Landtag Brandenburg **Drucksache 4/6537**
4. Wahlperiode

Bericht
der Landesregierung

Vierzehnter 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: 24.07.2008 / Ausgegeben: 24.07.2008

1 Einleitung

Der Bericht gibt einen Überblick über die Tätigkeit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich im Land Brandenburg. Grundlage auch für den regelmäßigen Berichtszeitraum ist § 38 Absatz 1 Satz 6 BDSG. Die Berichterstattung erstreckt sich auf der Grundlage von § 27 Brandenburgisches Datenschutzgesetz über einen Zeitraum von 2 Jahren und zwar vom 1. Januar 2006 bis 31. Dezember 2007.

2 Übersicht über die Kontrolltätigkeit

2.1 Meldungen zum Register

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich führt das Register nach § 4 d Bundesdatenschutzgesetz (BDSG). Es dient der Transparenz und kann von jedermann eingesehen werden. Das Einsichtsrecht erstreckt sich jedoch nicht auf die Angaben nach § 4 e Satz 1 Nr. 9 BDSG (Datensicherungs-maßnahmen/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. Für die übrigen Firmen gilt, wenn diese einen betrieblichen Datenschutzbeauftragten bestellt haben (§ 4 d Abs. 2 BDSG), entfällt die Meldepflicht. Sie entfällt ebenso, wenn bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten höchstens neun Arbeitnehmer beschäftigt sind und entweder eine Einwilligung des Betroffenen vorliegt oder die Datenverarbeitung zu Vertragszwecken beziehungsweise im Rahmen eines vorvertraglichen Vertrauensverhältnisses mit dem Betroffenen erfolgt. Im Berichtszeitraum wurden keine entsprechenden Auskunftsbegehren an die Aufsichtsbehörde herangetragen.

Die Registerübersicht gliedert sich folgendermaßen:

Gesamtmeldungen:	**9**
Davon	
Auskunfteien:	**6**
Markt- und Meinungs-	
Forschungsinstitute:	**3**

2.2 Beschwerden

Im Berichtszeitraum gingen **266** schriftliche Beschwerden sowie **28** schriftliche Informationsanfragen bei der Aufsichtsbehörde ein, die durch die Mitarbeiter weitestgehend zeitnah bearbeitet wurden. Telefonische Anfragen werden statistisch nicht erfasst.

Festzustellen ist, dass sich die Anzahl der schriftlichen Beschwerden im Vergleich zum vorigen Berichtszeitraum (ebenfalls 2 Jahre) um 93 Vorgänge erhöht hat. Die Anzahl der schriftlichen Informationsanfragen verringerte sich im Vergleich zum vorigen Berichtszeitraum um 46 Vorgänge. Ein Grund für diesen Rückgang ist der erhöhte Anteil von telefonischen Anfragen, die schon auf diesem Wege durch Erörterung und Informationsübermittlung abschließend erledigt werden konnten.

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 DSZustVO i.V.m. § 38 Absatz 6 BDSG).

Unter Punkt 3.4 werden nähere Ausführungen zu einigen Beschwerden gemacht.

3 Allgemeines

3.1 Neuregelung der Verpflichtung zur Bestellung eines (internen oder externen) Beauftragten für den Datenschutz (DSB)

Unter Abänderung eines Vorschlags zweier Bundesländer wurde im Rahmen des Mittelstandsförderungsgesetz § 4f Abs. 1 BDSG geändert und auf Vorschlag der Bundesregierung die Anzahl der Beschäftigten, ab der ein Datenschutzbeauftragter (DSB) zu bestellen ist, von vier auf neun erhöht. Diese Änderung des Gesetzes wurde auch von der Aufsichtsbehörde unterstützt, da dadurch insbesondere die kleineren mittelständischen Unternehmen (z.B. Tankstellen, Handwerksbetriebe etc.) entlastet werden.

3.1.1 Welche Person zählt?

Allein die Anzahl der „Personen“ ist entscheidend, die sich im Rahmen ihrer Aufgabenerfüllung mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten, und zwar unabhängig von ihrem arbeitsrechtlichen Status. Nicht nur „Arbeitnehmer“, auch freie Mitarbeiter oder Auszubildende müssen bei der Bestimmung der Anzahl der mit der automatisierten Datenverarbeitung Beschäftigten berücksichtigt werden. Im Gegenzug wird klargestellt, dass aus datenschutzrechtlicher Sicht die Personen, die nicht „in der Regel“ mit der automatisierten Verarbeitung personenbezogener Daten „ständig“ beschäftigt sind, unberücksichtigt bleiben können. Unternehmen, die z.B. nur kurzzeitig den Schwellenwert überschreiten, sind nicht zur Bestellung eines Beauftragten für den Datenschutz verpflichtet. Die Neuregelung soll vermeiden, dass Unternehmen nur deshalb einer anderen Kategorie zugeordnet werden, weil sie die maßgebliche Personengrenze für die Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz nur kurzzeitig überschreiten. Auch sind Personen nicht mitzuzählen, die nur gelegentlich, z.B. als Urlaubsvertretung personenbezogene Daten automatisiert verarbeiten (siehe BT-DS 16/1853 Abschnitt B zu Artikel 1, Buchstabe b, Doppelbuchstabe bb und BT-DS 16/1970).

Daraus ergibt sich, dass Personen, die in der Regel mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind, unabhängig vom quantitativen und qualitativen Anteil - wie bisher - in die Berechnung des Schwellenwertes einzubeziehen sind. Eine andere Beurteilung kann nur in den Fällen in Betracht kommen, in denen bei den Vor - und Nacharbeiten vom Inhalt der aus der automatisierten Verarbeitung stammenden Daten, z.B. Adressen, keine Kenntnis genommen werden kann und sich deshalb auch keine Gefährdung durch den Umgang mit den nach dem BDSG zu schützenden personenbezogenen Daten und für das informationelle Selbstbestimmungsrecht ergibt.

3.1.2 Externe DSB bei Berufgeheimnisträgern

Die Frage, inwieweit bei Apotheken und allgemein bei den unter § 203 Abs. 1 StGB fallenden Berufsgruppen (wie Ärzte, Apotheker, Rechtsanwälte, Notare, Steuerberater u.a.) die Bestellung externer betrieblicher DSB zulässig ist, war umstritten.

Nunmehr ist auch geregelt, dass die Bestellung von externen DSB bei Berufsgeheimnisträgern zulässig ist. Dem DSB steht ein Zeugnisverweigerungsrecht in dem Umfang zu, in dem es dem Geheimnisträger selbst aus beruflichen Gründen zusteht; insoweit unterliegen die Akten und andere Schriftstücke einem Beschlagnahmeverbot (§ 4f Abs. 4a BDSG).

(Folge)Änderung in § 203 StGB:
In Verbindung mit der Änderung des BDSG ist in § 203 StGB ein neuer Absatz 2a eingefügt worden. Danach gehören DSB nun zum Kreis möglicher Täter dieser Norm. § 203 Abs. 1 und 2 gilt entsprechend, wenn ein DSB unbefugt ein fremdes Geheimnis offenbart, das einem Geheimnisträger anvertraut oder sonst bekannt geworden ist und von dem er bei der Erfüllung seiner Aufgaben Kenntnis erlangt hat.

3.1.3 Die Aufsichtsbehörde wird oft zur nötigen Qualifikation des betrieblichen DSB befragt

a) Fachkunde
Es wird Fachkompetenz in Bezug auf EDV- Grundkenntnisse, Grundkenntnisse im allgemeinen Datenschutzrecht sowie im Bereich der datenschutzrechtlich relevanten Bestimmungen des BetrVG, Kenntnisse der Aufgaben-, Struktur- und Funktionsweise des Unternehmens sowie Schulungskompetenz gefordert.

b) Zuverlässigkeit
Im Hinblick auf die Zuverlässigkeit des betrieblichen DSB und seines Hilfspersonals sind deren Lernfähigkeit und Selbständigkeit sowie die Sensibilität für die betrieblichen Interessen und die Datenschutzbelange der Kunden und Mitarbeiter der Betriebe und sonstiger von der Datenverarbeitung Betroffener von besonderer Bedeutung

3.1.4 Mindestbestelldauer eines externen DSB

In Anlehnung an die in der Kommentarliteratur herrschende Meinung wird eine Mindestbestelldauer von zwei Jahren für verhältnismäßig gehalten. Die Vertragslaufzeit für Verträge mit externen DSB muss jedoch die dauerhafte Funktionsfähigkeit der Tätigkeit eines Datenschutzbeauftragten gewährleisten. Berücksichtigt man, dass der Datenschutzbeauftragte für die Erstellung und Umsetzung eines Datenschutzkonzeptes, dem Aufbau des Verfahrensverzeichnisses, der Schulung der Mitarbeiter bereits einen längeren Zeitrahmen benötigen wird, wird grundsätzlich eine Mindestlaufzeit des Vertrages von 3 Jahren für sinnvoll gehalten.

Die IHK Frankfurt/Main bietet im Übrigen unter der Internetseite

http://www.frankfurt-main.ihk.de/recht/themen/arbeitsrecht/datenschutzbeauftragter/index.html

Antworten auf die Fragen:

- Wann genau muss ein betrieblicher DSB bestellt werden?
- Wer kann zum betrieblichen Datenschutzbeauftragten bestellt werden?
- Wie wird ein betrieblicher DSB bestellt?
- Muster: Bestellung zum betrieblichen Datenschutzbeauftragten (mit Tätigkeitsbeschreibung)
- Anbieter von Datenschutz-Seminaren

3.1.5 Gefahr eines Interessenkonfliktes (Fall der Aufsichtsbehörde)

Kann ein Beschäftigter eines IT-Systemhauses gleichzeitig bei seinen eigenen Kunden als externer DSB tätig sein?

Zum DSB darf nach § 4f Abs. 2 Satz 1 BDSG nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.
Bei der Zuverlässigkeit sind subjektive genauso wie objektive Faktoren zu bedenken. Die subjektiven beziehen sich auf persönliche Eigenschaften, die objektiven auf mögliche Interessenskollisionen. Beide sind gleichwertige Kriterien. Eine Bestellung darf also nur erfolgen, wenn die erforderlichen persönlichen Eigenschaften gegeben sind *und* keine Interessenkollisionen vorliegen, die sich nachhaltig auf die Tätigkeit des Beauftragten auswirken können.
Die Gefahr eines solchen Interessenkonfliktes wäre im geschilderten Fall grundsätzlich gegeben. Das Systemhaus dürfte vertraglich verpflichtet sein, die Datenverarbeitung Hard- wie Softwareseitig so einzurichten und zu betreiben, dass den Verarbeitungszielen der verantwortlichen Stelle unter Berücksichtigung der von ihr definierten organisatorischen und finanziellen Ansprüche entsprochen werden kann. Genau diese Erwartungen müsste der DSB ständig überprüfen und zugleich versuchen, diese Erwartungen den Erfordernissen des Datenschutzes anzupassen. Sofern der DSB für die Erfüllung der vertraglichen Pflichten des Systemhauses gegenüber dem Kunden (wie z.B. die gesamte EDV-Betreuung von der Planung über die Lieferung und Installation bis hin zur Wartung) zuständig ist, bei dem er auch als DSB agiert, würde dies auf eine Kontrolle der eigenen Tätigkeit hinauslaufen.

Der Konflikt ließe sich nur lösen, wenn der DSB sowohl *nicht* mit der EDV-Betreuung befasst ist als auch hinsichtlich seiner Aufgabe als DSB gegenüber seinem Arbeitgeber – dem Systemhaus - *weisungsfrei* gestellt ist. Das BDSG sichert den DSB gegenüber der verantwortlichen Stelle, die ihn bestellt hat, unter anderem dadurch ab, dass sie ihn für weisungsfrei erklärt (§ 4f Abs. 3 Satz 2). Diese Weisungsfreiheit müsste also auch für den Beschäftigten des Systemhauses bezüglich seiner Funktion als externer DSB sichergestellt sein.

3.1.6 Darf ein betrieblicher DSB seinen Arbeitsplatz räumlich mit Dritten teilen? (Fall der Aufsichtsbehörde)

Nach § 4f Abs. 4 BDSG ist der DSB zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.
Diese Regelung schützt in erster Linie Betroffene, die sich an den Beauftragten wenden, um sich über die Verarbeitung ihrer Daten zu beschweren. Der Beauftragte soll, um sie vor möglichen Nachteilen zu schützen, ihren Fragen und Beanstandungen nachgehen, ohne dass sie damit in Zusammenhang gebracht werden. Er muss sich aber auch bei Anfragen und Beschwerden aller anderen Betroffenen genauso verhalten. Der Beauftragte muss über alle Angaben Stillschweigen bewahren, mit deren Hilfe der Betroffene direkt oder indirekt identifiziert werden kann. Die Verschwiegenheitspflicht gilt primär gegenüber der verantwortlichen Stelle sowie der Arbeitnehmervertretung und dem Werksarzt, ist aber genauso gegenüber Dritten und externen Kontrollinstanzen (Aufsichtsbehörden) zu beachten.

