Landtag Brandenburg **Drucksache 5/1803**

5. Wahlperiode

Bericht

der Landesregierung

Fünfzehnter Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörde an den Landtag des Landes Brandenburg

Datum des Eingangs : 11.08.2010 / Ausgegeben : 13.08.2010

1 Einleitung

Der Bericht gibt einen Überblick über die Tätigkeit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich im Land Brandenburg. Grundlage für den regelmäßigen Bericht ist § 38 Absatz 1 Satz 6 Bundesdatenschutzgesetz (BDSG). Die Berichterstattung erstreckt sich auf der Grundlage von § 27 Brandenburgisches Datenschutzgesetz über einen Zeitraum von 2 Jahren und zwar vom 1. Januar 2008 bis 31. Dezember 2009.

Im Zuständigkeitsbereich der Aufsichtsbehörde befinden sich derzeit ca. 94.000 Unternehmen (z.B. Handel, Gast-, Bau- oder Verarbeitendes Gewerbe). In dieser Angabe sind die Freiberufler und Unternehmen in der Landwirtschaft nicht enthalten, da entsprechende Zahlen nicht vorliegen. Gleichwohl fallen auch diese Stellen in den Zuständigkeitsbereich der Aufsichtsbehörde, sofern deren Sitz im Land Brandenburg liegt.

Zusätzlich erfolgt eine regelmäßige fachliche Befassung und Einbindung in Themenkomplexe, die im „Düsseldorfer Kreis“, einem Gremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, erörtert werden. Ferner werden jährlich 2 Sitzungen der Arbeitsgruppe „Auskunfteien“ des Düsseldorfer Kreises durchgeführt. Die Federführung teilten sich bisher abwechselnd das Ministerium des Innern des Landes Brandenburg und das Hessische Ministerium des Innern und für Sport. Ein Vertreter der Aufsichtsbehörde nimmt regelmäßig an den Sitzungen der Arbeitsgrupppe „Telekommunikation, Tele- und Mediendienste“ in Berlin teil.

2 Übersicht über die Kontrolltätigkeit

2.1 Meldungen zum Register

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich führt das Register nach § 4d BDSG. Es dient der Transparenz und kann von jedermann eingesehen werden. Das Einsichtsrecht erstreckt sich jedoch nicht auf die Angaben nach § 4e Satz 1 Nr. 9 BDSG (Datensicherungsmaßnahmen/Sicherheitskonzept) sowie auf die Angabe der zugriffsberechtigten Personen.

Alle Unternehmen, die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung speichern (z.B. Wirtschaftsauskunfteien, Adresshändler, Markt- und Meinungsforschungsinstitute), unterliegen der Meldepflicht bei der Aufsichtbehörde.
Für die übrigen Firmen entfällt die Meldepflicht, wenn diese einen betrieblichen Datenschutzbeauftragten bestellt haben (§ 4d Abs. 2 BDSG). Sie entfällt ebenso, wenn mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten höchstens neun Personen in der Regel ständig beschäftigt sind und entweder eine Einwilligung des Betroffenen vorliegt oder die Datenverarbeitung zu Vertragszwecken beziehungsweise im Rahmen eines vorvertraglichen Vertrauensverhältnisses mit dem Betroffenen erforderlich ist.
Im Berichtszeitraum wurden keine Auskunftsbegehren zur Einsicht in das Register an die Aufsichtsbehörde herangetragen.

Die Registerübersicht gliedert sich folgendermaßen:

Gesamtmeldungen:	**13**
Davon	
Auskunfteien:	**7**
Markt- und Meinungs-	
Forschungsinstitute:	**5**
Detektei:	**1**

2.2 Beschwerden

Im Berichtszeitraum gingen **425** schriftliche Beschwerden sowie **72** schriftliche Informationsanfragen bei der Aufsichtsbehörde ein, die durch die Mitarbeiter bearbeitet wurden. Telefonische Anfragen werden statistisch nicht erfasst.

Im Laufe des Berichtszeitraums hat das Thema Datenschutz bundesweit eine gesteigerte Aufmerksamkeit erfahren. Zahlreiche publik gemachte Skandale und Verfehlungen in Wirtschaftsunternehmen und sonstigen Daten verarbeitenden Stellen, haben den Datenschutz in den Focus des überregionalen öffentlichen Interesses gerückt.

Bei der Datenschutzaufsicht machte sich diese neue Entwicklung dadurch bemerkbar, dass die Anfragen und Beratungsbedarfe sowohl von Bürgerinnen und Bürgern als auch von Unternehmen im Berichtzeitraum enorm gestiegen sind. Auch in den Unternehmen wird den Anliegen der betrieblichen Datenschutzbeauftragten mehr Aufmerksamkeit geschenkt als dies vorher üblicherweise der Fall war. Viele sind sich ihrer Verantwortung und des Risikos datenschutzwidrigen Verhaltens für ihren wirtschaftlichen Erfolg bewusst geworden. Der Datenschutz wird vermehrt als Qualitätsmerkmal erkannt. Der vorliegende Bericht zeichnet die wesentlichen Entwicklungen im Datenschutzrecht nach und wirft ein Schlaglicht auf einzelne Datenschutzverstöße und -probleme, die der Aufsichtsbehörde bekannt geworden sind.

Beschwerden und Anfragen, die nicht der Zuständigkeit der Aufsichtsbehörde Brandenburg unterlagen, wurden an die zuständigen Behörden weitergeleitet. Die örtliche Zuständigkeit erstreckt sich auf die der Aufsicht unterliegenden zu kontrollierenden nicht-öffentlichen Stellen allein mit Sitz im Land Brandenburg
(§ 1 Datenschutzzuständigkeitsverordnung i.V.m. § 38 Absatz 6 BDSG).

Unter Punkt 5 werden nähere Ausführungen zu einigen Beschwerden gemacht.

3 Allgemeines

3.1 Neuregelungen im Bundesdatenschutzgesetz

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

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

3.1.1 Die BDSG-Novelle I umfasst Neuregelungen, die sich insbesondere auf die Tätigkeit von Auskunfteien und den Einsatz von Scoring-Systemen beziehen

Thematische Schwerpunkte dieser Novelle sind:

Zulässigkeit von Scoring

Hinsichtlich der seit einiger Zeit in immer größerem Umfang genutzten Scoring-Verfahren sollen verbindliche Regelungen zu deren Nutzung Rechtsklarheit schaffen und eine Verbesserung der Transparenz für die Betroffenen bezüglich dieser, insbesondere von Auskunfteien praktizierten, Verfahren erreicht werden.
Nach § 28b Nr. 1 BDSG dürfen zum Zwecke der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Verhalten eines Betroffenen nur noch dann erhoben oder verwendet werden, wenn die zur Berechnung von Wahrscheinlichkeitswerten genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind.
Die Vorgaben zum Scoring und zur Bonitätsbewertung haben neben dem Auskunfteibereich und der Kreditwirtschaft auch Auswirkungen auf andere Unternehmensbereiche wie etwa innerhalb der Telekommunikation, des Versandhandels oder der Versicherungen, da auch hier regelmäßig das Ausfallrisiko mit Hilfe von Scorewerten ermittelt wird, wenn das Unternehmen in Vorleistung geht.

Scoring – Verbesserung der Transparenz für den Betroffenen

Durch Einführung des § 28b BDSG hat der Gesetzgeber die Voraussetzungen für die Erhebung und Verwendung eines Wahrscheinlichkeitswerts (Score-Werts) für ein bestimmtes zukünftiges Verhalten des Betroffenen festgelegt.
Die Nutzer von Scoring-Verfahren müssen nun auf Anfrage Betroffenen Auskunft über das Zustandekommen und die Bedeutung eines Scorewertes in allgemein verständlicher Form erteilen. Nach § 34 Abs. 2 BDSG ist den Betroffenen bei dem Einsatz von Scoring-Verfahren auf Verlangen einzelfallbezogen und nachvollziehbar in allgemeinverständlicher Form Auskunft zu erteilen über

- die Wahrscheinlichkeitswerte,

- die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten sowie
- das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte.

Einmeldung von Forderungen bei einer Auskunftei

Für die Übermittlung personenbezogener Daten durch Unternehmen an Auskunfteien wurde als allgemeine Rechtsgrundlage bislang der § 28 BDSG herangezogen. Der Gesetzgeber hat nun mit dem § 28a BDSG eine Vorschrift geschaffen, mit der in einem konkreten Katalog festgelegt ist, unter welchen Voraussetzungen Daten über eine Forderung bei einer Auskunftei eingemeldet werden dürfen.
Mit Absatz 2 des neuen § 28a BDSG ist auch geregelt worden, unter welchen Umständen Kreditinstitute personenbezogene Daten über Vertragsverhältnisse an Auskunfteien übermitteln dürfen. Hierüber ist der Betroffene vor Vertragsabschluss zu unterrichten.

3.1.2 Mit der BDSG-Novelle II erfolgten vor allem Änderungen im Zusammenhang mit der Werbung und der Markt- und Meinungsforschung sowie zum Arbeitnehmerdatenschutz

Thematische Schwerpunkte dieser Novelle sind:

Kündigungsschutz für betriebliche Datenschutzbeauftragte

Der Gesetzgeber hat mit Hinblick auf die bestehenden Unsicherheiten hinsichtlich einer Kündigung des zugrunde liegenden Arbeitsverhältnisses nun durch einen expliziten Kündigungsschutz die rechtliche Stellung der betrieblichen Datenschutzbeauftragten, vergleichbar mit denen von Betriebsratsmitgliedern, gestärkt. Hierdurch soll die Unabhängigkeit in der Ausübung der Tätigkeit gewährleistet werden. Betriebliche Datenschutzbeauftragte haben nun auch einen Rechtsanspruch auf geeignete Aus- und Fortbildung, um den Anforderungen an ihre Fachkunde gerecht werden zu können

Auftragsdatenverarbeitung

Mit einer Präzisierung des § 11 BDSG wurden die gesetzlichen Anforderungen an die Ausgestaltung des Auftrags deutlicher herausgestellt, um mehr Rechtssicherheit für die beteiligten Auftragnehmer und -geber sowie die Aufsichtsbehörden zu gewährleisten. Bei der Auftragsdatenverarbeitung ist im Gesetz neuerdings ausdrücklich geregelt, zu welchen Punkten ein Auftragsdatenverarbeitungsvertrag dezidierte Aussagen treffen muss. Zudem wurde § 11 BDSG dahingehend konkretisiert, dass sich der Auftraggeber erstmals „vor Beginn der Datenverarbeitung und sodann regelmäßig" von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen hat. Durch die zusätzlich vorgesehene „regelmäßige" Kontrolle wird klargestellt, dass insbesondere bei längerfristigen Auftragsdatenverarbeitungen eine einmalige Kontrolle nicht ausreicht. Das Ergebnis der Prüfung ist zu dokumentieren.

Eine mit Stand vom 23. April 2010 aktualisierte Mustervereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen nach § 11 BDSG ist als Anlage beigefügt. Die Hessische Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich hält diese auch zum download auf ihrer Homepage http://www.rp-darmstadt.hessen.de unter der Rubrik „Sicherheit & Ordnung" Unterpunkt „Auftragsdatenverarbeitung" bereit.

Datenverarbeitung zum Zweck der Markt- und Meinungsforschung sowie der Werbung

Mit § 28 Abs. 3 und 4 BDSG wurde die Datenverarbeitung zum Zweck der Markt- und Meinungsforschung sowie der Werbung neu geregelt. Es gilt als Grundsatz das Einwilligungserfordernis der Betroffenen. Von diesem Grundsatz kann jedoch unter bestimmten Voraussetzungen abgesehen werden.

