Regierung von Mittelfranken

Bayerische Datenschutzaufsichtsbehörde
für den nicht-öffentlichen Bereich

2. Tätigkeitsbericht

2006

Impressum

Herausgeber:

Regierung von Mittelfranken
Bayerische Datenschutzaufsichtsbehörde
für den nicht-öffentlichen Bereich
Promenade 27
91522 Ansbach

Telefon: 0981 53-0
Telefax: 0981 53-1206
E-Mail: datenschutz@reg-mfr.bayern.de

Dieser Tätigkeitsbericht kann auch unter
www.regierung.mittelfranken.bayern.de abgerufen werden.

Inhaltsverzeichnis

Vorwort

Der 2. Tätigkeitsbericht der Bayerischen Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich gibt einen Überblick über die wahrgenommenen Aufgaben, stellt die Lösungen typischer datenschutzrechtlicher Fallgestaltungen vor und gibt Empfehlungen für ein datenschutzgerechtes Verhalten insbesondere bei den privaten Wirtschaftsunternehmen, Vereinen, Verbänden und freiberuflich Tätigen. Die Bandbreite der Themen reicht vom Gesundheitswesen über die Versicherungen, Banken, Auskunfteien und den Adresshandel bis hin zu den Tele- und Mediendiensten. Es geht also vor allem um die Branchen, bei denen naturgemäß viele personenbezogene Daten automatisiert verarbeitet werden.

Der Datenschutz bei staatlichen Behörden, öffentlichen Einrichtungen und Kommunalverwaltungen in Bayern wird hier nicht angesprochen. Die Aufsicht obliegt dort dem Bayerischen Landesbeauftragten für den Datenschutz.

Merklich gestiegen sind bei uns die Eingaben zur Videoüberwachung in öffentlich zugänglichen Bereichen. Dies hängt zum einen damit zusammen, dass die Überwachungskameras immer mehr zunehmen. Zum anderen wird vielen Menschen hierbei die Beeinträchtigung ihres Persönlichkeitsrechts offensichtlich eher bewusst als bei anderen Datenverwendungen, wo man sich im Hinblick auf den Schutz seiner personenbezogenen Daten meist weniger sensibel verhält, etwa bei der Teilnahme an Preisausschreiben oder im Internet.

Deshalb möchten wir mit diesem Bericht nicht nur diejenigen ansprechen, die die personenbezogenen Daten erheben und verwenden, sondern wir wollen den Datenschutz auch etwas mehr in das Bewusstsein derer rücken, deren Daten geschützt werden sollen.

Ansbach, im Dezember 2006

Inhofer
Regierungspräsident

1 Die Datenschutzaufsicht im nicht-öffentlichen Bereich

1.1 Aufgaben einer Datenschutzaufsichtsbehörde im nicht-öffentlichen Bereich

Nach § 38 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) kontrolliert die Aufsichtsbehörde die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln.

Die Aufgaben der Datenschutzaufsichtsbehörde lassen sich im Wesentlichen wie folgt beschreiben:

- Bearbeitung von Anfragen, Eingaben und Beschwerden
- Beratung und Unterstützung der betrieblichen Datenschutzbeauftragten und der für die Datenverarbeitung verantwortlichen Stellen
- Kontrollen in den Unternehmen und sonstigen verantwortlichen Stellen
- Beanstandungen bei Datenschutzverstößen
- Anordnungen bei Sicherheitsmängeln
- Führung des öffentlichen Registers der meldepflichtigen Unternehmen, vor allem im Hinblick auf Auskunfteien, Adressenhandel, Markt- und Meinungsforschungsinstitute
- Genehmigungen von Datenübermittlungen in Drittstaaten (also außerhalb der Staaten der Europäischen Union und des Europäischen Wirtschaftsraumes) gemäß § 4c Abs. 2 BDSG
- Durchführung von Bußgeldverfahren
- Stellung von Strafanträgen gemäß § 44 BDSG

Die Überprüfungen der Datensicherheit führt in Bayern gemäß Art. 34 Abs. 1 Satz 1 Bayerisches Datenschutzgesetz der Technische Überwachungsverein Bayern Sachsen e. V. durch.

