Landtag Brandenburg **Drucksache 4/3166**
4. Wahlperiode

Bericht
der Landesregierung

Dreizehnter 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: 13.07.2006 / Ausgegeben: 13.07.2006

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 erstmals über einen Zeitraum von 2 Jahren und zwar vom 1. Januar 2004 bis 31. Dezember 2005. Ausgangspunkt dafür ist die Änderung im § 27 Brandenburgisches Datenschutzgesetz durch das Gesetz zur Neuregelung des Landesorganisationsrechts und zur Umsetzung des Haushaltssicherungsgesetzes 2003 (Gesetz- und Verordnungsblatt für das Land Brandenburg Teil I Nr. 9 vom 24. Mai 2004).

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 (Datensicherungsmaßnahmen/Sicherheitskonzept) sowie auf die Angabe der zugriffsberechtigten Personen.
Alle Unternehmen, die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung speichern (z. B. Wirtschaftsauskunfteien, Adresshändler, Markt- und Meinungsforschungsinstitute), unterliegen der Meldepflicht.
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 vier 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:	**11**
Davon	
Auskunfteien:	**7**
Markt- und Meinungs-	
Forschungsinstitute:	**4**

2.2 Beschwerden

Im Berichtszeitraum gingen **173** schriftliche Beschwerden sowie **74** Informationsanfragen bei der Aufsichtsbehörde ein, die durch die Mitarbeiter weitestgehend zeitnah bearbeitet wurden.
Festzustellen ist, dass die Anzahl der schriftlichen Beschwerden zum vorigen Berichtszeitraum leicht angestiegen ist.
Die Anzahl der Informationsanfragen verdreifachte sich in diesem Berichtszeitraum.
Beschwerden und Anfragen, die nicht der Zuständigkeit der Aufsichtsbehörde Brandenburg unterlagen, wurden an die zuständigen Bundesländer weitergeleitet. Die örtliche Zuständigkeit erstreckt sich auf die der Aufsicht unterliegenden zu kontrollierenden Stellen allein mit Sitz im Land Brandenburg (§ 1 DSZustVO i.V.m. § 38 Absatz 6 BDSG).
Telefonische Anfragen wurden nicht gesondert erfasst.

Unter Punkt 4.2 werden nähere Ausführungen zu einigen Beschwerden, die auch eine oft längere Zeit der Klärung bedurften, gemacht.

3 Allgemeines

3.1 Beratung/Vortrag Steuerberaterkammer Brandenburg

Die Steuerberaterkammer Brandenburg ließ durch die conNect Organisation und Netzwerk GmbH Informationsveranstaltungen zum Thema "Datenschutzbeauftragter in Steuerberatungskanzleien" durchführen und gestalten. Ziel war es, dem Berufsstand das Bundesdatenschutzgesetz mit seinen Rechten und Pflichten näher zu erläutern. Mit gleichem Ziel entwickelte die Firma zeitgleich ein Datenschutzkonzept zum Thema „Datenschutz und Kanzleien“, das der Zielgruppe als Handreichung zur Verfügung gestellt werden soll. Die Aufsichtsbehörde begleitete die Informationsveranstaltung, stand mit einem Vertreter an mehreren Tagen persönlich für die Beantwortung von fachspezifischen Fragen zur Verfügung und unterstützte die Firma bei der inhaltlichen Gestaltung der Handreichung. Diese ist dem Tätigkeitsbericht als Anlage beigefügt.

Gemäß § 4g Abs. 1 BDSG hat der Beauftragte für den Datenschutz auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hinzuwirken. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle zuständige Behörde wenden.

Es ist im Rahmen der Beratungspflicht der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich generell sinnvoll, wenn mit ihrer Hilfe vorbeugend Fragen und Probleme im größeren Kreis von (potenziellen) Beauftragten für den Datenschutz besprochen werden, so dass im Ergebnis eventuelle Verstöße gegen datenschutzrechtliche Vorschriften vermieden werden können.

3.2 Piktogramm (Videoüberwachung)

Mit dem Gesetz zur Änderung des BDSG und anderer Gesetze vom 18. Mai 2001 (BGBl. S. 904) wurde erstmalig in § 6b BDSG eine Regelung zur Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen – Videoüberwachung – aufgenommen.

Der Umstand der Videobeobachtung und die verantwortliche Stelle sind nach § 6b Abs. 2 BDSG durch geeignete Maßnahmen erkennbar zu machen. Dieser Hinweis ist deutlich sichtbar anzubringen, er erfüllt nur dann seinen Zweck, wenn er für den Kunden ohne weiteres wahrnehmbar ist und von ihm nicht erst gesucht werden muss.

Wie bereits im 12. Tätigkeitsbericht der Aufsichtsbehörde erwähnt wurde, führte das Deutsche Institut für Normung (DIN) ein Normungsverfahren für ein einheitliches Piktogramm zur Kennzeichnung einer Videoüberwachung durch, das im Sommer 2005 zum Abschluss gebracht wurde. Neben potentiellen Anwendern aus der Privatwirtschaft ist das Projekt von den Aufsichtsbehörden aus Berlin und Brandenburg aktiv begleitet worden. Bei einer Nutzung dieses Piktogramms kann davon ausgegangen werden, dass man als nicht-öffentliche Stelle seine Verpflichtung zur Kenntlichmachung der Videobeobachtung erfüllt.

4 Kontrolltätigkeit der Aufsichtsbehörde

4.1 Vorortkontrolle und Beratung nach § 38 BDSG

4.1.1 Prüfung einer unabhängigen Unternehmungsgruppe

Der Arbeitsbesuch hatte seinen Ausgangspunkt in einer Datenschutzbeschwerde.
Hier wurde dem Unternehmen, welches mit Hilfe von Außendienstmitarbeitern gesellschaftsunabhängig unterschiedlichste Versicherungen der verschiedensten Anbieter vermittelt, vorgeworfen, dass sämtliche Kundendaten jederzeit jedem, der sich Zugang zum Büro verschaffe, offen liegen und für jedermann frei zugänglich sein würden. Da es sich bei den Kundendaten auch um Bankverbindungen und evtl. Mahnstufen handeln sollte, wurde eine Prüfung vor Ort durchgeführt. Ein weiterer Vorwurf bestand darin, dass im Büro auch Gehaltsnachweise und Provisionsabrechnungen verschiedener Mitarbeiter sowie Bewerbungsunterlagen offen liegen würden.
Nach einer Erläuterung des Geschäftsablaufes durch den Büroleiter und einer Begehung des Objektes wurden folgende Erkenntnisse festgehalten.
Es besteht grundsätzlich kein Kundenverkehr an diesem Standort. Die Bewerbungsunterlagen werden grundsätzlich nach den erfolgten Bewerbungsgesprächen an die Zentrale in verschlossenen Umschlägen weitergesandt.
Personenbezogene Daten werden grundsätzlich auf dem PC erfasst, der dabei nur als Terminal dient, da die Daten per Standleitung sofort an die Zentrale übertragen werden und auf dem PC keine Speicherung dieser Daten vorgenommen wird.
Anschließend werden die Unterlagen per Post an die Zentrale übersandt, da am Standort keinerlei personenbezogene Daten von Kunden, weder im PC noch in Form von Akten, gespeichert werden.
Die Beschäftigten müssen sich nach kurzer Abwesenheit am PC mit einem minütlich wechselnden Code neu einloggen. Das Sekretariat mit den Postfächern ist ständig besetzt.

Vor dem Hintergrund des geschilderten Geschäftsablaufes und der in Augenschein genommenen Rahmenbedingungen konnten die Vorwürfe des Beschwerdeführers durch die Besichtigung nicht untermauert werden.
Ein Verstoß gegen datenschutzrechtliche Bestimmungen konnte bei diesem Unternehmen somit nicht festgestellt werden.

4.1.2 Prüfung einer Partnervermittlung

Anlass des Arbeitsbesuches war eine Datenschutzbeschwerde einer Petentin, die behauptete, während ihrer Mitgliedschaft von einem anderen Mitglied angerufen worden zu sein, obwohl die Partnervermittlung von ihr keine Berechtigung zur Weitergabe ihrer Telefonnummer erhalten habe.
Die Petentin teilte mit, dass sie nach Kündigung des Vertragsverhältnisses von einem Kunden der Partnervermittlung zwecks Vereinbarung eines Kennenlerntermins angerufen wurde. Daraus schlussfolgerte sie, dass eine Weitergabe der Telefonnummer in Verbindung mit dem Namen erfolgt sein musste.
Zwischenzeitlich informierte die Beschwerdeführerin, dass die Telefonnummer des Kunden noch auf ihrem Handy gespeichert sei und teilte uns diese mit.
Daraufhin wurde der Inhaber des Single-Treffs gebeten in der Kundenkartei zu recherchieren, wer der Anrufer gewesen sein könnte. Wenn diese Telefonnummer einem Kunden zuzuordnen sei, bestünde die Möglichkeit der Weitergabe der Daten der Petentin.
Gleichzeitig wurde darauf verwiesen, dass bei dem an die Aufsichtsbehörde übersandten Aufnahmeantrag folgende Anmerkung zu machen ist. Im § 4 Abs. 3 BDSG wird darauf verwiesen, dass der Betroffene über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten zu unterrichten ist. Es wurde eine Überarbeitung und Konkretisierung des Aufnahmeantrages angeregt.
Zwischenzeitlich wurde zusätzlich ein Arbeitsbesuch bei dem Unternehmen durchgeführt. Es war dabei kein konkreter Hinweis auf eine unberechtigte Übermittlung privater Telefonnummern an Dritte ermittelbar.
Allerdings wurde der Vorschlag unterbreitet, dass im Aufnahmevertrag zur Klarstellung ein Hinweis aufgenommen sollte, der inhaltlich wie folgt lauten sollte: Die o. g. Daten werden nur für Verwaltungs- und Abrechnungszwecke verwandt.
Zwischenzeitlich hatte die Petentin den Gesprächsteilnehmer mit Adresse mitgeteilt und äußerte gleichzeitig, dass dieser auch bereit wäre zu bestätigen, dass er die private Telefonnummer von dem Single-Treff erhalten habe. Daraufhin wurde ein Schreiben an den

Betreffenden gesandt, in welchem gebeten wurde mitzuteilen, wann und von wem er die private Telefonnummer der Beschwerdeführerin erhalten habe. Leider blieb dieses Schreiben unbeantwortet und es bestand auch keine Handhabe, die entsprechende Aussage nachdrücklich abzufordern. Da hiermit alle notwendigen Maßnahmen zur Prüfung der Angelegenheit ausgeschöpft waren, wurde die Beschwerde als erledigt betrachtet.

Bei der Prüfung des Unternehmens wurde vom Geschäftsführer bestätigt, dass eine Sperrung der Telefonnummer der Beschwerdeführerin in der Eingabemaske des PC erfolgt sei. Im Falle einer Interessenabfrage müssen die Mitarbeiter nachsehen, ob ein entsprechender Sperrvermerk vorhanden ist. Ein fehlender Sperrvermerk setze voraus, dass ein Zusatzformular ausgefüllt und unterschrieben worden ist, in dem das Mitglied freiwillig zusätzliche Angaben zu seiner Person mache, mit dem Ziel, leichter mit anderen Mitgliedern in Kontakt zu treten. In diesem Falle dürfe auch die Telefonnummer weitergereicht werden. Dieses Formular habe die Petentin zwar ausgefüllt und unterschrieben, jedoch im selben Moment wieder zurückgezogen. Daraufhin sei die Telefonnummer mit einem Sperrvermerk versehen worden.
Die Prüfung der Partnervermittlung ergab keine Anhaltspunkte für eine bewusste unberechtigte Übermittlung der Telefonnummer der Beschwerdeführerin an einen Dritten.

4.1.3 Arbeitsbesuch bei einer Versicherung

Auslöser dieses Besuches war eine von mehreren Beschwerden über das Unternehmen. Dieser Petent hatte eine Prämienberechnung durchführen lassen und sich anschließend über unerwünschte Werbepost beschwert.
Im Ergebnis der Fallprüfung konnte jedoch kein Verstoß gegen datenschutzrechtliche Bestimmungen festgestellt werden.

Dennoch war die Intention des Besuches, Näheres über das Prozedere bei der Inanspruchnahme der Dienstleistung – unverbindliche Angebotsberechnung sowie weiterführend und darauf aufbauend die Onlinebestellung eines Antrages auf eine Kraftfahrtversicherung – zu erfahren.
Es wurde erläutert, dass der Kunde bis zur Präsentation des Ergebnisses, also der günstigsten Versicherung zu seinen Konditionen anonym bleibe. Will dann der Kunde das günstigste Angebot angezeigt bekommen, hat er auf der Grundlage seiner Einwilligung personenbezogene Daten anzugeben.
Bleibt die Nutzung anonym, werden sämtliche Daten (z.B. IP- Adresse) gelöscht.