Ohne ausdrückliches Einverständnis bleibt erlaubt, listenmäßig zusammengefasste Daten über Angehörige einer bestimmten Personengruppe mit deren Berufs-, Branchen- oder Geschäftsbezeichnung, Namen, Titel (akademischer Grad), Anschrift und Geburtsjahr für Werbung mit eigenen Angeboten, für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit der Betroffenen sowie für Zwecke der Spendenwerbung zu gebrauchen.

Ferner können zusammengefasste personenbezogene Daten für Zwecke der Werbung auch bei einer sogenannten „transparenten Übermittlung“ nach Maßgabe des § 34 Abs. 1a Satz 1 BDSG übermittelt werden. In diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen. An diese Stelle können sich die Betroffenen dann wenden und Auskunft verlangen über die Herkunft ihrer Daten und die/den Empfänger derselben. Die Betroffenen erhalten hierdurch – jedenfalls mehr als bisher – eine Chance, bezüglich ihrer Daten die Übermittlungskette nachzuvollziehen und die einzelnen Stellen, die im Besitz ihrer Daten sind, zu identifizieren. An diese können sie dann herantreten und eine weitere Nutzung bzw. Übermittlung zu Werbezwecken untersagen.
Eine Nutzung von personenbezogenen Daten zum Zwecke der Werbung für *fremde* Angebote ist zulässig, wenn für die Betroffenen bei der Ansprache die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist.

Der Betroffene ist bereits bei der Erhebung seiner Daten darauf hinzuweisen, dass er der Nutzung zu Werbezwecken widersprechen kann. Nach alter Rechtslage bestand die Möglichkeit erst bei der Ansprache zu Werbezwecken.

In einem gemeinsamen Beschluss des Düsseldorfer Kreises vom 26./27. November 2009 weisen die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich darauf hin, dass für Daten, deren erstmalige Speicherung nicht eindeutig erkennbar ist, die neuen Regelungen angewendet werden. Sie weisen weiterhin darauf hin, dass eine Übermittlung für Werbezwecke nur zulässig ist, wenn Herkunft und Empfänger der Daten gespeichert werden und eine Gruppenauswahl nach einem Merkmal erfolgt (Listenübermittlung). Bei der Werbemaßnahme muss den Adressaten die erstmalig erhebende Stelle mitgeteilt werden. Die bisher weit verbreitete Praxis der Übermittlung von nach mehr als einem Merkmal selektierten Adressen ist unzulässig, sofern keine entsprechende Einwilligung der Betroffenen vorliegt.

Im Übrigen sind folgende Übergangsregelungen des § 47 BDSG zu beachten:

„Für die Verarbeitung und Nutzung vor dem 1. September 2009 erhobener oder gespeicherter Daten ist § 28 BDSG in der bis dahin geltenden Fassung weiter anzuwenden
1. für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010,
2. für Zwecke der Werbung bis zum 31. August 2012.“

Je nach Verwendungszweck gilt das sog. Listenprivileg nach § 28 Abs. 3 Satz 1 Nr.3 BDSG (alt) für die vor dem 1. September 2009 erhobenen oder gespeicherten personenbezogenen Daten bis zu diesen Stichtagen.

Für nach dem 1. September 2009 erhobene oder gespeicherte personenbezogene Daten ist grundsätzlich die Einwilligung des Betroffenen zur Verarbeitung oder Nutzung seiner Daten einzuholen (sog. Opt-in), wenn ein Unternehmen diese für Zwecke des Adresshandels oder für *fremde* Werbezwecke verarbeiten oder nutzen will.

Arbeitnehmerdatenschutz

Im Rahmen von Beschäftigungsverhältnissen werden personenbezogenen Daten aus ganz unterschiedlichen Lebensbereichen der Arbeitnehmer und Arbeitnehmerinnen erhoben, verarbeitet und genutzt.

Mit dem § 32 BDSG ist in der BDSG-Novelle II eine Regelung zum Schutz von Arbeitnehmerdaten aufgenommen worden, ohne dass der Bundesgesetzgeber den Datenschutz im Arbeitsverhältnis umfassend oder speziell für alle Fallgestaltungen einer abschließenden gesetzlichen Regelung zugeführt hätte. Die negativen Erfahrungen im Umgang mit diesen Daten im Bereich der Discounter, der Telekom AG, der Bahn AG und der zunehmende Einsatz von verschiedensten neuartigen Techniken (z.B. Videoaufzeichnungen, Navigation via GPS) durch Arbeitgeber haben eine Verbesserung des Arbeitnehmerdatenschutzes zunehmend notwendig gemacht und den Gesetzgeber zu diesem Schritt veranlasst.

Obgleich Rechtsvorschriften zum Arbeitnehmerdatenschutz noch diskutiert werden, hat der Gesetzgeber für Verarbeitungen von Arbeitnehmerdaten zu Zwecken des Beschäftigungsverhältnisses eine erste Regelung formuliert und die Verarbeitungen zu diesen Zwecken unter einen konsequenten Erforderlichkeitsvorbehalt gestellt. § 32 BDSG enthält eine allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten, die die von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen und ein Arbeitnehmerdatenschutzgesetz weder entbehrlich machen noch inhaltlich präjudizieren soll. Daneben wird der Schutz der Arbeitnehmer vor unzulässi-

gen Eingriffen in ihre Persönlichkeitsrechte auch noch durch arbeitsrechtliche Maßstäbe und entsprechende Arbeitsgerichtliche Judikatur bestimmt.

Informationspflicht bei Sicherheitslecks und Datenpannen

Die Einführung einer Informationspflicht bei unrechtmäßiger Übermittlung oder schierer Kenntniserlangung von Daten anlässlich von Datenpannen oder vorsätzlichem Datenmissbrauch ist ein Novum. Demnach sind sowohl die Betroffenen als auch die zuständige Datenschutzaufsicht grundsätzlich zu informieren, wenn bestimmte Arten von personenbezogenen Daten, z.B. besondere Arten personenbezogener Daten oder Daten zu Bank- und Kreditkartenkonten, unrechtmäßig übermittelt oder Dritten auf andere Weise unrechtmäßig zur Kenntnis gelangt sind.
Die mitzuteilenden Verstöße gegen Datenschutzvorschriften umfassen auch solche eines Auftragnehmers bzw. einer dort beschäftigten Person im Falle von Auftragsdatenverarbeitungsverhältnissen.

Erweiterte Befugnisse der Aufsichtsbehörde

Neben den Erweiterungen des Bußgeldkatalogs und der Erhöhung des Bußgeldrahmens ist auch das aufsichtsbehördliche Instrumentarium wesentlich ausgeweitet und die bisher auf technisch-organisatorische Maßnahmen beschränkte Anordnungsbefugnis der Aufsichtsbehörden ausgedehnt worden. Die Aufsichtsbehörden können bei allen festgestellten Verstößen gegen das Datenschutzrecht Maßnahmen zur Beseitigung anordnen. Bei besonderen Gefährdungen für das Persönlichkeitsrecht und Nichtbefolgung der Anordnung dürfen die Aufsichtsbehörden die Datenverwendungen bzw. einzelne Verfahren sogar untersagen.

3.1.3 Die BDSG-Novelle III beinhaltet Regelungen zur Umsetzung der europäischen Verbraucherkreditrichtlinie.

Mit dieser Novelle wurden in § 29 Abs. 7 BDSG Auskunftspflichten von Kredit ablehnenden Stellen bei Bonitätsanfragen innerhalb der EU / des EWR verankert.

3.2 Videoüberwachung

Im Berichtszeitraum hat es zum Teil medienwirksame Vorfälle in Bezug auf opto-elektronische Überwachungen gegeben. Auch dies hat zu einer verstärkten Wahrnehmung der in allen Lebensbereichen präsenten Videoüberwachung geführt. Tendenziell konnte festgestellt werden, dass sowohl die Bereitschaft zur Installation von Videokameras gewachsen, als auch die Einstellung der hiervon betroffenen Bürgerinnen und Bürger kritischer geworden ist.
Die Hemmschwelle, eine opto-elektronische Überwachungslage zu installieren und zu betreiben sinkt auch analog mit den Preisen. Sie wird so zu einem Mitnahmeartikel im Baumarkt und Co. Dieses Verhalten führt verstärkt zu Streitigkeiten unter Nachbarn, in Geschäften und Cafés sowie zwischen Unternehmen und deren Beschäftigten. Die Anzahl der Eingaben und Beschwerden stieg im Vergleich zu früheren Berichtszeiträumen stark an.

3.3 Google Street View

Das amerikanische Internet-Produkt „Google Street View“ ist als Thema Gegenstand der Beratungen der Datenschutzaufsichtsbehörden der Länder und des Bundes und wird bereits seit längerem intensiv erörtert. Der Düsseldorfer Kreis hat sich bereits im Jahre 2008 mit „Google Street View“ befasst und in seinem Beschluss vom 13./14.11.2008 Anforderungen formuliert, an denen die datenschutzrechtliche Zulässigkeit des Produkts „Street-View“ zu messen ist:

„Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den

betroffenen Bewohnern und Grundstückeigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen." (http://www.bfdi.bund.de/cln_136/DE/Entschliessungen/DuesseldorferKreis/DKreis_node.html)

Die Hamburgische Datenschutzaufsichtsbehörde ist für das in Hamburg ansässige Tochterunternehmen von Google Inc. zuständig und hat die Ergebnisse der Erörterungen der Aufsichtsbehörden in ihrer Aufsicht mit entsprechenden Vorgaben berücksichtigt. Gegenüber dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit konnten eine Reihe von Zusagen von Google im Verhandlungswege erreicht werden. Diese können unter http://www.hamburg.de/datenschutz/aktuelles/1569338/google-street-view-zusage.html eingesehen werden.

So können u.a. von "Google Street View" betroffene Bürger gegen die Erfassung individueller Eigenschaften wie Gesichter aber auch Kfz-Kennzeichen oder Hausnummern bindenden Widerspruch direkt bei der Google Inc. einlegen. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein hält unter der folgenden Internetadresse ein Musterexemplar für den Widerspruch zum download bereit:
https://www.datenschutzzentrum.de/geodaten/streetview.htm

4 Kontrolltätigkeit der Aufsichtsbehörde

4.1 Vorortkontrolle und Beratung nach § 38 BDSG

Im Rahmen von Vorortkontrollen und Beratungen wurden in erster Linie die folgenden Punkte thematisiert:

- Die Verpflichtung zur Bestellung eines Datenschutzbeauftragten nach § 4f BDSG und die Fachkunde des Datenschutzbeauftragten nach § 4g Abs. 1 BDSG,

- das Verfahrensverzeichnis nach § 4g Abs. 2 BDSG,
- die Verpflichtung der Mitarbeiter, die personenbezogene Daten verarbeiten, auf das Datengeheimnis nach § 5 BDSG,
- die erforderlichen technischen und organisatorischen Maßnahmen nach § 9 nebst Anlage zu § 9 BDSG,
- die Anforderungen bei einer Auftragsdatenverarbeitung nach § 11 BDSG,
- die Meldepflicht nach § 4d BDSG.

4.2 Sicherheitslücke in Portalen zur Online-Melderegisterauskunft

Eine im Land Brandenburg ansässige Soft- und Hardwarefirma veröffentlichte – wenn auch nur für Insider erkennbar – über mehrere Monate hinweg ein Standardpasswort des Benutzers „inforeg“ auf der Website www. meldebehörde.de.
Bei der Installation des Inforegisters einschließlich der entsprechenden Software wurde von der Firma dieses Standartpasswort regelmäßig mitgeliefert, mit dem dann alle weiteren Funktionen (Anlegen von Nutzern, Vergabe von Rechten usw.) gesteuert werden konnten.
Bei einigen Angeboten einer Online-Melderegisterauskunft wurde seitens der verantwortlichen Stellen unterlassen, den Standardzugang des Benutzers „inforeg“ zu sperren oder dessen Passwort zu ändern. Das Unternehmen war sofort bemüht, einen eigenen Überblick über das Ausmaß der Sicherheitslücke und die Folgen zu erhalten, um eigene Maßnahmen zur Eindämmung der Missbrauchsgefahr einzuleiten.
Zwischenzeitlich wurde den Kommunen eine Software zur Verfügung gestellt, die die Verwaltungen bei der Organisation der Datensicherheit für das Inforegister unterstützt. Weiterhin wurde das Verfahren dahingehend erweitert, dass der Anwender nach der Installation zu einem Passwortwechsel systemseitig gezwungen wird. Die neue Software ermöglicht darüber hinaus auch weitere Möglichkeiten für eine datenschutzgerechte Passwortverwaltung.
Die Aufsichtsbehörde arbeitete mit der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht bei der Aufarbeitung und datenschutzrechtlichen Bewertung des Sacherhaltes zusammen.