1.2 Gesetzliche Grundlage für die Erstellung des Tätigkeitsberichts

Die gesetzliche Verpflichtung der Aufsichtsbehörden, Tätigkeitsberichte zu erstellen, ergibt sich aus § 38 Abs. 1 Satz 6 BDSG. Diese Bestimmung beruht auf Art. 28 Abs. 5 der Richtlinie 95/64/EG des Europäischen Parlaments und des Rates vom 24.10.1995. Danach muss jede Kontrollstelle regelmäßig einen Bericht veröffentlichen.

1.3 Die Bayerische Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich bei der Regierung von Mittelfranken

Die Regierung von Mittelfranken ist von der Bayerischen Staatsregierung ab 01.06.2002 zur bayernweit zuständigen Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich bestimmt worden.

Die Aufgaben der Datenschutzaufsicht werden von folgenden Personen wahrgenommen:

Leiter	Ltd. Regierungsdirektor Dorn
Stv. Leiter	Oberregierungsrat Meier
	Regierungsamtsrat Ilgenfritz
	Regierungsoberinspektor Andörfer
	Regierungsoberinspektor Fromm
	Regierungsoberinspektorin Dierauff

1.4 Örtliche Zuständigkeit der Bayerischen Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich

Nach Art. 3 BayVwVfG ist die Bayerische Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich zuständig, wenn sich der Sitz des Unternehmens, die Betriebsstätte, die Zweigniederlassung, die Geschäftsstelle oder der Selbstständige usw., deren Datenverwendung einer Kontrolle oder einer Einzelüberprüfung aufgrund einer Beschwerde unterzogen werden soll, in Bayern befindet.

Für ein Unternehmen mit mehreren Niederlassungen sind somit mehrere Aufsichtsbehörden zuständig. Zur Bestimmung der in einem konkreten Beschwerdefall zuständigen Aufsichtsbehörde gelten folgende Kriterien:

- Für Prüfungsgegenstände, die grundsätzlicher Art sind bzw. das ganze Unternehmen betreffen, muss die für den Sitz des Unternehmens zuständige Aufsichtsbehörde tätig werden. Ein derartiger Fall liegt z. B. vor, wenn es um eine Datenübermittlung aufgrund einer unternehmensweiten Richtlinie geht.

- Bezieht sich eine Überwachung oder Kontrolle auf eine Datenverwendung oder Datensicherheitsmaßnahme, die ausschließlich einer Filiale zuzuordnen ist, ist die Aufsichtsbehörde zuständig, in deren Bereich die Filiale liegt.

Wird eine Eingabe bei einer unzuständigen Behörde eingereicht, wird sie von dort an die zuständige Behörde weitergeleitet. Der Eingabeführer erhält in der Regel eine Abgabenachricht.

Stellt sich erst im Rahmen der Überprüfung heraus, dass eine andere Aufsichtsbehörde zuständig ist, gibt die bis dahin tätige Behörde den Vorgang zur weiteren Bearbeitung an die zuständige Behörde ab.

* * *

2 Überblick und Statistik

2.1 Bearbeitung von Anfragen und Beschwerden

Den größten Raum in der alltäglichen Arbeit nimmt die Bearbeitung von Anfragen und Beschwerden von Betroffenen ein, in denen Verletzungen von Datenschutzvorschriften geltend gemacht werden.

Ein hoher Arbeitsaufwand ist wegen der oft komplexen Sachverhalte mit der Bearbeitung der Eingaben im Bereich der Auskunfteien, der Banken und der Versicherungen verbunden.

Die Zahl der Beschwerden gegen Direktwerbemaßnahmen, insbesondere Telefonwerbung, sowie gegen Adressenverarbeitungen und -nutzungen ist nach wie vor hoch.

Beschwerden über Videoüberwachungen nehmen immer mehr zu. Das Gleiche gilt für Beschwerden gegen Datenschutzverletzungen bei der Nutzung der neuen Medien wie Internet und E-Mail.