Erst bei Eintritt in den Vertrag erfolgt die nötige Speicherung personenbezogener Daten.
Eine Verschlüsselung der Daten erfolgt mit einem 128 Bit Verfahren. Die Serversicherheit wurde mittels Schaubild erläutert und verdeutlicht.
Gleichzeitig wurde erwähnt, dass die Beschäftigten des Hauses in Sachen Datenschutz PC-gestützt mit einem speziellen Programm geschult werden. Das Schulungsmaterial wurde überreicht.
Die Unterbindung unzulässiger Werbemails für die Zukunft hat das Unternehmen glaubhaft versichert.

4.1.4 Arbeitsbesuch eines Markt- und Meinungsforschungsinstitutes

Dieser Arbeitsbesuch wurde seitens des Unternehmens angeregt, um anstehende datenschutzrechtliche Fragen in einem persönlichen Gespräch zu klären. Die Fragen konnten weitestgehend in diesem Gespräch ausgeräumt und erörtert werden.
Bei dieser Gelegenheit wurde das Unternehmen vorgestellt und es wurde erläutert, dass sich der Konzernhauptsitz in den USA befindet.
Das Unternehmen selbst berät andere Unternehmen und führt in deren Auftrag Mitarbeiter- und Kundenbefragungen durch. Die Daten werden dann in die USA transferiert, damit sie dort im Datenverarbeitungszentrum technisch analysiert und zusammengeführt werden können. Danach werden die Daten wieder zurück übermittelt und hier inhaltlich analysiert. Hier wurde besonders darauf verwiesen, dass bei Beteiligung eines Drittlandes (vgl. §§ 4 b und 4 c BDSG) bei der Frage der Zulässigkeit der Datenverarbeitung immer das Datenschutzniveau des entsprechenden Landes zu berücksichtigen ist.

Eine Prüfung des Unternehmens wurde bei diesem Arbeitsbesuch bereits anvisiert.

4.1.5 Videoüberwachung in einem Büro- und Geschäftsgebäude

Der Betriebsrat eines in einem Geschäftsgebäude arbeitenden Unternehmens wandte sich an die Aufsichtsbehörde und teilte mit, dass der Zugang zu den Geschäftsräumen, das Treppenhaus sowie die Fahrstuhlkabinen videoüberwacht würden. Der Vermieter sei zwischenzeitlich bereits angeschrieben worden und man habe mitgeteilt, dass diese Maßnahme aufgrund zahlreicher Einbrüche in der Vergangenheit erfolgt sei.
Eine Vor-Ort-Begehung des Objektes wurde durch die Aufsichtsbehörde durchgeführt, da sich die Beschäftigten des Hauses beobachtet fühlten und die Videoüberwachung durch den Vermieter nicht vorher angekündigt war. Die Mitarbeiter dieses Unternehmens fass-

ten diese Videoüberwachung als eine eventuelle Verhaltens- und Leistungskontrolle auf, da auch eine Kamera im Aufzug angebracht ist.
Die Kennzeichnung zur Videoüberwachung konnte bei der Kontrolle als nicht ausreichend festgestellt werden, sie wurde eher als Werbung für die betreffende Firma angesehen. Die angebrachten Schilder entsprachen auch nicht den Vorgaben des § 6 b Abs. 2 BDSG. Gleichzeitig fehlte ein Hinweis auf die verantwortliche Stelle.
In einem Schreiben an den Vermieter wurde gebeten, einen entsprechenden Hinweis entsprechend § 6 b Abs. 2 BDSG durchzuführen. Gleichzeitig ließe die gewählte Formulierung offen, ob tatsächlich Kameras mit Aufzeichnungstechnik zum Einsatz kommen. Verwiesen wurde auf die DIN Norm, die u. a. Vorgaben zur Beschriftung, Gestaltung und Größe derartiger Schilder beinhaltet.
Durch den Vermieter wurde zwischenzeitlich eine Beschriftung nach dieser DIN Norm in der entsprechenden Größe und Gestaltung im Gebäude angebracht.
Der Betriebsrat bestätigte der Aufsichtsbehörde die erfolgte Beschilderung und damit auch die Klärung der Angelegenheit.

4.1.6 Kontrollbesuch bei der Land Brandenburg Lotto GmbH (LBL)

Die Aufsichtsbehörde stattete im Rahmen der Ausführung des § 38 BDSG der Land Brandenburg Lotto GmbH (LBL) anlassunabhängig einen Arbeitsbesuch ab.
Besprochen wurde die Frage, wie die Datensicherheit bei der Abwicklung der von der LBL angebotenen Produkte durch die LBL selbst und durch beauftragte Firmen gewährleistet und kontrolliert wird.

Datensicherung umfasst alle Maßnahmen, die notwendig sind, um die Datenverarbeitung selbst (z.B. Daten, Programme, Datenverarbeitungsgeräte und Kommunikationsnetze) zur Gewährleistung der Datenschutzvorschriften vor unbefugtem Zugriff, Missbrauch, Diebstahl, Fehlern und Störungen jeder Art in angemessener Weise zu sichern; sie ist also eine technisch-organisatorische Aufgabe.

Gemäß § 9 BDSG haben öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Im Ergebnis eines konstruktiven Gespräches mit den Vertretern der LBL und nach Prüfung der vorgelegten Unterlagen (Verfahrensübersicht nach § 4g Abs. 2 i.V.m. § 4e BDSG sowie Rahmenverträge und Verträge für eine Datenverarbeitung im Auftrag gemäß § 11 BSDG) gab es vor dem Hintergrund der durch die LBL zugesagten Umsetzung der Hinweise der Aufsichtsbehörde keinen Anlass zu Beanstandungen.

4.1.7 Bewertung von Teilnahmebedingungen und Internetteilnahmebedingungen für Glücksspiele

Die Aufsichtsbehörde prüfte relevante Abschnitte von Teilnahmebedingungen bzw. Internetteilnahmebedingungen (IntTB) zum Zwecke der Teilnahme an Glücksspielen unter datenschutzrechtlichen Aspekten.

Das Unternehmen bietet auf der Grundlage der zu prüfenden IntTB einen Teledienst an und unterliegt damit dem Teledienstedatenschutzgesetz (TDDSG).

Der Spielteilnehmer hat sich vor der ersten Spielteilnahme entsprechend dem festgelegten Verfahren auf elektronischem Wege anzumelden. Dazu erhebt das Unternehmen vom Spielteilnehmer gemäß § 22 Nr. 2 IntTB folgende personenbezogenen Daten: Name, Vorname, Aliasname, vollständige Adresse, Geburtsdatum, E-Mail-Adresse, Bankverbindung. Dabei wird ihm einmalig ein Datenänderungscode angezeigt, den er sich merken und geheim halten muss. Spätere Änderungen sind unverzüglich unter Benutzung des Datenänderungscodes in den dafür vorgesehenen Eingabemasken nachzutragen.
Ferner unterhält das Unternehmen für jeden Spielteilnehmer ein Kundenkonto (Spieleinsatz- und Gewinnkonto). Die Zuordnung zum Spielteilnehmer erfolgt durch die vom Unternehmen vergebene Kunden-ID-Nummer.

Es ist davon auszugehen, dass der Spielteilnehmer nach der ersten Spielteilnahme bzw. der Anmeldung jede weitere Teilnahme lediglich mit seinem Anmelde-Passwort einleiten und durchführen kann, da die o.g. personenbezogenen Daten mit der ersten Anmeldung als Bestandsdaten gespeichert werden und bei jedem neuerlichen Spiel deren Zuordnung zum Anmelde-Passwort erfolgt. Diese personenbezogenen Daten sind für die Begründung, inhaltliche Ausgestaltung oder Änderung des Vertragsverhältnisses über die Nutzung des Telediensten notwendig und sind somit nach dem TDDSG zu bewerten. Ferner werden diese Bestandsdaten für Abrechnungszwecke (Gebühr und ggf. Gewinnausschüttung) mit den Nutzungsdaten kombiniert.

In den zu prüfenden IntTB wurde die mögliche Verarbeitung aller o.g. personenbezogenen Daten für die Markt- und Kundenanalyse angekündigt. Mit einer Einwilligung in den Vertrag und mithin Anerkennung der IntTB würde der Nutzer die Verarbeitung seiner personenbezogenen Daten über das im § 6 Abs. 3 TDDSG genannte Maß hinaus legitimieren. Dass die Einwilligung „an der Erforderlichkeit der Daten für den jeweiligen Zweck“ zu messen ist (so der Berliner LfD, Tätigkeitsbericht 1998, S. 169 und Bericht der Bundesregierung zur Umsetzung des IuKDG, BT-Drs. 14/1191, S. 16) ist jedenfalls dann gegeben, wenn für die Einwilligung auch die Rechtmäßigkeitsvoraussetzungen des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (AGBG) maßgebend sind. Dies ist hier der Fall, da die IntTB Allgemeine Geschäftsbedingungen im Sinne des § 1 AGBG bzw. seit dem Gesetz zur Modernisierung des Schuldrechts vom 26.11.2001 Allgemeine Geschäftsbedingungen im Sinne der §§ 305 ff. Bürgerliches Gesetzbuch (BGB) sind.
Die Verarbeitung der o.g. Daten (Name, Vorname, Aliasname, vollständige Adresse, Geburtsdatum, E-Mail-Adresse, Bankverbindung) dienen ausschließlich zum Zwecke der Teilnahme des Nutzers an den Wettrunden und der entsprechenden finanziellen Abrechnung. Ein anderer Zweck ist nicht erkennbar. Auch die herkömmliche (schriftliche) Teilnahme an Lotterie und Wettrunden erfordert keine Verarbeitung personenbezogener Daten für eine Markt- und Kundenanalyse. Das herkömmliche Verfahren ermöglicht im Gegenteil eine anonyme Spielteilnahme. Mithin ist es für den Zweck des Vertrages nicht erforderlich, eine Markt- und Kundenanalyse mit personenbezogenen Daten durchzuführen.
Gemäß § 307 BGB sind Bestimmungen in Allgemeinen Geschäftsbedingungen unwirksam, wenn sie den Vertragspartner des Verwenders entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Eine unangemessene Benachteiligung ist im Zweifel anzunehmen, wenn eine Bestimmung

- mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist, oder
- wesentliche Rechte oder Pflichten, die sich aus der Natur des Vertrags ergeben, so einschränkt, dass die Erreichung des Vertragszwecks gefährdet ist.

Die gesetzliche Regelung, von deren Grundgedanken in den IntTB abgewichen werden sollte, ist § 6 Abs. 3 TDDSG. Gemäß dieser Regelung darf der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im

Rahmen der Unterrichtung nach § 4 Abs. 1 TDDSG hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Der wesendliche Grundgedanke des § 6 Abs. 3 TDDSG ist also die Trennung von personenbezogenen und nicht-personenbezogene Daten.

Im Ergebnis wurde übereinstimmend mit dem Unternehmen festgelegt, dass eine Markt- und Kundenanalyse ausschließlich mit anonymen Daten erfolgen soll. Alternativ wurde dem Unternehmen vorgeschlagen, die Einwilligung für die Markt- und Kundenanalyse unter Bezugnahme der o.g. personenbezogenen Daten gesondert abzufragen. Mit dem Angebot einer zweiten, gesonderten Einwilligung würde dem Kopplungsverbot gemäß § 3 Abs. 4 TDDSG Rechnung getragen werden.

4.1.8 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 2002/2003 trotz ständig wachsender Mitgliederzahlen auf gleichem Niveau bewegt. 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 § 34 BDSG bzw. § 4 Abs. 7 TDDSG,
- neue AGB nebst Einwilligungserklärung,
- Identitätsmissbrauch,
- Identifizierung der Mitglieder und das
- Verifizierte Rechte Inhaber Programm (VeRI) mit Hilfe dessen eBay die Inhaber von Marken- und Schutzrechten unterstützen will.

Zu den anspruchsvolleren Fällen zählte die Prüfung eines Auskunftsanspruches nach § 34 BDSG bzw. § 4 Abs. 7 TDDSG.
Im Rahmen der Bewertung eines Auskunftsersuchens war die Frage zu klären, ob der Auskunftsanspruch nach dem TDDSG abschließend geregelt ist, so dass kein Raum für

eine Anwendung der § 34 Abs. 4 geltenden Ausnahmen des § 33 Abs. 2 BDSG besteht, oder ob das BDSG als allgemeine Norm ergänzend zur Anwendung kommen kann.
Der Petent wollte die Entscheidung von eBay überprüft wissen. Das Unternehmen habe seiner Ansicht nach sein Auskunftsersuchen zu unrecht nur unvollständig beantwortet. Zur Begründung hatte sich eBay gegenüber der Aufsichtsbehörde auf § 34 Abs. 4 BDSG i.V.m. § 33 Abs. 2 BDSG berufen. Die Aufsichtsbehörde nahm diesen Fall zum Anlass, das Verhältnis zwischen dem Auskunftsanspruch nach § 34 BDSG und nach § 4 Abs. 7 TDDSG grundsätzlich zu bewerten.

