Gesellschaft der Unternehmensgruppe betrieben werde, fließen alle Daten zu Privatpersonen aus der Wirtschaftsauskunftei-Datenbank ein. Diese Daten bilden die Grundlage für die Datenbank der Privatauskunftei. Sie werden vor allem mit weiteren Zahlungserfahrungen angereichert, die wiederum durch eine Vielzahl von Firmen bereitgestellt werden.

Auf entsprechenden schriftlichen Antrag und gegen Entgelt hätte der Betroffene diese Auskunftsdaten von der Privatauskunftei erhalten können.

Schließlich wurde uns unter Vorlage der schriftlichen Auskunft mitgeteilt, dass der betroffene Arbeitsuchende zweimal die eidesstattliche Versicherung abgegeben habe und dass vier weitere Verfahren wegen nicht bezahlter Rechnungen noch am „laufen“ seien. Diese Auskunft sei zum Zeitpunkt des Auskunftsabrufes auch richtig gewesen. Zwischenzeitlich sei aber die Löschung der eidesstattlichen Versicherung wegen Ablaufes der 3-Jahresfrist automatisch erfolgt. Würde zum jetzigen Zeitpunkt eine Auskunft über den Betroffenen abgerufen werden, wären die eidesstattlichen Versicherungen nicht mehr darin enthalten.

Es bleibt daher festzuhalten, dass das entsprechende Auskunftersuchen bei der zu besetzenden Stelle als Projektentwickler im Rahmen einer Geschäftsanbahnung datenschutzrechtlich nicht zu beanstanden war. Es hätte den beteiligten Personen und Firmen allerdings einigen Ärger und auch Schriftverkehr erspart, wenn der Arbeitgeber dem Betroffenen die

konkrete Adresse der Privatauskunftei genannt hätte anstatt allgemein auf die Wirtschaftsauskunftei („Adresse steht im Internet“) zu verweisen.

Entsprechend wurden der Betroffene und der Arbeitgeber von uns informiert.

6.2.5 Weitergabe von personenbezogenen Daten von Vereinsmitgliedern

Ein Mitglied eines Vereins beschwerte sich darüber, dass seine Anschrift mit weiteren personenbezogenen Daten den anderen Vereinsmitgliedern mitgeteilt worden sei. Ebenfalls seien seine Daten und die anderer Vereinsmitglieder an ein Versicherungsunternehmen weitergeleitet worden. Dieses Unternehmen habe nun Versicherungsvertreter zu den Vereinsmitgliedern geschickt, um diese zum Abschluss von Versicherungsverträgen zu bewegen.

Auf Nachfrage beim Vereinsvorsitzenden ergab sich folgender Sachverhalt: Der Beschwerdeführer hatte sich zur Wahl in den erweiterten Vereinsvorstand zur Verfügung gestellt und ist letztlich auch gewählt worden. Die Daten der gewählten Vorstandsmitglieder wurden den übrigen Vereinsmitgliedern zur Kenntnis gegeben.

Die Veröffentlichung von Daten der Funktionsträger eines Vereins durch den Verein stellt eine Datenübermittlung im Sinne des § 28 Abs. 1 Nr. 2 BDSG dar. Nach dieser Vorschrift ist eine allgemeine Veröffentlichung von personenbezogenen Daten zulässig, soweit es zur Wahrung berechtigter Interessen des Vereins erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des jeweils Betroffenen an dem Ausschluss der Veröffentlichung überwiegt.

Für den Verein ist ein berechtigtes Interesse anzuerkennen, die Anschriften der Funktionsträger zu veröffentlichen. Überwiegende schutzwürdige Belange derjenigen, deren Adressen veröffentlicht werden, sind nicht ersichtlich. Die Funktionsträger vertreten ihren Verein nach außen und dürfen dementsprechend auch öffentlich bekannt gemacht werden. Im Übrigen dürfte es auch dem Eigeninteresse der Funktionsträger als Verantwortliche ihres Vereins entsprechen, sich für diesen werbend in der Öffentlichkeit zu präsentieren.