4.3 Online-Portal zur Bewertung von Freiberuflern

Der Aufsichtsbehörde wurde im Jahr 2008 das Geschäftsmodell eines Onlinebewertungsportals mit der Bitte, dieses aus datenschutzrechtlicher Sicht zu bewerten, vorgestellt. Über das Portal sollte die Möglichkeit eröffnet werden, die Arbeit von Freiberuflern zu bewerten. Da auch schon in der Vergangenheit die Aufsichtsbehörde vergleichbare Projekte zu beurteilen hatte und wohl auch in der Zukunft zu bewerten hat, werden die damit einhergehenden Rechtsfragen nachstehend ausführlicher dargestellt.

Als freie Berufe werden Tätigkeiten bezeichnet, die nicht der Gewerbeordnung unterliegen. Sie betreffen selbständig ausgeübte ärztliche, künstlerische, schriftstellerische und ähnliche höchstpersönliche Tätigkeiten. Den Angehörigen freier Berufe stehen abgesehen vom allgemeinen Persönlichkeitsrecht spezielle Grundrechte zu. Diesen Schutzrechten steht gegenüber, dass es sich bei den in Internet-Portalen eingestellten Beurteilungen und Bewertungen von Einzelpersonen vielfach um sensible Informationen und subjektive Werturteile über Betroffene handelt, ohne dass die Urheber erkennbar sind und diese jederzeit von jedermann abgerufen werden können. Der Bundesgerichtshof hat sich bezogen auf die Bewertung von Lehrern durch Schüler auf einer Internetseite mit der Zulässigkeit von Bewertungsportalen auseinandergesetzt (BGH, Urteil vom 23.06.2009, VI ZR 196/08). Im konkreten Fall ist der BGH in Abwägung zwischen dem Schutz des Rechts auf informationelle Selbstbestimmung der Klägerin (einer Lehrerin) nach Artikel 2 Absatz 1 GG i.V.m. Artikel 1 Absatz 1 GG und dem Recht auf Kommunikationsfreiheit nach Artikel 5 Absatz 1 GG zu dem Ergebnis gelangt, dass hier die Erhebung, Speicherung und Übermittlung von personenbezogenen Daten im Rahmen eines Bewertungsforums im Internet zulässig sei.

Anbieter entsprechender Portale haben die Vorschriften des BDSG über die geschäftsmäßige Verarbeitung personenbezogener Daten einzuhalten (insbesondere § 29 BDSG). Ferner ist das Telemediengesetz zu beachten. Bei der danach gesetzlich vorgeschriebenen Abwägung ist den schutzwürdigen Interessen der bewerteten Personen Rechnung zu tragen. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen.

Das der Aufsichtsbehörde vorgestellte Geschäftsmodell sah die Verarbeitung von personenbezogenen Daten vor (§ 3 Abs. 1 BDSG). Auch Daten von Unternehmen können personenbezogene Daten im Sinne des BDSG sein. So sind z.B. Daten über die Situation einer sog. Ein-Mann-GmbH personenbezogene Daten des

Gesellschafters / Geschäftsführers (BGH, Urteil vom 17.12.1985, Neue Juristische Wochenschrift 1986, S.2505). Ebenso unterliegen auch die geschäftlichen Daten eines Einzelkaufmannes dem BDSG (vgl. hierzu Bergmann/Möhrle/Herb: Datenschutzrecht Kommentar, Richard Boorberg Verlag, 2002, § 3 BDSG RdNrn. 11 bis 13). Damit ist der Anwendungsbereich des BDSG auch hinsichtlich der Daten von Angehörigen freier Berufe eröffnet, die sich auf ihre berufliche Tätigkeit erstrecken.

Eine Domain ist als Auskunftei einzustufen, wenn hier Daten über Unternehmen / Privatpersonen zum Zwecke der Übermittlung bzw. des Online-Abrufes bereitgehalten werden, auch wenn es sich um reine Bewertungsportale handelt. Die Zulässigkeit der Einrichtung einer solchen Plattform richtet sich nach den Voraussetzungen des § 29 BDSG (vgl. BGH a.a.O. Rdnr. 24).

Da der potentielle Betreiber des Bewertungsportals keine konkreten Angaben zu den einzelnen Bewertungskriterien machen wollte, nach denen Daten eingestellt werden sollten, konnte ihm die Aufsichtsbehörde nur in allgemeiner Form Auskunft zur Zulässigkeit eines solchen Projekts geben. Die Aufsichtsbehörde konnte das oben genannte Urteil des BGH bei ihrer Prüfung noch nicht einbeziehen.

Gemäß § 29 Abs. 1 Satz 1 Nr. 1 BDSG dürfen personenbezogene Daten zum Zwecke der Übermittlung durch z.B. Auskunfteien nur erhoben und gespeichert werden, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Erhebung oder Speicherung hat. Ein schutzwürdiges Interesse des Betroffenen am Ausschluss der Speicherung besteht zum Beispiel dann nicht, wenn in einem Kreditinformationssystem hinsichtlich der Zahlungsweise gesicherte und beweisbare Daten (harte Negativdaten) gespeichert werden sollen. Dies wären z.B. Zwangsvollstreckung, Konkurs, Haftbefehl, Abgabe einer Eidesstattlichen Versicherung nach § 807 ZPO, Pfändung oder Inanspruchnahme einer Lohnabtretung. Nur soweit es sich also bei den auf der geplanten Domain gespeicherten Daten um objektiv richtige Tatsachen handelt, wäre eine Speicherung der Daten gemäß § 29 Abs. 1 Satz 1 Nr. 2 BDSG in bestimmten Grenzen zulässig.

Gemäß § 29 Abs. 2 Nr. 1 Buchst. a BDSG ist die Übermittlung der Daten jedoch nur erlaubt, wenn der Datenempfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt hat. Aufgrund der Tatsache, dass die Daten für jedermann abrufbar in das Internet gestellt werden sollten, wäre der Betreiber der Online-Plattform als verantwortliche Stelle kaum in der Lage gewesen, das berechtigte Interesse des

jeweiligen Datenempfängers zu prüfen. Hinsichtlich des Lehrer-Schüler Bewertungsportals kommt der BGH (a.a.O. Rdnr. 42) zu dem Ergebnis, dass die Vorschrift unter Berücksichtigung des Grundrechts auf Meinungsfreiheit verfassungskonform auszulegen ist. Im vom BGH zu entscheidenden Fall entfiel die Pflicht zur Darlegung eines berechtigten Interesses. Wegen der anderen Fallkonstellation bleibt es bei dem hier zu prüfenden Bewertungsportal für Freiberufler jedoch bei der Pflicht zur Prüfung des berechtigten Interesses.

Da die Übermittlung augenscheinlich durch ein automatisiertes Abrufverfahren erfolgen sollte, obliegt dem Datenempfänger die Aufzeichnungspflicht hinsichtlich des berechtigten Interesses. Gleichwohl besteht gemäß § 10 Abs. 4 Satz 3 BDSG für die speichernde Stelle die Pflicht, zu gewährleisten, dass die Übermittlung durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Dies beinhaltet auch die stichprobenartige Überprüfung des berechtigten Interesses der anfragenden Stelle (siehe auch hier BGH a.a.O.).

Darüber hinaus ist die Datenübermittlung nur zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Das schutzwürdige Interesse steht einer Übermittlung immer dann entgegen, wenn die Erhebung und Speicherung nicht rechtmäßig erfolgt ist.

Übermittelt werden dürften lediglich die Daten, die aus allgemein zugänglichen Quellen entnommen wurden bzw. objektiv richtig sind und schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Darüber hinaus dürfen nur die oben bereits erwähnten „harten“ Negativmerkmale übermittelt werden. Nach der Rechtsprechung des BGH (a.a.O.) ist auch die Übermittlung von Meinungsäußerungen, auch wenn sie einen Tatsachengehalt aufweisen, in dem vom Gericht beschriebenen Umfang zulässig.

Gemäß § 33 Abs. 1 Satz 2 BDSG besteht die Verpflichtung, den Betroffenen von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Auch das dürfte von vor dem Hintergrund der jederzeitigen und beliebigen Abrufbarkeit der Daten kaum sicherzustellen sein.

Nach § 35 Abs. 1 BDSG sind personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Ferner sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist und zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt (§ 35 Abs. 2 Satz 2 Nr. 1 u. Abs. 4 BDSG).

Spezielle datenschutzrechtliche Regelungen, die sich auf einzelne Problemstellungen von Bewertungsportalen, wie z.B. die Mehrfach- oder Eigenbewertungen beziehen, existieren nicht.

Konkrete Vorgaben zur Ausgestaltung der notwendigen technisch-organisatorischen Maßnahmen konnte die Aufsichtsbehörde gegenüber der verantwortlichen Stelle nicht abschließend übermitteln, da diese immer nur erforderlich sind, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Sie sind mithin nach jeder Änderung der Rahmenbedingungen erneut zu (über)prüfen und zu entscheiden.

Der potentielle Betreiber des Bewertungsportals hat sich bei der Aufsichtsbehörde nicht mehr gemeldet, Anfragen von möglichen Betroffenen sind bei der Aufsichtsbehörde im nachhinein nicht eingegangen, so dass davon ausgegangen werden kann, dass er das Geschäftsmodell nicht weiterverfolgt hat.

4.4 Standortbestimmung von Kundendienstfahrzeugen mittels eines Global Positioning Systems (GPS)

Die Aufsichtsbehörde wurde insbesondere von Arbeitnehmern befragt, ob es zulässig sei, wenn z.B. im Rahmen von Reparaturarbeiten bei Kunden die Kundendienstfahrzeuge der Monteure mit einem GPS ausstattet werden. Vielfach sollen durch das eingesetzte Verfahren die Betriebsabläufe während der Geschäftszeiten optimiert werden. Dafür werden grundsätzlich die Standorte der Fahrzeuge in Echtzeit erfasst und die zurückgelegten Fahrstrecken und die Fahrtunterbrechungen nach Ort und Zeit gespeichert. Auf diese Weise ließen sich, während das Fahrzeug unterwegs ist, leichter Aufträge erteilen und ändern. Auch könne man die elektronischen Aufzeichnungen für die Abrechnung der Anfahrts- und Arbeitszeiten mit den Kunden nutzen.