Aus den nachstehenden Gründen ist die Aufsichtsbehörde der Auffassung, dass der Auskunftsanspruch im TDDSG nicht abschließend geregelt ist und das im BDSG geregelte Auskunftsrecht ergänzend über § 1 Abs. 2 TDDSG zur Anwendung kommt.
Soweit das BDSG nicht durch dienstespezifische Regelungen - wie etwa die des TDDSG - verdrängt wird (§ 1 Abs. 3 BDSG) ist es für alle privaten Informations- und Kommunikationsdienste generell mit seinen Regelungen für den nicht-öffentlichen Bereich einschlägig. Nach § 1 Abs. 2 TDDSG sind „die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden“, d.h. dass das TDDSG die Bestimmungen des allgemeinen Datenschutzrechts nur insoweit verdrängt, wie es eine <u>besondere</u> Regelung enthält.
Dies ist bei § 4 Abs. 7 TDDSG aber nur hinsichtlich der <u>Art und Weise</u> der Auskunftserteilung der Fall.
Danach hat der Diensteanbieter dem Nutzer auf Verlangen <u>unentgeltlich</u> und <u>unverzüglich</u> Auskunft über die zu seiner <u>Person</u> oder zu seinem <u>Pseudonym</u> gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch <u>elektronisch</u> erteilt werden. Demgegenüber ist die Auskunft nach § 34 Abs. 3 BDSG i.d.R. schriftlich zu erteilen und es kann ggf. ein Entgelt erhoben werden (§ 34 Abs. 5 BDSG)
In der amtlichen Begründung zu § 4 Abs. 7 Satz 1 TDDSG heißt es: „Der bisherige § 7 <u>erweitert</u> das nach dem BDSG geltende Auskunftsrecht in ein Recht auf <u>elektronische Einsichtnahme</u>. Die Neufassung gestaltet diese Bestimmung in einer mit Blick auf die Entwicklung der Teledienste praktikableren Form.[1]“
Die alte Fassung des TDDSG regelte in § 7, dass das Auskunftsrecht im Falle einer kurzfristigen Speicherung im Sinne des § 33 Abs. 2 Nr. 5 des BDSG nicht nach § 34 Abs. 4 BDSG ausgeschlossen ist. Das Gesetz ging offenkundig von der Anwendung des BDSG aus. Auch die o.g. Auszüge aus der Begründung legen diesen Schluss nahe. Mit der Änderung des BDSG 2001 ist § 33 Abs. 2 Nr. 5 a.F. gestrichen worden. Mithin ist eine ausdrückliche Erwähnung der Norm mit der Folge, dass eine Auskunftserteilung doch entge-

[1] BT-Drs. 14/6098

gen § 34 Abs. 4 BDSG zu erfolgen hat, entbehrlich geworden. Es ist nicht ersichtlich, dass mit dieser redaktionellen Änderung einhergehen sollte, dass der heute im TDDSG geregelte Auskunftsanspruch nicht mehr über § 34 Abs. 4 BDSG Einschränkungen erfahren kann.

Der Kommentarliteratur zum TDDSG a.F. ist weiterhin zu entnehmen, dass das TDDSG zwar in § 7 (nachfolgend in diesem Absatz jeweils a.F.) eine eigenständige Auskunftsregelung enthält, die mangels völliger Deckungsgleichheit jedoch die allgemeine Regelung des § 34 BDSG nicht generell verdrängt.[2] Nicht ausgeschlossen werden damit die in § 34 Abs. 1 BDSG in die Auskunftspflicht einbezogenen Angaben. Mitzuteilen sind auch gespeicherte Angaben, die sich auf die Herkunft und Empfänger der Daten beziehen, der Zweck der Speicherung, Personen und Stellen, an die die Daten regelmäßig übermittelt werden.[3] Wenn aber der Anspruch hinsichtlich seines Umfangs über § 34 Abs. 1 BDSG erweitert wird, müssen auch die weiteren Regelungen der Norm gelten. Erst recht lässt die in § 7 Satz 3 TDDSG verfügte Nicht-Anwendung der für die Auskunft nach § 34 BDSG a.F. geltenden Ausnahmetatbestände bei kurzfristiger Speicherung (§ 33 Abs. 2 Nr. 5 BDSG a.F.) für das Auskunftsrecht nach § 7 TDDSG den Umkehrschluss zu, dass die übrigen das Auskunftsrecht einschränkenden Regelungen des BDSG auch im Rahmen des § 7 TDDSG zur Anwendung kommen sollen. Danach gilt die in § 34 Abs. 4 BDSG getroffene Verweisung auf die Ausnahmetatbestände nach § 33 Abs. 2 Nr. 2 bis 4 und Nr. 6 auch im Rahmen des § 7 TDDSG.[4]

Zur Unterstützung des Auskunftsersuchens führte der Petent gegenüber der Aufsichtsbehörde an, dass Art. 13 EG-Datenschutzrichtlinie nur Ausnahmen vom Auskunftsanspruch vorsieht, die im Interesse des Staates liegen, nicht aber im Interesse privater Unternehmen. § 34 BDSG sei demnach richtlinienkonform auszulegen. Insbesondere seien die Ausnahmebestimmungen des § 34 Abs. 4 i.V.m. § 33 Abs. 2 BDSG eng auszulegen, da die Richtlinie, die gegenüber dem nationalen Recht Anwendungsvorrang habe, Ausnahmen zugunsten von Privatunternehmen nicht erlaube.
Dies gelte ebenso im Hinblick auf Art. 8 Datenschutzkonvention des Europarates (DSK), der ebenfalls einen einschränkungslosen Auskunftsanspruch einräume.
Im Ergebnis der Prüfung der Aufsichtsbehörde erlauben sowohl die EG-DSRL als auch die DSK Einschränkungen des Auskunftsanspruchs auch zugunsten der Interessen privater Unternehmen:

---

[2] Gola/Müthlein: TDG/TDDSG Kommentierung für die Praxis, Datakontext-Fachverlag GmbH, 2000, 1.Auflage, § 1 RdNr. 5.1

[3] Gola/Müthlein: a.a.O. § 7 RdNr. 3.2

[4] Gola/Müthlein: a.a.O. § 7 RdNr. 4.1

Nach Art. 13 Abs. 1 lit. g) EG-DSRL können die Mitgliedstaaten Rechtsvorschriften erlassen, die die Auskunftspflichten gemäß Art. 12 beschränken, sofern dies notwendig ist für den Schutz der betroffenen Personen und der Rechte und Freiheiten anderer Personen (in der engl. Fassung: “to safeguard the protection of the data subject or of the rights and freedoms of **others**.”). Aus den Erwägungsgründen und der Begründung der Richtlinie ergibt sich, dass Einschränkungen des Auskunftsanspruchs auch im Interesse des für die Verarbeitung Verantwortlichen möglich sind. In Deutschland fand dieser, von der Richtlinie ausdrücklich eröffnete, Spielraum seinen Ausfluss in den Regelungen des § 34 Abs. 4 BDSG. Diese Vorschrift ist richtlinienkonform gestaltet, insoweit hat die Richtlinie keinen Anwendungsvorrang. Die Hinzuziehung der DSK führt zu keinem anderen Ergebnis.

Ob der Auskunftsanspruch nach dem TDDSG abschließend sei oder das im BDSG geregelte Auskunftsrecht ergänzend über § 1 Abs. 2 TDDSG zur Anwendung kommt, wurde im Rahmen des Düsseldorfer Kreises kontrovers diskutiert. Eine einheitliche Rechtsauffassung konnte nicht gefunden werden.
Der Wortlaut des § 4 Abs. 7 TDDSG lässt offenbar unterschiedliche Interpretationen des Umfangs des Auskunftsanspruchs zu. Deshalb sollte die Neuordnung des IuK-Datenschutzes im Bundesrecht als Gelegenheit wahrgenommen werden, eine Klarstellung im geplanten Telemediengesetz zu erreichen.

4.2 Schwerpunkte aus Beschwerden

4.2.1 Unerwünschte Werbung durch Internetmedizinvertreiber

Zwei Beschwerdeführer hatten ein Werbeschreiben über schnelle Hilfe bei Prostata-Beschwerden erhalten. In diesem Schreiben wurden speziell Männer über 50 Jahre angesprochen. Da beide Petenten dieser Alterskategorie angehörten, wunderte man sich darüber, woher der Vertreiber das jeweilige Geburtsdatum kenne.
Die Beschwerdeführer hatten sich auch schon selbst an das Unternehmen gewandt und darum gebeten, mitzuteilen, woher die Daten stammen und dass eine sofortige Löschung derselben erfolgen solle.
Eine Antwort erhielten die Beschwerdeführer nicht. Die Firma selbst war anfangs auch nicht bereit, eine schriftliche Stellungnahme abzugeben.
Nachfragen bei dem entsprechenden Gewerbeamt konnten leider auch nicht zum Erfolg führen. Das Unternehmen war nicht gemeldet. Unter der angegebenen Telefonnummer war lediglich ein Callcenter geschaltet und dort war man nicht in der Lage, auf die Fragen eine Antwort zu erteilen.

Jedoch gelang es dann über eine Mailadresse dem Vertretungsberechtigten der mit Hauptsitz in den USA ansässigen Firma das Problem zu erläutern und man teilte dann mit, dass die Adressen der Beschwerdeführer von einem deutschen Adresshändler bezogen wurden. Das Alter der Betroffenen ist dabei nicht bekannt. Auf das Alter würde geschlossen über die so genannte Vornamenanalyse oder über die Adressliste. Würden beispielsweise Adressen eines Versandhandels für konservative Herrenmode angemietet, wäre wahrscheinlich, dass die Käufer älter als 50 Jahre sind.
Aufgrund ergänzender Hinweise konnte dann mitgeteilt werden, dass die angemieteten Adressen von einer GmbH in Deutschland stammen. Vom Datenschutzbeauftragten dieses Unternehmens wurden zur Klärung der Angelegenheit die Werbecodierung und eine Kopie des Mailings benötigt, um klären zu können, ob die Adressen aus der vorhandenen Datenbank oder aus einem anderen Adressbestand stammen.
Letztendlich wurde nur ein Beschwerdeführer in der Datei gefunden und sofort gesperrt. Trotzdem wurden beide Beschwerdeführer auf die Sperrliste gesetzt.
Abschließend erwähnt sei noch, dass das Unternehmen mehrere Behörden in den Bundesländern beschäftigt hat.

4.2.2 Gewinnspiel zum Wahlverhalten von Bürgern

Durch ein Institut wurde in Vorbereitung der Bundestagswahl ein Gewinnspiel in Form einer Postkartensendung durchgeführt. Hier wurde nicht nur das Geburtsdatum und die Telefonnummer, sondern auf der Rückseite auch die politische Meinung der Befragten abverlangt.
In diesem Fall wurden Daten nach § 3 Abs. 9 BDSG verarbeitet. Eine Verarbeitung derartiger Daten ist jedoch nur unter besonderen Voraussetzungen (§ 4 a Abs. 3 und § 28 Abs. 6 BDSG) zulässig.
Die Meinungsumfrage wurde in diesem Fall auf einer beidseitig bedruckten Postkarte durchgeführt.
Es bestand somit nicht die Möglichkeit einer anonymen Auswertung. Ebenso war eine Trennung der politischen Meinungsumfrage und der personenbezogenen Daten nicht möglich.
Bestätigt wurde durch das Unternehmen, dass die Adressen nicht weiter genutzt und auch nicht weiter gegeben werden. Nach dieser Aktion seien diese Postkarten vernichtet worden.
Der Vertreter des Unternehmens wurde auf die datenschutzrechtlichen Bestimmungen in diesem Fall nochmals hingewiesen.

4.2.3 Verletzung des Bankgeheimnisses

Eine Beschwerdeführerin beklagte sich darüber, dass ihre Bank die Jahresabrechnung ihres Bausparvertrages an die Anschrift des geschiedenen Ehemannes verschickt hatte, was wohl auch schon im Jahr vorher passiert war. Hierbei muss erwähnt werden, dass beide Personen in der gleichen Strasse, aber unter einer unterschiedlichen Hausnummer wohnen.
Bereits damals wurde der Petentin zugesichert, dass dies nicht noch einmal passieren würde. Da zu diesem Zeitpunkt das Ehescheidungsverfahren anhängig war, lag die Übermittlung der Kontostände an den Ehemann nicht im Interesse der Petentin. Befürchtet wurde zum damaligen Zeitpunkt auch, dass eine Unterhaltsklage erfolgen könne.
Die Bank räumte einen vermeidbaren Bearbeitungsfehler ein, dessen Ursache auch festgestellt wurde. In dem bestehenden Bausparvertrag der Beschwerdeführerin war als Begünstigter am Anfang der Ehemann eingetragen. Nach der Trennung wurden weiterhin beide Postanschriften geführt und erst nach der Scheidung wurde der Begünstigte gestrichen. Irrtümlicherweise wurde jedoch der Kontoinhaberin die Postanschrift des geschiedenen Ehemannes zugeordnet. Die Verwechslung wurde dadurch begünstigt, dass die Wohnanschriften bis auf die unterschiedlichen Hausnummern identisch waren.
Der Vorfall wurde intern ausgewertet und die notwendige Korrektur wurde vorgenommen, so dass eine Wiederholung ausgeschlossen werden kann.
Durch die Bank wurde eingeräumt, dass die falsche Zuordnung durch höhere Sorgfalt hätte vermieden werden können. Gleichzeitig wurde versichert, dass die Sensibilität der Bearbeitung vermeintlich einfacher und formaler Vorgänge inzwischen erhöht worden sei.
Gleichzeitig wurde durch die Bank ein persönliches Entschuldigungsschreiben an die Petentin gesandt.

