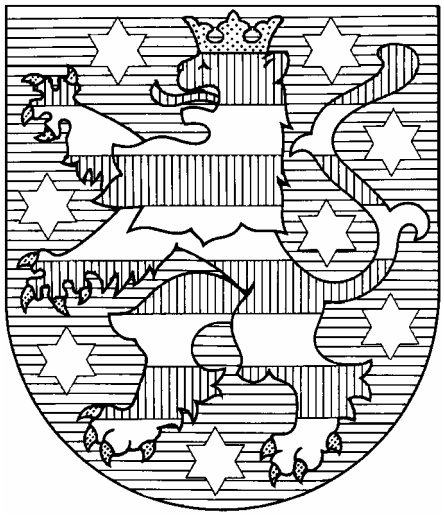

Datenschutz im nicht-öffentlichen Bereich Thüringen 2003/2004

Zweiter 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: 01.01.2003 bis 31.12.2004

Inhaltsverzeichnis

1.	Vorbemerkungen zum zweiten Tätigkeitsbericht	**3**
2.	Register der meldepflichtigen Verarbeitungen nach § 4d BDSG	**3**
3.	Anlassfreie Kontrollen des Datenschutzes in den Unternehmen	**4**
3.1	Kontrollen nach § 38 Abs. 1 BDSG als Vor-Ort-Kontrollen	**5**
3.2	Kontrollen nach § 38 Abs. 1 BDSG durch schriftliches Verfahren	**5**
3.2.1	Videoüberwachung bei Banken	**6**
3.2.2	Videoüberwachung in Handelseinrichtungen	**8**
4.	Beratungstätigkeit und Anfragen an die Behörde	**9**
5.	Anlasskontrollen nach Eingaben und Beschwerden	**10**
5.1	Allgemeine Übersicht	**10**
5.2	Darstellung ausgewählter Einzelbeispiele	**11**
5.2.1	Umgang mit E-Mail-Adressen in einem Hotel	**11**
5.2.2	Persönliche Werbung für "Arzneimittel"	**12**
5.2.3	Umgang mit Bewerbungsunterlagen	**13**
5.2.4	Eingaben zur Videoüberwachung	**14**
5.2.4.1	Einsatz von Web-Cams im öffentlichen Umfeld	**14**
5.2.4.2	Videoüberwachung im persönlichen Bereich	**16**
5.2.4.3	Videoüberwachung in Verkaufsstellen	**17**
5.2.5	Krankenversichertenkarte als Zutrittskontrollmedium	**18**
5.2.6	Patientendaten bei einem Krankenhausumzug	**20**
5.2.7	Erstellung einer Liste zur Hotelanmeldung während der Busreise	**21**
6.	Außenwirkung der Aufsichtsbehörde	**22**
7.	Datenübermittlungen in Drittstaaten	**23**
8.	Datenschutzgerechte Verhaltensregeln von Berufsverbänden	**23**
9.	Zusammenwirken mit dem Thüringer Innenministerium	**23**
10.	Abschließende Betrachtungen zur gegenwärtigen Entwicklung	**24**

1. Vorbemerkungen zum zweiten Tätigkeitsbericht

Mit diesem Tätigkeitsbericht für den Berichtszeitraum 2003 / 2004 kommt das Thüringer Landesverwaltungsamt als zuständige Aufsichtsbehörde für den Datenschutz bei den nicht-öffentlichen Stellen im Freistaat Thüringen seiner Verpflichtung nach § 38 Abs. 1 BDSG nach.

Im ersten Tätigkeitsbericht für den Zeitraum 2001 / 2002 wurde grundlegend informiert über:

- das Handeln der Aufsichtsbehörde im Freistaat Thüringen
- Aufgaben der Aufsichtsbehörde nach dem im Jahr 2001 novellierten BDSG
- Tätigkeit der Aufsichtsbehörde in den Jahren 1992 bis 2000
- Neuregelung der Meldepflichten nach dem novellierten BDSG

2. Register der meldepflichtigen Verarbeitungen nach § 4 d BDSG

"Die Aufsichtsbehörde führt ein Register der nach § 4 d meldepflichtigen automatisierten Verarbeitungen mit den Angaben gemäß § 4 e Satz 1." (§ 38 Abs. 2 Satz 1 BDSG)

Die Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme an die Aufsichtsbehörde zu melden. Die Meldungen sind von der verantwortlichen Stelle vorzunehmen, § 4 d Abs. 1 BDSG.

Ohne Einschränkungen meldepflichtig sind nach § 4 d Abs. 4 BDSG automatisierte Verfahren, in denen Daten

a) zum Zwecke der Übermittlung
(z.B. bei Wirtschaftsauskunfteien, Detekteien, Adressverlage, Adresshändler)

oder

b) zum Zwecke der anonymisierten Übermittlung gespeichert werden
(z.B. bei 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 vier Arbeitnehmer betraut hat

und

- entweder eine Einwilligung des Betroffenen vorliegt
  oder
- die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

Will sich die verantwortliche Stelle trotz Nichterfüllung dieser Kriterien von der Meldepflicht befreien, dann muss sie einen betrieblichen Datenschutzbeauftragten bestellen.

Diejenigen Stellen, die eine Auftragsdatenverarbeitung als Dienstleistungsunternehmen durchführen, sind keine verantwortlichen Stellen im Sinne des BDSG und unterliegen daher keiner Meldepflicht. Das sind 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.

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

3. Anlassfreie Kontrolle des Datenschutzes in den Unternehmen

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

Somit hat die Aufsichtsbehörde die Befugnis, Kontrollen zum Datenschutz anlassfrei bei allen nicht-öffentlichen Einrichtungen durchzuführen, die personenbezogene Daten

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

verarbeiten oder nutzen.

Im Berichtszeitraum 2003 / 2004 wurden 82 Einrichtungen einer anlassfreien Kontrolle unterzogen. Davon betroffen waren Einrichtungen folgender Branchen:

- 5 Rechenzentren als Auftragsdatenverarbeiter
- 1 Mikroverfilmungsunternehmen
- 1 Wirtschaftsauskunftei
- 7 Datenträger-Entsorgungsunternehmen
- 17 Banken
- 59 Handelseinrichtungen.

Für die Überprüfungen wurden die Verfahrensweisen der Vor-Ort-Kontrolle (14 Einrichtungen) und der Kontrolle im schriftlichen Verfahren (68 Einrichtungen) angewendet.

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

Diese Verfahrensweise stellt die bislang übliche Vorgehensweise der Aufsichtsbehörde dar, die Einhaltung des Datenschutzes in Einrichtungen anlassfrei zu kontrollieren.

Der Kontrollumfang ist hierbei breit gefächert und umfasst die Überprüfung der Verpflichtungen der Einrichtung zur Durchsetzung des Datenschutzes von der

- formal-rechtlichen Seite des BDSG (Meldepflichten nach § 4 d, Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten nach § 4 f und § 4 g, Verpflichtung der Mitarbeiter auf den Datenschutz 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 Vor-Ort-Kontrollen fanden bei den o.g. Einrichtungen statt, mit Ausnahme der Banken und der Handelseinrichtungen.

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

Die Kontrolle durch schriftliches Verfahren wurde im vorliegenden Berichtszeitraum erstmals von der Aufsichtsbehörde durchgeführt. Der Arbeitsaufwand für eine solche Verfahrensweise ist geringer als bei Vor-Ort-Kontrollen. Die Vorbereitung, die Durchführung und die Auswertung derart gestalteter Kontrollen senken den Arbeitsaufwand erheblich. Gleichzeitig können weit mehr Einrichtungen in die Kontrollen einbezogen werden als dies bei Vor-Ort-Kontrollen möglich wäre.

Erfahrungen in diesem Zusammenhang haben gezeigt, dass eine solche komplexe Aktion recht schnell in der gesamten Branche zur Kenntnis genommen wird und damit sicherlich zur Sensibilisierung des Problemkreises Datenschutz beiträgt.

Anzumerken bleibt aber, dass eine solche Verfahrensweise nicht bei allen datenschutzrechtlichen Problemstellungen wirkungsvoll eingesetzt werden kann. Besonders bei Rechenzentren mit unterschiedlichen räumlichen sowie Hardware- und Softwareausstattungen wird nach wie vor nur eine Vor-Ort-Kontrolle konkrete Kontrollergebnisse liefern können.

Bei den im Berichtszeitraum durchgeführten schriftlichen Kontrollen hat sich die Aufsichtsbehörde auf ein Thema konzentriert, welches sich in beiden Jahren kontinuierlich zu einem Schwerpunkt entwickelt hat, die Videoüberwachung.
Auf diesem Sektor ist eine sich ständig erhöhende Sensibilität der Bürger zu beobachten. Das ist sicherlich zum Einen den sich immer mehr sichtbar werdenden Überwachungseinrichtungen in allen Bereichen geschuldet, zum Anderen haben wohl auch bestimmte, durch die Medien publik gemachte, Vorgänge im öffentlichen Bereich des Landes dazu beigetragen.

Das BDSG regelt in § 6 b - Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen - die Videoüberwachung im nicht-öffentlichen Bereich:

"(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 §§ 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 Kontrolle im schriftlichen Verfahren wurde durchgeführt bei den im Freistaat Thüringen vertretenen Banken und in einer zweiten Phase bei großen Handelseinrichtungen im Freistaat.
Damit sollte dem Umstand Rechnung getragen werden, dass nach den Übergangsvorschriften in § 45 BDSG bestimmt ist, dass die am 23.05.2001 bereits begonnenen Verfahren innerhalb von 3 Jahren mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen sind.