Aus rein praktischen Gründen ist es vor dem Hintergrund seiner umfassenden Verschwiegenheitspflicht (siehe auch die Änderung im § 203 StGB) geboten, dass der DSB seinen Arbeitsplatz räumlich nicht mit Dritten teilt, auch wenn diese ebenfalls zur Verschwiegenheit verpflichtet sind.

Im Übrigen haben nach § 4f Abs. 5 Satz 1 BDSG die nicht-öffentlichen Stellen den DSB bei der Erfüllung seiner Aufgaben zu unterstützen. Dazu gehört u.a. auch, dass ihm Räumlichkeiten zu Verfügung gestellt werden.

3.2 Schulprojekt: „Datenschutz für Lehrer und Schüler“

Sowohl im öffentlichen Leben (Behörden und sonstige öffentliche Einrichtungen wie z.B. Stiftungen) als auch in der Privatwirtschaft werden personenbezogene Daten erhoben und verarbeitet.
Öffentliche Stellen haben in erster Linie einen gesetzlichen Auftrag zu erfüllen und müssen dafür von Bürgern bestimmte personenbezogene Daten erheben und verarbeiten. Daher ist der Betroffene auch oft dazu verpflichtet der öffentlichen Stelle die gewünschten Angaben zur Person zu offenbaren. (z.B.: Meldebehörden, Sozialämter, Schulen etc.)
Privatrechtlich organisierte Unternehmen handeln aufgrund eines Vertrages oder eines vertragsähnlichen Vertrauensverhältnisses. Hier basiert die Erhebung und Verarbeitung personenbezogener Daten überwiegend auf Freiwilligkeit und Einwilligung.

Die zentralen Fragen „Wer weiß was über mich? Welche Angaben sind für die Erfüllung des Vertragszweck überhaupt notwendig?“ stellen sich immer noch zu wenige Menschen. Insbesondere Kinder und Jugendliche fehlt es oftmals an der nötigen Sensibilität im Umgang mit persönlichen Daten und Informationen. Datenschutz will gelernt sein.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat deshalb das Projekt „Datenschutz für Lehrer und Schüler“ initiiert. Gemeinsam mit dem Ministerium des Innern des Landes Brandenburg als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich wurde ein Lehrmaterial erstellt, das Schülerinnen und Schüler auf datenschutzrechtliche Aspekte, die sie im Alltag berühren können, aufmerksam macht.
So können Lehrerinnen und Lehrer an Hand einzelner Themenkomplexe wie z.B. Gewinnspiele, Kundenkarten, Kundenbefragungen, SCHUFA oder andere Handels- und Wirtschaftsauskunfteien die Jugendlichen für den Schutz des allgemeinen Persönlichkeitsrechts sensibilisieren. Die Schülerinnen und Schüler sollen auf diesem Wege auch über ihre Ansprüche auf Auskunft, Berichtigung, Löschung oder Sperrung ihrer Daten aufgeklärt werden.

Der modulare Aufbau des Unterrichtmaterials ermöglicht es den Lehrkräften, auf aktuellen Interessen der Jugendlichen einzugehen und so die Akzeptanz im Unterricht zu erhöhen. Das Schulprojekt wurde bereits in ausgewählten Schulen vorgestellt. Anlässlich des Zweiten Europäischen Datenschutztages im Januar 2008 wurde es auch durch die LDA der Öffentlichkeit präsentiert. Das Material wird von der LDA sowohl auf deren Website als auch in Form einer CD-ROM zur Verfügung gestellt.

3.3 Soziale Netzwerke

Zwei webbasierte Internet-Dienste führen aufgrund ihrer zunehmenden Verbreitung und Nutzung zu einer höheren Bedeutung der mit ihnen verbundenen datenschutzrechtlichen Fragen: Weblogs (kurz: Blogs) sowie Online-Communities (soziale Netzwerke).

An der Bewertung dieser Themenkomplexe war die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich nur indirekt beteiligt (z.B. in den Arbeitsgruppen des Düsseldorfer Kreises), da entsprechende Betreiber nach derzeitigen Erkenntnissen keinen Firmensitz im Land Brandenburg eingerichtet haben und da auch keine entsprechende Beratungsersuchen bisher an die Behörde herangetragen wurden.

Seitens der Aufsichtsbehörde kann deshalb das Nutzerverhalten im Wesentlichen nur auf der Grundlage der in den verschiedenen Medien veröffentlichten Beiträge zum o.g. Thema eingeschätzt werden. Entscheidend ist hier insbesondere die vorhandene Einsichtsfähigkeit, welche Folgen eine Teilnahme bzw. eine Mitgliedschaft an Weblogs oder Online-Communities für den Einzelnen hat. Die Verantwortung für eine datenschutzrechtlich korrekte Erhebung und Verarbeitung von personenbezogenen Daten liegt bei den Betreibern entsprechender Websites. Die Betroffenen müss(t)en z.B. immer so tief greifend informiert werden, dass sie eine Vorstellung haben, in welchem Umfang und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden. Anderenfalls besteht für die Betreiber ein erhöhtes Risiko, dass sie eine unzulässigen Datenerhebung und –verarbeitung durchführen. Es wird in der Aufsichtsbehörde bezweifelt, dass insbesondere Kinder und Jugendliche die Tragweite einer solchen Entscheidung immer überblicken. Mit ihrem Beschluss „Datenschutzkonforme Gestaltung sozialer Netzwerke“ haben die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich auf ihrer Sitzung am 17./18. April 2008 in Wiesbaden bundesweit einheitliche geltende datenschutzrechtliche Eckpunkte für das Betreiben von sozialen Netzwerken verabschiedet. Der Beschluss wurde vom Bundesbeauftragten für Datenschutz und die Informationsfreiheit auf seiner Website unter der Rubrik „Entschließungen des Düsseldorfer Kreises“ veröffentlicht.
Soziale Netze wie schuelerVZ oder studiVZ müssen ihre Nutzer umfassend über die Verarbeitung ihrer Daten informieren und ihnen die Entscheidung überlassen, welcher Personenkreis ihre Daten sehen darf. Die Nutzer müssen weder personalisierte Werbung noch die Speicherung von Nutzungsdaten auf Vorrat hinnehmen. Sie haben das Recht, sich in solchen Gemeinschaften unter Pseudonym zu bewegen und müssen ihr Profil oder ihr Bild jederzeit löschen können.

3.4 Anwendungsbereich des Telekommunikationsgesetz (TKG)

Das Kommunikationsmittel E-Mail ist anerkanntermaßen ein Telekommunikationsdienst i.S.v. § 3 Nr. 24 TKG. Losgelöst von Einzelfällen konnte seitens der Aufsichtsbehörde jedoch festgestellt werden, dass hinsichtlich des Anwendungsbereiches des TKG noch Unsicherheiten bestehen.

3.4.1 Erlaubte oder geduldete Nutzung des E-Mail-Dienstes zu privaten Zwecken

Der Anwendungsbereich des TKG ist grundsätzlich eröffnet, soweit die verantwortlichte Stelle die Nutzung des E-Mail-Dienstes zu privaten Zwecken zulässt oder duldet.

Für die Frage, ob die verantwortliche Stelle als Diensteanbieter i.S.d. TKG agiert, ist ein etwaiger Drittbezug des E-Mail-Angebotes entscheidungsrelevant. Für die rechtliche Einordnung kommt es letztlich darauf an, ob der E-Mail-Dienst nur im Rahmen der funktionsgebundenen Tätigkeit der Arbeitnehmer oder der Mitglieder der verantwortlichen Stelle genutzt werden kann, oder ob auch eine Nutzung für private Zwecke zugelassen ist. Sofern es kein ausdrückliches Verbot der privaten Nutzung gibt, ist sie zumindest geduldet und somit zulässig. Das Merkmal „Drittbezug“ wäre in diesem Fall zu bejahen.

3.4.2 Die Verantwortliche Stelle betreibt selbst kein eigenes technisches System

Der Anwendungsbereich des TKG ist grundsätzlich eröffnet, auch wenn die verantwortliche Stelle selbst kein eigenes technisches System betreibt, um den Arbeitnehmern bzw. Mitgliedern oder außen stehenden Dritten eine Telekommunikation zu ermöglichen. Unerheblich ist auch, ob die verantwortliche Stelle hinsichtlich des technischen Systems eine Verfügungsgewalt hat oder nicht.

Ein Angebot von Telekommunikation, also dem technischen Aussenden, Übermitteln und Empfangen von Signalen mittels Telekommunikationsanlagen (vgl. § 3 Nr. 22 TKG), kann auch unabhängig vom Betrieb einer eigenen Telekommunikationsanlage oder eines eigenen Telekommunikationsnetzes erbracht werden, indem man sich in verschiedener Weise fremder Einrichtungen bedient. Folglich unterscheidet das TKG an einigen Stellen, so z.B. in § 109 TKG beim Umfang der Pflichten auch zwischen Diensteanbietern und Betreibern von Telekommunikationsanlagen, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen.
Die verantwortliche Stelle wird, soweit sie selbst kein eigenes technisches System betreibt, in der Regel als Auftraggeber einen Vertrag über die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag gemäß § 11 BDSG abschließen. Eine Auftragsdatenverarbeitung orientiert sich nicht am Begriff „Eigentum“. Sie liegt dann vor, wenn der Auftragnehmer lediglich als weisungsgebundener, verlängerter Arm oder als ausgelagerte Abteilung des Auftraggebers fungiert,

der Auftraggeber also als „Herr der Daten“ die volle Verfügungsgewalt behält und Art, Umfang und Zwecke der Datenverarbeitung selbst bestimmt. Dem Wortlaut des TKG ist zu entnehmen, dass der Gesetzgeber sowohl Auftraggeber als auch Auftragnehmer als Adressat anspricht. So ist gem. § 3 Ziff. 6 TKG "Diensteanbieter" jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste *mitwirkt*. Auch die speziellen Bestimmungen des Datenschutzes innerhalb des TKG regeln den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung *mitwirken* (§ 91 Abs. 1 Satz 1 TKG). Ein weiteres Indiz dafür, dass ein Diensteanbieter i.S.d. TKG kein eigenes technisches System betreiben muss, ist die Regelung des § 110 Abs. 1 TKG. An dieser Stelle wird ausdrücklich erwähnt, dass derjenige, der Telekommunikationsdienste für die Öffentlichkeit erbringt, *ohne hierfür eine Telekommunikationsanlage zu betreiben*, sich bei der Auswahl des Betreibers der dafür genutzten Telekommunikationsanlage über bestimmte Voraussetzungen zu vergewissern hat.

4 Kontrolltätigkeit der Aufsichtsbehörde

4.1 Vorortkontrolle und Beratung nach § 38 BDSG

Im Rahmen von Vorortkontrollen und Beratungen werden 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.

Ein Muster eines Verfahrensverzeichnisses (nach § 4g i.V.m. § 4e BDSG) ist als Anlage zu diesem Bericht beigefügt.

4.1.1 Veröffentlichung von Gebäudeansichten auf einer privaten Website eines Architekten

Ein Betreiber einer Website bat um eine datenschutzrechtliche Bewertung derselben, die er im Rahmen seiner Berufsausübung als Architekt betreibt. Er präsentiert auf seiner Internetseite sein berufliches Wirken und veröffentlicht gleichzeitig digitalisierte Bildaufnahmen von historischen und teils denkmalgeschützten Häusern aus seinem privaten Archiv, die er interessierten Kunden auch zum Verkauf anbietet.

Zunächst ist zu bemerken, dass er als Website-Betreiber mit gewerbsmäßigem Hintergrund das Telemediengesetz (TMG) zu beachten hat, welches am 01.03.2007 in Kraft getreten ist. Seine aktuelle Anbieterkennzeichnung entsprach nach hiesiger unverbindlicher Einschätzung den Regelungen des § 5 TMG, ohne dass hiermit die diesbezügliche Zuständigkeit des Ministeriums für Wirtschaft tangiert werden soll.

