

**Neudruck**

**Bericht**

der Landesregierung

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

## **0. Einleitung**

### **1. Übersicht über Kontrolltätigkeit**

- 1.1 Meldungen zum Register vor der Gesetzesänderung
- 1.1.1 Änderung des Registers durch das neue BDSG
- 1.2 Beschwerden

### **2. Novellierung des BDSG**

### **3. Kontrolltätigkeit der Aufsichtsbehörde**

- 3.1 Überprüfungen von Unternehmen
- 3.1.1 Geänderte Regelung zur Bestellung eines betriebliche Datenschutzbeauftragten
- 3.2 Schwerpunkte aus Beschwerden und Anfragen

### **4. Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden der Länder**

- 4.1 Besondere Beratungsthemen des Düsseldorfer Kreises
- 4.2 Schwerpunkte aus der Sitzung der Arbeitsgruppe "Auskunfteien"
- 4.3 Teilnahme an den Sitzungen der Arbeitsgruppe "Internationaler Datenverkehr"
- 4.4 Teilnahme an den Sitzungen der Arbeitsgruppe "Telekommunikation, Tele- und Mediendienste"

## **0. Einleitung**

Am 23.05.2001 trat das novellierte Bundesdatenschutzgesetz (BDSG) in Kraft. Zweck dieser Novellierung war überwiegend die (mit fast zwei einhalbjähriger Verspätung erfolgte) Umsetzung der EU-Datenschutzrichtlinie 95/46/EG durch den Bundesgesetzgeber.

Daneben enthält das neue BDSG jedoch auch bereits Elemente einer grundlegenden Erneuerung des Systems des geltenden Datenschutzrechtes. Dazu gehören z.B. die Regelungen über Datenvermeidung und Datensparsamkeit (§ 3a), Datenschutz durch Technik (§§ 9, 9a), die Selbstregulierung des Datenschutzes durch die Anwender, d.h. die datenverarbeitenden Stellen (§§ 4c, 38a). Darüber hinaus wurden u.a. Regelungen zur Videobeobachtung (§ 6b) und zum Einsatz von mobilen personenbezogenen Speicher- und Verarbeitungsmedien z.B. Chipkarten (§ 6c) aufgenommen.

Im Großen und Ganzen wurde die Grundkonzeption des BDSG mit einem erweiterten und für den öffentlichen und nicht-öffentlichen Bereich geltenden Allgemeinen Teil (Erweiterung z.B. durch Regelungen zur Übermittlung personenbezogener Daten ins Ausland §§ 4b und 4c; Vorschriften zur Meldepflicht und Vorabkontrolle §§ 4d und 4e; gesetzliche Neueinführung des behördlichen Datenschutzbeauftragten §§ 4f und 4g; Regelung zur automatisierten Einzelentscheidung § 6a) und nachfolgend für öffentliche und nicht-öffentliche Stellen getrennten ergänzenden Regelungen beibehalten.

Insgesamt kann festgestellt werden, dass das Gesetz für den Anwender noch schwerer lesbar und noch weniger überschaubar geworden ist.

Es ist denn auch von der Bundesregierung erklärt worden, dass dieser ersten Stufe der Novellierung des BDSG eine zweite folgen soll, die eine umfassende Neu- und Umgestaltung des geltenden allgemeinen und besonderen Datenschutzrechtes in Deutschland zum Ziel hat. Die ursprüngliche Zeitvorstellung, die zweite Stufe noch in dieser Legislaturperiode des Deutschen Bundestages abzuschließen, ist zwischenzeitlich aufgegeben worden.

Die Aufsichtsbehörde hat sich im Berichtszeitraum mit den für ihre Tätigkeit relevanten Gesetzesvorschriften vertraut gemacht, mit ihrer Umsetzung begonnen und die Fragen vieler datenverarbeitender Stellen dazu beantwortet.

Einige für die Aufgabenerfüllung der Aufsichtsbehörde wesentlichen neuen bzw. geänderten Vorschriften werden in Nummer 1 und 2 dieses Berichtes kurz umrissen.

## **1. Übersicht über die Kontrolltätigkeit**

### **1.1 Meldungen zum Register vor der Gesetzesänderung**

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich führte das Register nach § 32 Abs. 2 Bundesdatenschutzgesetz (BDSG).

Bei den registrierten Firmen gab es folgenden Stand:

Gesamtmeldungen:	168
Auskunfteien:	9
Markt- und Meinungsforschungsinstitute:	4
Dienstleistungsunternehmen:	155
davon:	
DV im Auftrag u. Schreibbüros:	123
Datenträgervernichtungsfirmen:	24
Mikroverfilmer:	8

### 1.1.1 Änderung des Registers durch das neue BDSG

Im neuen BDSG ist die Meldepflicht im § 4 d BDSG geregelt. Das Gesetz schreibt vor, dass generell von nicht-öffentlichen Stellen "Verfahren automatisierter Verarbeitungen" der zuständigen Aufsichtsbehörde zu melden sind (§ 4d Abs. 1 BDSG). In den nachfolgenden Absätzen werden Ausnahmen hiervon getroffen.

Danach entfällt die Meldepflicht für die Firmen, die einen betrieblichen Datenschutzbeauftragten bestellt haben (§ 4d Abs. 2 BDSG). Auch wenn die Datenverarbeitung nicht von einem betrieblichen Datenschutzbeauftragten kontrolliert wird, hat dies nicht zwingend eine Meldepflicht zur Folge. Sie besteht nämlich auch dann nicht, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, damit höchstens vier Arbeitnehmer beschäftigt sind und entweder eine Einwilligung der Betroffenen vorliegt oder die Datenverarbeitung der Zweckerreichung eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen (§ 4d Abs. 3 BDSG) dient.

Für Unternehmen, die personenbezogene Daten im Auftrag verarbeiten, ist die Meldepflicht entfallen.

Stellen, die personenbezogene Daten zum Zwecke der Übermittlung oder zum Zwecke der anonymisierten Übermittlung speichern (Adresshändler, Auskunfteien, Markt- und Meinungsforschungsinstitute) sind verpflichtet, die automatisierte Erhebung, Verarbeitung und Nutzung personenbezogener Daten unabhängig von der Mitarbeiterzahl selbst dann zu melden, wenn sie einen Datenschutzbeauftragten bestellt haben.

Das Formular zur Registermeldung ist in der Anlage abgedruckt. Alle Aufsichtsbehörden haben sich auf die einheitliche Verwendung der Registerformulare verständigt.

Die Registerübersicht sieht nach der Novellierung folgendermaßen aus:

Gesamtmeldungen:	12
Auskunfteien:	8
Markt- und Meinungsforschungsinstitute:	4

### 1.2 Beschwerden

Im Berichtszeitraum gingen 44 schriftliche Beschwerden sowie 29 Informationsanfragen bei der Aufsichtsbehörde ein, welche dann durch die Mitarbeiter ordnungsgemäß bearbeitet wurden.

Die Beschwerden und Anfragen, die nicht in die Zuständigkeit der Aufsichtsbehörde Brandenburg fielen, wurden an die betreffenden Bundesländer weitergeleitet. Telefonische Anfragen wurden nicht gesondert erfasst. Unter der Ziffer 3.2 werden nähere Ausführungen zu einigen Beschwerden und Anfragen gemacht.

## **2. Die Novellierung des BDSG**

Einige wesentliche Neuerungen des BDSG lassen sich mit den folgenden Eckpunkten benennen:

- erweiterter Anwendungsbereich,
- Erweiterung der Regelung zur Zulässigkeit der Datenverarbeitung,
- Regelung zur Videobeobachtung,
- erweiterte Befugnisse der Aufsichtsbehörde.