4.2.4 Videoüberwachung eines Freizeitbades

Ein Beschwerdeführer gab an, dass die Videoüberwachung eines Freizeitbades ohne Kennzeichnung erfolge.
Daraufhin wurde dem Betreiber mitgeteilt, dass eine Videoüberwachung öffentlich zugänglicher Räume u.a. zulässig ist, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (§ 6b Abs. 1 Nr. 3 BDSG). Die in § 6b Abs. 2 BDSG geforderte Kenntlichmachung der Videoüberwachung erfolgt in der Regel durch ein Hinweisschild, welches gut erkennbar (in Augenhöhe) auf die Videoüberwa-

chung hinweist. Der Betreiber wurde gebeten dazu Stellung zu nehmen.
Der Geschäftsführer der Anlage teilte hierauf mit, dass sicherheitsrelevante Bereiche der Schwimmhalle, Umkleidebereiche (ohne Umkleidekabinen), die Riesenrutsche und das Außenbecken videoüberwacht werden. Gefährdete Bereiche, in denen Personal nicht ständig zugegen ist, werden somit auch im Interesse der Gäste videoüberwacht. Im Mittelpunkt stehen hierbei u. a. die Verhinderung von Diebstählen und sexuelle Übergriffe sowie die Einhaltung der Badeordnung bzw. unfallrechtliche Aspekte, insbesondere im Rutschenbereich.
Unser Hinweis wurde zum Anlass genommen, im unmittelbaren Kassenbereich ein Hinweisschild zur Videoüberwachung der Anlage anzubringen.

4.2.5 Chipkartensystem einer Klinik

Durch den Betriebsrat einer Klinik wurde angefragt, ob das dort eingesetzte Chipkartensystem mit den datenschutzrechtlichen Bestimmungen in Einklang steht.
Seitens der Klinik wurde ausgeführt, dass es sich um ein Sicherheitssystem handelt, dass die Schließvorgänge im Schloss und auf der Karte protokollieren könne, um jeglichem Missbrauch vorzubeugen.
Da die Klinik u. a. im Bereich der Indikationen Sucht und Psychosomatik arbeite, müssten diese Vorkehrungen zum Schutz vor Einsicht Unbefugter in die Patientenakten getroffen werden. Ferner wurde mitgeteilt, dass jeder Mitarbeiter über das Schließsystem informiert worden sei und dies auch bei der Arbeitsaufnahme und Entgegennahme der Karten akzeptiert habe.
In rechtlicher Hinsicht sei die Datenerhebung bereits nach § 28 Abs. 1 und 2 BDSG zulässig, da auch vom Geschäftszweck der Klinik der Schutz der Patienten, insbesondere der patientenbezogenen Daten, umfasst sei. Darüber hinaus sei das System seit über 7 Jahren in der Klinik integriert und es habe keine Beanstandungen gegeben. Aufgrund der langjährigen Nutzung bestehe eine Regelungsabrede mit dem Betriebsrat, der das System ebenfalls nicht beanstandet habe.
Da es sich bei den Daten um besonders schutzwürdige Daten handelt, sind höhere Anforderungen an die zu treffenden Schutzmaßnahmen, insbesondere auch für die Kontrolle von Missbrauchsfällen und Verstößen gegen Sicherheitsvorschriften zu treffen. Insofern ist ein System, das die Schließvorgänge im Schloss und auf der Karte protokolliert zur Wahrung der berechtigten Interessen der Klinik (§ 28 Abs. 1 Nr. 2 BDSG) erforderlich. Schutzwürdige Belange der Mitarbeiter waren nicht verletzt, da diese mit dem System und den Sicherheitsvorschriften vertraut waren und sind.

Gegen das Chipkartensystem bestanden aus datenschutzrechtlicher Sicht keine Bedenken.
Inwieweit Kündigungen, die auf den Erkenntnissen aus der Auswertung der Schließvorgänge beruhen, einerarbeitsgerichtlichen Nachprüfung standhalten, konnte durch die Aufsichtsbehörde nicht beurteilt werden.

4.2.6 Aushang an einer Bushaltestelle

In diesem Fall wurde an einer Bekanntmachungstafel einer Bushaltestelle in einer Gemeinde ein Aushang angebracht, wo auf einer Arbeitsunfähigkeitsbescheinigung eine Mitteilung über die Suche von Pauschalkräften für eine Reinigungsfirma erfolgte.
Seitens des Unternehmens wurde hier die Schuld auf einen nicht mehr im Unternehmen tätigen Auszubildenden abgewälzt, obwohl seitens des Unternehmens nicht ausgeschlossen werden konnte, dass die Räumlichkeiten nicht rund um die Uhr besetzt sind.
Das Unternehmen wurde auf die nach § 9 BDSG notwendigen Maßnahmen zur Gewährleistung der Datensicherheit hingewiesen und auch auf Maßnahmen, die z. B. eine Möglichkeit des Zuganges zu personenbezogenen Daten durch nichtberechtigte Personen auszuschließen.
Wenn daneben ein Fehlverhalten eines Beschäftigten festgestellt werden kann, ist dies gegebenenfalls arbeitsrechtlich zu würdigen. Verfehlungen Einzelner können darüber hinaus nach den §§ 43, 44 BDSG (Bußgeldvorschriften, Strafvorschriften) unter den dort genannten Voraussetzungen geahndet werden.
Des Weiteren wurde die betreffende Firma darauf aufmerksam gemacht, dass sie unter anderem dafür Sorge zu tragen habe, dass die Räume beim Verlassen verschlossen sind, Personalakten in verschließbaren Schränken aufbewahrt und die Mitarbeiter auf das Datengeheimnis nach § 5 BDSG verpflichtet werden. Diese Verpflichtung gilt für eine automatisierte sowie nicht - automatisierte Verarbeitung personenbezogener Daten. Ein Muster einer Verpflichtungserklärung wurde dem Unternehmen zur Verfügung gestellt.

4.2.7 Unterlassene Auskunft über die Speicherung von personenbezogenen Daten bei einem Möbelunternehmen

Der Beschwerdeführer hatte von dem Unternehmen persönlich adressierte Werbepost erhalten und erkundigte sich, welche Daten und zu welchem Zweck über ihn gespeichert sind. Gleichfalls wollte er wissen, woher die Daten stammen und an wen sie ggf. weitergeleitet wurden.

Dem Petenten wurde lediglich mitgeteilt, dass die Daten aus dem System gelöscht worden seien und deshalb die gewünschte Auskunft nicht erteilt werden kann. Wie man an die Daten gekommen sei, sei nicht mehr nachvollziehbar.
Die Nachfrage bei dem Unternehmen ergab, dass die Quelle der zu Werbezwecken verwendeten Daten eine dafür bekannte Firma sei.
Das Möbelunternehmen sicherte dem Beschwerdeführer zu, ihn in die hauseigene „Robinson-Liste“ aufzunehmen, um jegliche Werbeaktionen zukünftig zu unterbinden. Ebenfalls bot das Unternehmen an, die Unterlassung des Gebrauches der Daten des Petenten an den Adresshandel weiterzuleiten.
Gleichzeitig wurde aber mitgeteilt, dass die durchgeführten Werbemaßnahmen eine Vorlaufzeit von 5-6 Wochen haben und so sei nicht auszuschließen, dass in diesem Zeitraum noch Werbepost versandt werden könnte.

4.2.8 Unerwünschte Werbung durch eine Kfz-Versicherung

Der Petent beschwerte sich über die Zusendung unerwünschter Werbepost, obwohl keine Kundenbindung mehr bestand. Die im Rahmen einer Werbeabfrage eingegebenen Daten seien wohl nicht gelöscht worden. In diesem Zusammenhang habe der Beschwerdeführer wohl eine Kundennummer erhalten, ohne dass ein Vertragsverhältnis bestanden habe.
Die von der Aufsichtsbehörde um Stellungnahme aufgeforderte Kfz-Versicherung hat hierzu mitgeteilt, der Petent habe über ein Portal eine Prämienberechnung für eine Kfz-Versicherung durchführen lassen und sich dementsprechend mit der Weitergabe und Speicherung der Daten an Finanzdienstleistungsunternehmen bis auf Widerruf auf elektronischem Wege einverstanden erklärt. Die Anerkennung der angeführten AGB, die die Erhebung, Speicherung und Übermittlung der Kundendaten regeln, sei damals erfolgt. Eine Löschung der Daten sei erfolgt, als sich der Beschwerdeführer nicht für das Versicherungsangebot entschieden habe. Durch das Unternehmen wurde versichert, dass diese Löschung sofort nach der Aufforderung durch den Petenten erfolgt sei.
Zwecks Überprüfung wurde der Weg einer Vergleichsberechnung bei dem Portal des Finanzdienstleisters nachvollzogen. Dabei wurde festgestellt, dass bis zu einem Stand von 97 % der Berechnung keine personenbezogenen Daten abgefragt werden. Ab dann werden jedoch für die Anzeige der günstigsten Versicherung wahlweise zwei Einwilligungen erbeten.
Bei der ersten Option ist die Auswertung kostenlos und der Nutzer erhält ein unverbindliches Angebot der entsprechenden Versicherung per E-Mail oder per Post. Der Nutzer erklärt sich mit der Weiterleitung seiner Daten an die Versicherung einverstanden.

Mit der zweiten Option ist die Verpflichtung des Nutzers zur Zahlung von 10 Euro für die Auswertung verbunden. Die Daten würden in diesem Fall vom Finanzdienstleister nicht weitergegeben werden.
Mit dem Angebot der zweiten Wahlmöglichkeit wird dem so genannten Kopplungsverbot gemäß § 3 Abs. 4 des Gesetzes über den Datenschutz bei Telediensten (TDDSG) Rechnung getragen.
Das Kopplungsverbot besagt, dass der Anbieter die Erbringung von Diensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen darf. Die Abgabe der entsprechenden Einverständniserklärung kann nach § 3 Abs. 3 TDDSG auch auf elektronischem Wege erfolgen.
Hinter den beiden genannten Wahlmöglichkeiten ist jeweils ein Pop - Up mit entsprechenden Erklärungen platziert. Bei der ersten Wahlmöglichkeit wird der Nutzer u. a. darüber informiert, dass er sich durch die Bestätigung der Eingaben mit Absender der Suchanfrage mit der Erhebung, Verarbeitung und Nutzung der eingegebenen Daten einverstanden erklärt, auch zum Zwecke der Beratung, der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des Dienstes.
Sofern man sich wirksam mit der ersten Option einverstanden erklärt hat, kann auch kein Verstoß gegen datenschutzrechtliche Bestimmungen erkannt werden.

4.2.9 Verkauf von Bewerbungsmappen über eBay

Die Verbraucher-Zentrale NRW e.V. informierte das Ministerium des Innern über ein Angebot auf dem Deutschen eBay-Marktplatz 250 Bewerbungsmappen unterschiedlicher Berufe zu versteigern. Gemäß dem Angebot seien sämtliche Bewerbungsmappen noch im verschlossenen Umschlag und ungelesen gewesen. Bei manchen könne sogar die Briefmarke noch einmal verwendet werden. Ferner seien 1000 ungelesene, ungeöffnete Bewerbungsmappen auf Anfrage erhältlich.

Dem Hinweis der Verbraucher-Zentrale NRW e.V. folgend wurde eBay von der Aufsichtsbehörde aufgefordert das o.g. Angebot unverzüglich zu löschen, um einen möglichen Verstoß gegen datenschutzrechtliche Bestimmungen zu verhindern. Eine entsprechende Löschung der Auktion wurde daraufhin umgehend von eBay vorgenommen.

Die Aufsichtsbehörde stellte bei der Staatsanwaltschaft Potsdam Strafanzeige gemäß § 44 Abs. 2 Bundesdatenschutzgesetz (BDSG) wegen eines möglichen Verstoßes gegen § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 1 BDSG gegen das eBay-Mitglied. eBay wirkte insoweit

an der Aufklärung des Sachverhaltes mit, als der Aufsichtsbehörde die notwendigen personenbezogenen Daten übermittelt wurden.