Somit war die Weitergabe der Daten als gewähltes Vorstandsmitglied rechtlich zulässig und datenschutzrechtlich nicht zu beanstanden.

Hinsichtlich des zweiten Vorfalles teilte uns der Vereinsvorsitzende mit, dass der Verein mit einer bestimmten Versicherung eine Vereinbarung abgeschlossen habe, wonach die Mitglieder einen bestimmten Versicherungsvertrag bei dieser Versicherung abschließen würden. Anhand der vom Vereinsvorstand übergebenen Mitgliederliste hat eine Mitarbeiterin der Versicherung die Vereinsmitglieder aufgesucht.

Bei den sogenannten Gruppenversicherungsverträgen handelt es sich um Rahmenverträge zwischen Vereinen und Versicherungsunternehmen, die den Vereinsmitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen.

Nach den zwischen den Datenschutzaufsichtsbehörden und den Verbänden der Versicherungswirtschaft getroffenen Absprachen darf ein Verein im Rahmen eines Gruppenversicherungsvertrags dem Versicherungsunternehmen bzw. dem Versicherungsvertreter die Daten seiner Mitglieder nur unter folgenden Voraussetzungen übermitteln:

- Bei Neumitgliedern, die nach Abschluss des Gruppenversicherungsvertrags dem Verein beitreten, muss eine schriftliche Einwilligung eingeholt werden. Dies sollte zweckmäßigerweise in der Beitrittserklärung oder im Aufnahmeantrag vorgesehen werden, wobei das Mitglied darüber aufzuklären ist, welche Daten an welches Unternehmen weitergegeben werden sollen.

- Bei Altmitgliedern, die bei Abschluss des Gruppenversicherungsvertrags bereits Vereinsmitglieder waren, genügt es, wenn der Verein sie vor der Übermittlung ihres Namens und ihrer Anschrift an die Versicherung in einem Schreiben informiert und ihnen den Besuch eines Versicherungsvertreters ankündigt. In dem Schreiben muss auf die Möglichkeit des Widerspruchs gegen die Datenübermittlung und den Vertreterbesuch hingewiesen und dem Vereinsmitglied mindestens vier Wochen Zeit eingeräumt werden, von dieser Widerspruchsmöglichkeit Gebrauch zu machen.

Einzelne Versicherungen haben für Vereine eine „Stellungnahme zur Zulässigkeit von Datenübermittlungen“ oder ähnlich betiteltes Papier erarbeitet, in dem geringere Anforderungen an den Datenschutz genannt werden. Es wird dringend empfohlen, sich hiervon nicht irritieren zu lassen und der vorstehend wiedergegebenen Absprache zu folgen.

Der Vereinsvorstand wurde auf die Rechtslage hingewiesen und es wurde ihm angeraten, schnellstmöglich rechtmäßige Zustände herzustellen, was dieser auch zugesagt hat.

6.3 Weitere Themen zu den Eingaben und Beschwerden

6.3.1 Unerwünschte Werbe-E-Mails

Eine größere Anzahl von Beschwerden betraf den Erhalt von unerwünschten Werbe-E-Mails, sogenannten Spam-Mails. Diese Mails erhalten die Betroffenen in aller Regel von Stellen, mit denen sie bislang nicht in Kontakt gestanden haben. Sehr oft handelt es sich inhaltlich dabei um Erotik- und Partnervermittlungsangebote, aber auch um Werbeangebote anderer Art.

Der Bundesgerichtshof hat in seinem Urteil vom 11. März 2004 (Aktenzeichen I ZR 81/01) festgestellt, dass die Zusendung einer unverlangten E-Mail zu Werbezwecken grundsätzlich gegen die guten Sitten im Wettbewerb verstößt. Ein die Wettbewerbswidrigkeit ausschließendes Einverständnis des Empfängers der E-Mail hat der Werbende darzulegen und gegebenenfalls zu beweisen.