Die Beantwortung der Frage nach der datenschutzrechtlichen Zulässigkeit der Website hängt davon ab, ob es sich bei den fotografischen Abbildungen von Wohngebäuden um personenbezogene Daten handelt. Durch die Zuordnung der Bilder mit postalischen Adressen und die Möglichkeit einer Zuordnung der Adressen zu einzelnen Personen (z.B. durch Telefonbücher) war dies zu bejahen.
Des Weiteren erfüllen die vom Architekten erstellten Listen, Datenbanken und Aufstellungen von Wohngebäuden auf seiner Website den Datei-Begriff des § 3 BDSG. Der Anwendungsbereich des BDSG war folglich eröffnet.

Wie der Architekt der Aufsichtsbehörde mitteilte, betreibt er die Website als Inhaber eines Architektur- und Planungsbüros im Wesentlichen zum Zwecke der Eigenwerbung und Kundenakquisition. Mit der Einstellung der von ihm erstellten Aufnahmen von architekturhistorisch interessanten Gebäuden wolle er offensichtlich seine berufliche Erfahrung und Kompetenz unterstreichen. Er offeriert diese Bild- und Adressdaten auf seiner Website zum Zwecke eines geringen Nebenerwerbs. Die Übermittlung dieser Daten dürfte mithin seinem eigenen Geschäftszweck dienen; die Übermittlung ist jedoch nicht selbst der angestrebte Zweck seiner beruflichen Tätigkeit.

Nach § 28 Satz 1 Nr. 3 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, 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 vom Architekten erstellten Gebäudeabbildungen sind dem Augenschein nach von öffentlichem Straßenland aus aufgenommen worden. Die Bilddaten stammen also aus einer öffentlich zugänglichen Quelle. Die jeweilige postalische Adresse (Strasse und Hausnummer), die er den Bildern zugeordnet hat, konnte er mit Sicherheit durch bloßes Ablesen erheben, da diese Angaben ebenfalls öffentlich zugänglich sind.

Bei der Bewertung, ob schutzwürdige Interessen der Eigentümer /Bewohner der Immobilien an dem Ausschluss der Verarbeitung oder Nutzung gegenüber Ihrem berechtigten Interesse überwiegen, ist zu prüfen, ob sich ein Abwehranspruch aus dem allgemeinen Persönlichkeitsrecht und dessen Ausgestaltungen im Recht auf angemessenen Schutz der Privatsphäre, dem Recht am eigenen Bild und dem Recht auf informationelle Selbstbestimmung herleiten lässt.

Dies wurde bereits vor dem Hintergrund eines ähnlichen Sachverhaltes vom VG Karlsruhe geprüft und verneint (Beschluss vom 01.12.1999; Az. 2 K 2911/99). Ausgangspunkt war die bundesweite digitale Aufnahme des öffentlichen Straßenraums sowie der angrenzenden Gebäudeansichten zum Zwecke des Aufbaus einer elektronischen Häuser- und Gebäudekarte.

Das Gericht führt in seiner Begründung aus:
„Durch die Aufnahme und gewerbliche Weiterverbreitung von Abbildungen der Außenansicht der Wohngebäude der Anlieger wird nur der Teilbereich des Persönlichkeitsrechtes berührt, der ohnehin der Öffentlichkeit zugewandt ist und deshalb von vornherein allenfalls einen sehr begrenzten Schutz genießen kann. Denn dass aus den sich im normalen Verkehrsfluss bewegenden Aufnahmefahrzeugen der Antragstellerin Abbildungen aufgenommen werden können, die über die äußere Gebäudefassade hinaus tiefergehende Einblicke in die Privat- oder Intimsphäre der Anlieger erlaubten, wird von der Antragsgegnerin nicht behauptet und ist auch sonst nicht ersichtlich. Die Öffentlichkeitssphäre als der Bereich des menschlichen Lebens, von dem jedermann Kenntnis nehmen kann, genießt aber von vornherein keinen Schutz gegen Indiskretionen. Allenfalls gegen unrichtige oder ehrverletzende Darstellungen kann sich der Betroffene auch in diesem Teilbereich seiner Persönlichkeit mit Erfolg zur Wehr setzen. Solche Eingriffe drohen den Anliegern von dem völlig objektiven und wertneutralen Aufnahmeverfahren der Antragstellerin aber offensichtlich nicht. Auch die mit den technischen Möglichkeiten einer digitalen Bilderfassung und weitgehend automatischen Abrufbarkeit und Reproduzierbarkeit der Gebäudeabbildungen in der Bilddatenbank der Antragstellerin verbundenen erweiterten Verwertungschancen begründen insoweit keinen erweiterten Persönlichkeitsschutz. Zwar stehen die Abbildungen der Gebäude der Anlieger auf diese Weise dem Zugriff eines nicht mehr überschaubaren Personenkreises offen; dies ändert jedoch nichts daran, dass es sich bei den veröffentlichten Gebäudeansichten nur um einen sehr marginalen Ausschnitt aus dem Persönlichkeitsbild der Anlieger handelt, dessen Aussagekraft andere öffentlich zugängliche personenbezogene Daten nicht übersteigt (vgl. Landgericht Waldshut- Tien-

gen, a.a.O.).“

Schon das LG Waldshut-Tiengen stellte in seinem Urteil vom 28.10.1999; Az. 1 O 200/99 zum selben Sachverhalt fest, dass ein Hauseigentümer weder aus dem Eigentums- noch aus dem allgemeinen Persönlichkeitsrecht ein auf § 823, § 1004 BGB gestütztes Verbot ableiten kann, sein Hausgrundstück digital zu erfassen und diese Abbildungen im Rahmen einer Gebäude-Bilddatenbank zu verwerten. Dieses Verbot besteht auch dann nicht, wenn der Gebäudeabbildung innerhalb der Datenbank der dazugehörige Straßenname nebst Ortsnamen und Postleitzahl zugeordnet wird (Leitsatz der Redaktion Datenschutz und Datensicherheit 24 (2000) 2).

Vor diesem Hintergrund dürften die schutzwürdigen Interessen der Eigentümer /Bewohner der vom Architekten erhobenen und auf seiner Website offerierten Immobilienabbildungen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dessen berechtigten Interesse nicht überwiegen. Ein Verstoß gegen datenschutzrechtliche Vorschriften in Bezug auf seiner Website konnte nicht festgestellt werden.

4.1.2 Auslagerung von Patientenakten privater Krankenhäuser an private Archivdienstleister

Ein Unternehmen mit den Schwerpunktgeschäftsfeldern Lagerung und Verwaltung von Daten in physischer und elektronischer Form bat um eine Beratung, wie die Auslagerung von Patientendaten eines privaten Krankenhauses mit Sitz in Brandenburg an einen privaten Archivdienstleister mit Sitz im Bundesland Sachsen datenschutzrechtlich zu bewerten ist. Hintergrund war die beabsichtigte Bewerbung um einen Auftrag, der durch das Krankenhaus öffentlich ausgeschrieben wurde.
Zunächst war die Zulässigkeit einer solchen Patientendatenverarbeitung im Land Bandenburg zu klären. Im Ergebnis ist eine entsprechende Datenverarbeitung unter folgenden Voraussetzungen zulässig:

Die Auftragsdatenverarbeitung im nicht-öffentlichen Bereich ist grundsätzlich in § 11 BDSG geregelt. Diese allgemeine Vorschrift wird verdrängt, soweit Spezialgesetze entsprechende Regelungen enthalten. Das anfragende Unternehmen hätte als Auftragnehmer im vorliegenden Fall u.a. die Vorschriften des Krankenhausgesetzes des Landes Brandenburg (LKGBbg) und der Verordnung zum Schutz von Patientendaten im Krankenhaus (Krankenhausdatenschutzverordnung-KHDsV) zu beachten. Ungeachtet dessen bleibt der Auftraggeber (im vorliegenden Fall das Krankenhaus) für die Einhaltung der datenschutzrechtlichen Vorschriften durch den Auftragnehmer verantwortlich.

Nach § 28 LKGBbg gelten für den Umgang mit Patientendaten die Vorschriften des Brandenburgischen Datenschutzgesetzes vom 22. Januar 1992 (GVBl. I S. 2).
Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen hat auf der Grundlage von § 28 Abs. 3 Ziff. 9 LKGBbg in der KHDsV u.a. die Voraussetzungen der Datenverarbeitung im Auftrag, insbesondere durch Personen oder Stellen außerhalb des Krankenhauses geregelt. Diese Verordnung gilt für die Verarbeitung personenbezogener Daten in Krankenhäusern im Land Brandenburg (§ 2 Abs. 1 KHDsV). Soweit in dieser Verordnung nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden (§ 2 Abs. 2 KHDsV). Für die Verarbeitung von Patientendaten durch andere Personen oder Stellen im Auftrag des Krankenhauses gilt § 11 Abs. 1 und 3 Brandenburgisches Datenschutzgesetz (BbgDSG) entsprechend, soweit er nicht unmittelbar Anwendung findet (§ 6 Abs. 3 Satz 1 KHDsV).

Nach § 6 Abs.1 KHDsV sind Patientendaten grundsätzlich in dem Krankenhaus selbst oder im Auftrag dieses Krankenhauses durch ein anderes Krankenhaus als Auftragnehmer zu verarbeiten. Der Absatz 2 fordert, dass eine Verarbeitung von Patientendaten durch andere Personen oder Stellen im Auftrag des Krankenhauses nur zulässig ist, wenn

1. beim Auftraggeber sonst Störungen im Betriebsablauf nicht vermieden werden können oder
2. lediglich Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger besorgt werden können, wobei der überwiegende Teil der Speicherung des gesamten Datenbestandes beim Auftraggeber verbleiben muss.

Sofern die Bestimmungen des BbgDSG auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt (§ 11 Abs. 1 Satz 3 BbgDSG). Erfolgt die Durchführung des Auftrages außerhalb des Geltungsbereiches des BbgDSG durch eine nicht-öffentliche Stelle, so ist sicherzustellen, dass sich diese Stelle der Kontrolle des Landesbeauftragten für den Datenschutz, in dessen Land die Verarbeitung erfolgt, unterwirft, soweit dieser hierzu durch Landesrecht befugt ist (§ 11 Abs. 1 Satz 4 BbgDSG).[1]

1 Die Bewertung erfolgte auf der Grundlage des Brandenburgischen Datenschutzgesetzes mit altem Stand 2007.

4.1.3 Anfrage zur Errichtung einer Mieterdatei via Internet

Das Interesse der Vermieter, „schwarze Schafe“ unter den Mietinteressenten zu erkennen und dadurch das betriebswirtschaftliche Risiko von Ausfällen zu minimieren, ist nachvollziehbar. Viele Vermieter errichten als „Gläubigerschutzgemeinschaften“ gemeinsame Warndateien. Der Aufsichtsbehörde wurde ein Geschäftsmodell vorgestellt, bei dem Anfragen von Vermietern zu potentiellen Mietern mit Hilfe eines Internetportals bearbeitet werden sollten.

Diese Variante einer sog. Mieterwarndatei – in Form einer öffentlich zugänglichen Auskunftei im Internet – war jedoch im vorliegenden Fall datenschutzrechtlich unzulässig.
Eine Einstellung von Daten in das Internet ist datenschutzrechtlich jedenfalls eine Übermittlung. Da die Daten geschäftsmäßig zum Zweck der Übermittlung erhoben und verarbeitet werden sollten, war im vorliegenden Fall der § 29 BDSG als Rechtsgrundlage zu prüfen.

Nach § 29 Abs. 1 Satz 1 BDSG ist das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zweck der Übermittlung zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt.

§ 29 Abs. 1 Satz 1 Nr. 2 BDSG scheidet als Zulässigkeitsalternative für die Speicherung von Daten zur Zahlungsmoral von Mietern aus, wenn entsprechende Daten nicht aus allgemein zugänglichen Quellen, wie dem Schuldnerverzeichnis oder dem Insolvenzregister entnommen werden können.

Die Zulässigkeitsalternative des § 29 Abs. 1 Nr. 1 BDSG erfordert eine Vorabprüfung möglicher der Erhebung, Speicherung oder Veränderung der Daten entgegenstehender schutzwürdiger Interessen des Betroffenen. Es müssen die Belange der Wohnungssuchenden beachtet werden. Die Wohnung ist ein notwendiger Mittelpunkt des privaten Lebensbereiches. Dies wird allein schon dadurch deutlich, dass das Recht auf angemessenen Wohnraum im Artikel 47 der Verfassung des Landes Brandenburg als soziales Grundrecht definiert ist.