### **Erweiterter Anwendungsbereich**

- Während im "alten" BDSG bisher nur die geschäftsmäßige Datenverarbeitung in oder aus Dateien erfasst wurde, unterliegt nunmehr jede automatisierte Datenverarbeitung dem Geltungsbereich des BDSG. Der Dateibezug blieb lediglich bei der nicht-automatisierten Verarbeitung erhalten. Die bisher geltenden Ausnahmen für Zwischendateien sowie für Daten aus nicht-automatisierten Dateien, die nicht zur Übermittlung an Dritte bestimmt waren, sind entfallen (§ 1 BDSG).
- Erhebt, verarbeitet oder nutzt eine in der EU/ in der EWR belegene verantwortliche Stelle personenbezogene Daten in Deutschland, so findet das Datenschutzrecht dieses EU- bzw. EWR-Staates Anwendung. Das BDSG kommt nur dann zur Anwendung, wenn die verantwortliche Stelle mit Hilfe einer in der Deutschland gelegene Niederlassung die jeweilige Datenverarbeitung durchführt. Bei Stellen, die ihren Sitz außerhalb der EU haben, gilt das sogenannte "Sitzprinzip" uneingeschränkt; d.h. bei Datenverarbeitungen in Deutschland gilt das BDSG (§ 1 Abs. 5 BDSG). Die Aufsichtsbehörden haben sich also darauf einzustellen, dass sie im Einzelfall das Datenschutzrecht eines anderen EU/EWR-Staates anzuwenden haben. Dies spielte jedoch bisher bei der Tätigkeit der hiesigen Aufsichtsbehörde noch keine Rolle.

### **Erweiterung der Regelung zur Zulässigkeit der Datenverarbeitung**

Die Zulässigkeitsvoraussetzungen in § 4 BDSG wurden um den Vorgang der "Erhebung" erweitert und gleichzeitig die Kriterien für eine ohne Mitwirkung des Betroffenen stattfindende Erhebung präzisiert.

Diese Neuregelungen stellen eine wichtige Verbesserung des Schutzes personenbezogener Daten gerade im nicht-öffentlichen Bereich dar, in dem bisher insbesondere die Datenerhebung lediglich nach den Grundsätzen "Treu und Glauben" erfolgte.

## **Regelung zur Videobeobachtung**

Das neue BDSG enthält erstmals auch eine Vorschrift zur "Beobachtung öffentlich zugänglicher Räume mit optisch–elektronischen Einrichtungen" (§ 6b BDSG). Diese Regelung gilt sowohl für den öffentlichen als auch für den nicht–öffentlichen Bereich.

Die Aufsichtsbehörde Brandenburgs war in der Vergangenheit bereits des Öfteren mit Anfragen aber auch mit Beschwerden zum Thema Videobeobachtung durch Private befasst. Die diesbezüglichen Erfahrungen und Positionierungen wurden u.a. im Neunten Bericht der Landesregierung über die Tätigkeit der Aufsichtsbehörde an den Landtag dargelegt.

Nach der neuen Gesetzesvorschrift ist sie nur anwendbar, wenn öffentlich zugängliche Räume mit optisch–elektronischen Einrichtungen beobachtet werden, wobei es auf eine Speicherung des gewonnenen Bildmaterials nicht ankommt.

Eine rechtliche Definition des Begriffes "öffentlich zugänglicher Raum" gibt es nicht. Ausgehend von der auch in der Literatur überwiegend vertretenen Auffassung dazu kann man dann von einem öffentlich zugänglichen Raum sprechen, wenn er nach dem erkennbaren oder mutmaßlichen Willen des Berechtigten von jedermann betreten werden darf.

Die Videobeobachtung im Sinne des Gesetzes ist zulässig nach den im Gesetz abschließend festgelegten Zwecken.

Sowohl die Tatsache der Videobeobachtung als auch die dafür verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen. Dies können beispielsweise entsprechende Hinweisschilder sein. Zur Zeit streben die im "Düsseldorfer Kreis" kooperierenden Aufsichtsbehörden sogar die Entwicklung eines für die Kenntlichmachung der Videobeobachtung geeigneten einheitlichen Piktogramms an. Die durch die Videobeobachtung gewonnenen Daten dürfen nur gespeichert werden, wenn sie zur Erreichung des verfolgten Zweckes erforderlich sind. Die gespeicherten Daten sind unverzüglich zu löschen, wenn sie für die im Gesetz geregelten Zwecke nicht mehr erforderlich sind oder wenn schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegen stehen.

Es besteht darüber hinaus eine Verpflichtung zur Benachrichtigung des Betroffenen gem. § 33 BDSG, wenn durch die Videobeobachtung erhobene Daten einer bestimmten Person zugeordnet werden können.

## **Erweiterte Befugnisse der Aufsichtsbehörde**

Von großer Bedeutung für die Tätigkeit der Aufsichtsbehörden ist es, dass die Beschränkung der Befugnisse auf eine Anlasskontrolle weggefallen ist. Außerdem haben die Aufsichtsbehörden die Berechtigung erhalten, über datenschutzrechtliche Verstöße sowohl den Betroffenen als auch die für die Ahndung dieser Verstöße zuständigen Behörden zu unterrichten. Im Falle schwerwiegender Verstöße gegen das Datenschutzrecht können auch die Gewerbeaufsichtsbehörden verständigt werden.

Die Aufsichtsbehörde hat bei strafbaren Datenschutzrechtsverstößen neuerdings ein eigenes Strafantragsrecht.

Durch die Erweiterung der Bußgeldtatbestände besteht für die Aufsichtsbehörde nunmehr auch die Möglichkeit, materielle Datenschutzverstöße durch die Verhängung von Bußgeldern zu ahnden.

Eine Übersicht über die Gesamtheit der Aufsichtsbefugnisse im Einzelnen und deren entsprechende Rechtsgrundlage im neuen BDSG wird im Folgenden dargestellt:

- Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten und nutzen (§ 38 Abs. 1 S. 2 BDSG).
- Die Aufsichtsbehörde darf zum Zwecke der Aufsicht Daten an andere Aufsichtsbehörden übermitteln (§ 38 Abs. 1 S. 3 BDSG).
- Sie leistet den Aufsichtsbehörden anderer Mitgliedstaaten der EU auf Ersuchen Amtshilfe (§ 38 Abs. 1 S. 4 BDSG).
- Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen (§ 38 Abs. 4 S. 1 BDSG).
- Sie kann geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 S. 1 BDSG sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen (§ 38 Abs. 4 S. 2 BDSG) – entsprechende Geltung von § 24 Abs. 6 BDSG.
- Bei Feststellung eines Verstoßes gegen datenschutzrechtliche Vorschriften darf die Aufsichtsbehörde
  - + den oder die Betroffenen darüber unterrichten,
  - + den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzeigen,
  - + bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerblicher Maßnahmen unterrichten (§ 38 Abs. 1 S. 5 BDSG).
- Bei Feststellung von Verstößen gegen datenschutzrechtliche Vorschriften
  - + entsprechend dem Katalog des § 43 BDSG liegt die sachliche Zuständigkeit für die Durchführung entsprechender Bußgeldverfahren gem. § 36 Abs. 1 Nr. 2a OWiG i.V.m. der Datenschutzzuständigkeitsverordnung (DSZustV) des Landes Brandenburg bei der Aufsichtsbehörde;
  - + entsprechend § 44 Abs. 2 BDSG hat auch die Aufsichtsbehörde ein Strafantragsrecht.
- Gem. § 38 Abs. 5 S. 1 BDSG kann die Aufsichtsbehörde anordnen, dass im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden; gem. § 38 Abs. 5 S. 2 kann die Aufsichtsbehörde bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechtes verbunden sind, den Einsatz einzelner Verfahren untersagen, wenn die Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden.
- Die Aufsichtsbehörde kann die Abberufung des betrieblichen Datenschutzbeauftragten verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Sachkunde nicht besitzt (§ 38 Abs. 5 S. 3 BDSG).