Weitere Schwerpunktthemen sind die Datenverwendungen in Arbeitsverhältnissen, im Gesundheitswesen sowie in Vereinen und Verbänden.

Die interessantesten Fälle sind in den nachstehenden Fachabschnitten behandelt.

Statistik 2004

- Schriftliche Eingaben insgesamt 564

  Überprüfungsergebnisse:

Keine Verstöße	366
Verstöße (davon 12 Bußgeldbescheide)	198

- Anfragen/Beratungen von Betroffenen per Telefon oder E-Mail: 418

Statistik 2005:

- Schriftliche Eingaben insgesamt 514

  Überprüfungsergebnisse:

Keine Verstöße	263
Verstöße (davon 3 Bußgeldbescheide)	251

- Anfragen/Beratungen von Betroffenen per Telefon oder E-Mail: 496

2.2 Beratung der betrieblichen Datenschutzbeauftragten und der verantwortlichen Stellen

Die Beantwortung von Anfragen betrieblicher Datenschutzbeauftragter und von verantwortlichen Stellen war schon immer ein wichtiges Mittel, um den Datenschutz "unter die Leute zu bringen". Im Rahmen der am 26. August 2006 in Kraft getretenen Änderung des BDSG wurde diesbezüglich in § 4g Abs. 1 Satz 3 und in § 38 Abs. 1 Satz 2 BDSG eine ausdrückliche Regelung geschaffen.

Zur schnellen Beratung wird meist der telefonische Kontakt gesucht. Schwierigere Fallgestaltungen werden schriftlich (einschl. E-Mail) vorgetragen oder in Besprechungen bei uns bzw. in den Unternehmen erörtert.

Folgende Themen standen im Berichtszeitraum im Vordergrund:

- Anfragen zur Umsetzung des BDSG in der Betriebspraxis
- Arbeitnehmerdatenschutz in all seinen Ausprägungen
- Rechtsfragen zur Videoüberwachung
- Fragen zu Datenübermittlungen ins Ausland.

Statistik 2004:

Anfragen/Beratungen per Telefon, schriftlich oder per E-Mail:	697
Besprechungen	26

Statistik 2005:

Anfragen/Beratungen per Telefon, schriftlich oder per E-Mail:	709
Besprechungen	23

Datenschutzseminare und -vorträge:

In den Jahren 2004 und 2005 wurden von uns auf Wunsch und im Zusammenwirken mit Unternehmensverbänden und Berufskammern auch verstärkt Vortragsveranstaltungen zum Datenschutz durchgeführt, um auf diesem Weg eine Breitenwirkung in der Datenschutzinformation zu erreichen. Im Berichtszeitraum waren dies insgesamt 17 Vortragsveranstaltungen.

2.3 Kontrolltätigkeit

Es handelt sich hier um umfassende oder nur Teilbereiche betreffende Kontrollen, bei denen die Belange des Datenschutzes und der Datensicherheit in einem Unternehmen oder Betrieb auf den Prüfstand gestellt werden. Sie können auf schriftlichem Weg, online oder vor Ort durchgeführt werden.

2.3.1 Die Häufigkeit der Kontrollen

Eine flächendeckende Durchführung von Kontrollen durch die Aufsichtsbehörden entspricht nicht der Intention des BDSG.

Das BDSG geht vielmehr davon aus, dass bereits die interne Kontrolle durch die betrieblichen Datenschutzbeauftragten in den Unternehmen einen wesentlichen Beitrag zum Schutz des informationellen Selbstbestimmungsrechts leistet. Mit ihr nehmen die datenverarbeitenden Stellen die ihnen im Datenschutzrecht zukommende Selbstverantwortung wahr.

Das bedeutet für die staatliche Kontrolle, dass sie im Gegensatz zu anderen staatlichen Aufsichtstätigkeiten nicht als alleinige und stets präsente Staatsaufsicht ausgestaltet ist. Vielmehr ist sie neben der internen Kontrolle ein Teil einer auf mehreren Füßen stehenden Kontrollsystematik.