Ein schutzwürdiges Interesse des Betroffenen, hier also der Mieter, besteht auch darin, nicht durch ungeprüfte Eingaben von Daten, die dem Betreiber der Warndatei ein Vermieter mitteilt, in Warndateien zum „Negativmieter“ zu werden. Es lässt sich nicht ausschließen, dass Personen unverschuldet und ohne berechtigten Anlass in diesen Ruf geraten. Mit Blick auf die zentrale Bedeutung von Wohnraum im Leben jedes einzelnen Bürgers muss daher die Gefahr unberechtigter Einschränkungen bei der Wohnungssuche vermieden werden. Besteht auch nur Grund zu der Annahme, dass die Interessen des Betroffenen an der Verarbeitung entgegenstehen, so ist die Verarbeitung unzulässig. Ein solcher Grund kann sich bereits mit Blick auf die Sensibilität der Daten und eventuelle Auswirkungen ihrer Übermittlung für den Betroffenen ergeben. Da bei Warndateien die Auswirkungen auf den einzelnen Mieter sehr weit reichen können, ist eine Abwägung zwischen den verschiedenen Interessen sehr sorgfältig vorzunehmen.
Zudem werden Art und Umfang der für eine Mieterwarndatei erhebbaren und speicherbaren Daten auch danach bestimmt, welche Daten im Fall einer Anfrage eines Vermieters zulässiger Weise an diesen übermittelt werden dürfen.

Gemäß § 29 Abs. 2 Nr.1a BDSG ist die Übermittlung personenbezogener Daten im Rahmen der Zwecke nach Absatz 1 zulässig, wenn der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat.

Vermieter, welche sich an eine Warndatei wenden, müssen demzufolge ein berechtigtes Interesse an den begehrten personenbezogenen Daten nachweisen. Eine bloße Veröffentlichung von Bewertungen von Mietern gegen Bezahlung, zumal im Internet wäre datenschutzrechtlich unzulässig. Die verantwortliche Stelle hat grundsätzlich in jedem Einzelfall das berechtigte Interesse der anfragenden Person zu prüfen. Den Nachweis, wie das technisch-organisatorisch auf der Basis des Internets gelöst werden könnte, wurde der Aufsichtsbehörde nicht vorgelegt. Im Ergebnis wurde von dem Geschäftsmodell Abstand genommen.

Anerkannt wird das berechtigte Interesse der Vermieter an einer Minimierung des Mietausfallrisikos durch Übermittlung von Daten zum Zahlverhalten der Mieter.

Ein vollständiger Katalog von personenbezogenen Daten, welche an Vermieter übermittelt werden dürfen, existiert nicht. Von den Aufsichtsbehörden für den Datenschutz werden derzeit die Daten des nachfolgenden Kataloges als ohne jeden Zweifel an den Vermieter übermittelbar angesehen:

- Daten aus öffentlichen Schuldnerverzeichnissen
- Rechtskräftige Titel zum Zahlungsverzug im Mietbereich

- Rechtskräftige Urteile zur fristlosen Kündigung wegen
  - Zahlungsverzug, sonstiger Vertragsverletzung
- Rechtskräftiges Räumungsurteil wegen fristloser Kündigung
- bei so genannten „Mietnomaden“, wenn innerhalb der ersten 3 Monate zwei Monatsmieten nicht gezahlt wurden und Strafantrag/ -anzeige gestellt wurde.

Diese Daten können grundsätzlich auch zum Zwecke der Errichtung einer Warndatei erhoben und gespeichert werden. Sie dürfen ohne Einwilligung des Mieters durch den Vermieter abgefragt bzw. eingemeldet werden, jedoch nur, wenn der betroffene Mieter darüber angemessen informiert wird.

Insgesamt ist festzustellen, dass für ein datenschutzrechtlich nicht zu beanstandender Betrieb einer Mieterwarndatei ein nicht zu unterschätzender Aufwand bei der Pflege und dem Betrieb einer solchen Datenbank entsteht und auch hinsichtlich der Übermittlung der gespeicherten Daten enge Voraussetzungen erfüllt sein müssen.

4.1.4 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 2004/2005 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. In den meisten Fällen konnten die Probleme der Petenten umgehend gelöst werden, bzw. konnte im Ergebnis der Prüfung kein Verstoß gegen datenschutzrechtliche Vorschriften festgestellt werden.

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.

4.1.5 Prüfung des Consulting-Unternehmens GALLUP® in Potsdam

Anlass der Prüfung des Unternehmens war ein Informationsgespräch im Jahr 2005, wo durch das Unternehmen Fragen zum Datenschutz an die Aufsichtsbehörde herangetragen wurden, die in dem Gespräch am 17.05.2006 ausgeräumt und beantwortet werden konnten.
Da die Gallup GmbH seit dem 24.02.2003 zum Register gemäß § 4d BDSG bei der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich im Land Brandenburg gemeldet ist, wurde für das darauf folgende Jahr ein Prüfungstermin anvisiert. Der externe Datenschutzbeauftragte stellte das Unternehmen Gallup GmbH Deutschland mit seinen Geschäftstätigkeit näher vor. Zu den wesentlichen Aufgaben gehört die Anleitung und Schulung der Mitarbeiter im Unternehmen. Alle Beschäftigten sind auf das Datengeheimnis verpflichtet. Dies erfolgte durch eine separate Erklärung, die einmal in der Personalakte liegt und auch als Kopie den Beschäftigten ausgehändigt wird. Die Verpflichtung selbst wird durch die Personalabteilung durchgeführt. Ein Verfahrensverzeichnis nach § 4e i. V. mit § 4g BDSG ist vorhanden. Das Reinigungspersonal ist auf das Datengeheimnis durch die Reinigungsfirma selbst verpflichtet. Besucher werden von Mitarbeitern des Unternehmens begleitet. Bei Schulungen wird ein Besucherbuch geführt.

Insgesamt wurden gegenüber den Vertretern der Aufsichtsbehörde die technisch-organisatorischen Maßnahmen erläutert, die notwendig sind, um den gesetzlichen datenschutzrechtlichen Anforderungen gerecht zu werden (vgl. Anlage zu § 9 BDSG).

Die Gebäudesicherheit sowie der Umgang mit den personenbezogenen Daten im Unternehmen konnte als vorbildlich eingeschätzt werden.

4.1.6 Prüfung eines Callcenters betreffs Videoüberwachung

Anlass hierfür war eine Beschwerde eines Anwohners, der sich durch die Videoüberwachung an der Fassade des Unternehmens in seinem Persönlichkeitsrecht eingeschränkt fühlte. Gleichzeitig würde der Fußweg, die am Straßenrand parkenden Autos, der Eingang eines Friseursalons und der Durchgang zu den Eingängen der Mietwohnungen eingesehen.
Diese Beschwerde wurde zum Anlass genommen, vor Ort einen Augenscheintermin durchzuführen und gleichzeitig mit dem zuständigen Mitarbeiter die Angelegenheit zu erörtern. Die vorgefundene Kenntlichmachung der Videoüberwachung durch das Unternehmen wurde als nicht DIN-normgerecht befunden. Es wurde darauf hingewiesen, diese zu erneuern. Bei Einsichtnahme der Monitore im Eingangsbereich, gab es keine Beanstandungen. Die Leitung des Unternehmens rechtfertigte die Videoüberwachung zum Schutz des Eigentums, der Verbrechensprävention sowie zum Schutz vor Sprayern. Dem Unternehmen wurde vor Ort ein Realisierungstermin für die entsprechende Kenntlichmachung an allen Gebäuden unterbreitet. Der Sichtbereich der Kameras im

allgemein zugänglichen Bereich wurde auf ein Mindestmaß beschränkt und die Zustimmung zum Betrieb der Anlage durch den Vermieter eingeholt. Dies erfolgte ebenfalls nochmals in Schriftform.

4.2 Schwerpunkte aus Beschwerden

4.2.1 Möglichkeit einer unberechtigten Übermittlung von personenbezogenen Daten bei eBay

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich wurde über die Möglichkeit informiert, über eine API-Schnittstelle (engl. Abk. f. Schnittstelle zur Programmierung von Anwendungsprogrammen) mit Hilfe von Links bestimmte personenbezogene Daten von eBay-Mitgliedern (u.a. E-Mail-Adresse) unbemerkt zu erheben bzw. zu übermitteln. Diese Daten können von Betrügern dazu genutzt werden, ein gefälschtes „Angebot an den unterlegenen Bieter“ zu senden, wenn die betroffene Person bei Auktionen mitgeboten hat (sog. Second Chance Offer Fraud). Die Aufsichtsbehörde führte eine Beweissicherung durch, erstattete daraufhin Anzeige beim PP Potsdam und informierte den Datenschutzbeauftragten von eBay über den Vorfall. Das LKA ermittelte in diesem Fall. Im Rahmen eines persönlichen Gespräches zwischen Vertretern der Aufsichtsbehörde und der eBay GmbH wurde deutlich, dass die eBay Inc. als amerikanischer Konzern permanent Ziel krimineller Angriffe ist. Konzerninterne Umstrukturierungen hätten zu einem nunmehr gebündelten Trust & Safety-Management geführt. Das Unternehmen habe in jüngster Zeit seine technisch-organisatorischen Datenschutzmaßnahmen verstärkt. Unter Hinweis auf strengste Vertraulichkeit wurde eine Reihe von Maßnahmen erläutert, die einen verbesserten Schutz gegen einen unberechtigten Zugriff auf die Netzwerkstruktur des Unternehmens gewährleisten sollen.

4.2.2 „unrichtige“ negative Bewertungen von Käufern bzw. Verkäufern im Rahmen des eBay-Bewertungssystems

Nach § 35 Abs. 1 BDSG sind personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Berichtigung bedeutet, dass die Daten in Einklang mit der Realität gebracht werden müssen. Unrichtig können grundsätzlich nur objektiv greifbare Tatsachenangaben sein (z.B. über Beruf, Körpergröße, Anschrift). Demgegenüber entziehen sich Werturteile (z.B. guter Kunde, treuer Arbeitnehmer oder schwierig im Umgang) einer rechtlichen Einordnung als richtig oder unrichtig. Werturteile können also regelmäßig nicht Gegenstand eines Berichtigungsanspruches sein.

Das Bewertungssystem von eBay dient der Selbstregulierung des Marktplatzes und basiert auf Werturteilen. Sowohl die von den Beteiligten vergebenen Punkte (positiv, neutral oder negativ) als auch die Kommentare sind Werturteile, die jedoch bei z.B. irrtümlicher Vergabe gleichwohl berichtigt oder gelöscht werden.

Dies ergibt sich jedoch aus den Allgemeinen Geschäftsbedingungen (AGB) von eBay (und ist damit Bestandteil der vertraglichen Beziehung mit eBay), nicht aus dem Datenschutzrecht.

Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Personenbezogene Daten dürfen also auch abweichend vom BDSG verwendet werden, wenn sich der Betroffene damit einverstanden erklärt hat.

Die Einwilligung in die AGB bei eBay umfasst auch den Umgang mit negativen Bewertungen. Abgegebene Bewertungen werden durch eBay grundsätzlich weder verändert noch entfernt. Die Ausnahmen von diesem Grundsatz werden in den AGB geregelt, so dass durch die Einwilligung in die AGB die Regelungen des § 35 BDSG (Berichtigung, Löschung und Sperrung von Daten) nicht mehr einschlägig sind.

Im Übrigen wird eine Löschung von Bewertungen durch eBay in der Regel vorgenommen, wenn diesbezüglich Einvernehmen zwischen Käufer und Verkäufer herrscht.

Ungeachtet dessen herrscht im Privatrecht der Grundsatz der Privatautonomie, d.h. dem Einzelnen wird ermöglicht, seine Rechtsverhältnisse selbständig und nach seinem Willen durch Rechtsgeschäft zu gestalten. Letztlich ist dies ein Ausdruck der in Art. 1 Abs. 1, 2 Abs. 1 Grundgesetz verfassungsrechtlichen verbürgten Selbstbestimmung und Handlungsfreiheit.

Ein Aspekt der Privatautonomie ist die Vertragsfreiheit (Vertragsautonomie):

Jeder hat das Recht, frei darüber zu entscheiden, ob und auch mit wem er Verträge abschließen will (Abschlussfreiheit), sowie die Freiheit, den Inhalt der von ihm abgeschlossenen Verträge (im Einverständnis mit seinem Vertragspartner) zu bestimmen (Gestaltungsfreiheit). Eine Geschäftsbeziehung mit der eBay GmbH basiert folglich auf Freiwilligkeit und Einwilligung. Es ist somit niemand gezwungen, den Marktplatz eBay zu benutzen. Im Übrigen hat das Oberlandesgericht Brandenburg eine Monopolstellung bei eBay für nicht gegeben erachtet. (Urt. vom 11.01.2006 - Az.: 7 U 52/05).