3.2.1 Videoüberwachung bei Banken

Die Kontrolle wurde bei 17 Banken mit Filialen in Thüringen durchgeführt, bei denen die Zuständigkeit der Aufsichtsbehörde vorlag. Es wurde ein gleichlautender Fragenkatalog versandt mit der Bitte um Beantwortung in einem vorgegebenen Zeitraum.

Es wurden unter anderem folgende Informationen abgefragt:

- Zahl und Art der in den Filialen eingesetzten Überwachung, ggf. Planung eines Einsatzes
- Beschreibung der Zulässigkeitskriterien gemäß § 6 b Abs. 1 und 2 BDSG
- System von analoger oder digitaler Art
- Blickwinkel der Kameras und daraus resultierend Erfassung welcher Objekte
- Art der Überwachung (Monitorbeobachtung, Aufzeichnung analog/digital, Videosequenz oder Einzelbilder)
- Verknüpfung mit weiteren Transaktionsdaten (ggf. Benachrichtigung des Betroffenen in welcher Weise)
- Aufbewahrung der Datenträger, zugriffsberechtigte Personen, Löschfristen
- Kenntlichmachung der Überwachung entsprechend § 6 b Abs. 2 BDSG
- Erreichbarkeit des betrieblichen DSB

Die überwiegende Zahl der Banken hat in dem vorgegebenen Zeitraum den Fragebogen beantwortet. Die Antworten auf die einzelnen Fragen waren konkret gefasst und konnten somit in die Auswertung der Kontrolle eingehen, ohne dass Nachfragen bei den Banken notwendig waren. In 4 Fällen musste eine Anmahnung wegen Terminüberschreitung vorgenommen werden.

Wenn in öffentlich zugänglichen Bereichen von Geldinstituten der Umgang mit Banknoten erfolgt, ist nach § 6 Abs. 1 der Unfallverhütungsvorschrift Kassen (UVV Kassen) vorgeschrieben, dass diese Kassenräume mit optischen Raumüberwachungsanlagen auszustatten sind. Diese Anlagen sind nicht Bestandteil unserer Befragung gewesen.

Im Einzelnen ergaben sich folgende Erkenntnisse aus der Kontrolle:

a) Von den 17 kontrollierten Banken ist die Mehrzahl mit Überwachungseinrichtungen ausgestattet.
b) Bezüglich der Zulässigkeitskriterien für die Überwachung nach § 6 b Abs. 1 BDSG werden vorrangig Kriterien genannt, die Ziffer 3 (Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke) erfüllen, nämlich Reklamationen, Kartenmissbrauch, strittige Transaktionen, Schutz des Eigentums vor Beschädigung und Verlust.
c) Überwacht werden bei den jeweiligen Banken die Geldausgabeautomaten (kombinierte Aufnahmen vom Geldausgabefach und Porträtaufnahmen der Kunden), eine Überwachung der Kontoauszugsdrucker erfolgt nur in wenigen Fällen.
d) Die Kameras sind in die Automaten integriert, eine Ortung der Objektivaustrittsöffnungen ist nur mit Hintergrundwissen möglich. Die Blickwinkel der Kameras sind in allen Fällen auf das Geldausgabefach und den Kunden gerichtet. Bei der Porträtaufnahme des Kunden ist dessen Umfeld nur schemenhaft dargestellt. Die konkrete Frage, ob eventuell die PIN-Eingabe des Kunden durch eine der Kameras abgebildet wird, wurde von allen Geldinstituten verneint.
e) Generell werden die Überwachungsbilder aufgezeichnet.
f) Die verwendeten Systeme sind sowohl analoger als auch digitaler Art, wobei die digitalen Systeme überwiegen. Demzufolge sind die Speichermedien überwiegend Festplattenspeicher von PC, bei den wenigen analogen Systemen wird auf VHS-Kassette aufgezeichnet. Auf VHS erfolgen die Aufzeichnungen als fortlaufende Videosequenzen, bei den digitalen Systemen werden Sequenzen mehrerer Einzelbilder der Transaktion gespeichert.
g) Die Verknüpfung mit weiteren Daten erfolgt bei analoger VHS-Aufzeichnung i.d.R. durch die Einblendung von Datum und Uhrzeit. Die Auswertung der Bänder kann nur manuell erfolgen. Bei den digitalen Systemen können verschiedene weitere Daten im Rahmen der Transaktion aufgezeichnet werden (Datum, Uhrzeit, BLZ, Konto, Betrag, Karten- und Transaktionsnummer).
h) Auf eine gesonderte Benachrichtigung entsprechend § 6 b Abs. 4 BDSG wird in allen Fällen verzichtet. Die Benachrichtigung wäre notwendig in den Fällen der digitalen Aufzeichnung,

wenn beispielsweise über die Kontonummer eine Zuordnung der Porträtaufnahme zum Kunden erfolgen würde. Die Benachrichtigung kann entfallen, wenn der Kunde durch ein Hinweisschild über die Videoaufnahmen informiert wird (§ 33 Abs. 2 Nr. 1 BDSG). Ansonsten ist die Form der Benachrichtigung auch erfüllt, wenn der Kunde selbst reklamiert bzw. wenn bei Missbrauch die Ermittlungsbehörden informieren.

i) Zur Vermeidung unberechtigten Zugriffs wird in allen Antworten gleichermaßen darauf verwiesen, dass der zugriffsberechtigte Personenkreis namentlich festgelegt ist, dieser Kreis ausnahmslos auf das Datengeheimnis nach § 5 BDSG verpflichtet ist und die Datenträger in geschützten Bereichen (Raum und Rechner) verwahrt werden.

j) Die Speicherungsdauer hat der Forderung von § 6 b Abs. 5 BDSG zu entsprechen. Danach sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zweckes nicht mehr erforderlich sind. Die bestehenden Löschfristen wurden generell mit maximal 90 Tagen angegeben und damit begründet, dass aus den Erfahrungen heraus ungefähr in diesem Zeitabschnitt Kundenreklamationen, unklare Transaktionen bzw. die Nachfragen von Ermittlungsbehörden eine Einsichtnahme in die gespeicherten Daten erforderlich machen. Damit ist die Notwendigkeit der Speicherung für den genannten Zeitraum nachvollziehbar.

k) Alle Banken haben mitgeteilt, dass dem Erfordernis der Kenntlichmachung der Überwachung nach § 6 b Abs. 2 BDSG dadurch Rechnung getragen wird, dass Hinweise auf die Videoaufzeichnung entweder an Automaten direkt, im Eingangsbereich der Selbstbedienungszone oder an beiden Stellen angebracht sind.

l) Die Frage nach dem für die Bank zuständigen betrieblichen DSB und dessen Erreichbarkeit wurde in allen Fällen konkret beantwortet.

3.2.2 Videoüberwachung in Handelseinrichtungen

Basierend auf der schriftlichen Kontrolle bei den Banken wurde das gleiche Verfahren im Berichtszeitraum bei den großen Handelseinrichtungen im Freistaat durchgeführt. Der unter Punkt 3.2.1 angesprochene Fragenkatalog wurde - geringfügig verändert - auch bei diesen Einrichtungen verwendet.

Es wurden 59 Handelseinrichtungen angeschrieben, teilweise die Einrichtung selbst, teilweise aber auch die Zentrale der Thüringer Filialen.

Folgende Handelsbereiche umfasste die Kontrolle:

- 10 Elektronikmärkte
- 15 Warenhäuser
- 5 Baumärkte
- 6 Drogeriemärkte
- 3 Cash & Carry - Großmärkte
- 13 Lebensmittelmärkte
- 7 Möbelmärkte

Mit dieser Kontrolle sollte besonders dem Umstand Rechnung getragen werden, dass gerade die Handelseinrichtungen stark durch Kunden frequentierte Stellen sind und somit einen potentiellen Kreis für Anfragen und Beschwerden bei Erkennen von Überwachungseinrichtungen darstellen.