Diese Mails sind in erster Linie aus Sicht des Wettbewerbsrechts zu betrachten. Nach § 7 Abs. 2 Nr. 3 des Gesetzes über den Unlauteren Wettbewerb (UWG) ist derartige Werbung ohne ausdrückliche Einwilligung des Betroffenen unzulässig.

Da es sich also in erster Linie um Wettbewerbsverstöße handelt, sollten sich die Betroffenen an die Verbraucherzentralen wenden.

Die Verbraucherzentrale Bundesverband (vzbv) hat dazu eine Beschwerdestelle für private Verbraucher eingerichtet, die unter der Adresse beschwerdestelle@vzbv.de erreichbar ist. Informationen und die Vorgehensweise bei der Übermittlung der Mail an den vzbv sind im Internet unter www.vzbv.de/go/presse/608/index.html zu erhalten.

Unternehmen mit dem gleichen Ansinnen müssten sich an www.wettbewerbszentrale.de wenden.

Datenschutzrechtlich können wir als Aufsichtsbehörde insoweit tätig werden, dass wir die Auskunftsansprüche zu den gespeicherten Daten der Betroffenen gegenüber dem Versender nach § 34 BDSG geltend machen und dass wir die Löschung der Daten nach § 35 BDSG wegen unzulässiger Nutzung verlangen. Ferner können wir die Versender dieser E-Mails darauf hinweisen, dass sie künftig die Empfänger ihrer Mails gemäß § 28 Abs. 4 Satz 2 BDSG bei der Ansprache zum Zwecke der Werbung über die verantwortliche Stelle sowie über das Widerspruchsrecht zu unterrichten haben. Soweit von dem Ansprechenden personenbezogene Daten

des Betroffenen genutzt werden, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Ferner wurden die betroffenen Unternehmen aufgefordert, sowohl die Auskunftersuchen der Beschwerdeführer als zukünftig eingehende Auskunftersuchen sofort und umfassend zu beantworten.

Nachdem wir die Unternehmen auf die Einhaltung der datenschutzrechtlichen Bestimmungen hingewiesen haben, gab es keine negativen Rückmeldungen mehr durch die Beschwerdeführer.

6.3.2 Entsorgung von Personal- und Bewerbungsunterlagen über den „normalen“ Papiermüll

Es kommt hin und wieder vor, dass die Aufsichtsbehörde von aufmerksamen Bürgern darüber informiert wird, dass in einer öffentlich zugänglichen Mülltonne für Papierabfälle Bewerbungsunterlagen auftauchen, bei denen personenbezogene Daten der Bewerber z. B. auch der komplette berufliche Lebensweg mit den verschiedensten Zeugnissen, Beurteilungen und Zertifikate der Weiterbildung ohne weiteres eingesehen und auch mitgenommen werden können. Aufgrund der beiliegenden Anschreiben ist es in der Regel auch kein Problem gewesen, die Verursacher der unsachgemäßen „Altpapierentsorgung“ ausfindig zu machen.

Diese unsachgemäße Entsorgung der Bewerbungsunterlagen stellt einen Verstoß gegen § 9 BDSG dar. § 9 BDSG und die dazu gehörige Anlage enthalten die technischen und organisatorischen Maßnahmen, die beim Umgang mit personenbezogenen Daten einzuhalten sind. Nach Nr. 3 (Zugriffskontrolle) der Anlage zu § 9 ist zu gewährleisten, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Bei erfolglosen Bewerbungen hätten den Betroffenen ihre eingereichten Bewerbungsunterlagen entweder zurückgeschickt werden oder mit ihrem Einverständnis vernichtet werden müssen. Allerdings hätten auch andere Möglichkeiten vereinbart werden können, den Betroffenen ihre Unterlagen wieder zugänglich zu machen.