Das Kammergericht Berlin hat in seiner Entscheidung vom 05.08.2005 (Az.: 1 U 4/05) im Zusammenhang mit der Beendigung einer eBay-Mitgliedschaft festgestellt:
Der Inhaber eines Nutzerkontos auf einer Internetauktionsplattform könne vom Betreiber die Löschung negativer Bewertungen nicht alleine aufgrund der Behauptung verlangen, bei den Bewertungen handele es sich um unzutreffende Rachebewertungen. Voraussetzung eines Anspruchs gegen den Betreiber der Plattform sei vielmehr entweder die Zustimmung der Bewertenden oder

der Nachweis der Regelwidrigkeit der Bewertung durch rechtskräftige Verurteilung des Bewertenden.

4.2.3 Faktisches Vertragsverhältnis mit einem Energieversorger

Ein Energieversorgungsunternehmen wurde über den Einzug in eine Wohnung informiert und gleichzeitig um Abgabe eines Versorgungsangebotes gebeten. Daraufhin wurde der Petent zum Einzugtag als Kunde im Rahmen der Allgemeinversorgung angemeldet. Der Versorgungsvertrag war jedoch nicht schriftlich geschlossen worden. Mit dem Einzug in besagte Wohnung und der damit einhergehenden Entnahme von Energie sei jedoch kraft schlüssigen Verhaltens ein Versorgungsvertrag zwischen dem Petenten und dem Energieversorgungsunternehmen abgeschlossen worden. In der Folgezeit wurde dem Petenten mehrfach ein Wechsel des Tarifs und damit der Abschluss eines Sondervertrages angeboten. Eine Annahme dieser Angebote erfolgte nicht. Der Vertrag über die Allgemeinversorgung wurde ca. 12 Wochen nach dem Einzug in die Wohnung beendet, da der Petent nunmehr die Energie von einem anderen Versorger bezog. Anlässlich der Vertragsbeendigung wurde eine Endrechnung über den Lieferzeitraum von 12 Wochen erstellt. Der Zahlungsausgleich wurde vom Petenten mit dem Hinweis auf einen angeblich fehlenden Vertragsabschluss verweigert.
In mehreren Mahnschreiben wurde der Petent zur Zahlung aufgefordert und jeweils darauf hingewiesen, dass das Energieversorgungsunternehmen die Daten über gerichtliche Maßnahmen zur Realisierung der Forderung an die SCHUFA Holding AG übermittelt, soweit dies nach Abwägung aller getroffenen Interessen zulässig ist. Darüber hinaus wurde der Petent schriftlich auf sein Auskunftsrecht nach § 34 BDSG auch gegenüber der SCHUFA hingewiesen. Mit Einleitung des gerichtlichen Mahnverfahrens ist eine Forderungseinmeldung an die SCHUFA über nicht vertragsgemäßes Verhalten erfolgt. Die Datenübermittlung basierte auf § 28 Abs. 3 BDSG und ist erfolgt, da sich der Petent trotz mehrerer Mahnungen und einem ausführlichen Schriftwechsel – unter der Behauptung eines fehlenden Vertragsverhältnisses – als zahlungsunwillig gezeigt habe, obwohl eine Zahlungspflicht bestünde. Aufgrund des Widerspruchs des Petenten ist ohne Anerkennung einer Rechtspflicht zunächst die Löschung des o.g. SCHUFA-Datenbestandes vorgenommen worden.

Grundsätzlich ist in dem Leistungsangebot für Elektrizität, Gas, Fernwärme und Wasser aus dem bestehenden Versorgungsnetz eines Versorgungsunternehmens ein Vertragsangebot in Form einer so genannten Realofferte zum Abschluss eines Versorgungsvertrages zu sehen, das von demjenigen konkludent angenommen wird, der aus dem Leitungsnetz des Versorgungsunternehmens Elektrizität, Gas, Wasser oder Fernwärme entnimmt. Vor diesem Hintergrund ging die Aufsichtsbehörde im vorliegenden Fall nach Aktenlage davon aus, dass zwischen dem Petenten und dem Energieversorgungsunternehmen ein faktisches Vertragsverhältnis, zumindest ein vertragsähnliches Vertrauensverhältnis für den besagten Zeitraum von ca. 12 Wochen bestand. Der Anspruch

auf die entsprechende Gegenleistung für die beanspruchte Energie ist offensichtlich wirksam entstanden.

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient, 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 (§ 28 Abs. 1 Nr. 1 u.2 BDSG). Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat (§ 28 Abs. 3 Nr. 1 BDSG). Nach den AGB der SCHUFA Holding AG darf die Übermittlung von Merkmalen über nichtvertragsgemäßes Verhalten nur dann erfolgen, wenn die in § 28 Abs. 3 BDSG genannten Voraussetzungen erfüllt sind.

Das Energieversorgungsunternehmen kann mithin auf der Grundlage des § 28 Abs. 3 Nr. 1 BDSG, soweit diese Voraussetzungen vorliegen und die Erhebung und Speicherung der Daten für die Zweckbestimmung eines Vertrages oder eines vertragsähnlichen Vertrauensverhältnis erfolgte, bestimmte Angaben über Zahlungsunfähigkeit oder Zahlungsunwilligkeit ihrer Kunden an die SCHUFA übermitteln. Die Merkmale, die von den Vertragspartnern der SCHUFA eingemeldet werden können, sind in den SCHUFA AGB definiert. Im vorliegenden Fall hat das Energieversorgungsunternehmen als Vertragspartner der SCHUFA nach mehrmaliger Mahnung und Einleitung eines gerichtlichen Mahnverfahrens offensichtlich die erforderlichen Angaben zur Person und das Merkmal „SD Fällig“, d.h. „Saldo nach Gesamtfälligstellung“ nebst Höhe des Saldos eingemeldet. Nach Auffassung der Aufsichtsbehörde stellt dies keinen Verstoß gegen datenschutzrechtliche Vorschriften dar. Nach Auskunft des Energieversorgungsunternehmens wurde der Petent in den Mahnschreiben jeweils darauf hingewiesen, dass das Energieversorgungsunternehmen die Daten über gerichtliche Maßnahmen zur Realisierung der Forderung ggf. an die SCHUFA übermitteln wird. Somit wurde der Petent über eine mögliche Übermittlung seiner Daten an die SCHUFA informiert und hatte die Gelegenheit, eigene Stellungnahmen sowohl gegenüber dem Energieversorgungsunternehmen als auch der SCHUFA abzugeben. Das Energieversorgungsunternehmen war zwar verpflichtet, die etwaige Stellungnahme des Petenten sorgfältig im Rahmen der vom Gesetz geforderten Berücksichtigung der schutzwürdigen Interessen zu prüfen und abzuwägen, ob diese einer Übermittlung der personenbezogenen Daten und Angaben entgegenstehen. Betroffene haben aber grundsätzlich keinen Einfluss auf die gemäß § 28 Abs. 3 Nr. 1 getroffenen Entscheidungen der Verantwortlichen Stelle. Sie kann auf berechtigte Interessen Dritter selbst dann verweisen, wenn sich die Betroffenen der Übermittlung oder Nutzung widersetzen, also keine Einwilligung vor-

liegt.[1]

Eine datenschutzrechtliche Pflichtverletzung seitens des Energieversorgungsunternehmens konnte nach Prüfung der Aktenlage nicht festgestellt werden.

4.2.4 Vorortkontrolle bei einer Wirtschaftsauskunftei

Im Vorfeld des Gespräches wurde der von der Auskunftei ausgefüllte Fragebogen zu technisch-organisatorischen Maßnahmen erörtert. Einzelne Punkte insbesondere des Komplexes Zugriffs- und Eingabekontrolle wurden vertieft hinterfragt, da diese im schriftlichen Verfahren zum Teil nicht bzw. nur missverständlich beantwortet wurden. Im Ergebnis der abschließenden Auswertung des Fragebogens wurden keine technisch-organisatorischen Mängel festgestellt.
Der Aufsichtsbehörde wurde ein Muster der Verpflichtungserklärung auf das Datengeheimnis überreicht, das jeweils von allen Mitarbeitern der Auskunftei zu unterschreiben ist. Ferner wurde ihr im Vorfeld eine Beschreibung der meldepflichtigen Tätigkeit nach § 4 d BDSG, d.h. eine Beschreibung der Art der gespeicherten personenbezogenen Daten übermittelt.
Die für den Geschäftszweck relevanten personenbezogenen Daten werden aus den folgenden Quellen erhoben:

- öffentliche Register
- Selbstauskünfte
- Schätzdaten
- statistische Daten
- Informationen durch Vertragspartner

Es werden keine Informationen von Banken oder öffentlichen Einrichtungen erhoben und verarbeitet.

Die Auskunftei führt stichprobenartig Kontrollen durch, ob der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft darlegt und ob ggf. das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung überwiegt.
Der Aufsichtsbehörde wurde ein Exemplar des von der Auskunftei verwendeten Formulars überreicht, das ein Dritter, der Auskunft begehrt, vollständig ausfüllen muss. Dieses Formular wird online bereitgestellt und entsprechend an die Auskunftei übermittelt. Nach der Auswertung wird es 5 Jahre lang gespeichert. Das Unternehmen wurde seitens der Aufsichtsbehörde darauf hingewiesen, dass der Auskunftsgrund „sonstiges“ einer präzisierenden Erklärung seitens der Auskunftsbe-

1 Simitis, Kommentar zum BDSG, 5 Auflage, Nomos Verlagsgesellschaft Baden-Baden, § 28 Seite 1100 RdNr. 209

gehrenden erfordert.
Den Vertretern der Aufsichtsbehörde wurde das Prozedere der Verarbeitung eines Auskunftsersuchens nach § 34 BDSG (Selbstauskunft) und einer geschäftsmäßigen Auskunftserteilung am Beispiel erläutert.
Nach § 34 Abs. 1 BDSG kann der Betroffene Auskunft verlangen über
1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

4.2.5 Online-Reiseunternehmen

Ein Online-Reiseunternehmen hatte einer Petentin mitgeteilt, dass sie bei der Frühjahrsverlosung das große Los gezogen habe. Zur Sicherheit und Kontrolle wurde die Teilnahmekarte aus dem Rätselspiel in Kopie beigefügt. Der Hauptpreis, so das Unternehmen, sei ein Urlaub für 2 Personen, 4 - 5 Tage Sonnenurlaub in Südtirol oder eine Erlebnisreise nach Paris stünden zur Auswahl und alles kostenlos. Im „Kleingedruckten“ war jedoch zu lesen, dass pro Reisegast eine einmalige Bearbeitungsgebühr in Höhe von 49 Euro fällig ist, die auch bei Stornierung der Reisebuchung nicht zurückgezahlt wird. Hierauf wurde das Unternehmen durch die Aufsichtsbehörde für den Datenschutz im nicht-öffentlich Bereich um Stellungnahme gebeten und nachgefragt, woher die eingescannte Gewinnspielkarte stamme, welche Art von Daten in der Firma verarbeitet also auch gespeichert werden und auf welche Weise die Einwilligung der Betroffenen eingeholt wird. Gleichzeitig wurde die verantwortliche Stelle aufgefordert, die Daten der Petentin zu löschen und darüber einen Nachweis bzw. eine Bestätigung an die Aufsichtsbehörde zu übersenden. Auch in dieser Angelegenheit wurde seitens des Unternehmens nicht sofort reagiert, es musste mehrmals gemahnt werden. Im Nachhinein wurde mitgeteilt, dass die Daten von der Familie bei einer Verkaufsveranstaltung freiwillig ausgefüllt worden seien. Eine Löschung der vorhandenen Daten habe man veranlasst. Die Bestätigung der gelöschten Daten musste jedoch gesondert abgefordert werden.
In einem Forum der Verbraucherzentrale wurde bereits auf diese Masche des Reiseunternehmens aufmerksam gemacht. So sei die Gewinnmitteilung bei Kreuzworträtselfreunden ein Vorwand die Empfänger auf eine Verkaufsveranstaltung zu locken.
Das Unternehmen wurde darauf hingewiesen, dass eine Teilnahme an einem Gewinnspiel keinesfalls eine Einwilligung zu einer anderweitigen Verwendung der Verarbeitung von personenbezogenen Daten darstellt.