Im Einzelnen ergaben sich folgende Erkenntnisse aus der Kontrolle:

a) Von den 59 kontrollierten Einrichtungen führen 19 keine Überwachung durch. Dort sind derzeit auch keine Einsatzplanungen vorhanden. Bei den nichtüberwachten Einrichtungen handelt es sich vorwiegend um solche aus dem Food-Bereich. Bei Einrichtungen mit

höherpreislichem Sortiment wird hingegen durchweg überwacht. Wird bei einer Handelskette überwacht, dann betrifft dies auch alle in Thüringen vertretenen Filialen dieser Kette.

b) Bezüglich der Zulässigkeitskriterien für die Überwachung nach § 6 b Abs. 1 BDSG steht an erster Stelle die Wahrnehmung des Hausrechtes (Punkt 2) verbunden mit Kriterien, die Punkt 3 (Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke) erfüllen, nämlich Diebstahlverhinderung, Schutz und Aufklärung bei Einbrüchen sowie besondere Vorkommnisse im Kassenbereich.
c) Überwacht werden Ein-/Ausgangsbereiche, der ganze Verkaufsbereich und/oder spezielle Regalbereiche.
d) Die Kameras sind im Deckenbereich teils fest installiert und auf einen Überwachungsbereich ausgerichtet, teils werden Domekameras eingesetzt, die einen Rundumblick gestatten und die Funktion der Brennweitenveränderung (Zoom) nutzen.
e) Es wird eine reine Monitorbeobachtung bzw. eine Kombination von Monitorbeobachtung und Videoaufzeichnung vorgenommen, wobei letzteres überwiegt.
f) Die verwendeten Videosysteme sind sowohl analoger als auch digitaler Art, wobei die analogen Systeme überwiegen. Demzufolge sind die Speichermedien vorrangig VHS-Kassetten. Bei den weniger eingesetzten digitalen Systemen wird auf Festplattenspeicher von Computern aufgezeichnet. Alle Aufzeichnungen erfolgen als fortlaufende Speicherung, da einzelne Bildsequenzen dem Zweck der Überwachung nicht gerecht würden.
g) Eine Verknüpfung der aufgezeichneten Bilder mit weiteren Daten erfolgt in keiner der Einrichtungen. Das Problem einer gesonderten Benachrichtigung entsprechend § 6 b Abs. 4 BDSG ist somit nicht vorhanden.
h) Die Überwachungen im Verkaufsbereich durch Monitorbeobachtung werden durch eigene Mitarbeiter und durch beauftragte Detekteien durchgeführt.
i) Zur Vermeidung unberechtigten Zugriffs wird in allen Antworten gleichermaßen darauf verwiesen, dass der zugriffsberechtigte Personenkreis namentlich festgelegt ist, dieser Kreis ausnahmslos auf das Datengeheimnis nach § 5 BDSG verpflichtet ist und die Datenträger in geschützten Bereichen (Raum und Rechner) verwahrt werden.
j) Die Speicherungsdauer hat der Forderung von § 6 b Abs. 5 BDSG zu entsprechen. Danach sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zweckes nicht mehr benötigt werden. Die bestehenden Löschfristen wurden im Normalfall mit maximal 3 Tagen angegeben. Beim Eintritt von strafrechtlich zu verfolgenden Vorkommnissen verlängern sich diese Fristen entsprechend der notwendigen Einsichtnahme durch die Ermittlungsbehörden.
k) Dem Erfordernis der Kenntlichmachung der Überwachung nach § 6 b Abs. 2 BDSG wird dadurch Rechnung getragen, dass Hinweise auf die Videoüberwachung in der Regel im Eingangsbereich der Einrichtung durch Schilder als Piktogramm oder in Textform, ggf. auch kombiniert angebracht sind. Ergänzt wird dies in manchen Einrichtungen durch das Aufhängen von Großmonitoren im Eingangsbereich. In vier Fällen musste die Aufsichtsbehörde das Fehlen entsprechender Hinweise an die Kunden beanstanden.
l) Die Frage nach dem für die Einrichtung zuständigen betrieblichen DSB und dessen Erreichbarkeit wurde mehrheitlich konkret beantwortet. In 5 Fällen mussten fehlende Angaben bzw. Verweise auf den Filialleiter beanstandet werden. Beim Zusammentreffen von Leitungsfunktion und Tätigkeit als DSB ist eine Interessenkollision nicht ausgeschlossen.

4. Beratungstätigkeit und Anfragen an die Behörde

"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." (§ 4 g Abs.1 Satz 1 und 2 BDSG)

Damit ist der gesetzliche Auftrag der Aufsichtsbehörde hinsichtlich ihrer Beratungstätigkeit für betriebliche Datenschutzbeauftragte umrissen. Darüber hinaus werden auch alle Anfragen weiterer Kreise (insbesondere betroffener Bürger) 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 und 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 des vorhergehenden Berichtszeitraumes 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
- Anfragen öffentlicher/nicht-öffentlicher Stellen nach Datenträger-Entsorgungsfirmen zwecks geplanter Auftragsvergabe
- Einstellen von sog. Warndateien ins Internet
- Datensicherheitsaspekte bei räumlicher Umgestaltung im Unternehmen
- Nutzung der Videotechnik im Krankenhaus

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
- Fragen zu Markt- und Meinungsforschern, wenn von diesen schriftliche Befragungsaktionen durchgeführt werden
- Videoüberwachung im persönlichen Bereich
- Umgang mit Personalakten
- Personalausweisdaten im Kaufmarkt
- Werbewidersprüche und Datenlöschung

Im Berichtszeitraum 2003 / 2004 waren es 77 (im vorigen Zeitraum 64) Anfragen und Beratungen, die einer schriftlichen Beantwortung bedurften bzw. im persönlichen Gespräch abgearbeitet wurden. Die mittels Telefonat erledigten Anfragen und Beratungen wurden statistisch nicht erfasst.

5. Anlasskontrollen nach Eingaben und Beschwerden

5.1 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 weiterentwickelt hat.

Vergleichend mit den Zahlen der zurückliegenden Jahre ist eine allmähliche Entwicklung nach oben zu verzeichnen.

Im Berichtszeitraum 2003 / 2004 wurden insgesamt 67 schriftliche Eingaben und Beschwerden registriert. Das sind 15 Vorgänge mehr als im vorhergehenden Berichtszeitraum.
Darin enthalten sind 19 Fälle, bei denen eine Zuständigkeit der Aufsichtsbehörde nicht gegeben war. Dabei handelte es sich um Vorgänge aus dem öffentlichen Bereich des Bundes (Bundesbeauftragter für den Datenschutz zuständig), aus dem öffentlichen Bereich eines Bundeslandes (jeweiliger Landesbeauftragter für den Datenschutz zuständig) oder aus dem nicht-öffentlichen Bereich eines anderen Bundeslandes, in dem sich die Stelle befindet, über die eine Eingabe und Beschwerde vorlag (jeweilige regionale Aufsichtsbehörde zuständig).

Von den 48 Eingaben und Beschwerden im Berichtszeitraum, die zuständigkeitshalber bearbeitet worden sind, wurde in 32 Fällen im Laufe der Ermittlungen festgestellt, dass diese berechtigt waren, d.h. es lag ein Datenschutzverstoß vor.

Von der Einleitung von Bußgeldverfahren nach § 43 BDSG konnte deshalb abgesehen werden, weil auf alle festgestellten Verstöße, die lediglich geringfügig waren, in angemessener Weise und in kurzer Zeit durch die verursachenden Stellen reagiert wurde. Damit wurde in allen Fällen § 38 Abs. 5 Satz 1 BDSG dahingehend entsprochen, dass eine Beseitigung festgestellter technischer oder organisatorischer Mängel durch geeignete Maßnahmen vorgenommen wurde.
Strafrechtlich relevante Handlungen im Sinne von § 44 BDSG wurden nicht festgestellt.

Die Eingaben und Beschwerden zogen 4 Kontrollen vor Ort nach sich. Die anderen Fälle konnten aufgrund ihres Inhaltes im schriftlichen Verfahren anhand von Stellungnahmen der betroffenen Unternehmen bearbeitet und einer Klärung zugeführt werden.

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

- Umgang mit Bewerbungsunterlagen
- Unverlangte E-Mail-Werbung
- Einsatz von Web-Cams
- Erhebung von Kundendaten
- Missbräuchliche Verwendung von E-Mail-Adressen
- Missbräuchliche Verwendung von Chipkarten
- Videoüberwachung öffentlich zugänglicher Bereiche
- Videoüberwachung im persönlichen Bereich
- Umgang mit Patientendaten
- Werbung für ein "Arzneimittel"
- Umgang mit Versicherungsdaten

5.2 Darstellung von Einzelbeispielen

5.2.1. Umgang mit E-Mail-Adressen in einem Hotel

Der Beschwerde eines Betroffenen lag folgender Sachverhalt in einem Hotel zugrunde:

Der Beschwerdeführer hatte sich per E-Mail nach der Möglichkeit einer Buchung zu einer bestimmten Zeit in einem Hotel erkundigt. Die Anfrage wurde durch das Hotel umgehend per E-Mail beantwortet.

Einige Wochen später erhielt der Beschwerdeführer per E-Mail einen Kettenbrief aus eben diesem Hotel. Diese E-Mail stand in keinem Zusammenhang mit seiner ursprünglichen Anfrage, sondern beinhaltete einen anderen Sachverhalt, den man einem großen Kreis von Personen bekannt machen wollte und um dessen Weiterverbreitung gebeten wurde.
Aus der E-Mail war eine Vielzahl weiterer Mail-Adressen zu entnehmen, die alle die gleichen Mails erhalten haben oder noch erhalten sollten. Dabei handelte es sich wohl um die Adressen von Kunden bzw. möglicher Kunden dieses Hotels.
Der Beschwerdeführer konfrontierte die Geschäftsführung des Hotels mit diesem Sachverhalt, bat um Aufklärung und die Löschung der über ihn im Hotel gespeicherten Daten.
Da die Geschäftsführung ihm gegenüber die Verantwortung des Hotels für diese Aktion ablehnte, schaltete der Beschwerdeführer die Aufsichtsbehörde ein.