2.3.2 Die Auswahlkriterien

Die Entscheidung, in welchem Unternehmen eine Kontrolle durchgeführt wird, steht im pflichtgemäßen Ermessen der Aufsichtsbehörde. Sie wird dabei in eigener Initiative von Amts wegen tätig.

Im Wesentlichen orientieren wir uns bei der Auswahl an folgenden Kriterien:

- Wir greifen stichprobenweise ein Unternehmen, einen Verband oder Verein heraus, um nähere Erkenntnisse über die Verwirklichung des Datenschutzes in bestimmten Branchen oder einzelnen Unternehmen zu gewinnen. Auf diese Weise können wir Fehlentwicklungen erkennen und ggf. mit präventiver Zielrichtung entsprechende Gegenmaßnahmen ergreifen.

- Nach einem Prüfplan gehen wir bevorzugt bei den Branchen vor, deren Datenverarbeitung ein größeres Gefährdungspotenzial mit sich bringt und denen deshalb eine besondere Verantwortung für den Umgang mit personenbezogenen Daten zukommt. Dies gilt vor allem für die meldepflichtigen Verarbeitungen wie Auskunfteien, Adresshandel und Marktforschung, aber auch für Versicherungen und Banken.

- Anlässe für Kontrollen geben Beschwerden und Hinweise aller Art, u. a. auch anonyme Eingaben, Mitteilungen eines Betriebsrats oder Berichte in den Medien, wenn sie hinreichende Anhaltspunkte für Datenschutzverletzungen in größerem Umfang oder bei komplexen Sachverhalten bieten.

- Bei vermehrten Beschwerden gegen ein bestimmtes Unternehmen oder gegen Unternehmen einer bestimmten Branche versuchen wir, durch gezielte Kontrollen einem Trend gegenzusteuern.

- Werden bei Kontrollen oder Überprüfungen erkannte Datenschutzverstöße nicht abgestellt, kann es auch zu einer Nachkontrolle kommen. Sie zielt dann vielfach auch auf möglicherweise vorhandene organisatorische Mängel ab.

2.3.3 Kontrollen im Berichtszeitraum

Im Jahr 2004 haben wir 18 Unternehmen vor Ort geprüft, davon

9 Markt-/Meinungs-/Sozialforschungsunternehmen
3 Auskunfteien
2 Industrie/Handel/Dienstleistung
1 Adressenhändler
1 Internetdiensteanbieter
1 Privatärztliche Verrechnungsstelle
1 Versicherung

Im Jahr 2005 wurden 21 Unternehmen vor Ort geprüft, davon

6 Markt-/Meinungs-/Sozialforschungsunternehmen
5 Industrie/Handel/Dienstleistung
4 Adressenhändler
2 Dienstleister im Gesundheitswesen
1 Auskunftei
1 Bank
1 Internetdiensteanbieter
1 Versicherung

Handlungsbedarf aus den Feststellungen der Datenschutzprüfungen hat sich insbesondere ergeben:

- zur Formulierung und Gestaltung von datenschutzrechtlichen Einwilligungserklärungen nach § 4a BDSG,
- im Hinblick auf die schriftlichen Vertragsregelungen bei der Auftragsdatenverarbeitung nach § 11 BDSG,
- bei den Regelungen zur Kontrolle der Nutzung von Telefon, Internet und E-Mail am Arbeitsplatz,
- für notwendige Sicherheitsmaßnahmen im Sinne von § 9 BDSG,
- bei der Auswahl und der Tätigkeit der betrieblichen Datenschutzbeauftragten und
- beim Verfahrensverzeichnis nach § 4g Abs. 2 BDSG.

Spezielle Beanstandungen sind in den folgenden Fachkapiteln dargestellt.

Prüfungen zur Datensicherheit

In Bayern wird die Prüfung der nach § 9 BDSG erforderlichen Datensicherheitsmaßnahmen nicht von der Datenschutzaufsichtsbehörde, sondern in deren Auftrag vom Technischen Überwachungsverein Bayern Sachsen e. V. vorgenommen.