4.2.6 Erhebung von personenbezogenen Daten bei Bezahlung mittels EC-Karte in einer Möbelgesellschaft

Auch in diesem Berichtszeitraum gab es mehrere Datenschutzbeschwerden zu einer Möbelgesellschaft mit Sitz im Land Brandenburg.

Einer Beschwerde lag folgender Sachverhalt zu Grunde:
Beim Einkauf mit EC-Lastschrift muss nach dem Zufallsverfahren der Personalausweis vorgezeigt werden, was dem Beschwerdeführer grundsätzlich nachvollziehbar erschien. Nicht mehr nachvollziehbar erschien ihm jedoch, dass Daten des Personalausweises dann auf dem Kassenbon handschriftlich notiert werden.

Allgemein ist dazu folgendes festzustellen:
Einzelhandelsunternehmen verlangen nicht selten die Vorlage eines Personalausweises, wenn mit EC-Karte gezahlt wird. Nicht selten werden die personenbezogenen Daten der Kunden notiert, eine Kopie des Ausweises angefertigt und dem EC-Zahlungsbeleg für die Bank beigefügt. Damit wollen sich die Unternehmen gegen Betrug schützen und die Durchsetzung ihrer Forderung verbessern. Stichprobenkontrollen der Ausweise sind problemlos möglich. Hierbei wird ausschließlich die Namensgleichheit des Bezahlenden mit dem Kontoinhaber festgestellt. Die Speicherung personenbezogener Daten kommt jedoch nur bei einer EC- Kartenzahlung mit Unterschrift in Betracht. Bei der EC-Kartenzahlung mit Unterschrift kann eine kurzzeitige Speicherung von Name und Anschrift erfolgen, wenn durch gut erkennbare Hinweisschilder an der Kasse auf den Zweck der Erhebung hingewiesen wird. Wegen besonderer Umstände - Zeitdruck an der Kasse - kann auf die schriftliche Einwilligung verzichtet werden. Die Anfertigung einer Ausweiskopie stellt jedoch eine nicht erforderliche Datenerhebung dar.
Wie vom Datenschutzbeauftragten des Unternehmens mitgeteilt, ist eine Mitteilung an alle Filialen ergangen, wo unter anderem auf die Bezahlung mit EC-Karten hingewiesen wurde. Folgende Punkte sollten insbesondere dabei Berücksichtigung finden:

- die Daten (Name, Vorname, Anschrift, Geburtsdatum) werden ausschließlich auf dem Online-Lastschriftverfahren-Beleg (OLV-Beleg) im dafür vorgesehenen Bereich schriftlich notiert;
- auf keinen Fall sind Kopien des Personalausweises zu erstellen;
- die Belege werden in der Finanzbuchhaltung aufbewahrt, aber nicht automatisiert gespeichert oder verarbeitet; nach spätestens 3 Monaten (Frist für EC-Rücklastschriften) werden diese Belege vernichtet.

Gleichzeitig sei nochmals auf den notwendigen dauerhaften Aushang im Kassenbereich hingewiesen worden, auf dem die Kunden deutlich darauf hingewiesen werden, dass bei einer EC-Kartenzahlung mit Unterschrift stichprobenartig die Daten Name, Vorname, Anschrift, Geburtsdatum notiert werden. Dadurch können sich die Kunden in angemessener Zeit vor dem Bezahlen hinsichtlich der Zahlungsart entscheiden. Dem Beschwerdeführer konnte unter Hinweis auf die Veröffentlichung des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) - Erhebung von Ausweisdaten bei der EC-Kartenzahlung - mitgeteilt werden, dass beispielsweise bei der EC-Kartenzahlung mit Unterschrift eine kurzzeitige Speicherung von Name und Anschrift wegen eventueller Forderungsdurchsetzungen im berechtigten Interesse des Unternehmens liegt.
Gegenüber der Aufsichtsbehörde wurde seitens des Unternehmens versichert, dass Belege nicht generell 3 Monate aufbewahrt werden vielmehr werden diese bei endgültiger Zahlung sofort vernichtet. Ferner werden die Belege in abgeschlossenen Behältnissen aufbewahrt. Diese sind mit dem jeweiligen Datum versehen und werden nach endgültiger Einlösung der Vernichtung zugeführt. Etwaige problematische Zahlungsvorgänge werden vorher von der Buchhaltung aussortiert. Diese werden in einer separaten Box in der Rechtsabteilung verwahrt. Angaben von Kontonummern und Bankleitzahlen sind bei EC-Karten-Zahlung allgemein üblich.
Hinsichtlich der Speicherung des Geburtsdatums herrscht unter den Datenschutzaufsichtsbehörden der Länder jedoch kein Konsens. Nach Aussage des Unternehmens wird dieses Datum vor dem Hintergrund der Möglichkeit von Namensgleichheiten innerhalb derselben Wohnanschrift erhoben. Nach Ansicht der Aufsichtsbehörde des Landes Brandenburg konnte eine Erhebung des Geburtsdatums in diesem Fall ebenfalls unter das berechtigte Interesse des Unternehmens subsumiert werden.

Die Speicherung des Namens, Vornamens, Anschrift und *Geburtsdatum* auf dem OLV-Beleg ist mit mehreren Datenschutzbehörden abgestimmt. Das ULD teilt diese Auffassung nicht.

Zur Sicherstellung der datenschutzrechtlichen Konformität einer Erhebung von personenbezogenen Daten bei Bezahlung mittels EC-Karte empfiehlt das ULD den Unternehmen die folgende Vorgehensweise:

- Bei der EC-Kartenzahlung im PIN-Verfahren wird die Freigabe des konkreten Zahlungsbetrages online bei dem kartenausgebenden Kreditinstitut eingeholt. Die Deckung des Betrages wird in Echtzeit bestätigt. Eine Identifizierung zur Forderungsrealisierung oder Betrugsbekämpfung ist in diesen Fällen nicht erforderlich. Bei der EC-Kartenzahlung im PIN-Verfahren darf ein Ausweis daher nicht verlangt werden.
- Bei der EC-Kartenzahlung mit Unterschrift des Karteninhabers kann die stichprobenartige *Kontrolle* eines Ausweises zur Betrugsbekämpfung erfolgen. Bei der Kontrolle ist ausschließlich die Namensgleichheit des Bezahlenden mit dem Karteninhaber sicherzustel-

len. Bei Karten mit dem Foto des Inhabers ist eine Ausweiskontrolle daher nicht erforderlich. Generell sollten Ausweiskontrollen nur oberhalb einer festzulegenden Bagatellgrenze durchgeführt werden.

- Bei der EC-Kartenzahlung mit Unterschrift kann eine kurzzeitige *Speicherung* von Name und Anschrift im berechtigten Interesse des Unternehmens liegen (Forderungsdurchsetzung).
- In diesem Fall ist durch gut erkennbare Hinweisschilder an der Kasse auf den Zweck der Erhebung (Abrechnung mit der Bank / Betrugsbekämpfung) von Name und Anschrift hinzuweisen. Die Nutzung der EC-Karte mit Unterschrift kann in diesem Fall eine Einwilligung unter besonderen Umständen (Zeitdruck an der Kasse) gem. § 4a Abs. 1 S. 3 BDSG darstellen. Aufgenommen werden dürfen ausschließlich der Name und die Anschrift des Kunden.

  Das Anfertigen einer Kopie des Ausweisdokuments stellt eine Erhebung von nicht erforderlichen personenbezogenen Daten dar. Sie ist daher in der Regel unzulässig.

  Um die Freiwilligkeit der Einwilligung zu gewährleisten, ist an der jeweiligen Kasse zusätzlich eine andere angemessene Zahlungsmöglichkeit einzuräumen. Unternehmen, die vorwiegend hoch-preisige Waren verkaufen, sollten außer der Barzahlung noch eine weitere Zahlungsmöglichkeit (PIN-Zahlung, Kreditkarte) vorsehen. Kunden ist es heute kaum zumutbar, große Barbeträge mitzuführen, um die eigenen personenbezogenen Daten nicht preisgeben zu müssen.
- Die Speicherung des Namens und der Anschrift auf der Rückseite des EC-Beleges für das Unternehmen darf nur bis zum Zeitpunkt der Zahlung durch das Kreditinstitut erfolgen. Danach müssen diese Belege vernichtet werden. Aufbewahrungsfristen für Belege, die über den Zahlungszeitpunkt hinausgehen (z.B. handels- und steuerrechtliche Aufbewahrungsfristen von 6 oder sogar 10 Jahren) gelten nicht für Name und die Anschrift. Diese Angaben müssen nach Zahlung geschwärzt werden. Daher wird eine Speicherung in einer Form empfohlen, bei der eine Löschung sofort nach Zahlung durch das Kreditinstitut unproblematisch erfolgen kann. Die Einhaltung der Löschfrist ist organisatorisch sicherzustellen und vom betrieblichen Datenschutzbeauftragten zu überprüfen.
- Kassenbons bzw. -belege von Kunden, die am EC-Lastschriftverfahren teilnehmen, sollten wegen des Erforderlichkeitsgrundsatzes als auch wegen des Grundsatzes der Datensparsamkeit keine Ausdrucke bzw. Andrucke von Kontonummern und Bankleitzahlen enthalten.
- Eine andere Verwendung der Adressdaten als zur Durchsetzung der jeweiligen Zahlungsansprüche im Falle der Nichtzahlung durch das Kreditinstitut ist unzulässig und organisatorisch zu unterbinden. Insbesondere eine (auch pseudonyme) Zusammenführung und Auswertung zu anderen Zwecken (z.B. zu Marktforschungs- oder Werbezwecken) darf nicht erfolgen.

4.2.7 Videoüberwachung in einer Therme

Bei dieser Datenschutzbeschwerde wurde darauf hingewiesen, dass in einer Therme Besucher videoüberwacht werden und dies ohne jegliches Hinweisschild. Ob es sich hierbei um Bildaufzeichnungen handelte und wer auf die Daten Zugriff hatte, war nicht klar.
Das Unternehmen wurde durch die Aufsichtsbehörde um Stellungnahme und gleichzeitig um Ausfüllung des beigelegten Fragenkatalogs zur Videoüberwachung durch nicht-öffentliche Stellen gebeten.
Gleichzeitig wurde darauf aufmerksam gemacht, dass die Videoüberwachung und die verantwortliche Stelle problemlos erkennbar sein müssen, damit der Kunde frei entscheiden kann, ob er den Bereich auch betreten will. Empfehlenswert ist ein Hinweisschild mit einem kurzen prägnanten Text, dem Namen und in der Regel der Anschrift der verantwortlichen Stelle, damit Betroffene sich an diese im Zweifelsfalle wenden können. Statt eines Textes kann auch ein Piktogramm angebracht werden, das den Umstand der Videoüberwachung darstellt.
In der Stellungnahme kam zum Ausdruck, dass die Videoüberwachung alleinig dem Sicherheitsinteresse der Besucher und Mitarbeiter diene. Wertfächer, Umkleideschränke, Kassenbereiche, Eingangsbereich, Kinderbecken und Außenbecken und die Attraktionsbereiche wie der Strömungskanal würden videoüberwacht. Ziel sei es, Einbruchdiebstähle und Überfälle zu vermelden sowie gesundheitsgefährdende Situationen im Strömungskanal frühzeitig zu erkennen. Alle Aufnahmen würden automatisch nach 7 Tagen überschrieben. Zugriff auf die Daten habe alleinig die Geschäftsleitung. Die Kameras verfügen nicht über Zoomobjektive und sind nicht schwenkbar.
Der Hinweis der Aufsichtsbehörde auf das Piktogramm wurde seitens des Betriebsleiters sofort aufgenommen und umgesetzt. Die entsprechenden Bereiche wurden mit den Piktogrammen versehen. Gegen einen Einsatz von Kameras in den genannten Bereichen bestanden aus Sicht der Aufsichtsbehörde keine Bedenken. Aus datenschutzrechtlicher Sicht bestand somit kein Handlungsbedarf.
Da im Nachhinein durch den Beschwerdeführer auch noch darauf hingewiesen wurde, dass im Internetauftritt nicht auf die Videoüberwachung hingewiesen wird, wurde diesem Hinweis genüge getan und die Geschäftsleitung des Unternehmens gebeten, diesen Hinweis in die Hausordnung einzuarbeiten.
Dies wurde durch die Geschäftsleitung umgehend mit der Werbefirma, die den Internetauftritt gestaltet hat, abgesprochen und auch umgesetzt.
Auch im Internetauftritt wird nun unter der Rubrik Sicherheit der Hinweis gegeben, dass eine Videoüberwachung erfolgt.