### **3. Kontrolltätigkeit der Aufsichtsbehörde**

#### **3.1 Überprüfung von Unternehmen**

In diesem Berichtszeitraum wurden wenige Überprüfungen von Unternehmen durchgeführt. Dabei konnten keine gravierenden Verstöße gegen datenschutzrechtliche Bestimmungen festgestellt werden. Einem Unternehmen wurde ein Hinweis auf die Bestellung eines betrieblichen Datenschutzbeauftragten gegeben, da bei der Einstellung eines weiteren Mitarbeiters die Mindestanzahl von Arbeitnehmern erreicht ist (§ 36 Abs. 1 BDSG (alt)).

##### **3.1.1 Geänderte Regelung zur Bestellung eines betrieblichen Datenschutzbeauftragten**

Der oben angeführte § 36 BDSG wurde mit der Novellierung des BDSG aufgehoben. Regelungen zur Bestellung eines betrieblichen Datenschutzbeauftragten sind seit dem 23.05.2001 in §§ 4f, g BDSG enthalten.

Der neue § 4 f BDSG gilt für öffentliche und nicht-öffentliche Stellen und regelt die Voraussetzungen, wann ein betrieblicher Datenschutzbeauftragter zu bestellen ist. Danach haben öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, einen Beauftragten für den Datenschutz schriftlich zu bestellen. Diese Regelung findet auch Anwendung, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt und damit in der Regel mindestens 20 Personen beschäftigt werden. Der Beauftragte für den Datenschutz ist bei nicht-öffentlichen Stellen innerhalb eines Monats nach Aufnahme der Tätigkeit zu bestellen.

Nicht-öffentliche Stellen, die höchstens 4 Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigen, sind von dieser Vorschrift befreit.

Unabhängig von der Anzahl der Mitarbeiter haben nicht-öffentliche Stellen, die automatisierte Verarbeitungen vornehmen und einer Vorabkontrolle unterliegen oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung bzw. anonymisierten Übermittlung erheben, verarbeiten oder nutzen, einen Beauftragten für den Datenschutz zu bestellen.

Auch der § 37 BDSG ist durch die Änderung des BDSG weggefallen. Die Aufgaben des Beauftragten für den Datenschutz werden nun durch § 4 g BDSG geregelt. § 37 Abs. 1 BDSG (alte Fassung) wurde mit wenigen Änderungen übernommen. Entfallen ist die Pflicht des Datenschutzbeauftragten, bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen beratend mitzuwirken. Neu aufgenommen wurde die Pflicht, dass der Beauftragte für den Datenschutz ein Verzeichnisse (Angaben nach § 4 e Satz 1 BDSG) vorhält und dies jedermann auf Antrag in geeigneter Weise verfügbar macht (§ 4 g Abs. 2 BDSG).

Die Funktion des Beauftragten für den Datenschutz ist durch Änderung des BDSG gestärkt worden, da die Meldepflicht an die zuständigen Aufsichtsbehörden grundsätzlich geändert wurde. Gemäß § 4 d Abs. 2 BDSG entfällt die Meldepflicht, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

## 3.2 Schwerpunkte aus Beschwerden und Anfragen

### *"Videoüberwachung"*

Am Anfang des Jahres gingen zwei Beschwerden zu einem Sachverhalt ein. In diesen Fällen fand noch das alte BDSG Anwendung. Die Petenten führten aus, dass sich auf einem öffentlich zugänglichen Gelände eines Objektes zwei Kameras befänden. Diese Kameras könnten verschiedene Bereiche bzw. Menschenansammlungen überwachen bzw. filmen.

Die Aufsichtsbehörde holte eine Stellungnahme des Geschäftsführer des Objektes ein. Der Geschäftsführer teilte mit, dass die Kameras auf die Türen gerichtet seien und diese Ausrichtung unverändert sei. Das Bild würde mittels eines Kabels wechselnd auf Monitore übertragen. Mitarbeiter des Objektes hätten die Möglichkeit, die Bilder zu überwachen. Wichtig sei der Monitor vor allem für den Wachtschutz in der Nacht. Es würden keine Aufzeichnungen erfolgen.

Das BDSG gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen, soweit sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen (§ 1 Abs. 2 Nr. 3 BDSG). Gemäß § 3 Abs. 2 BDSG ist eine Datei eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei) oder jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei).

Das damals noch geltende BDSG enthielt keine spezielle Regelung zur Videoüberwachung. Durch den Betreiber des Objektes erfolgte keine Aufzeichnung der Bilder, daher wurde der Dateibegriff nicht erfüllt, der zwingende Voraussetzung für die Anwendung des BDSG im privaten Bereich war. Nur eine digitale Aufzeichnung von Bildern hätte diese Voraussetzung erfüllt.

Den Petenten wurde mitgeteilt, dass zur Zeit das BDSG geändert würde und darin eine Regelung zur Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen vorgesehen sei. Nach dem zur der Zeit vorliegenden Entwurf des § 6 b BDSG wäre die Videoüberwachung des Objektes zulässig.

Nach Inkrafttreten des geänderten BDSG ging erneut eine Beschwerde zu der Videoüberwachung dieses Objektes ein.

Der Geschäftsführer wiederholte, dass die Kameras auf die Eingangstüren oder andere schützenswerte Bereiche seines Objektes gerichtet seien und nicht dazu dienen würden, Personen auf ihren Spaziergängen zu beobachten.

Vertreter der Aufsichtsbehörde führten unangemeldet eine Besichtigung vor Ort durch. Nach der Ankunft auf dem Objekt wurde ohne Begleitung ein Rundgang um das Gebäude gemacht. Dabei wurde festgestellt, dass 4 Kameras auf dem Gelände angebracht sind. Anschließend wurde vom Geschäftsführer die Funktion der Anlage vorgeführt. Die Bilder können auf einem Monitor verfolgt werden. Die Kameras sind in einem bestimmten Umkreis schwenkbar und über die Anlage steuerbar.

In der Beschwerde wurde ausgeführt, dass der Petent auf einem Spaziergang auf dem öffentlichen Weg am See beobachtet worden sei. Nach Auskunft vom Geschäftsführer habe er das komplette Grundstück gekauft. Im Kaufvertrag sei jedoch vereinbart worden, dass der Uferweg als Wanderweg rund um den See der Öffentlichkeit zugänglich bleiben solle (Wegerecht). Dies hat der Besitzer des Objektes

umgesetzt und den Weg für die Bürger offen gelassen. Eine Kamera ist auf dieser Seite des Hause angebracht, so dass ein Teil des Weges eingesehen werden kann. Am Tag der Besichtigung war die Kamera so eingestellt, dass auf dem Weg befindliche Personen nicht erfasst wurden. Auf Befragen wurde erklärt, dass die Kamera generell so eingestellt sei.