Gemäß § 43 Abs. 2 Nr. 1 BDSG handelt ordnungswidrig, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. Gemäß § 44 Abs. 1 BDSG wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

Dem Angebot bei eBay ließ sich nicht entnehmen, dass die Firma die Bewerbungsmappen mit Einwilligung der/aller Betroffenen zum Verkauf angeboten hat. Es lag daher der Verdacht nahe, dass sich die Firma bereits unter Missachtung datenschutzrechtlicher Bestimmungen die Bewerbungsmappen beschafft hat, da diese üblicherweise nur zum Zwecke der Bewerberauswahl an den entsprechenden Adressat versandt werden.
Zum Anwendungsbereich des BDSG ist zu bemerken, dass bereits jede strukturierte Sammlung personenbezogener Daten den Dateibegriff des Gesetzes (§ 3 Abs. 2 Satz 2 BDSG) erfüllt. Eine Sammlung von Umschlägen mit Absender- und Adressangaben kann somit als nicht automatisierte Datei angesehen werden. Dem Angebot bei eBay kann überdies entnommen werden, dass eine Sortierung nach Berufssparten möglich ist.
Die Erfüllung weiterer Straftatbestände im Zusammenhang mit der Beschaffung der Bewerbungsmappen konnte nicht ausgeschlossen werden. Über die Einleitung eines Ermittlungsverfahrens und ggf. den Abschluss eines nachfolgenden Strafverfahrens liegen der Aufsichtsbehörde keine Erkenntnisse vor.

4.2.10 Internetfahndung eines Unternehmens (Verkehrsbetrieb)

Ein Verkehrsbetrieb suchte über ein Internetportal mit Hilfe von Fotos aus der Aufzeichnung einer Videokamera zwei offensichtlich jugendliche Personen. Die Aufnahmen entstanden nachdem mindestens einer der Jugendlichen mutmaßlich den Tatbestand einer Sachbeschädigung in einem öffentlichen Verkehrsmittel erfüllt haben soll.
Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich befand sich bei der Bewertung des Falls im Spannungsfeld zwischen dem Schutz des allgemeinen Persönlichkeitsrechts und dem Schutz des Eigentums. Im Abwägungsprozess sind die nachfolgend aufgeführten Gesichtspunkte eingeflossen:

Die von dem Verkehrsbetrieb veranlasste Einstellung der Fotos mit dem Untertitel „Wer kennt diese Personen?“ hat den Charakter einer Öffentlichkeitsfahndung. Zumal auch die Öffentlichkeit aufgefordert wird, die abgebildeten Personen zu erkennen. Dass die Augenpartien mit einem Balken unkenntlich gemacht wurden, erschwerte zwar den Personenbezug, schloss ihn jedoch nicht aus. Der von dem Unternehmen beabsichtigte Sinn dieser Veröffentlichung war ja gerade die Identifizierung der abgebildeten Personen. Auch die Möglichkeit einer elektronischen Bearbeitung der PDF-Datei am eigenen PC, wie das Vergrößern der farbigen Bilder, war geeignet einen Personenbezug auch anhand der Kleidung herzustellen. Die Polizei fahndet zuweilen ausschließlich mit Kleidungsstücken.

Die Veranlassung einer Öffentlichkeitsfahndung ist jedoch ausschließlich Staatsanwaltschaften oder Gerichten unter engen Voraussetzungen (§ 131 Abs. 3 Strafprozessordnung StPO) vorbehalten. Das Unternehmen hatte dazu keine Befugnis. Zumal eine Internetfahndung, wie vom Unternehmen veranlasst, eine qualitativ höhere Eingriffsqualität hat als Fahndung in Funk, Fernsehen oder Printmedien. Es handelt sich beim Internet um einen sehr großen, räumlich nicht eingeschränkten Verbreitungsradius für Fahndungsinformationen. Durch die dauerhafte Abrufbarkeit wird die Einwirkung auf die Persönlichkeitssphäre des Betroffenen im Vergleich zu Presse- und Fernsehpublikationen gesteigert. Hierbei ist insbesondere der Grundsatz der Verhältnismäßigkeit zu beachten. Das Internet soll nur dann für die Fahndung genutzt werden, wenn andere, den Betroffenen weniger beeinträchtigende Fahndungsmittel nicht Erfolg versprechend erscheinen und die Inanspruchnahme des Fahndungsmittels nicht außer Verhältnis zur Bedeutung der Sache steht, also in der Regel nur bei Straftaten von erheblicher Bedeutung. Ferner ist anzustreben, dass bei der Fahndung nach bekannten Straftätern ein internationaler Haftbefehl vorliegt.

Ein weiterer Aspekt der betrachtet werden musste, war die offensichtliche Minderjährigkeit der abgebildeten Personen. Zum Schutz von jungen Tätern und hinsichtlich einer erfolgreichen Resozialisierung werden Jugendstrafverfahren Kraft Gesetz unter Ausschluss der Öffentlichkeit abgehalten (§ 48 Jugendgerichtsgesetz). Vor diesem Hintergrund sind insbesondere an eine Öffentlichkeitsfahndung nach Minderjährigen besonders enge Voraussetzungen zu knüpfen, die in diesem Fall nicht vorlagen.

Aus den oben darstellten Gründen war ein Personenbezug herstellbar und insofern das allgemeine Persönlichkeitsrecht der abgebildeten Jugendlichen verletzt. Die Maßnahme dürfte selbst dann unverhältnismäßig sein, wenn sie von den zuständigen Behörden ver-

anlasst worden wäre, da sie nur ergriffen werden darf, wenn es um die Aufklärung einer Straftat von erheblicher Bedeutung geht (§ 131 Abs. 3 StPO).

Diese Abwägung vorangestellt wurden die Voraussetzungen des § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG), wonach

> *eine Übermittlung zulässig ist, wenn sie 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*,

für nicht gegeben angesehen. Bei einer Veröffentlichung von Daten im Internet müssen zusätzlich die Voraussetzungen der §§ 4b und 4c BDSG erfüllt sein. Diese regeln die Übermittlung personenbezogener Daten ins Ausland sowie an über- und zwischenstaatliche Stellen. Von einer derartigen Prüfung wurde zunächst abgesehen.
Das Unternehmen wurde gemäß § 38 Abs. 5 BDSG aufgefordert, unverzüglich technische oder organisatorische Maßnahmen zu ergreifen, die geeignet sind, den Personenbezug auszuschließen.
Die entsprechenden Maßnahmen wurden daraufhin umgehend veranlasst.

4.3 Einleitung von Ordnungswidrigkeitenverfahren in drei Fällen

4.3.1 Owi-Verfahren gegen eine Facharztpraxis

Ausgangspunkt im ersten Fall war eine Beschwerde eines Petenten, der folgenden Sachverhalt schilderte. Mit einer Überweisung vom Kinderarzt zum Neurologen begab er sich mit seinem Kind in die Praxis, um ein EEG erstellen zu lassen.
Gewisse Zeit später beantragte der Petent bei der privaten Krankenversicherung einen erweiterten Versicherungsschutz für sein Kind. Bei der Prüfung der aus den vergangenen Monaten erstellten Rechnungen an die Krankenkasse, stieß man auf die Inrechnungstellung des Befundberichts der neurologischen Praxis und bat um Aushändigung des Berichtes, da sonst dem Versicherungsantrag nicht stattgegeben würde.
Der Beschwerdeführer bat nun mehrmals schriftlich in der Praxis um die Aushändigung des Befundberichtes, jedoch leider ohne Reaktion.
Daraufhin wandte sich der Petent an die Aufsichtsbehörde und bat um Unterstützung und Prüfung.
Die Facharztpraxis wurde mehrmals angeschrieben und um Stellungnahme gebeten. Leider ohne Erfolg. Selbst ein Schreiben mit Postzustellungsurkunde und dem ausdrücklichen Hinweis auf die Auskunftspflicht sowie den Bußgeldtatbestand blieb unbeantwortet.

Nach drei Monaten wurde dann eine Anhörung der Ärztin der Facharztpraxis durchgeführt. Gemäß § 55 OWiG wurde ihr die Gelegenheit zur Äußerung zu dem genannten Sachverhalt eingeräumt. Eine Stellungnahme erfolgte auch hier nicht.
Auf Grund dessen erfolgte einen Monat später die Einleitung des Ordnungswidrigkeitenverfahrens gegen § 43 Abs. 1 Nr. 10 Bundesdatenschutzgesetz (BDSG) und § 111 Abs. 1 Ordnungswidrigkeitengesetz (OWiG). Es wurde vorgeworfen, entgegen § 38 Abs. 3 Satz 1 BDSG der Auskunftspflicht gegenüber der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich nicht nachgekommen zu sein. Die Nichterteilung einer Auskunft stellt eine Ordnungswidrigkeit im Sinne des § 43 Abs. 1 Nr. 10 BDSG dar. Außerdem wurde vorgeworfen, entgegen § 111 Abs. 1 OWiG gegenüber der Aufsichtsbehörde keine Angaben zur Person gemacht zu haben.
In diesem Fall sollte erwähnt werden, dass eine Zahlung des Bußgeldes, wenn auch in Raten, erfolgte.

4.3.2 Owi-Verfahren gegen eine Netauskunftei

In dem zweiten Fall wurde die Aufsichtsbehörde durch ein anderes Bundesland darauf aufmerksam gemacht, dass eine Netauskunftei aufgrund eines Umzuges jetzt in Brandenburg tätig sei. Da ein solches Unternehmen nach § 4d BDSG zum Register meldepflichtig ist, wurde das zuständige Gewerbeamt um Auskunft gebeten, ob das Unternehmen entsprechend der gewerberechtlichen Regelungen angemeldet ist. Von dort wurde lediglich die Auskunft erteilt, dass ein Gewerbe Marketing gemeldet sei.
Daraufhin wurde die Betreiberin des Unternehmens angeschrieben und ihr mitgeteilt, dass nach § 4d Abs. 4 Nr. 1 BDSG automatisierte Verarbeitungen personenbezogener Daten zu melden sind. Gleichzeitig wurde ausgeführt, dass über die meldepflichtigen Angaben (§ 4e BDSG) die Aufsichtsbehörde ein Register führt, welches nach § 38 Abs. 2 Satz 2 BDSG von jedem eingesehen werden kann.
Des Weiteren wurde ein Anmeldeformular mitgeschickt und gebeten, dies nach Prüfung ausgefüllt zurückzusenden.
Dieser und auch die darauf folgenden Briefe blieben unbeantwortet. Ein Kontakt über die im Internet angegebene E-Mail-Adresse brachte auch keinen Erfolg.
Demzufolge wurde eine Anhörung durchgeführt und der Betreiberin des Unternehmens angeraten bis zu dem vorgeschriebenen Termin zu antworten, da sonst ein Bußgeldverfahren eingeleitet würde.
Der darauf folgende Bußgeldbescheid wegen Verstoßes gegen § 43 Abs. 1 Nr. 10 BDSG kam von der Post zurück, da es die Geschäftsführerin vorgezogen hatte, den Wohnort zu

wechseln.
Eine erneute Anfrage beim Gewerbeamt ergab, dass die Familie verzogen sei, aber der Eigentümer des Hauses die neue Anschrift habe. So war es möglich, die neue Anschrift zu ermitteln und den Bußgeldbescheid an diese Adresse zu senden.
Eine Reaktion darauf erfolgte nicht, so dass das Verfahren in Vollstreckung ging. Leider endete dieses Vollstreckungsverfahren mit einer Niederschrift über eine fruchtlose Pfändung.
Das Verfahren wurde zwischenzeitlich befristet niedergeschlagen.

4.3.3 Owi-Verfahren gegen ein Adressenhaus

Die Einleitung eines dritten Ordnungswidrigkeitenverfahrens wurde begründet in einer Beschwerde zu einem Adressenhaus, über welches Adressenstämme in CD-Format, CDs mit Emailadressen und Adressen für Telefonmarketing angeboten wurden. Betreiberin dieses Unternehmens war ebenfalls die gleiche Person wie im Fall der unter 4.3.2. berichteten Netauskunftei.
Aus datenschutzrechtlicher Sicht handelte es sich bei dem Geschäftsfeld des Unternehmens offensichtlich um das geschäftsmäßige Erheben personenbezogener Daten zum Zwecke der Übermittlung gemäß § 29 BDSG.
Auch in diesem Fall wurde das Unternehmen aufgefordert, sich zum Register nach § 4d BDSG anzumelden. Nachdem dieses Schreiben unbeantwortet blieb, wurde nochmals auf die Meldepflicht hingewiesen und gleichzeitig darauf aufmerksam gemacht, dass bei Nichtbeantwortung dieses Schreibens ein Ordnungswidrigkeitenverfahren gemäß § 43 Abs. 3 BDSG eingeleitet werden kann.
Dieses Schreiben wurde gleichfalls ignoriert, so dass eine Anhörung gem. § 55 OWiG eingeleitet wurde.
Eine Reaktion der Betreiberin des Adressenhauses gab es nicht. Daraufhin wurde wegen Verstoßes gegen § 4d BDSG i. V. m. § 4e BDSG auf der Grundlage des § 43 BDSG ein Bußgeldbescheid erstellt.