Wir haben von der Geschäftsführung eine nochmalige Überprüfung des Vorganges gefordert, da es den Anschein hatte, dass die betreffende Nachricht vom Server des Hotels abgesendet worden sei.
In ihrer Stellungnahme hat dies die Geschäftsführung schließlich eingeräumt. Ein Mitarbeiter des Hauses, der in diese "Kettenbriefaktion" eingebunden war, hatte zu deren Weiterverbreitung die Kundenadressen des Hotels verwendet. Die Geschäftsführung des Hotels hat daraufhin disziplinarische Maßnahmen gegen diesen Mitarbeiter eingeleitet. Dem Beschwerdeführer gegenüber hat man eine Entschuldigung ausgesprochen.

Der Geschäftsführer des Hotels wurde von uns darauf hingewiesen, dass die Adressen von Kunden und potentiellen Kunden entsprechend § 28 Abs. 1 Nr. 1 BDSG nur zur Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke des Hotels erlaubt sind, soweit keine weitere Einwilligung der Kunden über die Verwendung ihrer Daten für Werbezwecke oder ähnliches eingeholt worden ist.
Darüber hinaus erfolgten Hinweise zur Löschung der Daten, die nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG zu erfolgen hat, wenn die Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Dies trifft insbesondere auf die Daten über potenzielle Kunden zu, mit denen bislang kein vertragliches Verhältnis zustande gekommen ist.
Bezüglich der Kundendaten haben wir auf § 35 Abs. 3 Nr. 1 BDSG verwiesen, wonach an Stelle der Löschung eine Sperrung der Daten tritt, wenn gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen einer Löschung entgegenstehen.
Der Hinweis auf eine aktenkundige Datenschutzunterweisung der Mitarbeiter des Hauses wurde seitens der Hotelleitung aufgegriffen.

5.2.2 Persönliche Werbung für "Arzneimittel"

Im Berichtszeitraum haben uns mehrere Beschwerden erreicht, die alle einen ähnlichen Sachverhalt betrafen. Zeitnah zu Untersuchungen bei einem Facharzt für Urologie mit anschließender Blutuntersuchung in einem Labor wurde ein Teil der Beschwerdeführer von einer Medizinproduktevertriebsfirma mit einem recht persönlich gehaltenen Brief eines Dr. W. oder Dr. Z. mit einem Prostatapräparat beworben.
Ein anderer Teil der Beschwerdeführer erhielt den gleichen Brief, allerdings ohne dass dieser zu Untersuchungen gewesen war.

Wir haben unsere Ermittlungen bei der Vertriebsfirma, die laut Absenderangabe in Thüringen ansässig sein sollte, unter der angegebenen Adresse durchgeführt. Auf schriftliche Anfrage haben wir keine Antwort erhalten. Im Gewerberegister des zuständigen Landratsamtes war die Vertriebsfirma nicht eingetragen. Am Haus mit der postalischen Adresse befand sich lediglich ein Briefkasten. Mehr konnte vor Ort nicht ermittelt werden.

Unsere weiteren Recherchen im Internet haben ergeben, dass eine Vertriebsfirma mit dem angegebenen Namen eine Serviceadresse für Europa in den Niederlanden hat. Der Sitz des Unternehmens befindet sich in den USA.
Es war daher davon auszugehen, dass in Thüringen lediglich eine Postadresse eingerichtet ist. Somit konnten wir nicht weiter tätig werden.

Da diese Werbeaktion für das Prostatapräparat bundesweit durchgeführt wurde (und zum Zeitpunkt der Fertigstellung dieses Berichtes immer noch wird) und uns Hinweise auf die Beteiligung eines Adressenhändlers als möglicher Lieferant der Adressen vorlagen, waren in diesen Vorgang auch weitere Aufsichtsbehörden eingebunden. Der schnelle Informationsaustausch zwischen mehreren Datenschutzaufsichtsbehörden hat damit zu einer raschen Klärung der Angelegenheit beigetragen.

Durch eine Aufsichtsbehörde wurde uns bestätigt, dass bei der Werbeaktion durch die Vertriebsfirma Datenbestände aus einer sogenannten Haushaltdatei eines Adressenhändlers verwendet worden seien, bei denen Namen und Anschriften durch die Altersangaben (in Jahren) angereichert seien.
Damit erscheint es wahrscheinlich, dass eine Weitergabe von Daten durch die Ärzteschaft bzw. die Labors oder Kassenärztliche Organisationen an die Medizinproduktevertriebsfirma ausgeschlossen werden kann.

Nach unseren weiteren Recherchen ist ein Strafverfahren gegen die Vertriebsfirma in den Niederlanden bei einer deutschen Staatsanwaltschaft anhängig. Nach Auskunft des zuständigen Staatsanwaltes wird aufgrund einer Strafanzeige aus dem Bereich des Verbraucherschutzes unter anderem ermittelt wegen des Verstoßes gegen das Arzneimittelgesetz und zwar wegen des Inverkehrbringens in Deutschland nichtzugelassener Arzneimittel.
Der Staatsanwaltschaft als zuständiger Ermittlungsbehörde liegen nach unserer Kenntnis auch weitere Anzeigen in dieser Angelegenheit von betroffenen Werbeadressaten, Ärzten und Journalisten vor.

5.2.3 Umgang mit Bewerbungsunterlagen

Die Aufsichtsbehörde erreichen immer wieder Beschwerden von Bürgern, denen nach Durchführung einer Bewerbung um eine Arbeitsstelle keine Informationen zugehen, was mit ihren Bewerbungsunterlagen geschieht, wenn die Bewerbung erfolglos geblieben ist.

Dieses Problem wurde bereits im vergangenen Tätigkeitsbericht thematisiert. Da es nach wie vor aktuell ist, soll es an dieser Stelle nochmals dargestellt werden.

Die Unterlagen enthalten eine Vielzahl personenbezogener Informationen. Dies sind Einzelangaben über persönliche Verhältnisse einer bestimmten natürlichen Person, wie z.B. Name, Anschrift, Geburtsdatum, Familienangaben, Ausbildung, Beruf, Passfoto.

Bei den Beschwerden sind prinzipiell zwei Fälle zu unterscheiden:
Im ersten Fall werden die Bewerber formlos über die Ablehnung ihrer Bewerbungen informiert, Informationen über den Verbleib ihrer Unterlagen erhalten sie dabei nicht.
Im zweiten Fall erhalten die Bewerber überhaupt keine Nachricht.

Auf Grund der o.g. vielfältigen persönlichen Angaben muss den Bewerbern das Recht zugestanden werden, über den weiteren Verbleib ihrer Unterlagen informiert zu werden.

Eine Anwendbarkeit des BDSG ist in diesen Fällen nicht gegeben, da es sich bei den Bewerbungsunterlagen um eine Sammlung von schriftlichen Unterlagen in Form einer Akte handelt. Damit sind die Voraussetzungen für die Anwendung des Gesetzes nach § 27 Abs. 1 BDSG nicht erfüllt:
Die personenbezogenen Daten werden zum einen nicht unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben. Zum anderen stellt diese Aktensammlung auch keine nicht-automatisierte Datei dar, da die dafür nötigen Voraussetzungen eines gleichartigen Aufbaus, einer Zugänglichkeit nach bestimmten Merkmalen und einer Auswertungsmöglichkeit nach bestimmten Merkmalen nicht gegeben sind.

Die entsprechenden verantwortlichen Stellen wurden durch die Aufsichtsbehörde auf die Verletzung des Persönlichkeitsrechtes des Betroffenen hingewiesen. Des Weiteren erfolgte der Hinweis auf ein Urteil des Bundesarbeitsgerichtes aus dem Jahre 1984 (Az.: 5 AZR 286/81), das noch heute Gültigkeit besitzt. Danach ist das Bewerbungsverhältnis beendet, wenn der Arbeitgeber seine Einstellungsentscheidung getroffen hat. Gleichzeitig hat damit die vertragsähnliche Beziehung zwischen Bewerber und potenziellem Arbeitgeber ein Ende gefunden. Der Arbeitgeber ist verpflichtet, die Bewerberdaten zu löschen und den Personalfragebogen an den Bewerber zurückzugeben oder gleichfalls zu vernichten.

Es ist auch vorgekommen, dass der Eingang der Bewerbung durch das ausschreibende Unternehmen in Abrede gestellt wurde und der Bewerber die Einreichung seiner Unterlagen nicht nachweisen konnte.

Wir haben den Beschwerdeführern den Hinweis gegeben, bei zukünftigen Fällen bereits bei der Einreichung ihrer Unterlagen festzulegen, wie mit diesen bei Nichteinstellung verfahren werden soll (Vernichtung oder Selbstabholung oder Rücksendung, ggf. mit Portobeilegung).

5.2.4 Eingaben zur Videoüberwachung

5.2.4.1 Einsatz von Web-Cams im öffentlichen Umfeld

Über den folgenden Sachverhalt wurde die Aufsichtsbehörde durch eine Veröffentlichung in den Medien informiert:
Auf dem Bauwerk in einer Stadt befinden sich an dessen Spitze eine öffentlich zugängliche Aussichtsplattform und ein Café mit Außenplätzen. Auf dieser Plattform sind Web-Cams installiert.
Die Bilder dieser Kameras sind über die Internetseiten verschiedener Einrichtungen verfügbar. Die eingesetzte Technik gestattet es dem Betrachter, von seinem PC aus eine Steuerung der Kameras in horizontaler und vertikaler Richtung vorzunehmen und gleichfalls die Zoomfunktion zu nutzen.
Mit den Einstellungen der Kameras mit Blick auf die Plattform waren Bilder zu erzielen, bei denen von der Ausgangstür auf die Aussichtsplattform bei vollem Zoom Personen ohne Probleme zu erkennen waren.
Durch weitere Einstellungen der Kameras konnten durch den Blick auf den Außenbereich des Cafés Gäste dieser Einrichtung identifiziert werden.
Es war nicht auszuschließen, dass durch die Zoom-Möglichkeit besonders bei Dunkelheit Einblicke in die beleuchteten Innenräume umliegender Wohnungen möglich waren und bei vollem Zoom eventuell auch Passanten im Straßenbereich zu erkennen waren.