Gemäß § 6 b Abs. 1 Ziffer 2 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch–elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Unter die Wahrnehmung des Hausrechts fallen Beobachtungen, die dazu dienen, die Begehung von Straftaten zu verhindern oder aufzuklären. Auch die Überwachung von Hausverboten gehört hierzu. Zulässigkeitsvoraussetzung für eine Videoüberwachung ist weiterhin, dass keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen. Dies setzt eine Güter– und Interessenabwägung unter Beachtung der rechtlich geschützten Positionen sämtlicher Beteiligten unter Würdigung aller Umstände des Einzelfalls voraus. Im Rahmen der Abwägung ist u.a. zu berücksichtigen, wie oft der Betroffene den überwachten Raum aufsucht bzw. aufsuchen muss (Duhr, Naujok, Peter, Seiffert, "Neues Datenschutzrecht in der Wirtschaft" DuD 26(2002), S. 5 ff.).

Im Fall der Videobeobachtung dieses Objektes kann festgestellt werden, dass der überwachte Raum nicht aufgesucht werden muss. Es ist die freiwillige Entscheidung der Bürger, diesen Weg zu benutzen. Eine Aufzeichnung der übertragenen Bilder erfolgt nicht. Des weiteren wird dieser Raum nicht ständig überwacht, da auf dem Monitor im Wechsel die Bilder aller Kameras eingestellt werden und die Mitarbeiter nicht unentweg die Bilder verfolgen. Aus diesem Grund überwiegen nicht die schutzwürdigen Interessen der Betroffenen. Die Videobeobachtung wird demnach für zulässig gemäß § 6 b Abs. 1 Nr. 2 BDSG erachtet.

Nach § 6 b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Geeignete Maßnahmen können z.B. allgemein verständliche Hinweisschilder oder entsprechende Piktogramme sein. Die Aufsichtsbehörde teilte dem Geschäftsführer mit, dass am Haupteingang des Objektes ein Hinweis auf die Videobeobachtung des Geländes angebracht werden sollte.

#### *"Datenschutzrechtliche Prüfung eines Computerprogramms zur Regressanalyse"*

Eine Ärztin hat sich mit einer Anfrage an die Aufsichtsbehörde gewandt, die die Bitte um datenschutzrechtliche Prüfung eines Computerprogramms zur Regressanalyse zum Inhalt hatte. Diese Programm wurde von einem Unternehmen mit Sitz in Brandenburg bundesweit angeboten.

Mittels der Software soll es den Ärzten ermöglicht werden, ihr Ordnungsverhalten vor dem Hintergrund der Budgetierung zu kontrollieren und zu optimieren.

In einer Präsentation stellte das Unternehmen das Programm vor. Mit diesem Programm werden zunächst die Patientendaten verschlüsselt, d.h. in der Arztpraxis wird jedem Patienten nach dem Zufallsprinzip eine Nummer zugeordnet. Anschließend erfolgt eine Überprüfung, ob tatsächlich alle Patientendaten, die Rückschlüsse auf bestimmte Personen zulassen, entfernt wurden. Weiterhin wird eine Plausibilitätsprüfung bzgl. der vorgenommenen Ordnungen (Text und Pharma–Nr.) durchgeführt, bei der der Arzt noch Korrekturen vornehmen kann. Es wurde ausge-

führt, dass der Arzt gezwungen ist, eine Pseudonymisierung der Patientendaten vorzunehmen, da anderenfalls das Programm nicht weiterarbeitet. Erst im Anschluss daran kann der Arzt die nunmehr pseudonymisierten Daten auf eine Diskette exportieren, die verschlüsselt an das Unternehmen übersandt wird. Der Export der Daten ist nur pseudonymisiert möglich. Im Unternehmen werden die für die Regressanalyse notwendigen Auswertungen vorgenommen und der Arzt erhält die Analyse auf einer verschlüsselten Diskette zurück. Beim Import in seinen Praxis-PC kann der Arzt diese Daten wieder entschlüsseln und seinen Patienten zuordnen. Es ist ihm damit möglich, sein Ordnungsverhalten unter vielfältiger Gesichtspunkten auszuwerten und ggf. Ausdrucke zu erzeugen.

Die Daten der Patienten wie Name und Adresse werden dabei nicht an das Unternehmen übermittelt. Seitens des Unternehmens erfolgt auch keine Datenübermittlung an die Krankenkassen oder die kassenärztlichen Vereinigungen.

Aufgrund der Tatsache, dass lediglich pseudonymisierte Daten übermittelt werden und es nur dem Arzt möglich ist, die Daten wieder zu entschlüsseln, bestanden gegen die Verwendung der Software keine datenschutzrechtlichen Bedenken.

#### *"Speicherung personenbezogener Daten in einem Wohnheim"*

Ein Petent wandte sich mit der Problematik der Speicherung personenbezogener Daten in einem Wohnheim an die Aufsichtsbehörde. Bei Betreten dieses Gebäudes wurden die Daten in eine Art Hausbuch eingetragen. Bei diesen Daten handelte es sich um den Namen, das Ankunftsdatum und die Personalausweisnummer. Danach bekam der Besucher des Wohnheimes einen sogenannten Besucherausweis. Die Daten seien nach Verlassen des Gebäudes nicht gelöscht worden, sondern man habe noch das Verlassen des Gebäudes mit Uhrzeit und handschriftlicher Signatur des Angestellten im Hausbuch versehen.

In der Stellungnahme des Wohnheimes wurde betont, dass eine optimale Sicherheit der Hausgäste erforderlich sei und deshalb der Eintrag in das Besucherbuch erfolge. So können beispielsweise bei einem Brand alle im Haus befindlichen Personen namentlich benannt werden und man habe auch schon Straftaten aufgeklärt. Beteuert wurde, dass im vorliegenden Fall die Daten unkenntlich gemacht wurden. In der Hausordnung wird die Vorgehensweise des Wohnheimes näher geregelt. Unter Ziff. 8 heißt es: "Für alle Bewohner besteht die Möglichkeit Besuch zu empfangen. Dieser muss sich mit Personalausweis in das Besucherbuch des Hauses eintragen."

In diesem Fall konnte kein Verstoß gegen datenschutzrechtliche Vorschriften festgestellt werden.

#### *"Handwerker-Datenbank"*

Zwei andere Beschwerden befassten sich mit einer Internetseite, auf welcher eine Sonderaktion unter dem Motto "Handwerker schützen sich selbst" angeboten wurde. Jeder Handwerker kann dort seine positiven und negativen Erfahrungen ( Bspl. Zahlungsmoral, gekürzte Rechnungen, verweigerte Abnahmen) in eine Datenbank einstellen und stellt diese anderen Handwerkern zur Verfügung. Beide Petenten behaupteten, dass diese Daten an Dritte weitergereicht würden und dies ohne deren berechtigtes Interesse zu prüfen.

Nach Prüfung der Angelegenheit konnte festgestellt werden, dass in dieser Datenbank Erfahrungen von Handwerkern über die geschäftliche Zusammenarbeit mit Firmen, welche als Auftraggeber auftreten, gespeichert werden. Die Grunddaten

über die Handwerkerfirmen sind auch im Handelsregister oder Gewerberegister öffentlich einsehbar. Der Zugang zur Internetseite erfolgt über eine Benutzer ID und ein geheimes Passwort. Erst nach Akzeptanz der allgemeinen gesetzlichen Bestimmungen und der Prüfung, ob diese Handwerksfirma überhaupt existiert, wird der Zugang gewährt.

In diesem Zusammenhang konnte festgestellt werden, dass das Unternehmen nach § 4 d BDSG bei der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich meldepflichtig ist.