Datenschutzrechtlich kann man es einem Firmeninhaber grundsätzlich nicht verwehren, stets darüber im Bilde zu sein, wo sich seine Kundendienstfahrzeuge gerade befinden, um deren Einsatz dirigieren zu können. Darüber müssten ihn seine Mitarbeiter auch ohne GPS auf dem Laufenden halten. Darüber hinaus hat ein Außendienstmitarbeiter seinen Arbeitgeber über die Anfahrts- und Arbeitszeiten zum und beim Kunden

wahrheitsgemäß zu informieren, damit dieser die dafür anfallenden Kosten abrechnen kann, sodass grundsätzlich der Einsatz dieses Ortungssystems auch zu diesem Zweck berechtigt ist.
Schutzwürdige Interessen der Beschäftigten werden im Falle des GPS-Einsatzes jedoch dann verletzt, wenn der Mitarbeiter losgelöst von einem betrieblich gerechtfertigten Informationsbedarf des Arbeitgebers einer umfassenden Kontrolle seines Verhaltens an seinem externen Arbeitsplatz unterworfen ist.
Da mit einer derartigen Nutzung eines GPS das Risiko eines nicht unerheblichen Eingriffs in das Persönlichkeitsrecht der Mitarbeiter verbunden ist, muss die Firma eine sogenannte Vorabkontrolle nach § 4 d Abs. 5 BDSG durchführen. Zusätzlich muss sie schriftlich festlegen, welche mit Hilfe des GPS erlangten Informationen für welche(n) Zweck(e) und wie lange gespeichert und genutzt werden dürfen. Dabei müssen die Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit beachtet werden. Ferner muss es eine Datenlöschkonzeption geben. Diese muss unter anderem vorsehen, dass die Angaben über den Standort der Kundendienstfahrzeuge alsbald nach Beendigung der Betriebsfahrten gelöscht werden. Dagegen können die Daten, die zu Abrechnungszwecken mit den Kunden erforderlich sind, so lange gespeichert bleiben, wie mit Reklamationen und dergleichen normalerweise zu rechnen ist. Außerdem müssen die Mitarbeiter nach § 4 Abs. 3 BDSG über die Zweckbestimmungen der Erhebung, Verarbeitung und Nutzung der Daten unterrichtet werden.

4.5 Regelmäßige Gespräche mit Vertretern des Internetauktionshauses eBay

Auch in diesem Berichtszeitraum fanden Gespräche mit Vertretern des Internetauktionshauses eBay mit dem Ziel statt, die Einhaltung der einschlägigen datenschutzrechtlichen Vorschriften zu begleiten und auftretende Rechtsfragen zu klären. Insgesamt war festzustellen, dass sich die Anzahl der Beschwerden und Anfragen im Zusammenhang mit der Tätigkeit von eBay im Vergleich zum Zeitraum 2006/2007 erhöht hat. Als Ursache können an dieser Stelle die steigende Zahl der eBay-Mitglieder in Deutschland, die zwischenzeitlichen Änderungen der Allgemeinen Geschäftsbedingungen von eBay und die zunehmende Internetkriminalität genannt werden. Die datenschutzrechtliche Tragweite der Beschwerden und Anfragen ist in ihrer Qualität sehr unterschiedlich.

Schwerpunkte der Diskussionen und Prüfungen waren die Themen

- Auskunftsanspruch nach § 13 Abs. 7 TMG i.V.m. § 34 BDSG,

- unzulässige Übermittlung von personenbezogenen Daten (Phishing),
- neue AGB nebst Einwilligungserklärung,
- Identitätsmissbrauch,
- Identifizierung der Mitglieder.

4.6 Ersatz der Seitenspiegel an Straßenbahnen durch Kameras

Ein Verkehrsbetrieb beabsichtigt, an seinen Straßenbahnen sukzessive die üblichen Außenspiegel durch elektronische Kameras zu ersetzen, um für das Fahrpersonal eine bessere Beobachtung des Fahrgastwechsels und des Fahrzeugs während der Fahrt zu ermöglichen, um so letztlich eine Erhöhung der Sicherheit im Bahn- und Straßenverkehr zu erzielen.

Bei der datenschutzrechtlichen Bewertung war zunächst zu eruieren, ob und in wie weit es sich um eine Beobachtung des öffentlich zugänglichen Raumes handelt. Nur wenn diese Voraussetzung gegeben ist, kommen die Regelungen des § 6b BDSG zum Tragen. Beurteilungskriterium war in diesem Fall die Widmung zum öffentlichen Verkehr oder ob die Flächen nach dem erkennbaren Willen der Berechtigten von jedermann benutzt oder betreten werden können. Vor diesem Hintergrund fallen die Bahnsteige und Haltestellen unter den Begriff des öffentlich zugänglichen Raumes, die Gleisanlagen hingegen nicht. Da nach dem Konzept der verantwortlichen Stelle die Kameras auch während der Fahrt Daten erheben und verarbeiten, kann nicht ausgeschlossen werden, dass – wenn auch nur am Rande – öffentlich zugänglicher Raum mit erfasst wird.
Das zum Einsatz kommende Videosystem erlaubt eine am Grundsatz der Verhältnismäßigkeit und an den Erfordernissen des § 6b BSDG angepasste Erhebung und Verarbeitung von personenbezogenen Daten. So können u.a. der Erfassungswinkel durch gezielte Verpixelung und die Speicherdauer abhängig vom Aufenthaltsort der Straßenbahn (z.B. Haltestelle oder offene Strecke) variabel programmiert und somit eingestellt werden.
Die verantwortliche Stelle wurde darauf hingewiesen, dass die notwendigen technisch-organisatorischen Maßnahmen gemäß BSDG zu treffen sind, eine geeignete Kennzeichnung der Videoaufzeichnung mittels Piktogrammen zu erfolgen hat und ein Verfahrensverzeichnis zu erstellen ist. Der Abschluss einer Betriebsvereinbahrung bzw. Dienstanweisung wurde vom Unternehmen in Aussicht gestellt.

4.7 Videoüberwachung in einem Einkaufszentrum der Unternehmensgruppe ECE

Aus Anlass einer koordinierenden Befassung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (Sitz der Unternehmensgruppe ECE welche bundesweit eine Vielzahl an derartigen Einkaufs- und Shoppingcenter betreibt ist Hamburg) wurde die Videoüberwachungsanlage eines Einkaufscenters durch persönliche Inaugenscheinnahme durch Vertreter der Aufsichtsbehörde einer datenschutzrechtlichen Prüfung unterzogen.

Als ein Grund für die Videobeobachtung nach § 6b BDSG wurde die Wahrnehmung des Hausrechtes angeführt. Zivilrechtlich ist das Hausrecht insbesondere in den Abwehrrechten der §§ 859 ff., 904 und 1004 BGB verankert. Es kann sowohl zu präventiven als auch zu repressiven Zwecken wahrgenommen werden – also z.B. sowohl zur Vermeidung von Straftaten oder Unfällen als auch zur Verfolgung von Straftätern. Zunächst muss die Maßnahme erforderlich sein. Das bedeutet, sie muss überhaupt geeignet sein, den angestrebten Überwachungszweck zu erreichen. Zweitens ist zu prüfen, ob es nicht mildere, ebenfalls geeignete Mittel gibt. Zuletzt ist eine Interessenabwägung zwischen den berechtigten Interessen der verantwortlichen Stelle und dem schutzwürdigen Interesse der Betroffenen vorzunehmen. Wenn diese Abwägung negativ verläuft, wäre eine Videoüberwachung unzulässig auch wenn ein Erlaubnisgrund und die Erforderlichkeit vorliegen.

Im gesamten Center waren 32 Kameras installiert. Es handelte sich um Kameras, die nach Angaben des Managements keine Zoomfunktion besitzen. Die Anlage ist seit Eröffnung des Centers seit rund 12 Jahren in Betrieb. Überwacht werden speziell die Eingänge auf den 3 Etagen, Verbindungen über Fahrsteige und -treppen, 2 Ein- und Ausfahrten sowie 3 Anlieferungen und Parkplatzeinfahrten. Eine Überwachung der Ladenpassagen erfolgt nicht. Die Daten werden automatisch nach 48 Stunden überschrieben, es erfolgt keine längerfristige Datenspeicherung. An allen Eingängen des Centers werden die Besucher durch ein Piktogramm auf die Videoüberwachung hingewiesen.

Die Videoüberwachung in den einzelnen Geschäften des Centers wird gesondert durch die jeweiligen Mieter durchgeführt und liegt nicht im Verantwortungsbereich des Centermanagements. Der Aufnahmebereich für derlei Anlagen endet an der jeweiligen Ladeneingangstür. Der Aufsichtsbehörde wurden Unterlagen überge-

ben, in denen Einzelheiten zum Umgang und Betreib der Videoüberwachungsanlage im Objekt dokumentiert sind. Die notwendigen technisch-organisatorischen Maßnahmen wie z.B. Zugangs- und Zugriffskontrolle waren datenschutzgerecht gestaltet. Eine Auswertung der Videoaufzeichnungen bzw. eine Weitergabe an Dritte erfolge nur in begründeten Einzelfällen. Bei Ermittlungsverfahren durch die Polizei werde das Bildmaterial zur Auswertung verwandt. Die entsprechenden Vorgänge werden dokumentiert.
Insgesamt wurde seitens der Aufsichtsbehörde eingeschätzt, dass im gesamten Objekt mit der Problematik Videoüberwachung sorgsam umgegangen wird. Die Prüfung erfolgte vorbehaltlich des abschließenden Meinungsbildungsprozesses im Düsseldorfer Kreis zum Thema Videoüberwachung in Einkaufszentren. Die im Rahmen einer Unterarbeitsgruppe beteiligten Behördenvertreter entwickeln zusammen mit ECE gemeinsame Standards in Bezug auf die Einhaltung der datenschutzrechtlichen Erfordernisse.

4.8 Prüfung eines Callcenters

Anlässlich des Bekanntwerdens der illegalen Weitergabe von Kunden- bzw. Kontodaten mutmaßlich durch einen Mitarbeiter eines Callcenters in einem anderen Bundesland, wurden zwei größere Callcenter mit rechtlich selbständigem Sitz im Bundesland Brandenburg kontrolliert.
Ein Unternehmen ist zu 80 % Dienstleister für einen Konzern und zu 20 % für andere Unternehmen tätig. Schriftliche Verträge mit allen Auftraggebern wurden eingesehen. Die Kundendaten werden zentral in Nürnberg gespeichert und verwaltet. Im Unternehmen selbst arbeiteten zum Zeitpunkt der Kontrolle ca. 600 Mitarbeiter. Es gab ca. 300 Auskunftsplätze. Der Betrieb war rund um die Uhr besetzt.
Die private Nutzung des Internets sowie der private E-Mail-Verkehr sind den Mitarbeitern laut Vertrag nicht gestattet. Nur spezielle Internetseiten waren benutzbar. Die Beschäftigten konnten an ihren Arbeitsplätzen keine Daten auf mobile Datenträger speichern. Aufzeichnungen von Mitarbeitern in Papierform, wurden in speziellen Containern gesammelt und durch eine Firma entsorgt. Ein externer Datenschutzbeauftragter war zum Zeitpunkt der Kontrolle bestellt. Die entsprechende Bestellungsurkunde wurde vorgelegt.
Am Prüfungstag konnten sich die Vertreter der Aufsichtsbehörde bei einem Rundgang am Geschäftssitz über die Sicherungsmaßnahmen des Betriebsgebäudes sowie der Sicherungsmaßnahmen innerhalb der Geschäftsräume informieren. Auf Betreiben der Aufsichtsbehörde wurden technisch-organisatorischen Maßnahmen optimiert.

Im Ergebnis war der Betrieb der geprüften Callcenter zum Prüfungszeitpunkt seitens der Aufsichtsbehörde nicht zu beanstanden.

5 Schwerpunkte aus Beschwerden

5.1 Überwachung von Mitarbeitern eines Discounters unter Einsatz von Videotechnik und Detektiven

Ende März 2008 hatten Medien bundesweit berichtet, Mitarbeiter eines Discounters würden systematisch durch Detekteien oder andere Sicherheitsunternehmen überwacht. Als Belege wurden Auszüge aus Einsatzberichten veröffentlicht, in denen unter anderem Informationen aus dem Privatleben, zum Beispiel über Beziehungsprobleme oder finanzielle Schwierigkeiten, sowie über das Verhalten der Kollegen bei der Arbeit und im Umgang miteinander protokolliert waren.