Das Deutsche Institut für Normung (DIN) hat im Übrigen ein einheitliches Piktogramm zur Kennzeichnung einer Videoüberwachung u.a. in Zusammenarbeit mit den Datenschutzaufsichtsbehörden Berlin und Brandenburg erarbeitet:

4.2.8 Videoüberwachung an bzw. über eine Brücke mit integriertem Wasserkraftwerk

In diesem Fall wurde der Aufsichtsbehörde durch eine Stadtverwaltung mitgeteilt, dass an bzw. über eine Brücke hinweg eine Videoüberwachung durch den Betreiber eines Wasserkraftwerkes erfolgt und Passanten eventuell in den Sichtwinkel der Kameras geraten könnten. Seitens der Stadtverwaltung seien die Gespräche mit dem verantwortlichen Unternehmen fehlgeschlagen, da dies der Meinung sei, in diesem vorliegenden Fall aus Gründen der Verkehrssicherung rechtens zu handeln.

Die Aufsichtsbehörde hat sich daraufhin schriftlich an das Unternehmen gewandt und um Stellungnahme zu dem Vorwurf gebeten. Das Unternehmen hat im vorliegenden Fall einen Anwalt mit der Angelegenheit betraut. Der Schriftverkehr zog sich in die Länge und verlief seitens des Anwaltes stellenweise unkooperativ.

Bei einem Ortstermin war die Stadtverwaltung und die Aufsichtsbehörde anwesend, das Unternehmen bzw. die anwaltliche Vertretung entschuldigte sich kurzfristig.

Am Tag der Vor-Ort-Kontrolle konnte lediglich die Videokamera selbst sowie der eventuelle Blickwinkel der Kameras festgestellt werden. Eine Beschilderung des Objektes war nicht erkennbar. Die Auswertung der Aufzeichnungskameras erfolgt in einem anderen Bundesland. Eine Kontrolle der Aufzeichnungen war nicht ohne weiteres möglich. Im Nachhinein wurden Bilder der Überwachungskamera durch den Anwalt übersandt, die seitens der Aufsichtsbehörde eindeutig eine Identifikation der Passanten zuließen, aber seitens des Anwaltes dies nicht der Fall zu sein schien.

Zwischenzeitlich konnte mit dem Anwalt des Unternehmens eine Lösung des anstehenden Problems erörtert und gefunden werden. Es wurde die Verblendung der Kamera sowie die Kenntlichmachung der Videoüberwachung des Objektes nach DIN-Norm vereinbart. Die Verblendung der Kamera wurde kurzfristig realisiert. Dadurch sind Fußgänger, die die Brücke überqueren, nicht mehr zu erkennen. Die Beschilderung nach DIN-Norm ist ebenfalls erfolgt.

4.2.9 Videoüberwachung einer Bankfiliale

Die Aufsichtsbehörde wurde in diesem Fall über eine Videoüberwachung innerhalb und außerhalb einer Bankfiliale aufmerksam gemacht.

Auch hier fand letztendlich eine Vor-Ort-Besichtigung statt. Der Filialleiter sowie der externe Datenschutzbeauftragte dokumentierten die Videoüberwachung an den Monitoren, die keine Passanten auf dem Gehweg erkennen ließen.
In diesem Fall erfolgte die Videoüberwachung des Objektes zum Schutz des Eigentums. So habe es in der Vergangenheit immer wieder Graffitischmierereien am unter Denkmalschutz stehenden Gebäude der Filiale gegeben. Eine Videoüberwachung durch private Stellen ist u.a. zulässig, wenn dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen (§ 6b Abs. 1 Nr.3 BDSG). Im Eingangsbereich war eine Kenntlichmachung der Videoüberwachung nach DIN-Norm nicht erkennbar. Dies wurde vor Ort bemängelt und gleichzeitig darauf hingewiesen, dies umgehend nachzuholen. Dieser Hinweis wurde seitens der Filialleitung unkompliziert und sofort erledigt. Als Beleg hierfür sind Bilder der Aufsichtsbehörde übersandt worden. Die Kameras, die angeblich den Gehweg in Augenschein genommen haben sollen, wurden technisch so umgerüstet, dass eine Aufnahme des Gehweges ausgeschlossen wird. Dazu wurde der Schwenkbereich der Kamera verblendet.
Die Aufsichtsbehörde stellte fest, dass die Videoüberwachung gemäß § 6b BDSG im diesem Fall zulässig ist.

4.2.10 Datenschutzbeschwerde über ein Versicherungsunternehmen

Eine Beschwerdeführerin hatte ein Angebot der Versicherung für ihren PKW erhalten, obwohl sie lt. ihren Angaben noch nie mit dieser Versicherung Kontakt gehabt habe. Daraufhin wandte sie sich an das Unternehmen und bat gleichzeitig um die Löschung der Daten. Dieses Schreiben sei seitens der Versicherung unbeantwortet geblieben. Bei einer Überprüfung der Angelegenheit wurde jedoch deutlich, dass die Petentin über die bei ihrer Bank ausliegenden Flyer der Versicherung ein Angebot erbeten hatte. Somit wurde ihr dann ein Angebot für eine Kraftfahrtversicherung erstellt und auch versandt.
Was von der Beschwerdeführerin wohl nicht erwähnt wurde, war eine vorherige Kontaktaufnahme ihrerseits gegenüber dem Unternehmen. Ohne diese Kontaktierung wäre kein Angebot seitens der Versicherung erstellt worden.
Vermutlich ist eine geraume Zeit zwischen der Kontaktaufnahme der Petentin zur Versicherung und der Versendung des Mailings verstrichen. Da zwischenzeitlich, wie gewünscht, die Daten komplett gelöscht wurden, ließ sich der Gesamtvorgang nicht mehr konkret nachvollziehen. Ein Daten-

schutzverstoß konnte dem Unternehmen nicht nachgewiesen werden.

An diesem exemplarischen Fall wird deutlich, dass sowohl im öffentlichen als auch im privaten Geschäftsverkehr der Grundsatz der Datenvermeidung und- sprarsamkeit beachtet werden sollte. Ein (zu) schnelles Ausfüllen einer Werbeschrift, ohne den genauen Verwendungszweck der Daten zu hinterfragen, kann eine zulässige Datenverarbeitung zur Folge haben, die vom Betroffenen so nicht gewollt ist.

4.3 Einleitung von Ordnungswidrigkeitenverfahren

Im Berichtszeitraum wurden gegen drei Personen Ordnungswidrigkeitenverfahren wegen des Verstoßes gegen datenschutzrechtliche Vorschriften eingeleitet, die erst im Jahr 2008 mit der gerichtlichen Einstellung der Verfahren ihren Abschluss fanden. Es wurde den Betreffenden vorgeworfen, gegen Vorschriften des Mediendienstestaatsvertrages verstoßen zu haben. Im Rahmen der umfangreichen Sachverhaltsaufklärung und intensiven Befassung waren zahlreiche neue Rechtsfragen zu klären. Strafrechtliche Ermittlungen wurden im Vorfeld der Ordnungswidrigkeitenverfahren durch die Staatsanwaltschaft geführt und letztendlich eingestellt.

5 Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden der Länder und dem BfDI

5.1 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.

5.1.1 Gesetzlicher Regelungsbedarf im Auskunfteibereich

Ein besonderer Schwerpunkt in der Arbeit dieser Arbeitsgruppe war die Erörterung eines zusätzlichen Regelungsbedarfs innerhalb des BDSG speziell im Bereich der geschäftsmäßigen Datenerhebung und Datenspeicherung zum Zwecke der Übermittlung (Auskunfteien). Ausgangspunkt der Diskussion war die Feststellung des Deutschen Bundestages, dass die fortschreitende Digitalisierung und die starke Zunahme von Datenströmen auch im nicht-öffentlichen Bereich zu einer immer stärkeren Verknüpfung von Daten führen können, die für unterschiedliche Zwecke erhoben wurden. Verbunden mit einem wachsenden Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien erscheint es technisch möglich, durch Profilbildung das Verhalten eines bestimmten Menschen ohne dessen Wissen und Wollen abzubilden und ihn so für Dritte berechenbar zu machen.

Nach dem Beschluss des Düsseldorfer Kreises von November 2005 sind branchenspezifische Auskunftssysteme gegenüber umfassenden Zentraldateien vorzuziehen. Ferner sollen die gesetzlichen Regelungen für eine Datenverarbeitung bei Auskunfteien präzisiert werden.
Die Teilnehmerinnen und Teilnehmer der AG Auskunfteien erörterten auch auf der Grundlage einschlägiger Erfahrungen aus ihrer Aufsichtstätigkeit mit einem Vertreter des Bundesministeriums des Innern zahlreiche Bewertungen und Vorschläge für einen Änderungsbedarf insbesondere der §§ 28 und 29 BDSG.

Ausblick:
Im aktuellen im Entwurf eines Gesetzes zur Änderung des BDSG sind u.a. Regelungen enthalten für:

- Scoring,
- Übermittlung von Angaben über untitulierte, vom Betroffenen weder bestrittene noch anerkannte Forderungen an Auskunfteien und
- Übermittlung sog. Positivdaten eines Kredit-, Garantie- oder Girovertrags durch bestimmte Unternehmen an Auskunfteien.

5.1.2 Nutzung von Daten aus dem Inkasso-Bereich für die Auskunftserteilung

Ein weiteres Beratungsthema war die Problematik der Nutzung von Daten aus dem Inkassobereich für die Auskunftserteilung. Eine generelle Übermittlung von weichen Negativdaten aus dem Inkassobereich für die Auskunftserteilung auf Grund entgegenstehender überwiegender schutzwürdiger Interessen des Betroffenen ist nicht zulässig. Kann jedoch nach sorgfältiger Einzelfallabwägung die Zahlungsunfähigkeit oder Zahlungsunwilligkeit zweifelsfrei festgestellt werden, d.h. besteht kein Grund zur Annahme, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, wird eine Übermittlung unter den folgenden Voraussetzungen als zulässig angesehen:

- Es muss sich um eine unbestrittene Forderung handeln.
- Sowohl Gläubiger als auch Inkassounternehmen haben die der Einmeldung zugrunde liegende Forderung gegenüber dem Schuldner nachweisbar jeweils mindestens zweimal vergeblich schriftlich gemahnt.
- Der Schuldner wird (z.B. in den Mahnschreiben) darüber informiert, dass eine Einmeldung bei einer Auskunftei erfolgt, soweit die Forderung unbestritten ist und keine Zahlung innerhalb der gesetzten Frist erfolgt.
- Die Einmeldung erfolgt frühestens dann, wenn vier Arbeitstage seit Ablauf der im letzten Mahnschreiben des Inkassounternehmens genannten Zahlungs- bzw. Rückantwortfrist von zehn Tagen verstrichen sind.

5.1.3 Versandhandelsspezifische Themen – Nachmeldeverfahren

Einzelne Mitglieder der AG Auskunfteien erörterten auf einer Sondersitzung mit Vertretern des Bundesverband des Deutschen Versandhandels e.V., des Verbandes der Handelsauskunfteien e.V., der SCHUFA Holding AG sowie der infoscore Consumer Data GmbH das so genannte Nachmeldeverfahren.
Konkret wurde die Praxis von weiteren Meldungen zu den Betroffenen, d.h. Versandhandelskunden nach der ersten Anfrage im Rahmen des Vertragsabschlusses, oder mit anderen Worten, die Praxis der Informationen (Beauskunftung) an den Versandhandel außerhalb der Antragssituation mit dem Ziel einer datenschutzgerechten Ausgestaltung erörtert. Unabhängig von den in den einzelnen Auskunfteiunternehmen unterschiedlich bezeichneten Verfahren muss im Zeitpunkt einer Datenübermittlung ein berechtigtes Interesse des Versandhandelsunternehmens vorliegen, etwa wie bei einem Dauerschuldverhältnis. Ein solches wird jedoch nicht dadurch begründet, dass Versandhändler intern zur Erleichterung der Geschäftsabläufe ein „Versandhauskonto“ für die Kunden einrichten.

Im Ergebnis konnten sich die Teilnehmer der Sitzung darauf einigen, dass ein berechtigtes Interesse seitens des Versandhandels gem. § 29 BDSG nur gegeben ist, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko gegeben ist.
Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) haben auf Ihrer Sitzung am 17./18. April 2008 u.a. den Beschluss „Keine fortlaufenden Bonitätsauskünfte an den Versandhandel“ zu diesem Thema gefasst. Der Beschluss wurde vom Bundesbeauftragten für Datenschutz und die Informationsfreiheit auf seiner Website unter der Rubrik „Entschließungen des Düsseldorfer Kreises“ veröffentlicht.