Gegen den Einsatz der Web-Cams zur Präsentation von Übersichtsbildern der Stadt, des Straßen- und Fußgängerverkehrs und des Stadtumfeldes bestehen grundsätzlich keine daten-

schutzrechtlichen Bedenken. Dabei darf es sich aber nur um Übersichtsbilder handeln. Mit solchen Totalaufnahmen werden in der Regel keine personenbezogenen Daten produziert.

§ 3 Abs. 1 BDSG definiert personenbezogene Daten als "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)". Eine Bestimmbarkeit der abgebildeten Personen liegt vor. Sachliche Verhältnisse der abgebildeten Personen liegen gleichfalls vor, nämlich der Aufenthalt zu einer bestimmten Zeit an einem bestimmten Ort, mit oder ohne Begleitperson (die auch wiederum bestimmbar ist).

Das BDSG regelt in § 6 b die Beobachtung öffentlich zugänglicher Räume mittels optisch-elektronischer Einrichtungen:

Im vorliegenden Fall handelt es sich sowohl um einen öffentlich zugänglichen Raum als auch bei den Web-Cams um die entsprechende optisch-elektronische Einrichtung.

Es ist fraglich, ob die wahrzunehmenden Interessen die Beobachtung von Personen erforderlich machen. Beim Einsatz der Web-Cams steht sicherlich der Werbeaspekt im Vordergrund, einmal für die Stellen, auf deren Internetseiten die Präsentation erfolgt. Zum zweiten dient diese Präsentation sicherlich auch der Imagedarstellung der Stadt. Dagegen ist prinzipiell nichts einzuwenden, nur ist dafür die Beobachtung von Personen nicht erforderlich.

Auf jeden Fall überwiegen die schutzwürdigen Interessen der Betroffenen. Mit der Einstellung ins Internet ist eine weltweite Übermittlung der Bilder verbunden. Damit ist eine nahezu unbegrenzte Verfügbarkeit und Weiterverwendung für jeden Internet-Nutzer möglich. Es können durch den Nutzer weitere Handlungen an und mit diesen Bildern vorgenommen werden. Dies könnte eine Vervielfältigung und Weiterverbreitung im Netz sein oder auch eine weitere Vergrößerung und Manipulierung der Bilder mittels spezieller Software.

Damit sind für das Betreiben der Web-Cams in der vorgefundenen Art die Zulässigkeitskriterien nach § 6 b Abs. 1 BDSG

"(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.

in diesem Fall nicht erfüllt.

Auf die Forderung der Aufsichtsbehörde, dass die Betreiber der Web-Cams geeignete technische Maßnahmen zu ergreifen hätten, die eine weitere Beobachtung von Personen ausschließen, wurde durch die Betreiber der Anlage folgendermaßen reagiert:

- Auf der Plattform wurden Sichtblenden so vor die Kameras montiert, dass die Blickwinkel auf die Aussichtsplattform und Einblicke in den Bereich des Cafés nicht mehr möglich sind.
- Unseren Feststellungen bezüglich der Beobachtung umliegender Häuserfronten und von Straßenszenen bei vollem Zoom wollten die Betreiber in dieser Form nicht folgen. Dessen ungeachtet sind sie unseren Forderungen insoweit entgegen gekommen, dass nunmehr nach 30 sec eine automatische Umschaltung der Kamera auf eine andere Einstellung erfolgt, so dass eine längere Betrachtung einer Szene nicht mehr möglich ist.

Die Bilder waren auch auf die Internet-Seiten einer Einrichtung aus dem öffentlichen Bereich gestellt. Daher war auch der Thüringer Landesbeauftragte für den Datenschutz (TLfD) mit der Angelegenheit befasst.

Der Vorgang ist insoweit noch nicht abgeschlossen, da es in Thüringen weitere Web-Cams im öffentlichen Umfeld gibt, bei denen ähnliche Einstellungen wie im vorliegenden Fall vorgenommen werden.
Aus diesem Grunde werden wir in Abstimmung mit dem TLfD versuchen, eine einheitliche Linie bei der Beurteilung von solchen Web-Cam-Installationen zu finden.

5.2.4.2 Videoüberwachung im persönlichen Bereich

Das BDSG regelt in § 6 b die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen, die Videoüberwachung.
Diese Vorschrift existiert seit der Novellierung des BDSG im Jahre 2001. Damit ist nachvollziehbar, dass in seiner Anwendung noch Erfahrungen zu sammeln sind und dass jede dazu vorliegende Eingabe einer tiefgründigen Einzelfallprüfung zu unterziehen ist.

Betroffene Bürger, die Probleme mit einer Videobeobachtung in ihrem persönlichen Umfeld haben, gehen meist von einer Anwendbarkeit des § 6 b BDSG aus. Drei Beispiele von Eingaben an die Aufsichtsbehörde sollen dies verdeutlichen:

a) Im Zuge eines Nachbarschaftsstreites über das Zufahrts- und Wegerecht wird die Zufahrt des Beschwerdeführers zu seinem Haus von seinem Nachbarn videoüberwacht. Für diese Zufahrt, die über das Grundstück des Nachbarn führt, besitzt der Beschwerdeführer eine Dienstbarkeit als Zufahrtsrecht.
   Durch eine dritte Person wurde der Beschwerdeführer darauf hingewiesen, dass der Nachbar die Zufahrt überwachte. Er fühlte sich nunmehr in seinem Persönlichkeitsrecht beeinträchtigt und vermutete, dass seine schutzwürdigen Interessen gegenüber der Überwachung laut BDSG zu überwiegen hätten.

b) In einem Wohngebiet wurden auf den Grundstücken der gegenüberliegenden Straßenseite vom Haus des Beschwerdeführers neue Wohnhäuser errichtet. Das Haus seines Gegenübers hat eine hohe Einfriedung und ist mit einer Videoüberwachungskamera ausgerüstet, deren Blickwinkel die Straße und den Eingangsbereich seines Hauses erfasst. Damit fühlten sich er, seine Familie und seine Besucher in ihrem Persönlichkeitsrecht eingeschränkt.

c) Im Zusammenhang mit einem Nachbarschaftsstreit zeigte ein Beschwerdeführer an, dass sein Grundstück tags und nachts von zwei Videokameras seines Nachbarn beobachtet wird. Die zum Beweis beigelegten Fotos dokumentierten das Vorhandensein zweier Kameras in der Fensterecke eines Zimmers im ersten Geschoss und am Balkon des Nachbarhauses.
   Der Beschwerdeführer leitete anhand § 6 b BDSG eine Unzulässigkeit dieser Überwachung ab und forderte des weiteren Schadensersatz für den erlittenen immateriellen Schaden für seine Familie.

Diesen drei Eingaben ist folgendes gemeinsam:

Die Videoüberwachung ist, soweit sie durch nicht-öffentliche Stellen durchgeführt wird, in § 6 b BDSG geregelt.
Das BDSG kommt aber insgesamt dann nicht zur Anwendung, wenn gemäß § 1 Abs. 2 Nr. 3 die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Dies ist in den vorliegenden Fällen gegeben.
Bei zwei der dargestellten Eingaben wäre auch die Anwendbarkeit von § 6 b BDSG bereits dadurch ausgeschlossen, dass keine öffentlich zugänglichen Räume mit optisch-elektronischen Einrichtungen beobachtet wurden.

Private Grundstücke und private Zufahrten zu solchen Grundstücken stellen keine öffentlich zugänglichen Räume dar.

Eine Anwendbarkeit des BDSG mit seinen Vorschriften zur Videoüberwachung war in allen drei Fällen nicht gegeben. Die Aufsichtsbehörde konnte somit nicht tätig werden.
Wir haben die Beschwerdeführer auf den Zivilrechtsweg verwiesen und haben ihnen jeweils die Kopie eines Urteils des LG Berlin vom 22.08.1986 (Az. 8.0.197/85) beigefügt, dem ein vergleichbarer Sachverhalt zugrunde lag.

5.2.4.3 Videoüberwachung in Verkaufsstellen

Der Aufsichtsbehörde lag eine Beschwerde vor, die die Videoüberwachung in verschiedenen Verkaufsstellen eines Fachgeschäftes zum Inhalt hatte.
In der Beschwerde wurde ausgeführt, dass diese Überwachung ohne jede Kenntlichmachung für die Kunden erfolgen würde.
Wir haben dies zum Anlass genommen, zwei dieser Geschäfte unangemeldet aufzusuchen und konnten uns dabei von der Installation jeweils einer Videokamera überzeugen. Die Blickwinkel der Kameras waren offensichtlich über den Verkaufstresen hinaus in den Bereich gerichtet, in dem sich Kunden aufhalten.