Auftraggeber der Sicherheitsunternehmen, die diese Einsatzberichte angefertigt hatten, waren rechtlich selbstständige Vertriebsgesellschaften. Daher leiteten die für die Unternehmenssitze zuständigen zwölf Datenschutzaufsichtsbehörden datenschutzrechtliche Überprüfungsverfahren ein. Da die unternehmensintern mit der bundesweiten Aufklärung der Vorgänge beauftragte zentrale Dienstleistungsgesellschaft des Discounters ihren Sitz in Baden-Württemberg hat, übernahm die baden-württembergische Aufsichtsbehörde die Koordinierung der Datenschutzüberprüfungen.

Die Aufsichtsbehörden stellten fest, dass die Vertriebsgesellschaften mit ihrer bis Ende März 2008 praktizierten Verfahrensweise in unterschiedlichem Ausmaß gegen Datenschutzvorschriften verstießen.

Alle Vertriebsgesellschaften hatten bis Anfang Juni 2008 keinen Beauftragten für den Datenschutz bestellt, obwohl sie nach § 4f des BDSG hierzu verpflichtet gewesen wären.
Beauftragte für den Datenschutz haben die Aufgabe, in den Unternehmen auf die Einhaltung des Datenschutzes hinzuwirken. Angesichts des Umfangs und der Art der Erhebung, Verarbeitung und Nutzung personenbezogener Daten wäre es bei den Vertriebsgesellschaften des Discounters besonders dringlich gewesen,

über betriebliche Datenschutzbeauftragte zu verfügen. Durch deren Einsatz hätte es möglicherweise vermieden werden können, dass es zu schwerwiegenden Verstößen kam.

Im Ergebnis der gesamten datenschutzrechtlichen Prüfungen wurden gegenüber den bundesweit ansässigen 35 Vertriebsgesellschaften Beanstandungen ausgesprochen und Bußgelder in beträchtlicher Höhe festgesetzt.
Anzuerkennen war, dass die betroffenen Unternehmen nach den Presseberichten sofort reagiert, die Videoüberwachungsgeräte abgebaut, den Einsatz von Detektiven gestoppt und damit begonnen haben, bislang fehlende Datenschutzkonzeptionen zu erarbeiten.
Da der Discounter künftig wieder Videoüberwachung und auch Detektive in den Filialen einsetzen will, erarbeitete die zentrale Dienstleistungsgesellschaft hierfür ein Gesamtkonzept und legte dieses der Baden-Württembergischen Aufsichtsbehörde zur Begutachtung vor. Diese machte deutlich, dass für sie insbesondere folgende Punkte von Bedeutung sind[1]:

1. Dass in einem Teil der Filialen Diebstähle und auch Überfälle auf Mitarbeiter vorkommen, rechtfertigt nicht die Überwachung aller Filialen unter Einsatz von Videotechnik und Detektiven. Es muss vielmehr filialbezogen festgestellt werden, dass Überwachungsmaßnahmen zur Verhinderung von Straftaten oder zu deren Aufklärung oder aus einem sonstigen rechtfertigenden Grund im Sinne des § 6 b BDSG erforderlich sind. Dies hat im konkreten Fall zur Folge, dass in einem Teil der Filialen keine Überwachung stattfindet.

2. Es ist jeweils sehr genau zu prüfen, worauf sogenannte Inventurverluste zurückzuführen sind. Anzunehmen, Ursache seien stets strafbare Handlungen von Kunden oder Mitarbeitern, weshalb eine Videoüberwachung gerechtfertigt sei, ist nicht zwingend. Die Aufsichtsbehörde hat es daher begrüßt, dass das vorgelegte Konzept hierfür ein Prüfschema vorsieht.

3. Mitarbeiter dürfen in öffentlich zugänglichen Räumen nur unter Beachtung des § 6b BDSG offen überwacht werden. Für die offene Videoüberwachung von Mitarbeitern in anderen Räumen, beispielsweise Aufenthaltsräumen, fehlt es derzeit ebenso an einem ausdrücklichen Erlaubnistatbestand wie für die heimliche Videoüberwachung von Arbeitnehmern. Die arbeitsgerichtliche Rechtsprechung lässt jedoch

[1] Fünfter Tätigkeitsbericht des Innenministeriums zum Datenschutz im nichtöffentlichen Bereich; Landtag von Baden-Württemberg 14. Wahlperiode Drucksache 14 / 4963

beide Maßnahmen unter den von ihr entwickelten Voraussetzungen zu. Bis zur Schaffung entsprechender Regelungen in einem Arbeitnehmerdatenschutzgesetz kann dies hingenommen werden. Notwendig ist jedoch, dass die verantwortliche Stelle das Vorliegen dieser Voraussetzungen in jedem Einzelfall sorgfältig prüft und das Ergebnis schriftlich dokumentiert. Im konkreten Fall will der Discounter auf offene Videoüberwachung in nicht öffentlich zugänglichen Räumen und heimliche Videoüberwachung verzichten. Dies ist zu begrüßen.

4. Soweit Überwachungsmaßnahmen in einer Filiale danach grundsätzlich zulässig sind, sind sie – was Intensität und räumliche sowie zeitliche Ausdehnung angeht – auf das Erforderliche zu beschränken. Eine notwendige Eskalation sollte in Stufen erfolgen, die klar definiert sind. Eine Ausweitung der Überwachung kommt dabei erst in Betracht, wenn zuvor die weniger tief in die Persönlichkeitsrechte eingreifende Maßnahme erfolglos eingesetzt wurde.

5. In regelmäßigen, nicht zu langen Zeitabständen ist zu prüfen, ob eine Videoüberwachungsmaßnahme noch gerechtfertigt ist.

6. Aufträge an Detektive sollten stets schriftlich erteilt werden. Deren Aufgaben sollten ebenfalls schriftlich festgelegt und exakt beschrieben sein. Die Mitarbeiter sollten hierüber unterrichtet werden. Detektiven sollte es untersagt sein, Protokolle über das Verhalten von Mitarbeitern zu erstellen.

7. Es müssen die erforderlichen technischen und organisatorischen Maßnahmen getroffen werden. In Betracht kommen unter anderem folgende Maßnahmen:
   Vier-Augen-Prinzip beim Zugriff auf aufgezeichnete Videodaten,
   Schutz der Aufzeichnungsgeräte vor unberechtigtem Zugriff,
   Vorschriften über die (deutlich sichtbare) Anbringung der Kameras,
   die – auch bei schwenk- und zoombaren Kameras vorgesehene – Ausblendung der (Kassen-) Mitarbeiter sowie der PIN-Pads, über die die Kunden bei EC-Karten-Zahlung ihre PIN-Nummer eingeben.

8. Sämtliche Maßnahmen sollten in enger Abstimmung mit dem betrieblichen Datenschutzbeauftragten ergehen und jeweils schriftlich dokumentiert werden. Die vorgeschriebene Dokumentation sollte die Verantwortlichen dazu zwingen, das Vorliegen der jeweiligen Voraussetzungen sorgfältig zu prüfen.

5.2 Personenbezogene Fahrerkarten für Taxifahrer

Die Aufsichtsbehörde wurde von einem selbständigen Taxifahrer über die Einführung von Fahrerkarten durch eine Taxi-Genossenschaft und die in diesem Zusammenhang auftretenden Probleme im täglichen Betrieb informiert.

So sei in vielen Fällen, insbesondere bei selbständigen Taxiunternehmern, die als sog. Einmannbetrieb geführt werden, die Geschäftsadresse gleich mit der postalischen Adresse. Nach § 27 Abs. 2 der Verordnung über den Betrieb von Kraftfahrtunternehmen im Personenverkehr sei bei Taxen im Wageninneren an einer für den Fahrgast gut sichtbaren Stelle ein Schild mit Namen und Betriebssitz des Unternehmens anzubringen.
Ferner seien im Laufe dieses Jahres personenbezogene elektronische Fahrerkarten (mit Bild und Name) durch die Taxi-Genossenschaft hergestellt und für alle Mitglieder und angeschlossenen Taxiunternehmer verbindlich eingeführt worden. Die Fahrerkarten sind zwingend im Cockpit des Fahrzeuges, für den Fahrgast deutlich sichtbar, anzubringen.

Nach Aussagen von betroffenen Taxifahrer/-innen sei es nun u.a. zu folgenden Vorfällen gekommen:

Fahrgäste identifizierten die Fahrerin / den Fahrer anhand des Fotos und Namens auf der Fahrerkarte und anhand des Schildes mit Namen und Betriebssitz als Inhaber/in des Taxibetriebes und setzen auch voraus, dass dies auch deren Wohnanschrift sei. Auf der Grundlage dieser Erkenntnisse habe es Drohungen (z.B. sinngemäß "…wir wissen ja wo du wohnst…" oder "…wir werden dann mal deine Frau besuchen, während du im Dienst bist…" oder zu einer Fahrerin: "…ich kann dich ja mal Zuhause besuchen…") gegeben.

Um den Zusammenhang zwischen Identifikation der Fahrerin / der Fahrers und Wohnort zu unterbinden, kamen nur die folgenden zwei Möglichkeiten in Betracht:

1. Die Fahrerkarten ermöglichen keine eindeutige Identifikation der Fahrerinnen und Fahrer durch Inaugenscheinnahme oder

2. der Betriebssitz ist nicht gleich mit der postalischen Wohnanschrift.

Rechtsgrundlage für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch die Taxi-Genossenschaft ist der § 28 BDSG.
Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig,

1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Die Einführung der Fahrerkarten sei lt. Schreiben der Taxi-Genossenschaft an alle angeschlossenen Taxibetriebe vom 04.09.2007 „zur Vervollkommnung der Abläufe und vor allem zur Erhöhung der Anmelde- und Nutzungssicherheit der Datenfunkgeräte“ eingeführt worden. Dass die Fahrerkarten eine Identifikation der Fahrerin / des Fahrers zulässt, stehe mit dem Servicegedanken im Bereich der öffentlichen Personenbeförderung grundsätzlich im Einklang.

Die Einführung der Fahrerkarten mit Bild und Namen dient mithin der Zweckbestimmung des Vertragsverhältnisses zwischen der Taxi-Genossenschaft Potsdam e.G. und den Fahrerinnen und Fahrern.

Ob diese Vertragsverhältnis jedoch voll dem Grundsatz der Privatautonomie entspricht, wäre ggf. auf dem Zivilrechtsweg zu prüfen.

Dem Einzelnen wird es grundsätzlich ermöglicht, seine Rechtsverhältnisse selbständig und nach seinem Willen durch Rechtsgeschäft zu gestalten. Grundsätzlich bedeutet dies, dass es jedem Taxiunternehmer freigestellt ist, ob er der Taxi-Genossenschaft beitritt bzw. sich dieser anschließt oder nicht. Letztlich ist dies ein Ausdruck der in Art. 1 Abs. 1, 2 Abs. 1 Grundgesetz verfassungsrechtlichen verbürgten Selbstbestimmung und Handlungsfreiheit.

Jedoch müsste ein Taxiunternehmer, der nicht an der von der für den Stadtraum marktbeherrschenden Taxi-Genossenschaft betriebenen Funkvermittlung teilhaben kann, mit Sicherheit auf einen nicht unerheblichen Teil seiner Einkünfte verzichten. Vor diesem Hintergrund hat das Landgericht Magdeburg eine Taxi-Genossenschaft dazu verurteilt, einen Taxiunternehmer an der Funkvermittlung teilnehmen zu lassen, da eine Weigerung ansonsten zu einer unbilligen Behinderung des Unternehmers im Wettbewerb führen würde (LG Magdeburg vom 09.11.2001, Az.: 36 O 355/01 (045).