Im Berichtszeitraum wurden 6 Prüfungsaufträge abgeschlossen. Bei keinem der überprüften Unternehmen wurden wesentliche Sicherheitsmängel festgestellt.

2.4 Meldepflicht

Nach § 4d BDSG sind im wesentlichen die folgenden zwei Geschäftsfelder gegenüber den Datenschutzaufsichtsbehörden meldepflichtig:

- Die Datenspeicherung zum Zweck der Übermittlung, also der Handel mit personenbezogenen Daten, wie es bei Wirtschaftsauskunfteien und Adressenhändlern der Fall ist.

- Die Datenspeicherung zum Zweck der anonymisierten Übermittlung, also die Tätigkeit der Markt-, Meinungs- und Sozialforschungsinstitute.

Wir haben für Bayern zur Zeit 115 Anmeldungen vorliegen, die sich regional in den Regierungsbezirken wie folgt verteilen:

58 aus Oberbayern
33 aus Mittelfranken
10 aus Oberfranken
6 aus Unterfranken
7 aus Schwaben
1 aus der Oberpfalz

Aus Niederbayern liegt derzeit keine Anmeldung vor.

Von der Struktur her entfallen von den 115 Meldungen in etwa je die Hälfte auf Auskunfteien und Adressenhändler auf der einen Seite sowie auf Markt-, Meinungs- und Sozialforschungsunternehmen auf der anderen Seite.

Das bei uns geführte Register über die meldepflichtigen Unternehmen dient in erster Linie zur Unterstützung unserer Arbeit. Es kann nach § 38 Abs. 2 Satz 2 BDSG von jedem eingesehen bzw. aus ihm kann Auskunft erteilt werden. Bisher wurde aber von dieser Möglichkeit kaum Gebrauch gemacht.

2.5 Zusammenarbeit der für den Datenschutz Verantwortlichen

2.5.1 Konferenzen der Datenschutzaufsichtsbehörden

Die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich arbeiten bundesweit in dem zwei Mal jährlich tagenden sog. „Düsseldorfer Kreis“ zusammen, um grundsätzliche Rechtsfragen und die Entscheidungen länderübergreifender Fallgestaltungen abzustimmen. In das Gesamtgremium des

„Düsseldorfer Kreises“ sind wir ebenso eingebunden wie auch in die dazu gehörenden fünf Arbeitsgruppen Kreditwirtschaft, Auskunfteien/SCHUFA, Versicherungswirtschaft, Internationaler Datenverkehr und Telekommunikation/Tele- bzw. Mediendienste.

Einmal im Jahr treffen sich die Vertreter aller Datenschutzaufsichtsbehörden bei einem Workshop zur Klärung und Abstimmung von Praxisfragen.

2.5.2 Arbeitskreise der Wirtschaftsunternehmen

Betriebliche Datenschutzbeauftragte aus den Unternehmen haben sich unter der Federführung der Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) einen Erfahrungsaustausch in sogenannten „Erfa-Kreisen“ organisiert, um von- bzw. miteinander zu lernen und sich fortzubilden. In Bayern existieren inzwischen derartige branchenunabhängige Gesprächsrunden in München, Nürnberg, Würzburg und Coburg. Sie finden zwei- bis dreimal im Jahr statt.

Darüber hinaus haben die Datenschutzbeauftragten der bayerischen Versicherungen einen auf ihre speziellen Fachfragen ausgerichteten Datenschutz-Arbeitskreis installiert, der sich in der Regel zweimal im Jahr trifft.

An diesen Veranstaltungen nehmen wir auf Einladung der Veranstalter regelmäßig teil, halten mehrmals im Jahr Fachvorträge, nehmen zu den diskutierten Problemen Stellung und beantworten Anfragen.

2.5.3 Datenschutzfachtagungen und -kongresse

Mehrmals im Jahr besuchen wir derartige Veranstaltungen, bei denen über die aktuellen Fragen des Datenschutzes und der Datensicherheit in Deutschland referiert und diskutiert wird.