Wir haben daher den Inhaber dieser Geschäfte am gleichen Tag, ebenfalls unangemeldet, zwecks einer Datenschutzkontrolle nach § 38 BDSG aufgesucht.
In diesem Kontrollgespräch hat sich folgendes ergeben:
Die Überwachung mittels Video (Bild und Ton) in den vorgenannten Verkaufseinrichtungen wurde bestätigt.
Der Einsatz der Videoüberwachung wurde durch den Geschäftsführer als eine vorbeugende Maßnahme bezeichnet. Dies sei vor allem in Bezug auf die Vorgänge im Kundenbereich und damit zusammenhängender eventueller Vorkommnisse zu sehen.
Einen konkreten Anlass für die Installation der Überwachungstechnik habe es nicht gegeben.
Die Auswertung der Video- und Tonsignale finde ausschließlich im Büro des Inhabers statt. Eine Aufzeichnung von Bild und Ton werde nicht vorgenommen.
Die Art der Auswertung beschränke sich auf das sporadische Einschalten des Systems und Betrachten der Bilder durch den Inhaber. Andere Personen seien nicht damit betraut. Das Büro sei abschließbar und es sei bei Abwesenheit des Inhabers auch verschlossen.
Die bei der Überprüfung der beiden Ladengeschäfte festgestellten fehlenden Hinweise auf die Durchführung der Videoüberwachung wurden durch den Inhaber bestätigt.
Durch die Inbetriebnahme des Systems konnten wir uns von dem bei der Überprüfung der beiden Ladengeschäfte festgestellten Blickwinkel der Kameras in Richtung Kundenbereich vor den Verkaufstresen überzeugen.
Datenschutzrechtliche Bedenken im Zusammenhang mit der Installation der Videoüberwachung wurden seitens des Inhabers nicht gesehen. Die Regelungen im BDSG zur Videoüberwachung sind im Unternehmen nach Auskunft des Inhabers nicht bekannt.

Hinsichtlich der Zulässigkeitskriterien nach § 6 b Abs. 1 BDSG haben wir festgestellt:

Bezüglich des Wahrnehmung des Hausrechtes ist der Inhaber grundsätzlich befugt, geeignete Maßnahmen zum Schutz der Objekte zu ergreifen. Die vom Inhaber dargelegten Gründe für die Überwachung erfüllen allerdings dieses Kriterium nicht.

Für die Überwachung des öffentlichen Ladenbereiches reicht das Motiv einer allgemeinen abstrakten Gefahrenvorbeugung nicht aus. Es müssten belegbare Tatsachen eine Annahme rechtfertigen, dass schwerwiegende Beeinträchtigungen der durch das Hausrecht geschützten Interessen drohen.
Zu beachten ist auch die geforderte Abwägung mit den schutzwürdigen Interessen der betroffenen Kunden. Deren Interesse, unbeobachtet von Bild (und Ton!) einkaufen zu können, überwiegt den Schutzzweck des Inhabers.

Auch die dritte Alternative "Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke" kommt nicht zur Anwendung, da es allein schon an einer schriftlich Konzeption fehlt, die nach dem Willen des Gesetzgebers (Gesetzesbegründung zum BDSG) bereits vor Einführung der Maßnahme vorliegen muss.

Zu der in § 6 b Abs. 2 BDSG geforderten Kenntlichmachung der Überwachung stellten wir folgendes fest:

Eine Videoüberwachung ist durch geeignete Maßnahmen den Betroffenen kenntlich zu machen, das bedeutet, für alle Kunden gut sichtbare Hinweisschilder anzubringen, auf denen auf die Überwachung hingewiesen wird. Dies kann ein kurzer Text, aber auch ein entsprechendes Piktogramm sein. Der weiteren Forderung nach Bekanntgabe der verantwortlichen Stelle, die für die Überwachung zuständig ist, müsste nicht nachgekommen werden. Diese Stelle wäre im speziellen Fall ohne weiteren Hinweis dem Inhaber des Ladengeschäfts zuzuordnen.
Eine solche Kenntlichmachung ist im vorliegenden Fall nicht erfolgt. Damit kann der Kunde nicht frei entscheiden, ob er trotz Videoüberwachung in Bild und Ton das Geschäft betreten will oder aber auf einen Einkauf verzichtet.

Wir haben folgenden Schluss aus der Kontrolle der Videoüberwachung gezogen:

Die Aufsichtsbehörde ist nach § 38 Abs. 5 BDSG ermächtigt, Maßnahmen zur Beseitigung von technischen und organisatorischen Mängeln zu fordern. Bei schwerwiegenden Mängeln, wenn diese mit besonderer Gefährdung des Persönlichkeitsrechtes verbunden sind, kann sie den Einsatz einzelner Verfahren auch untersagen.

Wir sahen in unserer Bewertung der Videoüberwachung des öffentlich zugänglichen Kundenbereiches keine Möglichkeiten, dieses Verfahren in dieser Form zu akzeptieren. Aus diesem Grunde verlangten wir eine Stilllegung des Systems. Dem wurde nach einigen Korrespondenzen mit dem Anwalt des Inhabers dieser Fachgeschäfte auch entsprochen.

5.2.5 Krankenversichertenkarte als Zutrittskontrollmedium

Die Beschwerden eines betroffenen Bürgers und einer Krankenkassenvereinigung bezogen sich auf folgenden Sachverhalt in einer Gesundheitseinrichtung:

In der Einrichtung wird in Kombination eine kommerzielle Nutzung als Fitness- / Saunazentrum vorgenommen und es erfolgt die Leistungserbringung einer ambulanten Heilmittelversorgung in Form von Physiotherapie und Ergotherapie.
Im zentralen Eingangsbereich der Einrichtung war ein Chipkartenlesegerät installiert mittels dem den Besuchern beider Bereiche der Einrichtung Zutritt gewährt wurde. Als Chipkarte diente dabei nicht etwa eine hauseigene Karte, sondern die normale Krankenversichertenkarte der Besucher.

Die Karte erfüllte damit gewissermaßen die Funktion einer Art Club- bzw. Mitgliederkarte.

Der Gesetzgeber hat die Krankenkassen zum 01.01.1995 verpflichtet, für alle Versicherten die Krankenversichertenkarte (KVK) einzuführen. Die gesetzlichen Grundlagen für die Verwendung dieses Mediums finden sich im Sozialgesetzbuch (SGB), speziell in § 291 SGB V.
In Abs. 2 dieser Vorschrift sind die in maschinenlesbarer Form auf dem Chip der KVK gespeicherten Daten aufgeführt:

- Name, Vorname des Versicherten
- Geburtsdatum
- Anschrift
- Krankenversichertennummer
- Versicherungsstatus
- Datum des Beginns des Versicherungsschutzes
- Datum des Fristablaufs der Gültigkeit der Karte

Der Verwendungszweck der KVK ist in § 291 Abs. 1 Satz 3 SGB V dargelegt:
"Sie darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung sowie für die Abrechnung mit den Leistungserbringern verwendet werden."
Durch diese eindeutige Regelung hat der Gesetzgeber darüber hinausgehende Verwendungen nicht vorgesehen.
Aus diesen Festlegungen ergibt sich, dass die in der Einrichtung vorgenommene Zutrittskontrolle mittels der KVK unzulässig ist.

Das BDSG hat den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
Die Anwendbarkeit des BDSG ergibt sich in diesem Fall aus § 1 Abs. 2 Nr. 3:
"Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen, soweit sie Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben .... ."

Mit der von der Einrichtung durchgeführten Zutrittskontrolle mittels KVK liegt eine Verarbeitung der Daten der KVK unter Einsatz einer Datenverarbeitungsanlage vor.
Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.
Bevor eine Einwilligung des Betroffenen als alternative Zulässigkeitsvoraussetzung in Betracht kommt, hat die Einrichtung als verantwortliche datenverarbeitende Stelle die Zulässigkeit nach BDSG oder einer anderen Rechtsvorschrift zu prüfen.

Das BDSG kommt aber nur subsidiär zur Anwendung. Nach § 1 Abs. 3 Satz 1 BDSG gehen andere Rechtsvorschriften des Bundes, die auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, den Vorschriften dieses Gesetzes vor.

Damit gehen die Vorschriften des SGB denen des BDSG vor.

Die Aufsichtsbehörde kontrolliert nach § 38 Abs. 1 Satz 1 BDSG die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz.
Nach § 38 Abs. 5 Satz 1 BDSG kann die Aufsichtsbehörde zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz anordnen, dass

im Rahmen der Anforderungen nach § 9 BDSG Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden.

Zu den in § 9 BDSG genannten Anforderungen gehört gemäß Anlage zu § 9 unter Punkt 3, dass dabei insbesondere Maßnahmen zu treffen sind, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle).
Da eine solche Zugriffsberechtigung nach § 291 Abs. 1 Satz 3 SGB V auf die Daten der KVK nicht gegeben ist, musste die Organisationsform in der Einrichtung geändert werden.

Die im Zusammenhang mit der bisherigen Verwendung der KVK gespeicherten Daten waren entsprechend § 35 Abs. 2 Satz 2 Nr. 1 BDSG unverzüglich und unwiederbringlich zu löschen.
Wir haben nach § 38 Abs. 5 Satz 1 BDSG die Unterlassung der missbräuchlichen Verwendung der KVK und die Löschung der Daten gemäß § 35 Abs. 2 Satz 2 Nr. 1 BDSG angeordnet.