An dieser Stelle wurde deutlich, dass die Abschluss- und Gestaltungsfreiheit für Taxiunternehmer eingeschränkt sind, wenn der Zugang zu einer Funkvermittlung nur durch einen Vertragspartner mit örtlicher marktbeherrschender Stellung möglich ist. In dieses wettbewerbsrechtliche Spannungsfeld regelnd einzugreifen, oblag jedoch nicht der Datenschutzaufsichtsbehörde.

Eine praktikable Variante den o.g. Konflikt zu lösen, wäre das Auseinanderfallen von Betriebs- und Wohnsitz.

Die sog. Einmannunternehmen können es sich oft aus betriebswirtschaftlichen Gründen nicht leisten, ein extra Büro als Betriebssitz anzumieten und richten deshalb für diesen Zweck in ihrer Wohnung ein entsprechendes Arbeitszimmer her.

Der Bundesgerichtshof hat in seinem Urteil vom 16.06.1993 ausgeführt, dass Betriebssitz eines Mietwagenunternehmens i.S.d. § 49 Abs. 2 bis 4 PBefG auch der Tätigkeitsort einer rechtlich selbständigen Funkzentrale sein kann, wenn von dieser für den Betrieb des Mietwagenunternehmers wesentliche Tätigkeiten ausgeübt werden. Dazu gehören lt. Gericht die Entgegennahme und Weiterleitung der Beförderungsaufträge an die Fahrer, die Fahrzeugdisposition, die buchmäßige Erfassung der Beförderungsvorgänge, die Aufbewahrung der Aufzeichnungen (§ 49 Abs. 4 Satz 4 PBefG) und die Möglichkeit der Fahrzeugrückkehr (BGH vom 16.06.1993, Az.: I ZR 140/91).

In Ansehung der o.g. Entscheidung des BGH wurde hier ein Ansatz für eine Lösung hinsichtlich der Problematik Betriebssitz = Wohnsitz aufgezeigt und an die verantwortlichen und beteiligten Stellen appelliert, unter Auslegung der derzeit gültigen Rechtslage, Taxiunternehmer/-innen dahingehend zu unterstützen, dass ihnen die Möglichkeit eingeräumt wird, den Standort der Taxi-Genossenschaft auch als Betriebssitz zu nutzen, um deren allgemeines Persönlichkeitsrecht stärker zu schützen.

5.3 Prüfung eines Mietervereins

Die Aufsichtsbehörde prüfte den Umgang mit Mitgliederdaten eines Mietervereins auf Grund einer Anfrage des Vereinsvorstandes:

1. Es seien Daten von ca. 7000 Mitgliedern verarbeitet worden, deren Mitgliedschaft schon vor mehreren Jahren (bis zu 15 Jahre) endete.

2. Es erfolge eine Verarbeitung sämtlicher Vereinsdaten auf einem PC im privaten Umfeld des Geschäftsführers.

Der Geschäftsführer des Vereins und verantwortliche Leiter der Datenverarbeitung wurde daraufhin durch die Aufsichtsbehörde um schriftliche Stellungnahme gebeten. Ferner erfolgte eine Vorortkontrolle in den Räumlichkeiten der Geschäftsstelle des Mietervereins durch Mitarbeiter der Aufsichtsbehörde.

Der Vorwurf, es seien Daten von ca. 7000 Mitgliedern verarbeitet worden, deren Mitgliedschaft schon vor mehreren Jahren (bis zu 15 Jahre) endete, konnte im Ergebnis der Prüfung in diesem Umfang nicht bestätigt werden. Sofern das Vertragsverhältnis mit dem Mieterverein beendet worden ist, wurden im Ergebnis der Prüfung die personenbezogenen oder –beziehbaren Daten nach Ablauf der gesetzlichen Aufbewahrungsfrist von sechs bzw. zehn Jahren (§ 257 Handelsgesetzbuch) grundsätzlich gelöscht.

Die Verarbeitung von Vereinsdaten auf einem PC im privaten Umfeld des Geschäftsführers erfolgte auf der Grundlage der zum Zeitpunkt des Geschehens aktuellen Geschäftsordnung des Vorstandes. Im Ergebnis der

Prüfung durch die Aufsichtsbehörde wurde die Verarbeitung personenbezogener Daten auf dem privaten PC des Geschäftsführers jedoch eingestellt.

Vorsätzliche oder fahrlässige Verstöße gegen datenschutzrechtliche Regelungen wurden nicht festgestellt.

5.4 Veröffentlichung von Spielsperren im Internet

Ein Betroffener beschwerte sich bei der Aufsichtsbehörde darüber, dass ein Sportverband seinen Vor- und Nachnamen, die ihm vorgeworfene Tat, deren Datum, die verhängte Verbandsstrafe (Spielsperre) sowie weitere Angaben in der Rubrik „Spielsperren“ in seinem Internetangebot für jedermann einsehbar veröffentlicht hatte. Dies war in dieser Form nicht zulässig.

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG (alt) kann ein Verband personenbezogene Daten über einen Spieler, mit dem ein vertragsähnliches Vertrauensverhältnis besteht, im Rahmen des Grundsatzes der Verhältnismäßigkeit übermitteln, soweit dies der Zweckbestimmung dieses vertragsähnlichen Verhältnisses dient und die Verbandsstatuten dies vorsehen (§ 28 Abs. 1 Satz 2 BDSG). Nicht gerechtfertigt ist jedoch, diese Informationen so in das Internet einzustellen, dass weltweit jedermann davon Kenntnis nehmen kann. Damit würden Spieler, die mit einer Verbandsstrafe belegt wurden, regelrecht an den Pranger gestellt. Ein legitimes Interesse daran, sich über die Dauer von Spielsperren informieren und deren Beachtung kontrollieren zu können, hat nur ein begrenzter Personenkreis, beispielsweise Mannschaften derselben Spielklasse oder Schiedsrichter. Aber auch dieser muss nicht wissen, welche Gründe zu der Sperrung geführt haben. Erst recht muss er keine Kenntnis von anderen Verbandsstrafen, etwa Geldbußen, haben. Die Verbandsmitglieder oder die Sportler allgemein über Verbandsstrafen zu informieren, um dadurch einen Abschreckungseffekt zu erzielen, würde eine personenbezogene Veröffentlichung im Internet nicht rechtfertigen. Das Mitteilungssystem des Verbands ist daher so auszugestalten, dass nur der jeweils berechtigte Personenkreis auf die einzelnen Daten zugreifen kann. Dies lässt sich durch eine Intranetlösung erreichen, bei der den berechtigten Nutzern durch Verwendung von Benutzerkennungen und Passwörtern individuelle Zugriffsberechtigungen eingeräumt werden. Diese sind so zu vergeben, dass jeder Nutzer nur auf diejenigen personenbezogenen Daten zugreifen kann, die er zur Wahrnehmung seiner (Vereins-) Aufgaben benötigt.

Um die einheitliche Auffassung der obersten Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich zu veröffentlichen wurde folgender Beschluss veröffentlicht:

„Keine Internetveröffentlichung sportgerichtlicher Entscheidungen

Entgegen der Auffassung des OLG Karlsruhe in seinem Urteil vom 30. Januar 2009 gehen die zuständigen Aufsichtsbehörden in Anwendung des BDSG davon aus, dass die uneingeschränkt zugängliche Veröffentlichung von sportgerichtlichen Entscheidungen im Internet unzulässig ist. Entsprechendes gilt auch für die Veröffentlichung von personenbezogenen Sperrlisten.
Eine Veröffentlichung in geschlossenen Benutzergruppen ist zulässig, wenn gewährleistet ist, dass in den Vereinen nur zuständige Personen zugreifen können. Soweit der Personenbezug nicht erforderlich ist, sind sportgerichtliche Entscheidungen zu anonymisieren.
Bei der mit der Veröffentlichung im Internet verbundenen Datenübermittlung an Dritte wird der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen meist deswegen als besonders gravierend empfunden, weil hierdurch nicht nur ein weltweiter Zugriff auf die Daten, sondern darüber hinaus vor allem eine elektronische Recherchierbarkeit ermöglicht wird, welche auch zur Erstellung eines Persönlichkeitsprofil genutzt werden kann.
Der beabsichtigten „Prangerwirkung“ mit Abschreckungsfunktion könnte bereits dadurch Genüge getan werden, dass entsprechende Ahndungen organisations-/verbandsintern in zugriffsgeschützten Internetforen „für die, die es angeht“, publizieren würden. Die intendierte Information der Öffentlichkeit über das Vorgehen gegen Rechtsverstöße könnte ohne Personenbezug im Rahmen einer Ahndungsstatistik erfolgen.“[2]

5.5 Kopie des Personalausweises bei Abschluss eines Wohnungsmietvertrages

Im Rahmen der Erhebung von personenbezogenen Daten von Mietinteressenten erbat eine Wohnungsbaugesellschaft auch eine Kopie des Personalausweises. Bei Abschluss eines Vertrages seien jedoch nur die dafür notwendigen Daten verarbeitet und die jeweilige PA-Kopie vernichtet worden.

[2] http://www.bfdi.bund.de/cln_136/DE/Entschliessungen/DuesseldorferKreis/DKreis_node.html

Diese Praxis stieß berechtigterweise auf Kritik der Mietinteressenten. Auf eine entsprechende Beschwerde hin wandten sich die Aufsichtsbehörde an das Unternehmen und wies darauf hin, dass diese Praxis mit den Regelungen des BDSG nicht im Einklang stehe. Es dürfen von vornherein nur diejenigen Daten erhoben werden, die für die Begründung, Durchführung oder Beendigung eines Vertrages erforderlich sind.
Die in der Kopieanfertigung liegende Erhebung und Speicherung der überschüssigen auf der Personalausweisvorderseite befindlichen personenbezogenen Daten, wie Lichtbild, Geburtsort, Nationalität, Ausweisgültigkeit, Ausweisnummer, war für die Vertragszwecke nicht erforderlich und damit nach § 28 Absatz 1 Satz 1 Ziffer 1 BDSG unzulässig. Das Unternehmen reagierte auf unseren Hinweis umgehend und stellte die Praxis der Anfertigung von Ausweiskopien ein.

5.6 Post vom Autohaus nach Hotelbesuch

Mit Verwunderung stellten verschiedene Personen fest, dass sie (Werbe)Post von einem Autohaus erhielten, mit welchem sie keinerlei Geschäftsbeziehungen in der Vergangenheit unterhielten.
Bereits die Anrede „Sie als Stammgast des Hotels …“ legte die Vermutung nahe, dass die Kundendaten der Hotelgäste an das Autohaus weitergegeben wurden. Die Weitergabe der Daten sei ohne Zustimmung der Betroffenen erfolgt.

Sowohl das Autohaus als auch das Hotel werden unter derselben Geschäftsführung betrieben. In der Stellungnahme des Hotels wurde erwähnt, dass die Kundenstammdaten des Hotels und der Autohäuser getrennt seien. Die Werbeaktion erfolgte durch die EDV-Abteilung, die sowohl für das Hotel als auch für die Autohäuser zuständig ist. In den Autohäusern sei ein Zugriff auf Kundendaten des Hotels nicht möglich, auch nicht umgekehrt. Insofern habe es sich um ein einmaliges Versehen gehandelt.

Auch wenn beide Unternehmen unter einheitlicher Leitung stehen, handelt es sich datenschutzrechtlich um von einander unabhängige Stellen, also im Sinne des Datenschutzrechtes um „Dritte“. Sollen die Daten eines der Unternehmen durch das jeweils andere genutzt werden, handelt es sich datenschutzrechtlich um eine Übermittlung personenbezogener Daten.

Die verantwortliche Stelle wurde auf die einschlägigen datenschutzrechtlichen Regelungen insbesondere zur Übermittlungsbefugnis sowie zur Nutzung von personenbezogenen Daten für andere als in § 28 Abs. 1 BDSG genannten Zwecke hingewiesen. Um weiteren Beschwerden vorzubeugen hat die Aufsichtsbehörde angeregt, dass zukünftig Werbung nur auf ausdrücklichen Wunsch bzw. mit Einwilligung der Kunden zugesandt wird.
Die Unternehmensleitung sicherte zu, dies zukünftig zu berücksichtigen und bedauerte die einmalig stattgefundene Aktion.