Wie die vorliegenden Bürgerbeschwerden belegten, hatte sich die Betreiberin des Unternehmens nicht nur der behördlichen Kontrolle dauerhaft entzogen, sondern darüber hinaus offensichtlich eine Vielzahl Betroffener in ihrem Recht auf informationelle Selbstbestimmung verletzt.
Angesichts der Bedeutung des Verstoßes gegen die datenschutzrechtlichen Bestimmungen und die mittelbar daraus resultierenden Eingriffe in die Rechte der Betroffenen wurde

seitens der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich die Verhängung eines Bußgeldes für erforderlich gehalten.
In diesem Fall kam die Aufsichtsbehörde zu dem Ergebnis, dass nur eine empfindliche Geldbuße geeignet war, um auch für die Zukunft mit Nachdruck das Unternehmen zur Erfüllung der gesetzlichen Pflichten anzuhalten. Die festgelegte Summe erschien für diesen Zweck angemessen.
Auch dieses Verfahren ging in Vollstreckung, konnte jedoch nur nach einer fruchtlosen Pfändung befristet niedergeschlagen werden.

5 Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden der Länder

5.1 Besondere Beratungsthemen des Düsseldorfer Kreises

5.1.1 Vertragsverletzungsverfahren der EU-Kommission gegen die BRD wegen der Umsetzung der EU-Datenschutzrichtlinie im Hinblick auf die Unabhängigkeit der Aufsichtsbehörden

Die Länder sowie alle Aufsichtsbehörden hatten sich im Jahr 2005 mit der o.g. Thematik auseinander zu setzen. Auch der „Düsseldorfer Kreis“ als Beratungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich hat sich in der November-Sitzung 2005 mit der Problematik befasst.
Ausgangspunkt der Debatte ist die Tatsache, dass die Europäische Kommission im Juli 2005 gegen die Bundesrepublik Deutschland ein Vertragsverletzungsverfahren eingeleitet hat, weil sie die Rechtsauffassung vertritt, dass die Organisation der Aufsichtsbehörden für den nicht-öffentlichen Bereich in allen 16 Bundesländern der Bundesrepublik gegen Art. 28 der EU-Datenschutzrichtlinie verstoße, weil die notwendige völlige Unabhängigkeit der Aufsichtsbehörden nicht gewährleistet sei. Die Aufsichtsbehörden seien deshalb nicht unabhängig, weil sie einer Fach- oder Rechtsaufsicht unterlägen oder in eine Behördenstruktur mit Weisungsrechten eingebunden seien.
Das Verfahren betrifft also nicht nur die Bundesländer, die die Datenschutzaufsicht über den nicht-öffentlichen Bereich wie in Brandenburg den Innenministerien zugeordnet haben, sondern auch die Länder, in denen der öffentliche und nicht-öffentliche Datenschutzaufsichtsbereich von den Landesdatenschutzbeauftragten wahrgenommen wird. Sind diese für beide Bereiche zuständig, unterliegen sie hinsichtlich der Kontrolle des privaten Bereichs je nach Ausgestaltung im jeweiligen Landesrecht einer Rechts- oder Fachaufsicht. Zusätzlich unterfallen sie der Dienstaufsicht. So unterliegt z.B. die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg gem. § 22 Abs. 4 Brandenburgisches Datenschutzgesetz (BbgDSG) der Dienstaufsicht des Präsidenten

des Landtages.

Die Bundesrepublik ist von der Europäischen Kommission aufgefordert worden, zu der von ihr dargelegten Rechtsauffassung Stellung zu nehmen. Die Stellungnahme des Bundesministeriums des Innern ist mit allen 16 Bundesländern abgestimmt worden.

Bisher einhellige Auffassung von Bund und Ländern war, dass die Aufsichtsbehörden ihre Aufgaben in der von Art. 28. Abs. 1 der EU-Datenschutzrichtlinie geforderten völligen Unabhängigkeit wahrnehmen. Sie sind frei von sachfremden Einflüssen und unabhängig von den zu Überprüfenden. In dieser Weise interpretiert die Bundesrepublik Deutschland von Anfang an die EU-Datenschutzrichtlinie. Das Verfahren für die Bundesrepublik Deutschland ist auch deshalb von grundsätzlicher Bedeutung, weil es die organisatorische Umsetzung einer Richtlinie zum Gegenstand hat; sie somit in den Verwaltungsaufbau eines Mitgliedstaates eingreift.

5.1.2 Informationsbeziehungen zwischen Auskunfteien und der Wohnungswirtschaft

Zu der kontroversen Diskussion, inwieweit es zulässig ist, dass Auskunfteien und Warndateien Auskünfte über Mietinteressenten an Vermieter vor Eingehung eines Mietverhältnisses erteilen, hat der „Düsseldorfer Kreis“ einstimmig einen Beschluss gefasst.

> Danach sind aus der Sicht des Datenschutzes auf branchenspezifische Daten beschränkte Auskunftssysteme vorzuziehen, bei denen die Daten gesicherte Rückschlüsse auf Mietausfallrisiken zulassen. Eine uneingeschränkte Auskunft über bei branchenübergreifenden Auskunfteien gespeicherte Daten an potentielle Vermieter ist dagegen unzulässig. Bei der Prüfung, in welchem Umfang nach § 29 BDSG an potentielle Vermieter personenbezogene Daten übermittelt werden dürfen, sind die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung in besonderer Weise zu berücksichtigen. Auskünfte über Eintragungen im Schuldnerverzeichnis sind stets zulässig.
>
> Es bestehen auch Zweifel an der Zulässigkeit einer Beauskunftung auf Grund einer Einwilligung. Entsprechendes gilt auch für das Verlangen gegenüber dem Mietinteressenten auf Vorlage einer Selbstauskunft. (Auszug aus dem Protokoll der Sitzung des Düsseldorfer Kreises am 25./26.November 2004)

5.1.3 Bestellung von Beauftragten für den Datenschutz gem. §§ 4f, 4g BDSG bei Rechtsanwaltskanzleien

Zu dieser Thematik vertritt die Bundesrechtsanwaltskammer die Auffassung, dass es keine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten hinsichtlich mandatsbezogener Daten gebe. Die Kammer geht mit Ausnahme der Beschäftigtendaten davon aus, dass das BDSG auf die Datenverarbeitung in Kanzleien nicht anwendbar sei, da die Bundesrechtsanwaltsordnung (BRAO) ein dem BDSG nach § 1 Abs. 3 Satz 1 BDSG vorgehendes Regelwerk enthalte. Der Struktur des Berufsgeheimnisses, dem Rechtsanwälte unterliegen, werde das BDSG nicht gerecht.

Der „Düsseldorfer Kreis“ vertrat in mehreren Sitzungen innerhalb des Berichtszeitraumes einstimmig die Meinung, dass das BDSG auf Rechtsanwälte auch hinsichtlich mandatsbezogener Daten anwendbar sei. Lediglich soweit bereichsspezifische Datenschutzvorschriften bestehen, treten die entsprechenden Vorschriften des BDSG gem. § 1 Abs. 3 Satz 1 BDSG zurück. Die punktuellen Regelungen in der Bundesrechtsanwaltsordnung (§ 43a Abs. 2 – Schweigepflicht, § 50 – Handakten, §§ 56, 73 – allgemeine Kontrollbefugnisse der Kammern wegen Berufsverstößen) bewirken nicht, dass das BDSG bei der mandatsbezogenen Informationsverarbeitung überhaupt nicht anwendbar ist. Somit sind die Vorschriften für die Notwendigkeit der Bestellung eines Beauftragten für den Datenschutz nach §§ 4f, 4g BDSG auch für Rechtsanwälte anwendbar, und zwar auch hinsichtlich ihrer mandatsbezogenen Informationsverarbeitung.

Die Wahrung des durch § 203 Abs. 1 Nr. 1 StGB strafrechtlich geschützten Berufsgeheimnisses steht der Geltung des BDSG nicht entgegen. § 1 Abs. 3 Satz 2 BDSG bestimmt lediglich, dass die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, unberührt bleibt. Dies bedeutet, dass sie neben den Bestimmungen des BDSG zu beachten sind. Insbesondere gelten die Informationsrechte der Aufsichtsbehörden nach § 38 Abs. 4 BDSG in Verbindung mit § 24 Abs. 6 und 2 BDSG.

Diese Rechtsauffassung des „Düsseldorfer Kreises“ wurde der Bundesrechtsanwaltskammer und den Bundesministerien des Innern und der Justiz übermittelt.

Die Mitglieder des „Düsseldorfer Kreises“ sind sich jedoch darüber einig, dass eine endgültige Klärung der Problematik wahrscheinlich erst durch eine gesetzliche Regelung oder die Änderung des Berufsrechtes erfolgen wird.

5.2 Sitzungen der Arbeitsgruppe „Auskunfteien“

Im Berichtszeitraum fanden 4 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.
Ein besonderer Schwerpunkt in der Arbeit der Arbeitsgruppe waren Gespräche mit Vertretern der Auskunfteien und der Wohnungswirtschaft zur Thematik „Informationsbeziehungen zwischen Wohnungsunternehmen und Auskunfteien“ und deren Rechtsgrundlagen. Die aus den Diskussionen resultierende Beschlusslage des Düsseldorfer Kreises ist bereits in diesem Tätigkeitsbericht unter dem Punkt 5.1.2 dargestellt.

Da die SCHUFA im Berichtszeitraum begonnen hatte Versicherungsunternehmen als B-Vertragspartner zu gewinnen, oblag es der Arbeitsgruppe, die datenschutzrechtliche Zulässigkeit zu bewerten. Ausschlaggebend war zum einen die Frage, ob ein kreditorisches Risiko für die Versicherungsunternehmen überhaupt anzunehmen ist und ob ein Zusammenhang zwischen Bonität und Versicherungsrisiko besteht. Die Vertreter der SCHUFA und der Aufsichtsbehörden haben dazu bis dato gegensätzliche Auffassungen.

Ausblick:
Die Arbeitsgruppe hat sich künftig u.a. mit dem gesetzlichen Regelungsbedarf bei Auskunfteien zu befassen. Ausgangspunkt ist 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. Deshalb forderte der Deutsche Bundestag die Bundesregierung auf, zu prüfen, wie etwa durch Regelungen zur Beschränkung der Profilbildung, zur Begrenzung der zentralen Auskunfteien auf branchenspezifische Auskunftssysteme und zur Stärkung der Rechtsposition der Betroffenen gegenüber zentralen Auskunfteien und ihren Vertragspartnern, ein wirksamer Schutz der Betroffenen und ihres Restitutionsinteresses insbesondere bei der Verarbeitung unrichtiger Daten erreicht werden kann (BT-Drs. 15/4597 vom 22.12.2004).

5.3 Teilnahme an den Sitzungen der Arbeitsgruppe „Internationaler Datenverkehr“

Die Arbeitsgruppe „Internationaler Datenverkehr“, in der auch die Aufsichtsbehörde Brandenburg vertreten ist, befasste sich im Berichtszeitraum u.a. mit der Entscheidung der Europäischen Kommission zu alternativen Standardvertragsklauseln. Diese alternativen Standardvertragsklauseln hat die EU-Kommission neben den bereits vorhandenen Standardvertragsklauseln zur Vereinfachung von Übermittlungen personenbezogener Daten insbesondere durch international tätige Unternehmen in Länder außerhalb der EU – in Drittstaaten – verabschiedet. Sie können seit Anfang April 2005 verwendet werden. Wesentlicher Unterschied zu den vorhandenen Klauseln ist u.a. die Regelung zur Haftung.
Auch Unternehmensrichtlinien im Sinne des § 4c Abs. 2 BDSG, die von verschiedenen Unternehmen den Aufsichtsbehörden zur Beurteilung vorgelegt wurden, waren wieder ein wichtiges Thema in der Tätigkeit der Arbeitsgruppe. Mit der Einführung solcher verbindlichen Unternehmensrichtlinien können durch die betreffenden Unternehmen ausreichende Garantien für die personenbezogener Daten in Drittländer geschaffen werden. Die Artikel-29-Datenschutzgruppe als unabhängiges EU-Beratungsgremium in Datenschutzfragen hat eine „Muster-Checkliste für Anträge auf Genehmigungen verbindlicher unternehmensinterner Datenschutzregelungen“ erstellt, die als einheitlicher Maßstab für die Arbeit der Aufsichtsbehörden dienen kann. Darüber hinaus wird angestrebt, dass die Anerkennung solcher Datenschutz-Unternehmensrichtlinien europaweit zwischen den jeweiligen Datenschutzaufsichtsbehörden koordiniert wird.
Darüber hinaus spielte auch die Übermittlung von Flugpassagierdaten an die US-Behörden im Rahmen der dortigen Antiterrorgesetzgebung wieder eine wesentliche Rolle in den Beratungen der Arbeitsgruppe. Diesbezüglich wurde zwischen der EU und den USA am 20.05.2004 ein internationales Abkommen darüber geschlossen, dass diese – in etlichen Gesprächen zwischen EU-Kommission und US-Behörden ausgehandelten - Datenübermittlungen zulässig sein sollen. Gegen dieses Abkommen hat das Europäische Parlament Klage vor dem Europäischen Gerichtshof eingelegt. Bei einem Erfolg der Klage bliebe das Abkommen nach völkerrechtlichen Grundsätzen in Kraft; die EU-Kommission müsste ein neues Abkommen mit den USA aushandeln.