* * *

3 Die Abwicklung von Beschwerdeverfahren durch die Aufsichtsbehörde und bei den verantwortlichen Stellen

Datenschutzrechtliche Beschwerden über private Unternehmen haben wir bisher - soweit er uns bekannt war - direkt an den jeweiligen betrieblichen Datenschutzbeauftragten mit der Bitte um Prüfung und Stellungnahme weitergeleitet. Der Datenschutzbeauftragte schaltete die Fachabteilung ein, in deren Bereich die angesprochene Datenverwendung durchgeführt wurde, ließ sich von dort berichten und gab dann im Namen des Unternehmens eine Stellungnahme ab.

Stellte die Datenschutzaufsichtsbehörde bei ihrer datenschutzrechtlichen Wertung des Vorgangs fest, dass ein Datenschutzverstoß vorliegt, konnte es in der Folgezeit auch einmal zu einer längeren Korrespondenz zwischen ihr und dem Datenschutzbeauftragten kommen. Der Datenschutzbeauftragte trat dann häufig voll in der Funktion eines Vertreters seines Unternehmens auf und verteidigte dessen Standpunkt. Von einer eigenen datenschutzrechtlichen Wertung des innerbetrieblichen Überwachungsorgans war dabei in zahlreichen Fällen nicht mehr viel wahrzunehmen.

Auf Grund einer eingehenden Überprüfung der Rechtslage entstanden bei uns nicht unerhebliche Zweifel, ob eine derartige Vertretungsfunktion des betrieblichen Datenschutzbeauftragten mit der in § 4g BDSG festgelegten Kontrollaufgabe zu vereinbaren ist. Der Datenschutzbeauftragte hat neben der Datenschutzaufsichtsbehörde eine eigene Überwachungsfunktion. Er ist gerade nicht der Anwalt oder der Beschwerdesachbearbeiter des Unternehmens, der gegenüber der Datenschutzaufsichtsbehörde Stellung zu nehmen hat. Für diese Aufgabe sind vielmehr nach der eindeutigen Vorschrift des § 38 Abs. 3 BDSG in einem Unternehmen „die mit der Leitung beauftragten Personen“ zuständig.

Unter Beachtung dieser Rechtslage werden wir in Zukunft Eingaben und Beschwerden an die jeweilige Unternehmensleitung mit der Bitte um Prüfung und Stellungnahme senden. Die Leitung eines Unternehmens, dem ein Datenschutzverstoß vorgeworfen wird, hat ein Recht darauf, von der Datenschutzaufsicht direkt angesprochen zu werden. Nur so kann sie ihrer Verantwortung für die über-

prüften Datenverwendungen gerecht werden, indem sie sich verteidigt, ihre Sicht der Dinge darstellt oder einen erkannten Fehler abstellt.

Für die aus unserer Sicht jedoch auch dringend erforderliche Einbeziehung des betrieblichen Datenschutzbeauftragten in das aufsichtliche Prüfungsverfahren sind zwei Alternativen denkbar:

1. Soweit keine Bedenken bestehen, informieren wir den jeweiligen Datenschutzbeauftragten direkt durch Zusendung eines Abdrucks unseres Anschreibens an das Unternehmen oder

2. wir legen dem Anschreiben an das Unternehmen einen Abdruck an den Datenschutzbeauftragten mit der Bitte bei, diesen in die Überprüfung der Beschwerde mit einzubeziehen.

Wir halten es für selbstverständlich und begrüßen es ausdrücklich, wenn die interne Überprüfung der Beschwerde vom Datenschutzbeauftragten als dem Datenschutzfachmann des Unternehmens durchgeführt wird. Er macht der Unternehmensleitung einen Vorschlag, wie sie sich gegenüber der Aufsichtsbehörde äußern sollte.

Das abschließende Schreiben an die Aufsichtsbehörde muss dann von der Leitung als der für den Datenschutz im Unternehmen Verantwortlichen oder einem von ihr Beauftragten unterschrieben werden. Dabei ist denkbar, dass auch der Datenschutzbeauftragte mit unterschreibt.

Der Intention der §§ 4f und 4g BDSG würde es jedoch aus den oben genannten Gründen widersprechen, wenn die Beschwerdebearbeitung allein auf den Datenschutzbeauftragten delegiert werden würde.