6 Einleitung von Ordnungswidrigkeitenverfahren

Im Berichtszeitraum wurden zwei Ordnungswidrigkeitenverfahren wegen des Verstoßes gegen datenschutzrechtliche Vorschriften eingeleitet.

7 Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden der Länder und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

7.1 Sitzungen der Arbeitsgruppe „Auskunfteien“

Im Berichtszeitraum fanden 5 Sitzungen der Arbeitsgruppe „Auskunfteien“ statt. Die Federführung teilten sich abwechselnd sowohl das Ministerium des Innern des Landes Brandenburg als auch – speziell für den Themenkomplex SCHUFA - das Hessische Ministerium des Innern und für Sport.

7.1.1 Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig

Häufig holen Vermieter Informationen bei Auskunfteien über die Bonität von Mietinteressenten ein, bevor sie Wohnraum vermieten. Hierfür gelten nach einem Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich folgende Anforderungen:

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

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

- Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen,
- sonstige Daten über negatives Zahlungsverhalten, bei denen
  - die dem jeweiligen Eintrag zugrunde liegende Forderung noch offen ist oder – sofern sie sich zwischenzeitlich erledigt hat – die Erledigung nicht länger als ein Jahr zurückliegt und
  - eine Bagatellgrenze von insgesamt 1.500 € überschritten wird.

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

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

<u>Hintergrund:</u>

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

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

Bei der erforderlichen Abwägung sind allerdings auch die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung zu berücksichtigen. Ferner ist zu beachten, dass Mietkautionen in Höhe von bis zu drei Monatsmieten, das Vermieterpfandrecht und die bei nachträglicher Zahlungsunfähigkeit vielfach in die Zahlungspflicht eintretenden Sozialbehörden das finanzielle Risiko der Vermieter teilweise reduzieren.

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

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

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

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

Die Bagatellgrenze von 1500 € errechnet sich aus drei Monatsmieten der durchschnittlichen Kaltmiete. Nach der jüngsten Einkommens- und Verbrauchsstichprobe des Statistischen Bundesamtes beträgt sie monatlich 515 €. Auch wenn die Speicher- bzw. Überprüfungsfrist der Auskunfteien bei Forderungen, die nach der Einmeldung beglichen wurden, drei Jahre beträgt (§ 35 Abs. 2 Nr. 4, 2. Halbsatz BDSG neu), ist ein berechtigtes Interesse von Vermietern an der Kenntnis solcher Daten nur für ein Jahr anzuerkennen. Daher ist auch nur innerhalb dieses Zeitraums eine Übermittlung an Vermieter zulässig. Ansonsten wäre dem Schuldner die Eingehung eines Mietverhältnisses unvertretbar erschwert. Die Unzulässigkeit der Übermittlung von Score-

werten an Vermieter ergibt sich daraus, dass abgesehen von der allgemeinen Problematik der Scoreberechnung im Mietbereich die besondere Problematik besteht, dass die spezifischen Einschränkungen unterlaufen würden, wenn eine Scoreberechnung mit Daten erfolge, die über die unter Nummer 2 genannten Daten hinausgehen.
Die bisherige Praxis der Auskunfteien entsprach den hier gestellten Anforderungen nicht bzw. nicht in ausreichendem Maße. Obwohl den Auskunfteien ausdrücklich die Möglichkeit eingeräumt wurde, ggf. alternative Lösungen zu den im Beschluss genannten Anforderungen zu entwickeln, die auf das jeweilige Geschäftsmodell der Auskunfteien und deren speziellen Datenbestand zugeschnitten sind, haben die Auskunfteien diese Möglichkeit bislang nicht genutzt.
Die Einforderung von unbegrenzten Selbstauskünften oder Einwilligungen zur Einholung weit gefasster Auskünfte vom Mietinteressenten würde eine Umgehung der sich aus der Abwägung nach § 29 BDSG ergebenden gesetzlichen Begrenzung des Auskunftsanspruchs von Vermietern darstellen und wäre nicht zulässig. Die Aufsichtsbehörden haben in Gesprächen mit den Auskunfteien angekündigt, dass sie bei datenschutzwidrigen Übermittlungen ggf. aufsichtsrechtliche Maßnahmen ergreifen werden.

7.2 Teilnahme an den Sitzungen der Arbeitsgruppe „Telekommunikation, Tele- und Mediendienste“

Im Berichtszeitraum fanden 4 Sitzungen der Arbeitsgruppe „Telekommunikation, Tele- und Mediendienste“ unter der Federführung des Berliner Beauftragten für Datenschutz und Informationsfreiheit statt. Im Vordergrund der Sitzung standen Anwendungsprobleme des Telemediengesetzes (TMG) sowie des Mediendienste-Staatsvertrages (MDStV) bzw. des Telemediengesetztes (TMG).

7.3 Workshop der Aufsichtsbehörden

Im Berichtszeitraum fanden 2 Workshops der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich statt. Im Vordergrund stand der Erfahrungsaustausch über die Wahrnehmung der Aufgaben nach § 38 BDSG. Als Ergebnisse dieser äußerst praxisorientierten Veranstaltungen wurden Handreichungen oder Formularmuster wie z.B. zur Auftragsdatenverarbeitung (siehe Anlage) erarbeitet.

8 Ausblick

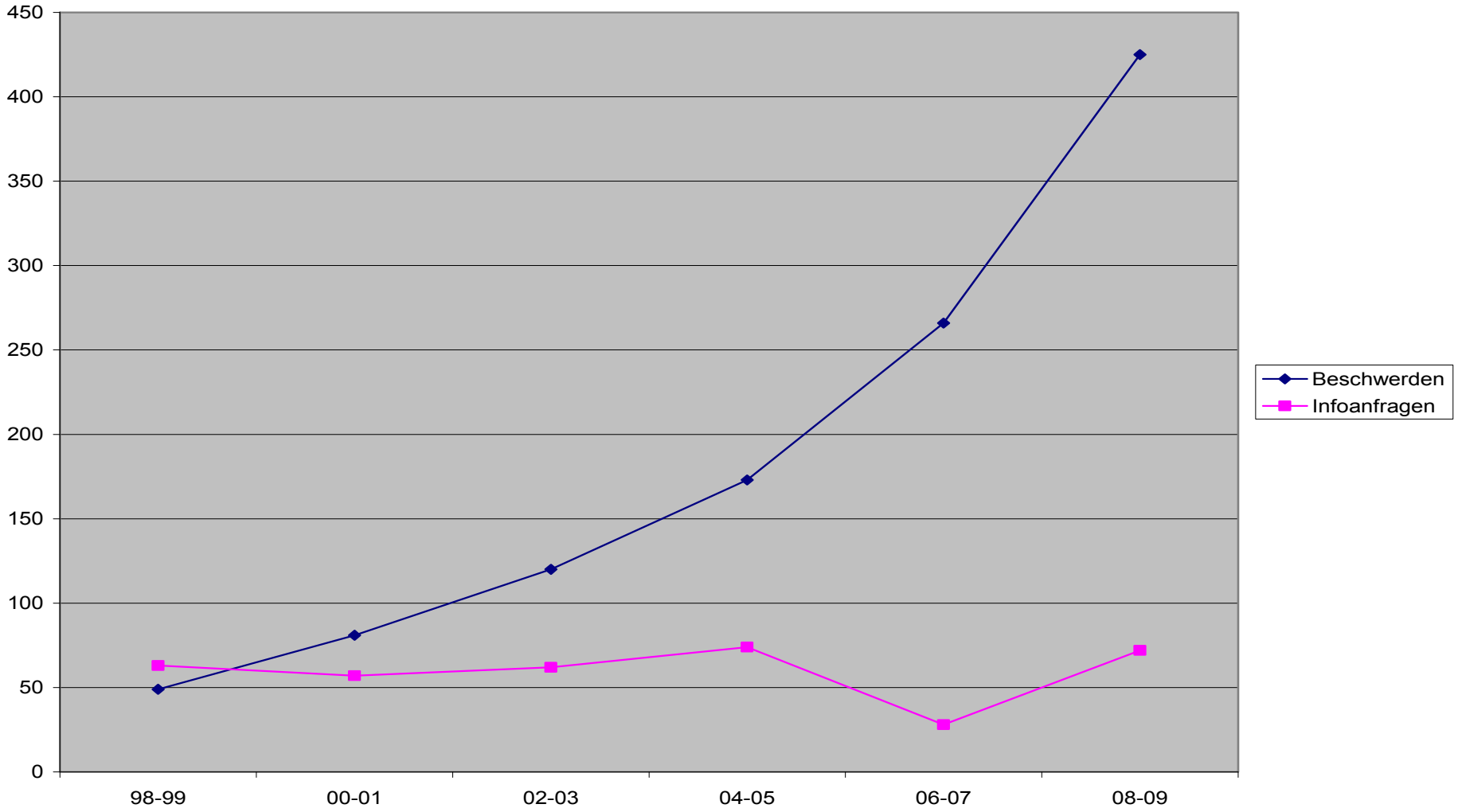
Nicht zuletzt durch die jüngsten „Datenschutzskandale“ hat die Sensibilität für die eigenen personenbezogenen Daten und letztlich für das allgemeine Persönlichkeitsrecht in der Bevölkerung zugenommen. Eine aktuelle Statistik über die Anzahl der schriftlich bearbeiteten Beschwerdevorgänge und Informationsanfragen seit 1998 ist als Anlage beigefügt. Rein telefonisch erledigte Vorgänge werden statistisch nicht erfasst.

Zu den Themenkomplexen mit wachsender Bedeutung gehören nach den Erfahrungen im Berichtszeitraum:

- Webbasierte Internet-Dienste
- Videoüberwachungen in Nachbarschaftsbeziehungen oder in öffentlich zugänglichen Räumen
- Datenschutz im Gesundheitsbereich
- Arbeitnehmerdatenschutz
- Auskunfteien
- Aufklärung der Öffentlichkeit über Datenschutzfragen

Der Brandenburgische Landtag hat mit Beschluss vom 06.05.2010 das Vierte Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes und anderer Rechtsvorschriften verabschiedet. Nach fast 20-jähriger Zugehörigkeit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich zum Ministerium des Innern des Landes Brandenburg erfolgte damit Kraft Gesetz vom 25.Mai 2010 die Verlagerung dieser Aufsicht zur Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht, Frau Dagmar Hartge. Damit ist diese Brandenburgische Datenschutzbehörde nicht mehr nur - wie bisher - für die Kontrolle der Datenverarbeitung in der öffentlichen Verwaltung, sondern ab dem 1. Juni 2010 auch für den privaten Bereich zuständig.

Entwicklung der Beschwerden und Informationsanfragen bei der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich in Brandenburg seit 1998



Mustervereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen nach § 11 BDSG

Stand 23. April 2010

Vorbemerkung: *Die nachstehende Mustervereinbarung soll als Orientierungshilfe für Auftragsdatenverarbeitungen dienen, auch für Wartungsverträge (§ 11 Abs. 5 BDSG). Sie ist bei Bedarf an den konkreten Einzelfall anzupassen und gegebenenfalls zu ergänzen oder abzuwandeln.*

.....
- Auftraggeber -

und

.....
- Auftragnehmer -

I. Gegenstand der Vereinbarung

1. Der Auftragnehmer erhebt / verarbeitet / nutzt personenbezogene Daten im Auftrag des Auftraggebers.

2. Der Auftrag umfasst Folgendes:

   2.1 Gegenstand des Auftrages (Definition der Aufgaben):

   ……..