Nachdem die Firma sich zum Register angemeldet hatte, wird sich die Aufsichtsbehörde demnächst über die Einhaltung der gesetzlichen Vorschriften gemäß § 38 Abs. 4 BDSG bei einem Besichtigungstermin überzeugen.

### *"Informationsgespräch mit Vertretern einer Versicherung"*

Dieses Informationsgespräch kam aufgrund mehrerer datenschutzrechtlicher Beschwerden im Berichtszeitraum sowie auch in den vergangenen Jahren zustande. In einer Präsentation der Versicherung wurden den Vertretern der Aufsichtsbehörde Hintergründe und aktuelle Bezüge des Unternehmens bekannt gegeben.

Die Versicherung startete 1996 in Deutschland mit Hauptsitz im Land Brandenburg. Derzeit werden ca. 3 Millionen Kunden betreut. Die Versicherung bietet als Direktversicherer Kfz-Versicherungen sowie Schutzbriefe an.

Durch die Mitarbeiter wurde mitgeteilt, dass die Angestellten in gewissen Schritten ausgebildet werden – es gibt ein Basistraining, Ausbildung über einen Monat im kleinen Team im Call-Center sowie ein Verkaufstraining. Das Hauptaugenmerk der Arbeit liegt auf der telefonischen Kundenaufnahme. Kundenwerbung durch die Medien und in Zeitschriften sei gering. Bei Interesse eines Kunden wird ein Antragspaket versandt.

Die Versicherung regelt datenschutzrechtlich die Abwicklung ihrer Geschäfte so, dass nach telefonischer Anfrage über ein Angebot bei Nichtinteresse des Kunden dieser weiter im Bestandssystem, wenn dieser nicht ausdrücklich eine Sperrung bzw. Löschung seiner Daten wünscht, verbleibt, außer es besteht ein entgegenstehendes rechtliches Interesse der Versicherung an der weiteren Speicherung.

Seitens der Aufsichtsbehörde wurde kritisch angemerkt, dass eine Speicherung personenbezogener Daten bei Nichtzustandekommen eines Versicherungsvertrages nach dem BDSG nicht tragbar ist. Nach § 4a BDSG hat der Kunde zwar seine Angaben freiwillig preisgegeben, aber gemäß § 35 Abs. 2 Nr. 3 BDSG sind die Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich sind.

Angeregt wurde eine Änderung der Praxis in diesem Punkt.

Des Weiteren wurde darauf verwiesen, dass nach § 4f BDSG der betriebliche Datenschutzbeauftragte nicht gleichzeitig der Vorstand des Unternehmens sein sollte. Auch wurde auf die schriftliche Bestellung des betrieblichen Datenschutzbeauftragten hingewiesen, die einen Monat nach Aufnahme der Tätigkeit erfolgen sollte.

Der Schriftwechsel in dieser Angelegenheit ist noch nicht abgeschlossen.

### *"Informationsgespräch mit Vertretern eines Internet-Marktplatzes"*

Im Berichtszeitraum sind mehrere Eingaben bei der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich eingegangen, die sich mit der Arbeitsweise eines Internet-Marktplatzes auseinandersetzen. Zur Klärung grundsätzlicher datenschutzrechtlicher Aspekte sowie zur Besprechung von Einzelfällen fand ein Gespräch mit Vertretern des Unternehmens statt.

Nach einer kurzen allgemeinen Einführung seitens der Aufsichtsbehörde stellten die Vertreter ihr Unternehmen vor. Das Unternehmen ist ein Internet-Marktplatz, der eine Plattform zur Verfügung stellt, über die die Mitglieder ihre Produkte versteigern oder zu einem Festpreis anbieten können. Außerdem haben die Nutzer die Möglichkeit, die von ihnen angebotenen Artikel (Auktionen und Festpreisartikel) in einem eigenen Shop einzustellen.

Die Firma hat auf die Verkäufe seiner Mitglieder keinen Einfluss und führt selbst keine Auktionen durch.

Zur Teilnahme an den Auktionen muss man sich registrieren lassen. Die Vertreter des Unternehmens erklärten am praktischen Beispiel das Anmeldeverfahren. Dieses Verfahren erfolgt in folgenden 3 Schritten:

- 1) Ausfüllen des Anmeldeformulars (Name, Anschrift, Telefonnummer, E-Mail-Adresse, Username)
- 2) Empfangen der Anmeldebestätigung
- 3) Bestätigung der Anmeldung

Nach Abschluß des 3. Schrittes kann der Nutzer die Webseite nutzen.

Des Weiteren wurden die datenschutzrechtlichen Anforderungen an die Feedbackverknüpfung sowie an die Übermittlung von E-Mail-Adressen diskutiert.

Wie bereits schon erwähnt, gingen im Berichtszeitraum einige Beschwerden zur Arbeitsweise des Internet-Marktplatzes ein. Aus diesen Beschwerden kristallisierten sich 3 Hauptprobleme heraus :

- a) Petenten verlangten Auskunft über die beim Unternehmen gespeicherten personenbezogenen Daten.

Nach Einschaltung der Aufsichtsbehörde wurde diese Auskunft erteilt

- b) Petenten verlangten die Löschung der vom Unternehmen gespeicherten personenbezogenen Daten. Es wurde wegen Missbrauchs des Marktplatzes (bzw. des Verdachts auf einen Missbrauch) ein sogenanntes "virtuelles Hausverbot" erteilt und der Account der Nutzer gesperrt.

Zu dieser Problematik wurde seitens des Unternehmens ausgeführt, dass personenbezogene Daten in Einzelfällen nicht vom Unternehmen gelöscht würden, soweit eine Speicherung der Daten zur Wahrung der berechtigten Interessen vom Unternehmen erforderlich sei und kein Grund zu der Annahme bestünde, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Nutzung überwiege. Die Petenten seien registrierte Nutzer der Plattform gewesen, bei dem sich das Unternehmen aufgrund missbräuchlichen bzw. rechtswidrigen Verhaltens gezwungen sah, sie von der weiteren Inanspruchnahme der Handelsplattform auszuschließen. Dieser Ausschluß von der Nutzung des Teledienstes erfordere es, die personenbezogenen Daten der Betroffenen auch künftig zu speichern. Die Speicherung der personenbezogenen Daten der somit gesperrten Mitglieder ermögliche dem Unternehmen, eine Neuanmeldung dieser Person zu verhindern und sicher-

zustellen, dass sie keine Möglichkeit mehr haben, über diesen Handelsplatz anderen Mitgliedern Schaden zuzufügen.

Auf das Unternehmen finden grundsätzlich die Vorschriften des Teledienst-  
tedatenschutzgesetzes (TDDSG) Anwendung. Daneben gelten die Rege-  
lungen des Bundesdatenschutzgesetzes (BDSG) (§ 27 ff. BDSG).

Die Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke ist im  
§ 28 BDSG geregelt. Danach ist das Erheben, Speichern, Verändern oder  
Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die  
Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berech-  
tigter 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. Auf dieser  
Grundlage können in diesen Fällen die Bestandsdaten weiterhin gespeichert  
werden, da das berechnigte Interesse des Unternehmens überwiegt, um zu  
verhindern, dass eine Neuanmeldung der ausgeschlossenen Mitglieder er-  
folgt.

Danach konnte kein Verstoß gegen datenschutzrechtliche Vorschriften fest-  
gestellt werden.

- c) Petenten kritisierten, dass Bewertungsprofile und alle vorangegangenen  
Auktionen im Internet veröffentlicht und von jedermann eingesehen werden  
können.