5.4 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).

Anlage zum Punkt 3.1

des dreizehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörde im Land Brandenburg

Das nachstehende Datenschutzkonzept der conNect Organisation und Netzwerk GmbH wurde mit Unterstützung der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich erstellt.

DATENSCHUTZ UND KANZLEIEN

conNect Organisation und Netzwerk GmbH · Geschäftsführer Matthias Krüger
Kapweg 3 · 13405 Berlin (Reinickendorf) · Telefon 030 / 498 59 95 - 0 · Fax 030 / 498 59 95 – 99
http:// www.systempartner- plus.de
Berliner Sparkasse · Konto 1 370 006 655 · Bankleitzahl 100 500 00
Sitz der Gesellschaft Berlin · Gerichtsstand Berlin · Amtsgericht Charlottenburg · 92 HRB 33121

Einleitung

Datenschutz und Kanzleien

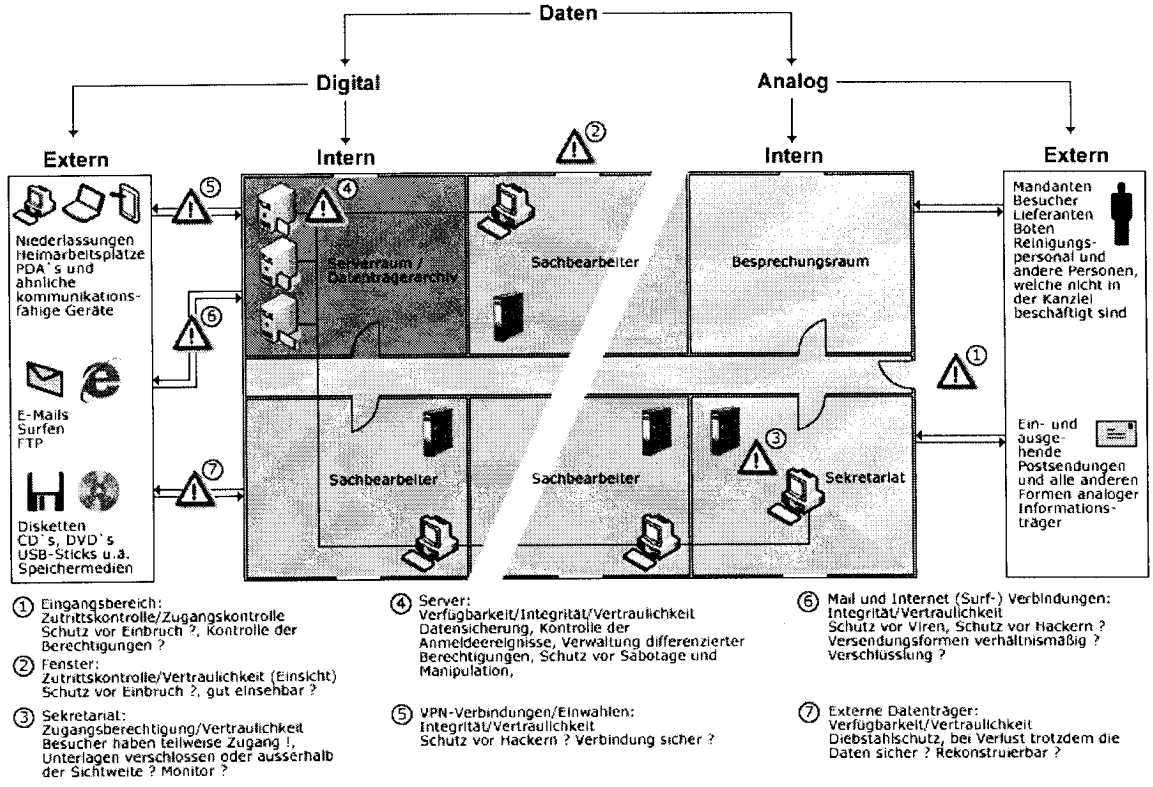
Seit einigen Monaten ist das Bundesdatenschutzgesetz und dessen Umsetzung in der steuerberatenden Branche eine häufig diskutierte Thematik. Viele Kanzleiinhaber und deren Mitarbeiter haben diverse Veranstaltungen besucht, um zu hinterfragen, was nun genau getan werden muss und inwiefern dies für das eigene Unternehmen zutrifft.

Zunächst hat jede Kanzlei, in der fünf oder mehr Mitarbeiter beschäftigt werden, einen internen oder externen Datenschutzbeauftragten schriftlich zu bestellen. Völlig unabhängig davon muss jedes Unternehmen dieser Branche ein Verfahrensverzeichnis erstellen, welches die Art der Datenmenge, den Zweck der Erhebung, Verarbeitung und Speicherung näher beschreibt. Die Erscheinungsform dieser „Übersicht" ist frei wählbar. Dennoch lässt sich der zu erfassende Inhalt recht präzise aus dem BDSG herleiten. Für die systematische Abarbeitung aller relevanten Punkte kann ebenfalls diverse Software genutzt werden (z.B. BDSG-Basics).

Bei Schnittmengen zu Gesetzgebungen Ihres Berufsstandes sollten Sie bei Unklarheiten in jedem Fall die Unterstützung eines Juristen in Anspruch nehmen. Oftmals sind es Detailfragen, die einer näheren Erörterung bedürfen.

Die nachfolgenden Seiten sollen Ihnen einen Eindruck vermitteln, welche Bereiche bei der Umsetzung der Datenschutzthematik tangiert werden bzw. welche relevanten Faktoren die Sicherheit Ihrer Kanzlei beeinflussen. Auf allgemeingültige Bereiche wie z.B. Brandschutz, die fachgerechte Entsorgung von Akten etc. wird nicht näher eingegangen. Individuelle Abweichungen müssen in jeden Fall erfasst und durch Ihren Datenschutzbeauftragten einer näheren Prüfung unterzogen werden.

Graphische Übersicht



1. Der Eingangsbereich

Der erste sicherheitsrelevante Punkt Ihrer Kanzlei ist bereits die Eingangstür. Hier werden gewisse Anforderungen an die Einbruchsicherheit gestellt, welche aber in der Regel schon beim Bau der Räumlichkeiten berücksichtigt wurden. Der Bauherr oder Vermieter sollte Ihnen darüber Auskunft erteilen können, welche Art von Tür, Schutzbeschlag und Schließzylinder hier verbaut wurden. Zur nachträglichen Ermittlung bzw. Bewertung empfiehlt es sich, den Sachverhalt aus Sicht der möglichen Bedrohung zu erörtern und die notwendige Widerstandsklasse zu ermitteln.
Unter *www.einbruchhemmung.de* steht Ihnen eine Punktetabelle zur Verfügung, die alle wesentlichen Kriterien berücksichtigt.

Abgesehen von der physikalischen Sicherheit findet in diesem Bereich ebenfalls eine Prüfung der Berechtigungen statt. Jeder Mitarbeiter, der über einen Sicherheitsschlüssel oder eine Karte verfügt, ist hier folglich zutrittsberechtigt. Für alle anderen/unbefugten Personen ist der Einlass nur nach erfolgter Sichtkontrolle zu gewährleisten. Darüber hinaus ist dafür Sorge zu tragen, dass sich Besucher, Mandanten u.ä. unter ständiger Aufsicht befinden und deren Aktionsradius auf den Sicherheitsbereich 1 beschränkt bleibt.

2. Fenster

Wie beim Eingangsbereich ist auch hier ein ausreichender Schutz gegen Einbruch zu gewährleisten. Die Lage des Büros ist hierbei maßgeblich. Sollten die Fenster nicht oder nur mit überdurchschnittlich hohem Aufwand erreichbar sein, werden hierzu keine Anforderungen formuliert. Befinden sich die Räumlichkeiten in den unteren Bereichen und der Zutritt zu den Fenstern ist ohne weiteres möglich, ist auch hier die Widerstandsklasse zur Ermittlung der zu ergreifenden Maßnahmen heranzuziehen. Die Frage der Vertraulichkeit von Informationen ist in diesem Fall näher zu erörtern. Monitore und Unterlagen sind so zu positionieren, dass keine Einsichtnahme von außen genommen werden kann.

3. Sekretariat

Dieser Bereich stellt in der Praxis ein großes Sicherheitsrisiko dar. Hier ist sicherzustellen, dass keinerlei Informationen für die Besucher ersichtlich sind. Der Arbeitsplatzmonitor, diverse Unterlagen, Akten, Post und ähnliches sind mit entsprechender Umsicht zu positionieren. Neben der visuellen Wahrnehmung ist darüber hinaus darauf zu achten, dass externe Personen bei Gesprächen zwischen Mitarbeitern oder bei Telefonaten mit im Raum anwesend sein können. Hier ist eine entsprechende Sensibilisierung der Mitarbeiter zu empfehlen.

4. Serverraum/Datenträgerarchiv

Die Serverumgebung ist das Kernstück Ihrer Kanzlei. Hier werden die Daten zentral gespeichert und in regelmäßigen Intervallen gesichert (Verfügbarkeit).

Aus physikalischer Sicht ist zunächst sicherzustellen, dass die Serverumgebung verschlossen ist und somit ein ausreichender Schutz vor Sabotage und Manipulation existiert (Serverraum oder –schrank). Der Zutritt sollte hier auf den Mitarbeiter beschränkt sein, welcher für den Wechsel der Datensicherungsmedien verantwortlich ist. Externe Dienstleister sind während ihrer Servicearbeiten zu beaufsichtigen.

Aus logischer Sicht ist die Anforderung an diese Struktur wesentlich umfangreicher. Zunächst muss sichergestellt werden, dass die hier gespeicherten Daten mit entsprechenden Berechtigungen versehen sind. Diese sollten nach dem Grundsatz der Datensparsamkeit und Datensicherheit so gestaltet sein, dass kein Mitarbeiter auf Informationen zugreifen kann, die nicht zwingend zur Erfüllung seiner Aufgaben notwendig sind (differenzierte Berechtigung). Für den Server, der die Daten und die logische Struktur verwaltet, ist die Benutzerkennung bzw. Systemanmeldung am Arbeitsplatz mit bestimmten Berechtigungen auf Daten gleichbedeutend.

Es ist also zwingend notwendig, die Eindeutigkeit und Integrität dieser Authentifizierungsinformation zu gewährleisten. Die Empfehlung ist daher, die Passwörter in regelmäßigen Abständen zu ändern und das Passwort selbst so zu gestalten, so dass es nur schwerlich herzuleiten bzw. nachzuvollziehen ist (komplexe Kennwörter).

Dies ist besonders im Hinblick auf die nachfolgende Protokollierung wichtig. Der Bezug zwischen einer natürlichen Person und den von ihr vorgenommenen Veränderungen im Datenbestand bzw. System muss eindeutig und nachvollziehbar sein.

Das Datenträgerarchiv ist ebenso wie der Serverbereich mit entsprechender Umsicht zu behandeln. Hier bietet es sich an, den Kreis der berechtigten Personen auf ein Mindestmaß zu reduzieren. Die sichere und fachgerechte Lagerung der Medien ist zu gewährleisten.

5. Anbindung von externen Arbeitsplätzen

Wird von externen Bereichen auf den Datenbestand der Kanzlei direkt oder indirekt zugegriffen, gelten grundsätzlich die gleichen Anforderungen für die eindeutige Identifikation, Authentifizierung und Zugriffskontrolle wie im internen Bereich (siehe 4.).

Besonders sicherheitsrelevant ist die Form der Datenübertragung, welche sehr von der verwendeten Technologie abhängig ist. Findet eine Einwahl über ISDN und Modem statt oder wird eine Standleitung genutzt, so ist das Risiko weitaus geringer als bei Verbindungsformen über das Internet. Dies basiert vor allen darauf, dass ein Angriff im Bereich von ISDN- oder Modemverbindungen zunächst gezielt auf eine Telekommunikationsanlage erfolgen muss. Selbst wenn dies erfolgreich wäre – und die dazu notwendige Kompetenz ist nur sehr selten anzutreffen – ist noch lange kein Datenzugriff möglich. Tiefgreifende Kenntnis über Protokolle und Netzwerke wären erforderlich, um die Sicherheitsmechanismen Ihres Systems zu überwinden. Die Kombination aus den beiden Fachrichtungen mit dem definierten Interesse, genau Ihre Daten zu erlangen, wird sich nur unwahrscheinlich in einer Person wiederfinden lassen.