   2.2 Dauer des Auftrags

   2.2.1 Der Vertrag

   □ beginnt am..... und endet am .....

   oder

   □ beginnt am …….... und endet mit Auftragserledigung.

   oder
   □ wird auf unbestimmte Zeit geschlossen.
   (Er ist mit einer Frist von ..... Monaten zum Quartalsende kündbar.)

   2.2.3 Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers vertragswidrig verweigert.

2.3 Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

……..

2.4 Art der Daten

……..

2.5 Kreis der Betroffenen:

……..

Ausfüllhinweis zu 2.3 bis 2.5: *Die Angaben sind so präzise zu gestalten, dass der Auftraggeber seiner Rolle als verantwortliche Stelle gerecht wird. Erfolgt die Datenerhebung, -verarbeitung oder -nutzung für verschiedene Zwecke sind die Art der Daten und der Kreis der Betroffenen jeweils gesondert anzugeben, gegebenenfalls ist hierbei zwischen den einzelnen Phasen der Datenverwendung (Erhebung, Speicherung, Veränderung, Übermittlung, Sperrung, Löschung, Nutzung) zu differenzieren, unter anderem sind auch etwaige Löschroutinen vorzugeben. Alternativ oder ergänzend zu entsprechenden Angaben an dieser Stelle kann auf eine entsprechende Leistungsvereinbarung oder die betreffende Passage in einem separaten Dienstvertrag verwiesen werden. In dem Dienstvertrag ist die Vereinbarung nach § 11 BDSG als Anlage zu kennzeichnen.*

II. Rechte und Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Datenerhebung / - verarbeitung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

2. Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und entsprechend Nr. I.2 dieses Vertrages schriftlich festzulegen.

3. Der Auftraggeber hat das Recht, in folgendem Umfang Weisungen gegenüber dem Auftragnehmer zu erteilen:

   ……..

4. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen. Die schriftliche Bestätigung der mündlichen Weisungen sollte von Auftraggeber und Auftragnehmer zusammen mit der Mustervereinbarung so aufbewahrt werden, dass alle maßgeblichen Regelungen jederzeit verfügbar sind.

   Weisungsberechtigte Personen des Auftraggebers sind:

   .....
   (Name, Organisationseinheit, Funktion, Telefon)

Weisungsempfänger beim Auftragnehmer sind:

.....
(Name, Organisationseinheit, Funktion, Telefon)

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen. Falls Weisungen die unter Nr. I. 2 dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Festlegung erfolgt.

4. Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen (s. Nr. IV) zu überzeugen. Der Auftraggeber kann diese Kontrolle auch durch einen Dritten durchführen lassen.

5. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

III. Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung (siehe oben Nr. I. 2.3) oder einer Weisung verlangt.
   Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

2. Der Auftragnehmer hat insbesondere folgende Kontrollen durchzuführen:

   ……...

   Ausfüllhinweis: *Hier sind konkrete Kontrollpflichten des Auftragnehmers anzuführen. Vergleiche dazu die Beschreibung der technisch-organisatorischen Maßnahmen gemäß § 9 BDSG im Anhang.*

3. An der Erstellung der Verfahrensverzeichnisse hat der Auftragnehmer mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

4. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden - automatisierten - Verwaltung. Eingang und Ausgang werden dokumentiert.

5. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

6. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

7. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen mitwirkt.

8. Die Verarbeitung von Daten in Privatwohnungen ist nur mit Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung durch den Auftraggeber vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

9. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen,

   □ dem Auftraggeber auszuhändigen.

   oder

   □ wie folgt zu löschen:

   ……..
   Ausfüllhinweis: *Verweis auf die Festlegungen unter Nr. I.2.3 möglich*

   Test- und Ausschussmaterial sowie Datensicherungskopien sind nach Abschluss der vertraglichen Arbeiten

   □ dem Auftraggeber auszuhändigen.

   oder

   □ wie folgt zu löschen:

   ……..
   Ausfüllhinweis: *Verweis auf die Festlegungen unter Nr. I.2.3 möglich*

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen.

10. Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers zugelassen. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer Namen und Anschrift des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer versichern, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. Insbesondere muss der Auftraggeber berechtigt sein, Kontrollen vor Ort beim Subunternehmer durchzuführen oder durch Dritte durchführen zu lassen. Der Auftragnehmer hat die Einhaltung der Pflichten regelmäßig zu überprüfen.

.....

Ausfüllhinweis: *Hier sind konkrete Vorgaben für diese Überprüfungen zu machen.*

Das Ergebnis der Überprüfungen ist zu dokumentieren.
Die Weiterleitung von Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach § 11 BDSG erfüllt hat. In dem Vertrag mit dem Subunternehmer sind die Angaben gemäß Nr. I.2.3 bis 2.5, III.9 und IV.1 so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.

□ Zurzeit sind die in Anlage ..... mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

11. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.
Falls ein Subunternehmer beauftragt werden soll, gelten diese Anforderungen zusätzlich zu den Bestimmungen in Nr. III.10.

12. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

13. □ Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz
Herr/Frau

.....
(Vorname, Name, Organisationseinheit, Telefon)

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

oder

□ Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die Voraussetzungen für eine Bestellung nicht vorliegen.

14. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis zu wahren. Er verpflichtet sich, auch folgende Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

.....

15. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften des BDSG bekannt sind. Der Auftragnehmer bestätigt, dass ihm auch folgende datenschutzrechtliche Vorschriften bekannt sind:

.....

Ausfüllhinweis: *Hier sind gegebenenfalls konkrete Angaben zu machen.*
Achtung: *Dies enthebt den Auftraggeber nicht von konkreten Vorgaben unter Nr. I.2.3 bis 2.5, so dass der Auftragnehmer weiß, was er zur Umsetzung der Spezialvorschriften zu beachten hat.*

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis schriftlich verpflichtet. Der Auftragnehmer überwacht die Einhaltung der hier angegebenen datenschutzrechtlichen Vorschriften**.**

16. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

IV. Technische und organisatorische Maßnahmen nach § 9 BDSG (Erläuterungen siehe Anhang)

Für die auftragsgemäße Bearbeitung personenbezogener Daten nutzt der Auftragnehmer folgende Einrichtungen:

.....
(Benennung der verwendeten Hardware und Software)

1. □ Das als Anlage beigefügte Datensicherheitskonzept (mit den Festlegungen entsprechend der Anlage zu § 9 BDSG) des Auftragnehmers wird als verbindlich festgelegt.

oder

□ Die im Anhang beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.

2. Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

3. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.
   Nr. II.2 ist zu beachten.

4. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

5. Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers nach § 42 a BDSG. Der Auftragnehmer sichert zu, den Auftraggeber bei seinen Pflichten nach § 42 a BDSG zu unterstützen.

V. Vergütung

.....

VI. Haftung

1. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

2. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem BDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

VII. Vertragsstrafe

Bei Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird eine Vertragsstrafe von ..... Euro vereinbart.

VIII. Nichterfüllung der Leistung

.....

IX. Sonstiges

1. Der Auftragnehmer übereignet dem Auftraggeber zur Sicherung die Datenträger, auf denen sich Dateien befinden, die Daten des Auftraggebers enthalten. Diese Datenträger sind besonders zu kennzeichnen.

2. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

3. Für Nebenabreden ist die Schriftform erforderlich.

Gegebenenfalls individualvertragliche Ergänzung:

Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Hinweis: *Diese Klausel muss wegen §§ 310 Abs. 1 S. 1 und 2, 307, 309 Nr. 2 lit. b BGB gegebenenfalls individualvertraglich vereinbart werden.*

X. Wirksamkeit der Vereinbarung

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Erläuterungen zu IV Datensicherungsmaßnahmen

In dem Vertrag müssen die technischen und organisatorischen Maßnahmen festgelegt werden, die bei der Datenverarbeitung umzusetzen sind.

Rechtsgrundlage ist § 11 Abs. 2 BDSG, in dem beschrieben ist, welche Prüfungen ein Auftraggeber vor einer Auftragsvergabe durchzuführen hat. So muss der Auftragnehmer unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. Im Auftrag sind insbesondere die technischen und organisatorischen Maßnahmen schriftlich festzulegen. Auch hat der Auftraggeber zu prüfen, ob beim Auftragnehmer die nach der Anlage zu § 9 BDSG erforderlichen Maßnahmen getroffen werden.

Werden personenbezogene Daten verarbeitet, deren Verarbeitung für die Betroffenen keine besonderen Risiken erwarten lässt, so bietet das Grundschutzhandbuch des BSI für bestimmte technische Konstellationen einen Katalog an Sicherheitsmaßnahmen. (Das Handbuch, in dem die Maßnahmen erläutert werden, kann auf Datenträgern beim BSI (www.bsi.de) bestellt werden.)

Wenn der Auftragnehmer ein Datensicherheitskonzept besitzt, muss der Auftraggeber prüfen und schriftlich festlegen, ob es seinen Anforderungen entspricht. Die Sicherheitsziele sind in der Anlage zu § 9 BDSG genannt. Ist das Konzept nicht ausreichend, sind ergänzende Maßnahmen zu vereinbaren. Das daraus resultierende Sicherheitskonzept sollte zum Vertragsbestandteil gemacht werden. In diesem Fall kann darauf verzichtet werden, im Sicherheitskonzept genannte Maßnahmen im Vertrag zu wiederholen.

Wenn der Auftragnehmer kein Datensicherheitskonzept vorlegen kann, müssen die Maßnahmen im Vertrag vereinbart werden. Dabei sind wiederum die in der Anlage zu § 9 BDSG genannten Sicherheitsziele zu erreichen. Aus dem Katalog sollten die einzelnen Maßnahmen in den Vertrag übernommen werden. Es handelt sich um keinen abschließenden Maßnahmenkatalog. Insbesondere bei der Verarbeitung sensibler Daten sind in der Regel zusätzliche Maßnahmen erforderlich.

Besonders wichtig sind Regelungen zu folgenden Sachverhalten:

- Verantwortlichkeiten: Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken.

- Abschottung von Netzen: Es müssen Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechnernetze soweit möglich zu verhindern. Da meist keine absolute Sicherheit zu erreichen ist, müssen derartige Versuche erkannt werden. Technische Komponenten, die in Betracht kommen, sind Firewalls, Intrusion Detection Systeme und insbesondere dem Stand der Technik entsprechende Verschlüsselungsverfahren.

- Abhören der Kommunikation: Zum Schutz gegen unberechtigtes Abhören bietet es sich an, die Daten entsprechend dem Stand der Technik zu verschlüsseln.

- Abmeldeprozeduren: Die Abmeldung am System oder Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Personen überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.

Beschreibung der technischen und organisatorischen Maßnahmen zu IV Datensicherungsmaßnahmen

1. Zutrittskontrolle

   Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

   (Beschreibung des Zutrittskontrollsystems, z.B. Ausweisleser, kontrollierte Schlüsselvergabe, etc.)

2. Zugangskontrolle

   Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

   (Verschlüsselungsverfahren entsprechend dem Stand der Technik.)

3. Zugriffskontrolle

   Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

   (Beschreibung von systemimmanenten Sicherungsmechanismen, Verschlüsslungsverfahren entsprechend dem Stand der Technik. Bei Online-Zugriffen des Auftraggebers ist klarzustellen, welche Seite für die Ausgabe und Verwaltung von Zugriffssicherungscodes verantwortlich ist.)

4. Weitergabekontrolle

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

   (Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z.B. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.)

5. Eingabekontrolle

   Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

   (Sämtliche Systemaktivitäten werden protokolliert; die Protokolle werden mindestens 3 Jahre lang durch den Auftragnehmer aufbewahrt.)

6. Verfügbarkeitskontrolle

   Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

   (Sicherungskopien des Datenbestandes werden in folgenden Verfahren hergestellt: hier Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und Aufbewahrungsort für Back-up-Kopien.)

7. Trennungskontrolle

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