* * *

4 Einwilligungserklärungen

4.1 Die Gestaltung von datenschutzrechtlichen Einwilligungserklärungen in Formularen

In Antragsformularen aller Art, insbesondere von Versicherungen, Banken, und Kundenkarten sowie bei Preisausschreiben usw. fällt immer wieder auf, dass die vorformulierten datenschutzrechtlichen Einwilligungserklärungen nicht den Erfordernissen des § 4a BDSG entsprechen. Man hat zuweilen den Eindruck, dass Unternehmen die Einwilligungen, die sie von ihren Kunden verlangen, geradezu vor ihnen verstecken wollen. Auf der einen Seite erwecken sie mit der Aufnahme entsprechender Absätze über den Datenschutz den Anschein, dass sie den Datenschutz ernst nehmen. Auf der anderen Seite tun sie jedoch alles, um den Kunden davon abzulenken, dass er auf dem Formular zusätzlich zum eigentlichen Hauptgeschäft eine datenschutzrechtliche Einwilligung erklären soll.

Dies stellt einen Verstoß gegen § 4a Abs. 1 BDSG dar und führt dazu, dass die beabsichtigte Datenverwendung nicht auf eine wirksame Einwilligungserklärung gestützt werden kann.

Nach § 4a Abs. 1 BDSG muss der Betroffene unter anderem die Möglichkeit zu einer freien Entscheidung haben. Davon kann er nur Gebrauch machen, wenn er durch eine besondere Hervorhebung im Formular auf die von ihm verlangte Einwilligungserklärung aufmerksam gemacht worden ist. Er muss geradezu darauf gestoßen werden, dass er neben seinen vertraglichen Erklärungen noch zusätzlich eine datenschutzrechtliche Einwilligungserklärung abgibt.

Im Folgenden soll an Hand von Negativ- und Positivbeispielen aufgezeigt werden, wie wir den § 4a BDSG auf die uns vorgetragenen Praxisfälle anwenden und was unserer Auffassung nach bei der Gestaltung einer rechtmäßigen und damit wirksamen datenschutzrechtlichen Einwilligungserklärung beachtet werden muss.

4.1.1 Besondere graphische Hervorhebung

Die datenschutzrechtliche Einwilligungserklärung darf im Formulartext nicht untergehen, sondern muss sich von den anderen Textpassagen deutlich abheben, z. B. durch

- Fettdruck, Schriftart oder Schriftgröße,
- farbliche Gestaltung der Schrift oder des Hintergrundes,
- Umrahmung der Erklärung.

4.1.2 Platzierung

Eine Einwilligungserklärung genügt dem Erfordernis der besonderen Hervorhebung u. a. dann nicht, wenn sie

- allein in die Allgemeinen Geschäftsbedingungen eingestellt oder
- in eine Fußnote "abgeschoben" ist.

Die Einwilligungserklärung muss vielmehr in aller Regel **unmittelbar vor der Unterschrift** platziert werden. So kann man am besten gewährleisten, dass der Unterzeichnende auf sie aufmerksam wird.

Es ist aber unbedenklich, an dieser Stelle nur eine Kurzfassung aufzunehmen, die wie folgt lauten kann:

> **Datenschutzrechtliche Einwilligungserklärung**
> In die auf der Rückseite in der Rubrik "Datenschutzrechtliche Einwilligungserklärung" abgedruckte Verwendung meiner personenbezogenen Daten willige ich ein.

4.1.3 Überschrift

Häufig führen bereits die Überschriften denjenigen, der einwilligen soll, auf einen falschen Weg, wie die folgenden **Negativbeispiele** zeigen:

- Datenschutzerklärung
- Datenschutz
- Datenschutzklausel
- Hinweis zum Datenschutz
- Erklärung zum Datenschutz
- Erklärung zur Datenverarbeitung

Aufgrund dieser Überschriften kann ein Antragsteller nicht erkennen, dass im Anschluss eine von ihm abzugebende Erklärung folgt, mit der er sich mit einer besonderen Verwendung seiner personenbezogenen Daten einverstanden erklärt. Die Überschriften sagen etwas ganz anderes aus. So ist es ein fundamentaler Unterschied, ob jemand einwilligt oder nur auf den Datenschutz hingewiesen wird. In gleicher Weise hat eine Erklärung zum Datenschutz nichts mit einer Einwilligung in eine Datenverwendung zu tun.