Die Vertreter des Unternehmens legten dar, dass die registrierten Mitglieder  
die Möglichkeit hätten, mit Hilfe von Bewertungen, die die Verkäufer und  
Käufer nach Durchführung der einzelnen Verträge übereinander abgeben  
können, auf Informationen über frühere, bereits abgeschlossene Geschäfte  
zugreifen zu können. Die Veröffentlichung dieser Informationen stehe im  
Einklang mit den geltenden datenschutzrechtlichen Bestimmungen. Sie sei  
für die Sicherheit dieses Markplatzes notwendige Voraussetzung, weil nur die  
Offenlegung der Bewertungen bei den anonym ablaufenden Geschäften  
wirksam zur Betrugsprävention beitragen könne. Hierüber würden die regis-  
trierten Mitglieder informiert.

Der Sinn dieser Bewertungen bestünde gerade darin, dass sich die Nutzer  
über die Seriosität potentieller Handelspartner informieren und vor Geschäf-  
ten mit unseriösen Partner gewarnt werden können. Ohne die Verknüpfungen  
zu bereits abgeschlossenen Geschäften sei dies nicht effektiv möglich. Für  
die Beurteilung der Seriosität sei nicht nur wesentlich, ob eine Transaktion zur  
Zufriedenheit der Beteiligten abgewickelt worden sei, sondern auch, welcher  
Artikel zu welchem Preis gehandelt worden sei.

Zur Überprüfung hat sich die Aufsichtsbehörde mehrere Bewertungen sowie  
Übersichten über alle Artikel eines Verkäufers angesehen. Auf diesen Seiten  
sind grundsätzlich keine Einzelangaben, die unmittelbar auf eine Person be-  
zogen werden können, enthalten. Es sind lediglich die Mitgliedsnamen er-  
sichtlich, die jedoch von jedem Nutzer selbst bestimmt werden können. Nur  
in den Fällen, in denen jemand im Rahmen eines konkreten Geschäftes seine  
Identität preisgibt, ist diese Person für ihren Geschäftspartner in dieser Liste  
reidentifizierbar. Aber auch wenn jemand unter seinem Klarnamen Geschäfte  
tätigt, ist er wegen weiterer fehlender Angaben (Ort, Straße) kaum zu ermit-  
teln.

Die Mitglieder dieses Internet-Marktplatzes haben mit der Registrierung einen Vertrag abgeschlossen und die Allgemeinen Geschäftsbedingungen akzeptiert, die u.a. Informationen zum Bewertungssystem enthalten. Auch hier lag kein Verstoß gegen datenschutzrechtliche Vorschriften vor.

#### **4. Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden der Länder**

##### **4.1 Besondere Beratungsthemen des "Düsseldorfer Kreises"**

###### **Novellierung des BDSG**

Zentrales Thema im Düsseldorfer Kreis war die Novelle des BDSG.

Die Umsetzung der Novellierung stellt nicht unerhebliche Anforderungen an die Tätigkeit der Aufsichtsbehörden. Um die bundeseinheitliche Auslegung der Vorschriften zu gewährleisten ist ein erhöhter Abstimmungsbedarf in bezug auf die neuen Aufgaben bzw. die geänderten Vorschriften notwendig.

Parallel wird bereits an der 2. Stufe der Novellierung gearbeitet. Ziel ist es, eine verständlichere, modernere und effektivere Fassung des Bundesdatenschutzgesetzes zu erarbeiten. Die Aufsichtsbehörden wirken hieran aktiv mit.

###### **Payback – Rabattkartensystem**

Das Payback – Rabattkartensystem, das eine Kundenbindung bewirken soll, wird inzwischen von einer Reihe großer Unternehmen eingesetzt. Es ermöglicht Kunden, Guthabenpunkte anzusammeln, die in Form von Sachprämien oder Bargeld eingelöst werden können. Aus datenschutzrechtlicher Sicht ist hierbei anzumerken, dass aufgrund der Verkaufsdaten zu einzelnen Kunden die Möglichkeit eröffnet wird, detaillierte Kundenprofile mit entsprechenden Bewertungen zu fertigen.

Das Landgericht München hat in einem Urteil die Datenschutzklauseln für rechtswidrig erklärt, weil u.a. wichtige Angaben in den Anmeldeformularen nicht eindeutig formuliert sind. Z.B. wird beanstandet, dass der Kunde nicht erfährt, in welchen Fällen und ggf. an welche Adressaten seine Daten weitergegeben werden können und welche Unternehmen über welche Daten verfügen. Auch ist der Zweck der Datenübermittlung nicht hinreichend abgegrenzt. Aufgrund der unangemessenen Kundenbenachteiligung wurde die Einverständniserklärung für unwirksam erklärt.

Payback hat sich verpflichtet, Anmeldeformulare mit entsprechenden geänderten Teilnahmebedingungen vorzulegen. Diese Verhandlungen konnten im Berichtszeitraum nicht abgeschlossen werden.

##### **4.2 Schwerpunkte aus der Sitzung der Arbeitsgruppe "Auskunfteien"**

Die Sitzung der Arbeitsgruppe fand am 08./08.11.2001 in Stuttgart statt.

Im Jahr 2001 wurden durch die Arbeitsgruppe u.a. folgende Schwerpunkte behandelt:

## 1. Scoring-Verfahren

Die Auskunftsteien greifen in immer größerem Umfang zur Beurteilung von Einzelpersonen oder auch Unternehmen auf automatisierte Verfahren zurück, mit denen personenbezogene Daten verknüpft und in Verhältnis zu anderen, im Regelfall statistischen, Daten gesetzt werden. Ziel dieser Verarbeitung ist es, Aussagen bezüglich der Kreditwürdigkeit von Personen und Unternehmen zu erhalten. Im Ergebnis wird ein Punktwert (Score) ermittelt, der sich aus unterschiedlichsten Daten zusammensetzt. Dabei werden personenbezogene Daten gewichtet und mit den Daten einer Vergleichsgruppe verknüpft.

Die Einzelperson, zu der angefragt wird, erhält dann einen der ganzen Gruppe zugeordneten Punktwert (Score), der aussagt, mit welcher Wahrscheinlichkeit eine Kreditverpflichtung auch bedient wird.

Diese Information benutzen wiederum Unternehmen aber auch Banken und Sparkassen für ihre Entscheidung, dem Kunden Kredite beziehungsweise Leistungen auf Kredit zu gewähren. In diesem Zusammenhang taucht immer wieder das Problem auf, dass die kreditgewährenden Unternehmen ihre Entscheidung allein auf den Score-Wert stützen. Dies ist jedoch gemäß § 6a BDSG nicht zulässig:

Nach § 6a Abs. 1 BDSG dürfen Entscheidungen mit rechtlichen Folgen (günstig o. ungünstig z.B. Kreditkündigung) oder erheblicher Beeinträchtigung für den Betroffenen (Ablehnung eines Vertragsantrages; nicht jedoch der Ausschluss von Werbeaktionen) nicht ausschließlich auf eine automatisierte Verarbeitung gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Die Ausschließlichkeit fehlt dann, wenn die Entscheidung von einem Menschen – nicht nur formal – verantwortet wird.

Mit den Auskunftsteien wurde in der Vergangenheit kontrovers auch über das Auskunftsrecht der Betroffenen bezüglich des Score-Wertes diskutiert.

Gemäß § 6a Abs. 3 in Verbindung mit § 34 Abs. 1 BDSG kann der Betroffene Auskunft über die zu seiner Person gespeicherten Daten und damit auch über den Scorewert verlangen. Dies gilt jedoch dann nicht, wenn die Daten die Daten gemäß § 33 Abs. 2 Satz 1 Nr. 2 BDSG nur für Zwecke der Datensicherung gespeichert werden.