Da dies nicht erfolgte, sind die Persönlichkeitsrechte der Bewerber im Umgang mit ihren persönlichen Daten verletzt worden. Das Bundesarbeitsgericht hat in einer Entscheidung aus

dem Jahr 1984 (Az.: 5 AZR 286/81), die auch heute noch zu beachten ist, festgestellt, dass bei erfolgloser Bewerbung das vertragsähnliche Verhältnis zwischen dem potenziellen Arbeitgeber und dem Bewerber beendet ist und die Pflicht zur Rückgabe oder Vernichtung der vollständigen Bewerbungsunterlagen besteht.

Die potenziellen Arbeitgeber haben in ihren Stellungnahmen uns gegenüber mitgeteilt, dass es ein Organisationsversehen war, dass die aufgefundenen Unterlagen in normalen Papiercontainern gelandet sind und dass ihnen sehr wohl bewusst ist, wie sie mit nicht mehr benötigten Bewerbungsunterlagen umzugehen haben. Das Gegenteil konnte ihnen nicht nachgewiesen werden, so dass von der Einleitung von Ordnungswidrigkeitsverfahren abgesehen wurde.

6.3.3 „Standardschreiben“ der Auskunfteien zu Datenübermittlungen

Die Aufsichtsbehörde erreichen immer wieder Eingaben/Beschwerden oder auch nur Anfragen zu den „Standardschreiben“ der Auskunfteien, wenn diese erstmals Daten von betroffenen Personen an Dritte übermitteln. Diese Informationen an die Betroffenen sind nach BDSG sogar vorgeschrieben, können von den Adressaten aber oft nicht verstanden werden. Aus diesem Grunde soll an dieser Stelle der Hintergrund solcher „Standardschreiben“ erläutert werden.

Handels- und Wirtschaftsauskunfteien sammeln Daten über Unternehmen und über Privatpersonen, sofern diese deren wirtschaftliche Aktivitäten, deren Kreditwürdigkeit und Zahlungsverhalten betreffen. Durch dieses Sammeln von Daten sollen der Handel und die Wirtschaft vor allgemeinen Zahlungsausfällen, vor Kreditmissbrauch aber auch vor Kreditbetrug geschützt werden. Das BDSG lässt eine solche Datensammlung zu. Die Auskunfteien erheben Daten zu den Betroffenen entsprechend § 29 BDSG zum Zweck der Übermittlung. Diese Daten dienen den Kreditentscheidungen bzw. Bonitätsprüfungen und beinhalten z.B. Anschrift, Beruf, Zahlungsweise, Verbindlichkeiten. Sie werden durch die Auskunfteien aus allgemein zugänglichen Quellen erhoben. Die Speicherung dieser Daten ist zulässig, solange kein Grund zu der Annahme besteht, dass ein schützwürdiges Interesse der Betroffenen vorliegt. Und für die o.g. Zwecke ist eine solche Annahme nicht gegeben (§ 29 Abs. 1 Satz 1 Nr. 1 BDSG). Über die reine Speicherung der Daten ist bei den Betroffenen keine Einwilligung einzuholen und sie sind über die Speicherung auch nicht zu informieren. Eine Information an die Betroffenen durch die Auskunftei muss nach § 33 Abs. 1 Satz 2 BDSG erst dann erfolgen, wenn erstmals diese Daten übermittelt werden. Dabei ist auch über die Art der übermittelten Daten zu informieren.