Bei Verbindungen über das Internet (VPN), bei denen z.B. der DSL-Anschluss zur Übertragung verwendet wird, wird die Technologie eines virtuellen Tunnels genutzt. Dadurch soll sichergestellt werden, dass der Datenfluss innerhalb dieser „Röhre" von anderen Internet-Nutzern nicht gelesen oder manipuliert werden kann. Im Gegensatz zu den Wählverbindungen ist hier das Risiko höher, dass dieser Mechanismus angegriffen wird. Dies resultiert hauptsächlich aus der großen Zahl an Internet-Nutzern und der Fülle an automatisierten Programmen, die nur nach potentiellen Angriffspunkten auf der Suche sind. Folglich ist hier ein ausreichender Schutz gegeben, wenn die verwendete Verschlüsselung sicher genug ist.

6. Internet und E-Mail

Die Nutzung von Internet und E-Mails bergen ebenfalls Risiken für Ihr internes Netzwerk. An erster Stelle stehen hier Computerviren, welche sich in ihrer Verbreitung und Erscheinungsform ständig verändern. Da diese hauptsächlich mit E-Mails oder heruntergeladenen Dateien übermittelt werden, ist hier aus technischer Sicht ein entsprechender Schutz zu gewährleisten. Es sollte darauf geachtet werden, dass in der logischen Abfolge die entsprechende Datei oder E-Mail erst geprüft wird, bevor diese im Netzwerk Verwendung findet.

Sollten Sie vertrauliche Informationen per E-Mail versenden, ist hier die Verschlüsselung des Inhalts dringend empfohlen, da sich diese Informationen auch über das Internet bewegen und der Übertragungsweg eher unsicher ist.

Im Bereich des Surfens stellt sich der Sachverhalt etwas anders dar. Oftmals sind es hier kleine Programme, die mit dem Besuch der Internetseite aktiv werden. Diese laden die Besucher ein, verschiedenste Zugangssoftware herunterzuladen, zu installieren, Fragen zu beantworten oder in irgendeiner Weise interaktiv tätig zu werden. Da man außer Filterfunktionen u.ä. innerhalb der Firma kaum Vorsichtsmaßnahmen treffen kann, ist hier die entsprechende Unterweisung der Mitarbeiter empfohlen.

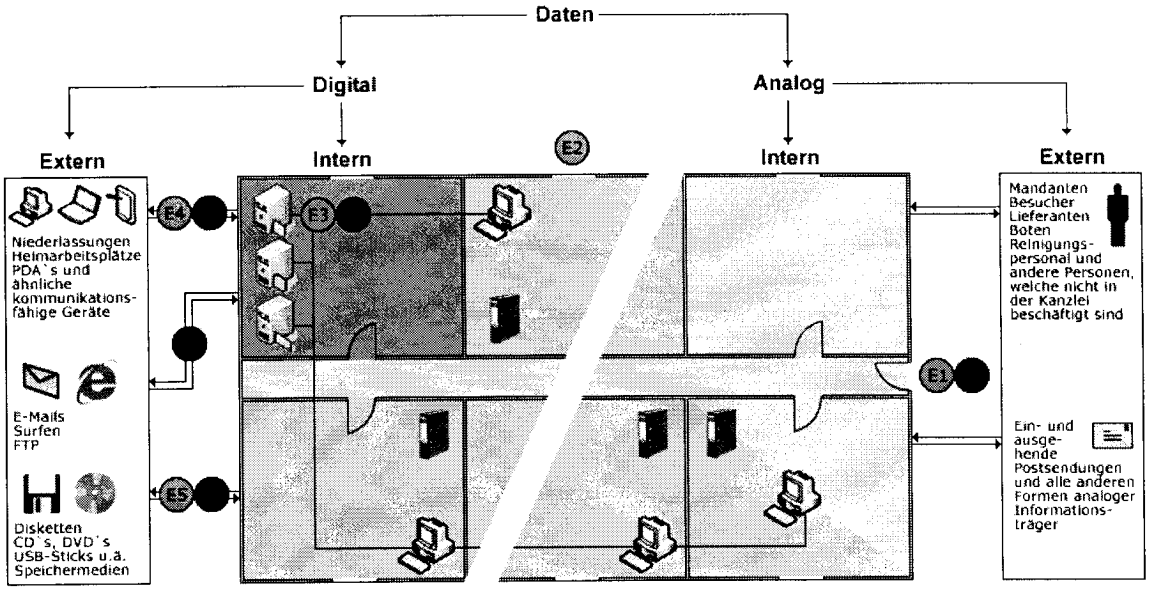
Generell sollte neben dem Virenscanner ebenfalls eine Firewall für diesen Kommunikationsweg vorhanden sein. Da es sich auch hier wieder um eine direkte Verbindung mit dem Internet handelt, ist das Risiko eines Angriffs nicht kalkulierbar und daher als hoch einzustufen.

7. Externe Datenträger

Externe Datenträger dienen in der Regel zur Übermittlung von Datenmengen zwischen zwei Punkten. Der Übertragungsweg ist nicht digital. Das heißt hier findet die Weitergabe oder der Transport des physikalischen Gegenstandes statt. Folglich ist das größte Risiko der Verlust der Verfügbarkeit (z.B. Diebstahl). Ist nun die Datenmenge unverschlüsselt bzw. auf andere Systeme leicht zu übernehmen, geht damit der Verlust der Vertraulichkeit dieser Information einher. Insofern sollten alle Datenmengen auf diesen Medien mindestens passwortgeschützt oder verschlüsselt sein.

Bei der Beschriftung der Datenträger sollte vermieden werden, dass die Bezeichnung einen Rückschluss auf die gespeicherten Daten und deren Ersteller bzw. Empfänger zulässt.Zudem ist dafür zu sorgen, dass die Informationen bei Verlust des Datenträgers aus anderen Quellen rekonstruiert werden können.

8. Protokoll/Erfassungspunkte



Sicherheitsbereich 1: für alle im "analogen" externen Bereich genannten Personengruppen;

Sicherheitsbereich 2: Ort der Datenerhebung und Datenvearbeitung; Datenspeicherung vorrangig in analoger Form (Akten, Unterlagen ...), kein Zutritt für in Sicherheitsbereich 1 genannte Personen (mit Ausnahmen);

Sicherheitsbereich 3: Ort der Datenspeicherung und Archivierung; kein Zutritt für Personen der Sicherheitsbereiche 1 und 2 (mit Ausnahmen);

(E) Erfassungspunkt: Informationen ohne oder mit geringem Aktualisierungsbedarf

● Protokollpunkt: Prozessprotokollierung/Informationen mit hohem Aktualisierungsbedarf

(E1) Erfassung Eingangsbereich/Sicherheitsbereich 1

- ☐ Tür, Schloss und Türbeschläge entsprechen der notwendigen Widerstandsklasse;
- ☐ Vor Einlass der Besucher ist eine Sichtprüfung gegeben;
- ☐ Besucher sind innerhalb der Kanzlei nie unbeaufsichtigt;
- ☐ Arbeitsplätze im Sekretariat u.ä. sind den Umständen entsprechend angepasst;

(E2) Fensterbereich

- ☐ Fenster entsprechen der notwendigen Widerstandsklasse;
- ☐ Prüfung der Einsichtnahme;

E3 Server/Datenträgerraum

- ☐ Ort und Art der Datenstruktur;
- ☐ Datensicherung (Festplattenspiegel, Bandsicherung);
- ☐ Wechsel und Aufbewahrung der Datensicherungsmedien;
- ☐ Definition der Schutzmechanismen (Virenscanner, Firewall etc.);

E4 Externe Arbeitsplätze, externe Geräte mit Datenzugriff

- ☐ Aufstellung der Geräte;
- ☐ Art der Anbindung;

E5 Externe Datenträger

- ☐ Aufstellung der Datenträger (bei externer Verwendung);

Eingangsbereich/Sicherheitsbereich 1

- ☐ Zugangsberechtigungen sind erfasst worden (Schlüsselliste);
- ☐ Vorgehen bei Verlust (z.B. Schlüssel) ist dokumentiert;

Datenserver intern (automatische Protokollierung)

- ☐ Datensicherungsprotokoll;
- ☐ An- und Abmeldeereignisse;
- ☐ Datenzugriffe;

Daten-/Programmserver extern (automatische Protokollierung)

- ☐ An- und Abmeldung;
- ☐ Datenzugriffe;
- ☐ Verbindungsdaten;

Server Kommunikationsdienste (automatische Protokollierung)

- ☐ Zugriffsversuche von außen;
- ☐ Kritische Systemereignisse;
- ☐ Verbindungsdaten;

Transfer externer Datenträger

- ☐ Transferweg des Datenträgers;

9. Rechtsgrundlagen

Das Bundesdatenschutzgesetz ist als Auffanggesetz konzipiert. Existieren Vorschriften des Bundes, die Gebote oder Verbote für die Erhebung, Verarbeitung, Nutzung oder den Schutz personenbezogener Daten formulieren, genießen diese Vorrang vor den Regelungen des BDSG.

Solche Rechtsvorschriften können sich unter anderem ergeben aus:

- Bestimmungen zur berufsständischen Verschwiegenheitspflicht (z.B. StGB, StBerG, WPO, BRAO, BORA)
- Steuervorschriften (z.B. EStG, LStDV, AO)
- Den Richtlinien der Datenerfassungs- und Übermittlungsverordnung (DEÜVO)
- Arbeits- und Sozialgesetzen (ArbGG, BetrVG, AFG, SGB X)
- Bestimmungen zur Telekommunikation (TKG, TDSV)
- Bestimmungen zur Multimedianutzung (TDG, TDSG, MDStV)
- Statistikgesetzen
- Zivilprozessordnung (ZPO)

In jedem Fall ist in der Kanzlei zu prüfen, welche Bereiche nicht durch die o.g. Gesetzgebungen erfasst werden und somit den Regelungen des BDSG unterliegen (wie z.B. der Bereich der Datenschutzorganisation und Datenverarbeitung).

10. Vertrag

Der zentrale Zulässigkeitstatbestand der Verarbeitung von z.B. Mandantendaten ergibt sich aus § 28 BDSG, nach dem das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist. „Eigene Zwecke" liegen vor, wenn die Datenverarbeitung lediglich als Mittel zur Erfüllung des Geschäftszweckes dient und diese nicht selbst Geschäftszweck ist (wie bei Adressverlagen oder Auskunfteien).

Besteht also ein Vertragsverhältnis mit dem Betroffenen (Mandant), ist eine rechtliche Grundlage zur Erhebung, Verarbeitung und Speicherung von Daten gegeben. Bedingung ist allerdings, dass nur die Daten erhoben und gespeichert werden, die der Zweckbestimmung des Vertrages mit dem Betroffenen dienen.

Weitergehende Informationen zu vertragsähnlichen Verhältnissen etc. sind in übersichtlicher Form dem Buch „Datenschutz und Datensicherheit im Kanzleibetrieb" zu entnehmen.

11. Die Einwilligung

Eine Einwilligungserklärung bei der „Datenverarbeitung im Auftrag" ist grundsätzlich nicht erforderlich. Sie sollte nur dann eingeholt werden, wenn sich keinerlei andere Rechtsgrundlage bzw. kein Erlaubnistatbestand für den jeweiligen Fall finden lässt.

Die datenschutzrechtliche Einwilligung ist an eine klar definierte Form gebunden, welche sich aus § 4a BDSG ergibt. Hiernach ist diese vom Betroffenen vorzugsweise in schriftlicher Form zu erteilen und muss in ihrem Erscheinungsbild deutlich von anderen Erklärungen zu unterscheiden sein.

Inhaltlich müssen die Zwecke der Erhebung, Verarbeitung und Nutzung erläutert werden. Ist es auf Grund besonderer Umstände erforderlich oder wird dies verlangt, so sind auch die Folgen einer Verweigerung dieser Einwilligung näher zu beschreiben.

Als praktisches Beispiel ist hier die Betreuung von IT-Dienstleistern zu nennen, da nicht auszuschliessen ist, dass bei Wartungs- oder Servicearbeiten Einsicht in Mandantendaten genommen wird. Der Interessenkonflikt zwischen den Verpflichtungen des Berufsstandes und der Notwendigkeit dieser Arbeiten kann durch eine Zustimmung des Betroffenen bzw. des Mandats umgangen werden.

12. Maßnahmen (nach Anlage zu § 9 Satz 1 BDSG)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),

2. zu verhindern, daß Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),

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

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten **getrennt verarbeitet werden können.**

Quellen

Literatur

Datenschutz und Datensicherheit im Kanzleibetrieb; Hund, Leistenschneider, Müthlein, Schäfer; DATEV-Edition Steuern & Recht, Juli 2002

Software

BDSG-Basics, Demal-GmbH

conNect Organisation und Netzwerk GmbH · Geschäftsführer Matthias Krüger
Kapweg 3 · 13405 Berlin (Reinickendorf) · Telefon 030 / 498 59 95 - 0 · Fax 030 / 498 59 95 – 99
http:// www.systempartner- plus.de
Berliner Sparkasse · Konto 1 370 006 655 · Bankleitzahl 100 500 00
Sitz der Gesellschaft Berlin · Gerichtsstand Berlin · Amtsgericht Charlottenburg · 92 HRB 33121