5.2.6 Patientendaten bei einem Krankenhausumzug

Die Fachklinik einer großen medizinischen Einrichtung plante ihren Umzug einschließlich der Verlegung der Patienten aus einem Innenstadtbereich in einen Neubaukomplex am Rande der Stadt. Über die logistischen und organisatorischen Vorbereitungen wurde bereits vor dem geplanten Umzugstermin in den Printmedien berichtet.
Nach der erfolgreichen Durchführung des Umzugs machte ein elektronisches Medium die Aufsichtsbehörde auf folgenden Umstand aufmerksam:

Das Kamerateam einer Fernsehstation suchte nach dem Umzug die offen stehende Immobilie der geräumten Klinik auf. Grund dieser Maßnahme sei nach Aussage des Senders die Information von Anwohnern gewesen, nach der fremde Personen am Wochenende nach dem offiziellen Umzug das Klinikgelände bevölkert hätten und alte Einrichtungsgegenstände mitgenommen hätten.
In dem ausgestrahlten Beitrag waren im Eingangsbereich verstreut Karteikästen mit Karteikarten zu sehen.
Bei der Kontaktaufnahme mit der Fernsehstation wurde uns von dieser mitgeteilt, dass die Klinik der Fernsehstation gegenüber keine Aussagen zu dem Vorgang machen wolle.

Die Aufsichtsbehörde hat daraufhin unverzüglich einen Vor-Ort-Termin in der alten Klinik vereinbart, an dem neben dem Vertreter der Aufsichtsbehörde der Datenschutzbeauftragte der Klinik und ein Verantwortlicher aus dem Bereich der Umzugsorganisation teilnahmen.

Bei der Kontrolle wurde folgendes festgestellt:
Im Eingangsbereich des Kellergeschosses wurden leere Holzkarteikästen gefunden. Es befanden sich Karteikarten in einem der vielen ansonsten leeren Holzkarteikästen. Die Karteikarten waren inzwischen durch Mitarbeiter der Klinik sichergestellt worden. Es war ungeklärt, warum diese Kästen dort lagen und es war auch ungeklärt, weshalb in einem der Kästen sich ca. 50 von diesen Karteikarten befunden hatten.

Die Karteikarten enthielten
Name, Vorname, Geburtsname, Geburtsdatum, Wohnanschrift, Beruf
von früheren Patienten.

Die Karteikarten stellten eine sog. Zwischenkartei dar. Auf den Rückseiten der Karteikarten befanden sich eine Jahreszahl und eine Nummer, die auf die eigentliche Patientenakte verwies. Die Patientenakten selbst waren bereits geraume Zeit vor dem Umzug in das Hauptarchiv auf dem Klinikhauptgelände verbracht worden.

Nach den Aussagen der Mitarbeiter seien die Außenzugänge zu den Gebäuden verschlossen gewesen bis auf diesen Kellergeschosszugang, der während des Umzugs benutzt worden sei.

Die Pforte zum Gelände sei montags bis freitags von 7.00 Uhr bis 15.30 Uhr besetzt, zu den übrigen Zeiten nicht. In den übrigen Zeiten sei es aber gewährleistet, dass alle Außentüren verschlossen seien. Hinweise auf gewaltsames Eindringen habe es nicht gegeben.

Es wurde von uns festgestellt, dass sich die Karteikarten mit den personenbezogenen Angaben in unverschlossenen Behältnissen und nicht in einem verschlossenen Extraraum befunden hatten. Dabei war die Aktualität dieser Daten unerheblich und es war auch unerheblich, dass der Zugang zu dem Kellergeschoss außerhalb der Zeiten des Umzuges verschlossen gewesen sein soll.

Datenschutzrechtlich war das ungesicherte Aufbewahren der Karteikarten an diesem Ort als Verstoß zu werten. Die Bestimmungen zu den technisch-organisatorischen Maßnahmen zur Datensicherheit nach § 9 BDSG und dessen Anlage waren nicht korrekt eingehalten worden.
In der Anlage zu § 9 Satz 1 BDSG heißt es in Nr. 4 unter anderem:

> *" ...es ist zu gewährleisten, dass personenbezogene Daten .... während ihres Transportes ... nicht unbefugt gelesen ....werden können..."*

Zu den unbeantwortet gebliebenen Fragen haben wir eine Stellungnahme der Klinik abgefordert, des weiteren wurden die aktuelle Datenschutzordnung des Hauses, die Unterlagen zum Umzug, aus denen der Umgang mit personenbezogenem Material zu ersehen ist und allgemeine und spezielle Verpflichtungs- bzw. Belehrungsmaterialien zum Umzug kontrolliert.

Die Auswertung hat ergeben, dass alle Unterlagen die notwendigen Ausführungen enthielten, den Datenschutz im Hause und einen ordnungsgemäßen Umzug zu gewährleisten. Der Vorfall war auf persönliches Fehlverhalten von Klinikmitarbeitern zurückzuführen.

Der später durchgeführte Umzug einer weiteren Fachklinik stand dann unter besonderer Beachtung der Sicherheitsanforderungen, damit auch des Datenschutzes, und wurde ohne diesbezügliche Vorkommnisse durchgeführt.

5.2.7 Erstellung einer Liste zur Hotelanmeldung während der Busreise

Ein Beispiel dafür, dass auch offenbar Nebensächlichkeiten, bei denen nicht einmal das BDSG zur Anwendung kommen kann, das Persönlichkeitsrecht des Einzelnen berühren können, stellt die folgende Beschwerde dar.

Anlässlich einer Urlaubsreise ins Ausland, organisiert und durchgeführt von einem Reisebüro, wurde während der Fahrt im Bus durch die Reisebegleitung die Vorbereitung der Hotelanmeldungen erledigt.

Zu diesem Zweck wurde im Durchlaufverfahren, d.h. durch Weitergabe einer Liste von Reiseteilnehmer zu Reiseteilnehmer, eine Erfassung der notwendigen Anmeldedaten (Name, Vorname, Geburtsort, Geburtsdatum, Wohnort und Ausweis-/Reisepassnummer) vorgenommen.

Der Beschwerdeführer fühlte sich dadurch in seinem Persönlichkeitsrecht beeinträchtigt und fragte an, ob diese Verfahrensweise mit dem Datenschutz vereinbar sei.

Mit der listenmäßigen Erfassung der Hotel-Anmeldedaten in Form eines Umlaufes im Reisebus bereits während der Fahrt ist sicherlich eine Variante gewählt worden, die eine Entlastung des Einzelnen bei der ansonsten teilweise zeitaufwändigen Anmeldung bei Gruppenreisen an der Hotelrezeption mit sich bringt.
Die hier gewählte Variante stellt jedoch einen Verstoß gegen das Persönlichkeitsrecht des Einzelnen dar, nämlich frei über die Preisgabe seiner persönlichen Daten entscheiden zu können. Mit der gewählten Form der Datenerhebung kann der einzelne Reisende unter Zugzwang stehen, diese Form akzeptieren zu müssen.
Zweck der Erhebung ist die Anmeldung des Reisenden beim Hotel. Diese Erhebung findet ansonsten individuell an der Rezeption des Hotels statt und zwar zwischen dem Reisenden und dem Hotelangestellten, also ohne dass unbefugte Dritte von den Daten des Reisenden Kenntnis nehmen können.
Will man diese Erhebung der Hotelanmeldedaten bereits während der Fahrt durchführen, dann sollte das in einer Form erfolgen, bei der Dritte keine Kenntnis erhalten können. Dazu sollten Zettel mit der Beschreibung der zu erhebenden Daten vorbereitet sein, um sie jedem Reisenden zum individuellen Ausfüllen übergeben zu können. Diese Zettel würden danach durch den Reisebegleiter eingesammelt und bei Ankunft an den Hotelangestellten übergeben. Damit wäre gewährleistet, dass keine Einsichtnahme unberechtigter Dritter, z.B. der Mitreisenden, in die Daten des Einzelnen möglich ist.

6. Außenwirkung der Aufsichtsbehörde

Nach § 38 Abs. 1 Satz 6 BDSG hat die Aufsichtsbehörde regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen.
Dieser Vorgabe kommt das Thüringer Landesverwaltungsamt mit dem vorliegenden Bericht über den Berichtszeitraum 2003 / 2004 nach.

Im Berichtszeitraum wurden 2 Vorträge über den Datenschutz im nicht-öffentlichen Bereich im Rahmen der Fortbildung betrieblicher Datenschutzbeauftragter eines Logistikunternehmens gehalten.

Die Aufsichtsbehörde ist seit dem Jahre 1993 im Erfahrungsaustauschkreis (ERFA-Kreis) Thüringen der Gesellschaft für Datenschutz und Datensicherheit 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 Berichtzeitraum nach den dienstlichen Möglichkeiten teilgenommen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich führen seit 1995 einen jährlichen Erfahrungsaustausch (Workshop) durch. Diese bundesweite Veranstaltung wird im Wechsel jeweils von einer anderen Aufsichtsbehörde organisiert.
Im Berichtszeitraum erfolgte die Teilnahme an den Workshops 2003 bei der Regierung von Mittelfranken als zentraler Aufsichtsbehörde für Bayern und 2004 beim Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen.