Beides geschieht durch die „Standardschreiben“. Die Übermittlung der Daten erfolgt an einen Empfänger, der als Anfragender vorher der Auskunftspflicht gegenüber sein berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft nachweisen muss. Der Anfragegrund wird bei der Auskunftspflicht gespeichert. Über die Korrektheit der Anfragegründe haben die Auskunftspflichtigen zwecks Verhinderung von Missbräuchen in regelmäßigen Abständen entsprechende Stichprobenkontrollen durchzuführen. Diese Kontrollen können auch durch die Aufsichtsbehörden zu Einzelfällen durchgeführt werden. Hierbei werden allgemeine Anfragegründe, wie „Anbahnung von Geschäftsbeziehungen“ nicht toleriert. Der Anfragegrund muss einen realen Hintergrund haben. Die Anfragenden können beispielsweise Unternehmen sein, bei denen der Betroffene gegen Rechnung einen Kauf tätigen will; es kann ein Mobilfunkunternehmen sein, mit dem ein Handy-Vertrag abgeschlossen werden soll; es kann ein Autohaus sein, mit dem der Betroffene einen Leasingvertrag abschließen möchte. Mietverträge, Ratenkäufe, Grundstücksangelegenheiten können weitere Anfragegründe sein. Nach § 34 Abs. 1 BDSG haben die Betroffenen einen Anspruch gegenüber der Auskunftspflichtigen, Auskunft zu den über sie gespeicherten Daten zu erhalten. Eine Auskunft über die Quelle der Daten und den oder die Empfänger können die Betroffenen nach § 34 Abs. 1 Satz 3 BDSG aber nur dann erhalten, wenn hierbei nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. Die Auskünfte sind unentgeltlich zu erteilen, es sei denn, die Betroffenen können daraus einen wirtschaftlichen Nutzen ziehen.

7. Register der meldepflichtigen Verarbeitungen nach § 4 d BDSG

Nach § 38 Abs. 2 Satz 1 BDSG führt die Aufsichtsbehörde ein Register der nach § 4 d BDSG meldepflichtigen automatisierten Verarbeitungen (sogenanntes „Melderegister“).

Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen (§ 3 Abs. 2 Satz 1 BDSG). Die Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen an die zuständige Aufsichtsbehörde zu melden, § 4 d Abs. 1 BDSG.

Ohne Einschränkungen meldepflichtig sind nach § 4 d Abs. 4 BDSG automatisierte Verfahren, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zwecke der Übermittlung oder
2. zum Zwecke der anonymisierten Übermittlung

gespeichert werden.

Unter die Tätigkeit der Ziffer 1 fallen die Wirtschaftsauskunfteien, Detekteien, Adressverlage und Adresshändler (also der Handel mit personenbezogenen Daten) und zu der Ziffer 2 die Markt-, Meinungs-, Sozialforschungsinstitute.

Für die weiteren verantwortlichen Stellen gibt es Ausnahmetatbestände von der Meldepflicht. Diese entfällt z.B. dann, wenn die verantwortliche Stelle gemäß § 4 d Abs. 2 BDSG einen betrieblichen Datenschutzbeauftragten bestellt hat.

Weiterhin entfällt die Meldepflicht, wenn die Voraussetzungen des § 4 d Abs. 3 BDSG gegeben sind. Dies ist dann der Fall, wenn die verantwortliche Stelle

- die Daten für ihre eigenen Zwecke erhebt, verarbeitet oder nutzt,
 - mit dieser Erhebung, Verarbeitung oder Nutzung höchstens neun Arbeitnehmer beschäftigt sind
- und
- entweder eine Einwilligung der Betroffenen vorliegt

oder

- die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

Diejenigen Stellen, die eine Auftragsdatenverarbeitung als Dienstleistungsunternehmen durchführen, sind keine verantwortlichen Stellen im Sinne des BDSG und unterliegen daher keiner Meldepflicht. Dazu gehören beispielsweise Servicerechenzentren, Datenerfassungsbetriebe, Lohnbüros, Datenträgervernichter, Mikroverfilmungsbetriebe, Telefonmarketingunternehmen (Call-Center).

Zum Ende des Berichtszeitraumes sind die Angaben zu den automatisierten Verfahren folgender verantwortlicher Stellen in dem Register gespeichert:

- 10 Handels- und Wirtschaftsauskunfteien
- 3 Markt- und Meinungsforschungsunternehmen
- 6 Detekteien.

Damit haben sich keine Veränderungen gegenüber dem letzten Berichtszeitraum ergeben.

Der Inhalt der Meldungen ergibt sich aus § 4 e BDSG und wird in das Register der Aufsichtsbehörde übernommen.