Eine große Auskunftstei gibt an, die übermittelten Score-Werte nur für Zwecke der Datensicherung zu speichern. Somit besteht nach Auffassung der Auskunftstei in diesen Fällen keine Informationspflicht gegenüber dem Betroffenen. Diese Auskunftstei hat sich jedoch bereit erklärt, dem Betroffenen einen tagesaktuellen Score-Wert zu ermitteln und mitzuteilen. Dies ist einerseits auf den Druck der Aufsichtsbehörden zurückzuführen, dient jedoch nicht zuletzt auch dazu, die Akzeptanz von Scoring-Verfahren in der Bevölkerung zu erhöhen. Dieses Verfahren wird kostenpflichtig sein und es ist durchaus wahrscheinlich, dass der ermittelte Score-Wert von bereits übermittelten Werten abweicht.

## 2. Warndatei im Wohnungswesen

Die Wohnungsunternehmen möchten sich mit einer Warndatei vor Mietausfall durch säumige Mieter schützen. Zu diesem Zweck sollen Daten zur Identifizierung des Mieters, Daten über Zahlungsprobleme und/oder Vertragsverletzungen und Daten des Vermieters/Mietobjektes gespeichert und gegebenenfalls beauskunftet werden.

Die Arbeitsgruppe Auskunfteien hatte nun die datenschutzrechtliche Zulässigkeit einer solchen Warndatei zu prüfen und ist zu dem Ergebnis gekommen, dass die Daten von "vertragstreuen" Mietern nicht an eine Warndatei übermittelt werden dürfen. Für derartige Übermittlungen besteht kein berechtigtes Interesse der Vermieter. Ein solches Interesse kann erst bei einem unstreitigen Mietrückstand von zwei Monatsmieten geltend gemacht werden. In diesen Fällen kann auf Zahlungsunwilligkeit oder Zahlungsunfähigkeit geschlossen werden, mit der Folge, dass der Betroffene zwar möglicherweise ein Interesse am Ausschluss der Übermittlung der Mietrückstände hat, dieses Interesse jedoch nicht schutzwürdig ist. Berechtigte Mietminderungen oder Rückstände von Betriebskosten dürfen nicht in eine solche Datei eingemeldet werden.

Brancheninterne Warndateien existieren nach Kenntnis der Aufsichtsbehörde des Landes Brandenburg noch nicht.

Es besteht jedoch für Wohnungsunternehmen zur Zeit schon die Möglichkeit, mit der SCHUFA einen Vertrag zu schließen, der die gegenseitige Übermittlung von Daten über das Mietverhältnis beinhaltet. Für eine solche Übermittlung ist Voraussetzung, dass der Wohnungssuchende eine SCHUFA-Klausel unterschreibt. Durch die Vermieter dürfen nur unbestrittene offene Forderungen an die SCHUFA gemeldet werden. Die SCHUFA meldet diese Informationen gegebenenfalls an andere anfragende Wohnungsunternehmen weiter.

Dieses Verfahren ist dem Verfahren beim Abschluss von Handyverträgen ähnlich, wo auf der Basis einer Einwilligungserklärung des Kunden vor Vertragsabschluss ebenfalls eine SCHUFA-Auskunft oder eine Auskunft über eine andere Auskunftei eingeholt wird und im Verlaufe der Vertragsabwicklung unabhängig von der Einwilligung Daten über nichtvertragsgemäßes Verhalten an die entsprechende Auskunftei übermittelt werden.

#### **4.3 Teilnahme an den Sitzungen der Arbeitsgruppe "Internationaler Datenverkehr"**

Da Brandenburg ständiges Mitglied der Arbeitsgruppe "Internationaler Datenverkehr" ist, nahm im Berichtszeitraum auch ein Vertreter der Aufsichtsbehörde an den regelmäßigen Sitzungen teil.

Schwerpunkte der geführten Diskussionen waren u.a. die Umsetzung der von der Europäischen Kommission getroffenen Entscheidungen zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer sowie zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländer nach der EU-Datenschutzrichtlinie 95/46/EG.

Darüber hinaus spielten Unternehmensrichtlinien im Sinne des § 4c Abs. 2 BDSG, die von verschiedenen großen Unternehmen und Unternehmensverbänden an die Aufsichtsbehörden herangetragen wurden, eine zunehmend wichtige Rolle.

Denn bei Vereinbarung von durch die EU erstellten Standardvertragsklauseln oder der Anwendung von (ausreichenden) verbindlichen Unternehmensrichtlinien ist gem. § 4c Abs. 2 BDSG eine Übermittlung personenbezogener Daten an Drittstaaten zulässig, auch wenn ansonsten in dem Staat kein angemessenes Datenschutzniveau existiert.

Die Aufsichtsbehörden gehen übereinstimmend davon aus, dass es bei Datenübermittlungen in Drittländer auf der Grundlage der von der Europäischen Kommission herausgegebenen Standardvertragsklauseln keiner ansonsten erforderlichen Genehmigung der Datenübermittlung durch die zuständige Aufsichtsbehörde gem. § 4c Abs. 2 Satz 1 BDSG bedarf.

#### **4.4 Teilnahme an den Sitzungen der Arbeitsgruppe "Telekommunikation, Tele- und Mediendienste"**

Auch in diesem Berichtszeitraum fanden 2 Sitzungen der Arbeitsgruppe "Telekommunikation, Tele- und Mediendienste" statt, an denen jeweils ein Vertreter der Aufsichtsbehörde Brandenburgs teilnahm.

Auf der Tagesordnung standen jeweils Probleme bei der Anwendung des Tele-dienste- und Teledienstedatenschutzgesetzes sowie des Mediendienstestaatsvertrages, die diskutiert wurden. Weiterhin wurde über den entsprechenden Bearbeitungsstand von Gesetzesänderungen berichtet (z.B. Entwurf eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr, Novellierung der Datenschutzbestimmungen des Rundfunk- und Mediendienste-Staatsvertrages).

Im Berichtszeitraum fand eine Präsentationsveranstaltung (Workshop) zu der Problematik "Elektronische Zahlungssysteme" statt. In den Sitzungen der Arbeitsgruppe wurde darüber berichtet. Die Informationen der einzelnen Firmen, die ihre Produkte vorgestellt haben, wurden aufbereitet und ausgewertet. Dazu wurde ein entsprechendes Papier ausgearbeitet, in dem die vorgestellten Verfahren vorgestellt und datenschutzrechtlich bewertet werden.

**Anmeldung nach § 4 d Bundesdatenschutzgesetz (BDSG)  
zum Register nach § 38 Abs. 2 BDSG  
beim Ministerium des Innern des Landes Brandenburg**

**Hauptblatt**

Zu den Ziff. **1 – 4** beachten Sie bitte die Ausfüllhinweise.

Sollte der vorhandene Platz nicht ausreichen, fügen Sie bitte ein gesondertes Blatt mit den Angaben bei.

**1. Verantwortliche Stelle 1**

Name oder Firma

Straße

Postleitzahl

Ort

Telefon /Telefax\*

E-Mail/Internet-Adresse \*

\*= freiwillige Angaben

**2. Vertretung**

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

Name(n), Vorname(n)

**2.2** mit der Leitung der Datenverarbeitung beauftragte Personen:

Name(n), Vorname(n)

2.3 Bei verantwortlicher Stelle in Drittstaaten, d.h. mit Sitz außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (Island, Norwegen und Liechtenstein), im Inland ansässiger Vertreter: **2**

Funktion

Name(n), Vorname(n)

3. Angaben zur Person der/des Datenschutzbeauftragten \*: **3**

Name(n), Vorname(n)

Straße

PLZ

Ort

Telefon/Telefax

E-Mail/Internet-Adresse

\*= freiwillige Angaben

---

(Ort, Datum, Unterschrift) **4**

## Anlage Nr.:

**(für jedes Verfahren automatisierter Verarbeitung ist eine separate Anlage zum Hauptblatt auszufüllen)**

Zu den Ziff. 5 – 17 beachten Sie bitte die Ausfüllhinweise.