5.2 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 Teledienstegesetzes (TDG) und Teledienstedatenschutzgesetzes (TDDSG) sowie des Mediendienste-Staatsvertrages (MDStV) bzw. des Telemediengesetztes (TMG).
Innerhalb des Berichtszeitraums wurde das TMG mit Artikel 1 des Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetzes verkündet. Es löste das TDG, das TDDSG sowie weitestgehend auch den MdStV ab, die alle zeitgleich mit dem Inkrafttreten des TMG außer Kraft traten.

5.3 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.

6 Anlage: Muster eines Verfahrensverzeichnisses nach § 4g i.V.m. § 4e BDSG

§ 4e BDSG – Verfahren automatisierter Verarbeitungen

Nach § 2 Abs. 2 BDSG sind automatisierte Verarbeitungen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Als „Verfahren automatisierter Verarbeitungen" versteht man alle Aktivitäten, die ein Verantwortlicher der Verarbeitung für einen bestimmten Zweck mit den diesen zugeordneten personenbezogenen Daten unternimmt. Dies bedeutet aber nicht für jede einzelne Verarbeitungsphase eine gesonderte Meldung. Aber jedes Verfahren automatisierter Datenverarbeitung, die unterschiedlichen Zwecken dient – wie etwa Vertragsverarbeitungen, Werbedateien, Personaldatenverarbeitung, Finanzbuchhaltung etc. – sind in das Verfahrenverzeichnis aufzunehmen. Mehrere gleichartige Verfahren können jedoch zusammengefasst werden.

Die verantwortliche Stelle hat die Angaben dem betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen. Dies gilt auch für Verfahren, die von anderen Stellen im Wege der Auftragsdatenverarbeitung durchgeführt werden.

1. Verantwortliche Stelle

Name oder Firma

2. Vertretung

2.1 Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter:

Name(n)

2.2 mit der Leitung der Datenverarbeitung beauftragte Personen:

Name(n)

3. Anschrift der verantwortlichen Stelle

Straße

Postleitzahl

Ort

Telefon

Telefax

E-Mail

4. Welche Zweckbestimmung(en) liegen der Datenerhebung, -verarbeitung oder -nutzung zugrunde?

Zu benennen sind hier die konkreten Zwecke der verschiedenen Datenverarbeitungsprozesse, nicht der allgemeine Geschäftszweck. Beispiele: Personalverwaltung incl. Lohn- und Gehaltsabrechnung - Erfüllung sozialversicherungsrechtlicher, gesetzlicher Verpflichtungen -, Bewerberauswahlverfahren, Zeiterfassung, Zugangskontrollsystem, Telefonverzeichnis zwecks Kommunikation intern und extern; Kontoführung, Kreditverwaltung, Wertpapierverwaltung; Kundenverwaltung incl. Rechnungswesen; Interessentenverwaltung z.B. für Werbezwecke; Abwicklung und Durchführung von Mietverträgen; Durchführung von Videoüberwachung als Sicherheitsmaßnahme (Vandalismus, Einbruch oder sonstige Straftaten).

4.1 ...

4.2 ...

... (ggf. weitere Zweckbestimmungen)

5. Betroffene Personengruppen und Daten oder Datenkategorien

Bitte nehmen Sie auf die Angaben zu Ziffer 4 Bezug und führen die personenbezogenen Daten bzw. Datenkategorien getrennt nach den einzelnen Zweckbestimmungen unter Nennung der Bezugsziffer stichwortartig auf und differenzieren Sie dabei nach den betroffenen Personengruppen (z.B. Kunden, Interessenten, Patienten, Schuldner, Versicherungsnehmer, Lieferanten, Dienstleister, Mitarbeiter-/Bewerberdaten). Mit „Daten" sind „personenbezogene Daten" i.S.d. § 3 Abs. 1 BDSG gemeint, d.h. Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. z.B. Name, Geburtsdatum, Anschrift, Einkommen, Kfz-Kennzeichen, Konto-Nr., Versicherungs- oder Personal-Nr., Beruf, Hausbesitzer, etc.
Weitere Beispiele für Kunden-/ Interessentendaten: Adressdaten, Telefon, Fax, Email, Bankverbindung, Interessengebiete / Angebotsdaten, bestellte Waren etc.
Bsp. für Mitarbeiterdaten: Privatadressen, Geburtsdatum, Familienstand, Vertrags-, Abrechnungsdaten, Angehörige, Sozialdaten, Steuerdaten, etc..
So genannte „besondere Arten personenbezogener Daten" sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (§ 3 Abs. 9 BDSG). Diese sind entsprechend anzugeben. Zur besseren Übersichtlichkeit ist es vorteilhaft, die verschiedenen Datenkategorien mit einer laufenden Nummerierung zu versehen.

5.1 Zweckbestimmung Ziffer 4.1

Beschreibung der betroffenen Personengruppen	Beschreibung der diesbezüglichen Daten oder Datenkategorien
...	...

5.2 Zweckbestimmung Ziffer 4.2

Beschreibung der betroffenen Personengruppen	Beschreibung der diesbezüglichen Daten oder Datenkategorien
...	...

...

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können; bei Datentransfers in Drittstaaten siehe Nr. 8

Bitte nehmen Sie bei der Darstellung auf die Antworten zu den Fragen 4 Bezug.
Bsp.: öffentliche Stellen (Sozialversicherungsträger, Finanzämter/-behörden, Aufsichtsbehörden, etc.), interne Stellen die an der Ausführung der jew. Geschäftsprozesse beteiligt sind (Personalverwaltung, Buchhaltung, Rechnungswesen, Einkauf, Marketing, Vertrieb, IT / EDV, etc.), externe Auftragnehmer (Dienstleistungsunternehmen) nach § 11 BDSG, Tochtergesellschaften in Konzernstrukturen, weitere externe Stellen wie z.B. Kreditinstitute, etc.

6.1 Zweckbestimmung Ziffer 4.1

...

6.2 Zweckbestimmung Ziffer 4.2

...

...

7. Wann werden die Daten gelöscht?

Hier ist der Zeitraum anzugeben, nach dessen Ablauf die Daten gelöscht werden. Es wird darauf hingewiesen, dass die Daten z.B. gemäß § 35 Abs. 2 Nr. 3 BDSG zu löschen sind, wenn sie für eigene Zwecke verarbeitet werden und ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Sofern einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, sind die Daten nach § 35 Abs. 3 Nr. 1 BDSG zu sperren.

7.1 Zweckbestimmung Ziffer 4.1

...

7.2 Zweckbestimmung Ziffer 4.2

...

...

8. Geplante Datenübermittlung in Drittstaaten

8.1 Zweckbestimmung Ziffer 4.1

☐ Eine Datenübermittlung in Drittstaaten ist geplant.

☐ Eine Datenübermittlung in Drittstaaten findet nicht statt ...

☐ und ist auch nicht geplant.

8.2 Zweckbestimmung Ziffer 4.2

☐ **Eine Datenübermittlung in Drittstaaten ist geplant.**

☐ **Eine Datenübermittlung in Drittstaaten findet nicht statt ...**

☐ **und ist auch nicht geplant.**

(Hier endet der Teil, der nach § 4g Abs. 2 Satz 2 BDSG jedermann auf Antrag in geeigneter Weise verfügbar zu machen ist.)

(Ab hier ist die Übersicht nur für den internen Gebrauch gedacht, § 4e Nr. 9, § 4g Abs. 1 Nr. 1, Abs. 2 Satz 1 BDSG.)

zu 8.1	**Name des Drittstaates**	**Empfänger oder Kategorien von Empfängern**	**Art der Daten oder Datenkategorien**
	...		
zu 8.2	**Name des Drittstaates**	**Empfänger oder Kategorien von Empfängern**	**Art der Daten oder Datenkategorien**
	...		
...			

9 Eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Eine stichwortartige Zusammenfassung für alle automatisierten Verfahren ist ausreichend, es sei denn, es sind für einzelne Verfahren besondere Vorkehrungen getroffen worden.

9.1 Art der eingesetzten DV-Anlagen und Software

HARDWARE = Anzahl der PC (vernetzt / Stand Alone / Betriebssystem), Anzahl der Server (Betriebssystem / Art der Vernetzung), Anzahl mobiler Geräte (Notebooks / PDA / etc. / netzwerkfähig / Stand Alone), Anzahl Abteilungsrechner / Großrechner (Betriebssysteme), eingesetzte Netzwerktechnik (Client-/Server-Struktur, Ethernet/Fast-Ethernet, Hubs, Router, Switches, etc.), Anbindung an die „Außenwelt" – ohne Internet (WAN, Standleitung zu anderen internen und externen Stellen - z.B. Fernwartung - / Filialbetrieben etc.,
SOFTWARE = Betriebs- und Anwendungsprogramme, Datenbankanwendungen, etc. mit denen die genannten personenbezogenen Daten verarbeitet werden (auch webbasierte Lösungen). Ferner Sicherheitssoftware, Datensicherungs- und Fernwartungstools.

9.2 Maßnahmen nach § 9 BDSG i.V.m. der Anlage dazu

	Beispiele für Stichworte
☐ Zutrittskontrolle	▪ Sicherheitsschlösser mit Schlüsselregelung ▪ verschlossene Türen bei Abwesenheit ▪ Fenstersicherung (Erdgeschoss) ▪ Festlegung von Sicherheitsbereichen ▪ Zutrittsberechtigungsregelung ▪ Ausweisleser ▪ Codeschloss ▪ Protokollierung der Zu- und Abgänge ▪ Zutrittsregelungen für betriebsfremde Personen ▪ Empfang
☐ Zugangskontrolle	▪ Tastatursicherung durch Schloss ▪ Identifizierung und Authentifizierung ▪ Begrenzung der Fehlversuche ▪ Protokollierung ▪ Systemverwalterbefugnisse / -protokollierung ▪ Dunkelschaltung des Bildschirms mit Passwortschutz ▪ Firewall

☐ Zugriffskontrolle	• Berechtigungskonzept • Identifizierung und Authentifizierung • Verschlüsselung • Aufbewahrung von Datenträgern in verschließbaren Schränken - Data Safes
☐ Weitergabekontrolle	• Kennzeichnung der Datenträger • Verschlüsselung von Daten auf Datenträgern • Bestandsverzeichnis und Bestandskontrolle der Datenträger • Festlegung der zur Abgabe von Datenträgern berechtigten Personen • Festlegung des Empfängerkreises • Regelungen für den Transport von Datenträgern • Kryptographische Verschlüsselung der übertragenen Daten • Fernwartungskonzept
☐ Eingabekontrolle	• Protokollierung der Eingaben
☐ Auftragskontrolle	• Schriftliche Festlegung der Weisungen • Kontrolle der Einhaltung beim Auftragnehmer
☐ Verfügbarkeitskontrolle	• Betriebsbereitschaft • Notfallkonzept • USV • Brandmelder • Datensicherung • Zusätzliche Sicherungskopien mit Lagerung an besonders geschützten Orten
☐ Trennungsgebot	• Physikalische oder logische Trennung

(Sind zu einem der vorstehenden Punkte keine Maßnahmen zu treffen, brauchen keine Angaben gemacht zu werden.)

10. Zugriffsberechtigte Personen (§ 4g Abs. 2 Satz 1 BDSG)
Die Nennung von Namen ist nicht erforderlich, ausreichend ist die Zugehörigkeit zu einer Funktionsgruppe oder einem Tätigkeitsbereich.

10.1 Zweckbestimmung 4.1:

...

10.2 Zweckbestimmung 4.2:

...

...

.....

(Unterschrift, Datum)

Ergebnis der Vorabkontrolle (§ 4d Abs. 5 BDSG)

Der betriebliche Datenschutzbeauftragte sollte das Ergebnis seiner Prüfung dokumentieren, auch wenn keine Vorabkontrolle wegen eines Ausnahmetatbestandes durchgeführt werden muss.
Das Prüfergebnis muss sich auf jedes einzelne Verfahren automatisierter Verarbeitungen beziehen.

Vorabkontrolle entfällt

Zweckbestimmung Ziffer .....

☐ gesetzliche Verpflichtung

.....

Zweckbestimmung Ziffer .....

☐ Einwilligung des Betroffenen
(z.B. Einwilligungserklärung geprüft)

Zweckbestimmung Ziffer .....

☐ Zweckbestimmung Vertragsverhältnis oder vertragsähnliches Vertrauensverhältnis

Risikoanalyse

Zweckbestimmung Ziffer .....

.....

(Unterschrift des bDSB, Datum)