Seit Beginn dieses Berichtszeitraumes ist die Aufsichtsbehörde, wie bereits eingangs erwähnt, im Internet präsent (siehe 1. Vorbemerkungen zum Tätigkeitsbericht).

Auch dieser Tätigkeitsbericht wird in das Internet eingestellt werden.

7. 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. Ein angemessenes Datenschutzniveau ist nicht erforderlich, wenn eine der Ausnahmen des Absatzes 1 vorliegt.

Im Berichtszeitraum wurden bei der Aufsichtsbehörde keine Genehmigungsanträge für Datenübermittlungen in Drittländer gestellt.

8. Datenschutzgerechte Verhaltensregeln von Berufsverbänden

Nach § 38 a BDSG kann die Aufsichtsbehörde Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen, die durch Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, erarbeitet wurden, überprüfen.

Solche Prüfungen sollen nach dem Willen des Gesetzgebers verhindern, dass sich die genannten Verbände interne Verhaltensregeln geben, die im Widerspruch zu den gesetzlichen Regelungen stehen. Daher überprüft die Aufsichtsbehörde die Vereinbarkeit der Regelungen mit dem geltenden Datenschutzrecht.

Entwürfe von Verhaltensregeln sind der Aufsichtsbehörde im Berichtszeitraum nicht zur Prüfung vorgelegt worden.

9. Zusammenwirken mit dem Thüringer Innenministerium

Das Thüringer Innenministerium (TIM) ist Oberste Aufsichtsbehörde für den Datenschutz. In dieser Funktion werden im zuständigen Fachreferat sämtliche Grundsatzangelegenheiten bezüglich des Datenschutzes bei den nicht-öffentlichen Stellen im Freistaat Thüringen bearbeitet. Insoweit gibt es zwischen dem TIM und der Aufsichtsbehörde Thüringer Landesverwaltungsamt einen ständigen fachlichen Kontakt. Der regelmäßige Informationsaustausch ist gewährleistet.

Die Vertretung Thüringens im Düsseldorfer Kreis, dem Gremium der Obersten Aufsichtsbehörden, wird durch das TIM wahrgenommen. Auch über die Beschlüsse dieses Gremiums, die als Richtschnur für das Handeln der Aufsichtsbehörden gelten, wird die Aufsichtsbehörde durch das TIM zeitnah und umfassend informiert.

Die Arbeit im Düsseldorfer Kreis, der regelmäßig zweimal jährlich zu seinen Beratungen zusammenkommt, ist darüber hinaus durch die Tätigkeit in Arbeitsgruppen gekennzeichnet. Das TIM vertritt Thüringen hierbei in der Arbeitsgruppe "Telekommunikation, Tele- und Mediendienste".

10. Abschließende Betrachtungen zur gegenwärtigen Entwicklung

Die gegenwärtige Zeit ist gekennzeichnet durch vielfältige technische Innovationen und daraus entstehenden Anwendungen gerade auch im nicht-öffentlichen Bereich, die umfangreiche Schnittstellen zu den personenbezogenen Daten der Bürgerinnen und Bürger besitzen.
Auf die daraus entstehenden datenschutzrechtlichen Probleme möchten wir abschließend in diesem Tätigkeitsbericht hinweisen. Dabei erlauben wir uns, auf zwei Veröffentlichungen des Bundesbeauftragten für den Datenschutz, Herrn Peter Schaar, zurückzugreifen.

Im Rahmen einer Datenschutzfachtagung der Gesellschaft für Datenschutz und Datensicherheit im November 2004, die unter dem Leitthema "Orwells 1984 - 20 Jahre danach" stand, referierte der Bundesbeauftragte für den Datenschutz zu dem Thema "Überwachung des Bürgers durch Staat und Wirtschaft - welche Perspektiven hat der Datenschutz?".
Daraus und aus einem Fachbeitrag des Bundesbeauftragten im Januar 2005 sollen abschließend einige Gedanken wiedergegeben werden.

George Orwell schrieb im Jahre 1948 vor dem Hintergrund des Totalitarismus von Faschismus und Stalinismus das Werk "1984", das einen Überwachungsstaat beschreibt, in dem mit fortgeschrittener Technik eine beinahe totale Überwachung in allen Bereichen des öffentlichen und privaten Lebens durchgeführt wird.

Dass sich diese Horrorvision ein halbes Jahrhundert nach Erscheinen des Werkes zumindest in Europa und anderen demokratischen Staaten zum Glück nicht verwirklicht hat, ist der gesellschaftlichen Entwicklung seit Ende des letzten Weltkrieges bis heute zu verdanken.
Demokratie bedeutet nicht zuletzt auch Begrenzung staatlicher Macht und Schutz von Menschenwürde und Privatsphäre.

Das Volkszählungsurteil des Bundesverfassungsgerichtes von 1983 setzte die rechtsstaatlichen Grenzen der Datenverarbeitung und bekräftigte das Recht auf Selbstbestimmung des Einzelnen über die Verwendung seiner persönlichen Daten.

Seit dieser Zeit hat sich das Bild gewandelt, die Gesellschaft verändert. Der Bürger misstraut nicht allein und vorrangig dem Staat, sondern das gegenseitige Misstrauen nimmt auch im Geschäftsverkehr zu.
Für die private Wirtschaft ist eine zunehmende Datenverarbeitung in den Unternehmen zu verzeichnen. Die Begehrlichkeiten der Datengewinnung drücken sich in folgenden Schwerpunktbereichen aus.

- Im Rahmen des Risikomanagements werden mittels Scoringverfahren die Kreditwürdigkeiten weitgehend unabhängig vom tatsächlichen Verhalten des Betroffenen beurteilt, selbst wenn keine negativen Informationen über das Zahlungsverhalten aus der Vergangenheit vorliegen. Es werden Prognosen mittels statistisch-mathematischer Methoden über das zukünftige Verhalten von Personengruppen erstellt, denen dann der Einzelne zugeordnet wird.
  Mikrogeographische und soziodemographische Daten dienen der Profilgewinnung, die dem Einzelnen die Möglichkeit nimmt, selbst über sein Erscheinungsbild in der Öffentlichkeit zu entscheiden oder dieses Erscheinungsbild durch eigenes Verhalten zu beeinflussen.

- Die verschiedensten Auskunfts- und Hinweissysteme in der Kreditwirtschaft, in der Versicherungswirtschaft und neuerdings auch in der Wohnungswirtschaft dienen der Beurteilung der Zahlungskräftigkeit und Vertrauenswürdigkeit potenzieller Kunden oder Geschäftspartner. Rufen verschiedenste Unternehmen aus unterschiedlichen Branchen Informationen ab, dann kann der Betroffene gläsern gemacht werden.

- Ein gläserner Käufer kann auch durch die Kundenkarten erzeugt werden. Als Gegenleistung für eine Rabattgewährung wollen die Unternehmen Angaben zu Interessen, Konsum- und Kaufgewohnheiten, sozialen und familiären Verhältnissen. Transparenz der Verfahren sowie umfassende und verständliche Informationen an den Kunden über Umfang und Zweck der Datenverarbeitung sind hier vonnöten.

- Die Analyse des menschlichen Genoms kann noch gravierendere Einschnitte für den Betroffenen erbringen. Außer der Anwendung der DNA-Analyse im Bereich der Verbrechensbekämpfung und Überführung von Straftätern sind Nutzungen denkbar und evtl. auch schon im Einsatz bei der Klärung von Kindschaftsverhältnissen, dem Abschluss von Lebens- und Krankenversicherungen oder bei Einstellungen und Kündigungen im Arbeitsleben.

- Die öffentlich umstrittenen Funkchips, deren Basis die sogenannte RFID-Technologie darstellt, werden momentan noch überwiegend als Produktkennzeichnungen in der Logistik eingesetzt. Damit ist noch keine direkte Verknüpfung mit personenbezogenen Daten hergestellt. Aber bereits die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 sollen RFID-Chips mit den personenbezogenen Daten des Kartenerwerbers zu dessen Eingangskontrolle in den Stadien enthalten.
  Mit einer geplanten umfassenden Kennzeichnung von Waren im Einzelhandel mit RFID-Chips könnten Verknüpfungen zwischen den Waren und deren Käufern hergestellt werden. Die Chips werden aktiv, sobald sie in die Reichweite eines passenden Lesegerätes gelangen, Damit erfolgt ein automatisiertes Erfassen der Waren an der Kasse unter Erfassung weiterer personenbezogener Daten bei Bezahlung durch den Kunden mittels EC-Karte.

  Durch die fortschreitende Verbreitung der RFID-Technologie können reale Gefahren entstehen, die wieder in Richtung "gläserner Kunde/Bürger" gehen. Somit steht auch hier die Forderung nach einer gesetzlichen Steuerung in Richtung Transparenz und möglicher Entscheidungsfreiheit für den Kunden.

Datenschutz will technische Entwicklungen nicht behindern. Alle sollten sich aber möglicher entstehender Gefahren für das freie Persönlichkeitsrecht des Einzelnen bewusst sein.

Ein wichtiger Grundsatz sollte daher das enge Zusammenwirken von Entwicklern, künftigen Nutzern und Datenschützern bereits in der Projektierungsphase neuer Anwendungen sein.