Sollte der vorhandene Platz nicht ausreichen, fügen Sie bitte ein gesondertes Blatt mit den Angaben bei.

### Verantwortliche Stelle

Firmenname

#### 4. Zweckbestimmungen der Datenerhebung, –verarbeitung oder –nutzung **6**

#### 5. Betroffene Personengruppen und Daten oder Datenkategorien

5.1 Beschreibung der betroffenen Personengruppen **7**

5.2 Beschreibung der diesbezüglichen Daten oder Datenkategorien **8**

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können; bei Datentransfers in Drittstaaten siehe Nr. 8 **9**

7. Regelfristen für die Löschung der Daten **10**  
Zeitraum

8. Geplante Datenübermittlung in Drittstaaten **11, 12**

8.1 Name des  
Drittstaates

8.2 Empfänger oder  
Kategorien von Empfängern

8.3 Art der Daten oder  
Datenkategorien

9. Angaben zur Beurteilung der Angemessenheit getroffener Sicherheitsmaßnahmen

9.1 Art der eingesetzten DV-Anlagen und Software **14**

9.2 Maßnahmen nach § 9 BDSG i.V.m. der Anlage dazu **15**  
Erläuterungen

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

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

10. Zeitpunkt der Aufnahme und Beendigung des meldepflichtigen Verfahrens **16**

---

(Ort, Datum, Unterschrift) **17**

# Ausfüllhinweise zum Meldeformular

## Hauptblatt

Die rechtliche Notwendigkeit für die im Formular geforderten Angaben ergibt sich aus § 4e BDSG und § 1 Abs. 5 Satz 3 BDSG (abgesehen von den unten als freiwillig bezeichneten Angaben). Das Hauptblatt mit den geforderten Angaben zur verantwortlichen Stelle und den dortigen Verantwortungsträgern (Nr. 1 – 2.3) ist von jeder Stelle nur einmal auszufüllen. Die Angaben zu den jeweiligen automatisierten Verfahren sind mit dem Formular **Anlagen** für **jedes einzelne betriebene Verfahren** gesondert zu melden.

- Nr. 1 Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§ 3 Abs. 7 BDSG). Angaben zu Telefon, Telefax, E-Mail und Internet sind freiwillig.
- Nr. 2 2.3 Angaben zu dem im Inland ansässigen Vertreter einer außerhalb der Europäischen Union oder der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR: Island, Norwegen und Liechtenstein) gelegenen verantwortlichen Stelle sind nach § 1 Abs. 5 Satz 3 BDSG notwendig.
- Nr. 3 Freiwillige Angabe.  
Für die Stellen, die trotz der Bestellung eines betrieblichen Datenschutzbeauftragten der Meldepflicht unterliegen, ist die Benennung des DSB sinnvoll, da dieser nach § 4f Abs. 5 Satz 2 BDSG auch der Ansprechpartner für Bürgerinnen und Bürger ist.

Das Hauptblatt ist mit einer rechtsverbindlichen Unterschrift zu versehen.

## Anlagen

Der Name und die Anschrift der verantwortlichen Stelle müssen im Kopf der Anlage nochmals angegeben werden. Wenn eine meldepflichtige Stelle nach der Meldung weitere meldepflichtige Verfahren durchführt oder durchführen lässt, genügt es, wenn sie lediglich eine neue Anlage ausfüllt und vorlegt. Ebenso ist zu verfahren, wenn sich Änderungen bei bereits gemeldeten Verfahren ergeben (wobei dann die Nummerierung der geänderten Anlage anzugeben ist). Das Hauptblatt ist nur dann neu auszufüllen, wenn sich auch insoweit Änderungen ergeben.

- 5 Bitte an dieser Stelle den Namen der verantwortlichen Stelle wiederholen. Die Angaben müssen den Angaben des Hauptblattes unter Nr. 1 entsprechen.
- 6 Nr. 4 Z.B. Datenverarbeitung zum Zweck der Übermittlung (Adresshandel, Erteilung von Wirtschaftsauskünften), Datenverarbeitung zum Zweck der anonymisierten Übermittlung (Mark- und Meinungsforschung).
- 7 Nr. 5 5.1 Als betroffene Personengruppen kommen beispielsweise Kunden, Arbeitnehmer, Patienten, Schuldner, Versicherungsnehmer usw. in Betracht.
- 8 Nr. 5.2 Mit "Daten" sind "personenbezogene Daten" i.S.d. § 3 Abs. 1 BDSG gemeint, d.h. Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Z.B. Name, Geburtsdatum, Anschrift, Einkommen, Kfz-Kennzeichen, Konto-Nr., Versicherungs- oder Personal-Nr., Beruf, Hausbesitzer.  
Grundsätzlich reicht jedoch die Angabe von Datenkategorien, z.B. Personaldaten, Kundendaten.  
Sog. "besondere Arten personenbezogener Daten" sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualeben (§ 3 Abs. 9 BDSG). Diese sind entsprechend anzugeben.

- 9 Nr. 6 Empfänger ist jede Person oder Stelle, die Daten erhält, z.B. Vertragspartner, Kunden, Behörden, Versicherungen, ärztliches Personal, Auftragsdatenverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter) usw.
- 10 Nr. 7 Zeitraum Hier ist der Zeitraum anzugeben, nach dessen Ablauf die Daten gelöscht werden. Es wird darauf hingewiesen, dass nach § 35 Abs. 2 Nr. 4 BDSG eine Überprüfung spätestens vier Jahre nach der Einspeicherung erforderlich ist.
- 11 Nr. 8 § 4e Nr. 8 BDSG fordert die Angabe der geplanten Übermittlungen in Drittstaaten (Nicht-EU-Länder und Nicht-EWR-Länder). Nur bei der Erstmeldung zum Register sind auch die bereits bestehenden Übermittlungen zu melden. Bei Änderungsmitteilungen wegen neu geplanter Übermittlungen in Drittstaaten brauchen bereits bestehende Übermittlungen nicht gemeldet werden.
- 12 8.1–8.3 Die Art der Daten oder Datenkategorien ist getrennt nach dem jeweiligen Drittstaat und den jeweiligen Empfängern oder Kategorien von Empfängern anzugeben.
- 13 Dieser Teil des Registers ist nicht öffentlich einsehbar und nur für die Aufsichtsbehörde bestimmt (§ 38 Abs. 2 Satz 3 BDSG).
- 14 Nr. 9 9.1 Z.B. Konfigurationsübersicht, Netzwerkstruktur, Betriebs- und Anwendungssoftware, spezielle Sicherungssoftware usw.
- 15 Nr. 9.2 Zutreffendes Ankreuzen und Maßnahme textlich erläutern.
- 16 Nr.10 Meldepflichtige Stellen, die bis zum 22.05.2001 im bisherigen Melderegister aufgenommen waren, tragen das ursprüngliche Datum der Aufnahme der meldepflichtigen Tätigkeit ein.
- 17 Unterschrift Die Anlagen sind mit einer rechtsverbindlichen Unterschrift zu versehen.