Die entsprechenden Formblätter, einschließlich einer Erläuterung, sind im Internet abrufbar als "Meldehauptblatt", "Meldeanlagen" und "Meldeerläuterungen" unter:

www.thueringen.de/imperia/md/content/tlvwa2/200/meldehauptbl.pdf

www.thueringen.de/imperia/md/content/tlvwa2/200/meldeanlage.pdf

www.thueringen.de/imperia/md/content/tlvwa2/200/meldeerlaeut.pdf

Das Register bei der Aufsichtsbehörde kann entsprechend § 38 Abs. 2 BDSG von jedem eingesehen werden.

8. Außenwirkung der Aufsichtsbehörde

Durch den nach § 38 Abs. 1 Satz 6 BDSG regelmäßig, spätestens alle zwei Jahre, zu erstellen- den Tätigkeitsbericht, der auch im Internet veröffentlicht wird, unterrichtet die Aufsichtsbehörde die Öffentlichkeit über ihre Tätigkeit in den jeweils vergangenen zwei Jahren.

Die Aufsichtsbehörde ist seit dem Jahre 1993 im Erfahrungsaustauschkreis (ERFA-Kreis) Thüringen der Gesellschaft für Datenschutz und Datensicherheit (GDD) vertreten. Dieses Gremium ist ein freiwilliger Zusammenschluss von Datenschutzbeauftragten Thüringer nicht-öffentlicher und öffentlicher Stellen, die sich in regelmäßigen Abständen zu Arbeitstagungen treffen.

An den Beratungen des ERFA-Kreises Thüringen wurde im Berichtszeitraum nach den dienstlichen Möglichkeiten teilgenommen.

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 2007 beim Landesverwaltungsamt Sachsen-Anhalt in Halle und 2008 bei der Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Nordrhein-Westfalen in Düsseldorf.

9. Datenübermittlungen in Drittstaaten

Wenn nicht-öffentliche Stellen personenbezogene Daten in Drittländer übermitteln wollen und diese Länder kein der EU-Datenschutzrichtlinie angemessenes Datenschutzniveau besitzen, kann die Aufsichtsbehörde gemäß § 4 c Abs. 2 BDSG solche Übermittlungen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechtes vorweist. Das BDSG geht davon aus, dass die Übermittlung von Daten an ausländische Stellen außerhalb der EU/EWR unterbleiben muss, wenn der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

Ein solches entgegenstehendes schutzwürdiges Interesse ist insbesondere dann anzunehmen, wenn bei der empfangenden Stelle die Angemessenheit des Datenschutzniveaus nicht gegeben ist, § 4 b Abs. 2 Satz 2 BDSG.

Dennoch ist eine Datenübermittlung möglich, wenn Maßnahmen getroffen werden, die „ausreichende Garantien“ für den Datenschutz schaffen und so ein fehlendes angemessenes Datenschutzniveau ausgeglichen wird.

Eine solche Garantie ist die Anwendung von Standardvertragsklauseln, die durch die EU-Kommission erarbeitet und verabschiedet worden sind. Zu diesen Standardvertragsklauseln gehören jene vom 15. Juni 2001 ebenso wie die vom 27. Dezember 2004.

Kommen diese Klauseln unverändert zur Anwendung, ist eine Genehmigung der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich nicht erforderlich.

Die allgemeinen Voraussetzungen für eine rechtmäßige Übermittlung im Inland (z. B. nach § 28 BDSG) sind aber auch bei einer Datenübermittlung in ein Drittland relevant, d.h. es ist von der übermittelnden Stelle zu prüfen, ob auch die allgemeinen Voraussetzungen für eine Übermittlung vorliegen (§§ 4 Abs. 1, 28 BDSG).

Im abgelaufenen Berichtszeitraum hatte die Aufsichtsbehörde einen Antrag zu bearbeiten. Nachdem feststand, dass die o. g. Standardvertragsklauseln zur Anwendung kamen, konnte auf die Erteilung einer gesonderten Genehmigung durch die Aufsichtsbehörde verzichtet werden.