Im Gegensatz dazu weisen folgende **Positivbeispiele** den Unterzeichnenden unmissverständlich auf die von ihm abzugebende Erklärung hin:

- Datenschutzrechtliche Einwilligungserklärung
- Einwilligungserklärung Datenschutz
- Einwilligungserklärung in die Datenverarbeitung
- Datenschutz/Einwilligung
- Datenschutzrechtliche Einwilligungsklausel
- Einwilligungserklärung nach dem Bundesdatenschutzgesetz
- Einwilligung in die Datenweitergabe

4.1.4 Wortlaut

Auch der vorformulierte Wortlaut muss für den Antragsteller klar erkennen lassen, dass er eine über das Hauptgeschäft hinausgehende Erklärung abgibt, mit der er in eine nicht schon vom Gesetzgeber erlaubte Verwendung seiner personenbezogenen Daten einwilligt.

Soll dagegen der Antragsteller dem Wortlaut nach bloß "Kenntnis nehmen“ oder wird er auf eine Datenverwendung „hingewiesen“ (vgl. folgende **Negativbeispiele**), so kann dies nicht als seine eigene Erklärung gewertet werden:

- „Mir ist bekannt, dass….“
- „Auf die auf der Rückseite abgedruckten Schlusserklärungen wird hingewiesen“
- „Der Unterzeichnende hat von den umseitigen Bedingungen Kenntnis genommen“

Dagegen kommt der Erklärungscharakter in den folgenden **Positivbeispielen** eindeutig zum Ausdruck:

- „Ich willige ein, dass ...“
- „Ich bin einverstanden, dass ...“
- „Mit der Unterschrift geben Sie Ihre Einwilligung, dass ...“
- „Durch Ihre Unterschrift wird die auf der Rückseite abgedruckte Einwilligungserklärung zur Datenverarbeitung und Datennutzung Bestandteil des Antrages.“

4.1.5 Inhalt

a) Die Einwilligungserklärung muss klar von den Datenschutzhinweisen im Sinne des § 4 Abs. 3 BDSG getrennt sein. Der Geschäftspartner kann sonst nur schwer erkennen, dass und inwieweit er eine Erklärung abgibt.

b) Datenschutzrechtliche Tatbestände, die bereits durch das BDSG oder eine andere Rechtsvorschrift geregelt sind, dürfen nicht in die Erklärung mit aufgenommen werden. Für den Erklärenden wäre der Umfang und damit auch die eigentliche Bedeutung seiner Erklärung nicht klar. Die Erklärung würde dadurch auch „verwässert“, man könnte auch sagen versteckt werden. Auf Grund der zunächst aufgeführten Selbstverständlichkeiten würden viele bis zur eigentlichen Einwilligungserklärung in den späteren Sätzen gar nicht mehr weiter lesen. Probleme gäbe es auch beim Widerruf der Erklärung.

c) Lediglich dann, wenn man sich nicht im Klaren ist, ob eine Datenverwendung einer Einwilligung bedarf, bestehen keine Bedenken, sie vorsichtshalber in die Einwilligungserklärung mit einzubeziehen.

d) Die Erklärung muss bestimmt genug und unmissverständlich sein. Auch ein Laie muss das, was er erklären soll, verstehen können.

e) So genügt es bei einer vorgesehenen Datenübermittlung nicht, nur den Begriff „Datenverarbeitung“ in die Erklärung aufzunehmen, da ein Laie nicht wissen kann, dass die Verarbeitung gemäß § 3 Abs. 4 BDSG die Übermittlung mit umfasst. Der Begriff „Übermittlung“ muss deshalb ggf. neben dem Begriff „Datenverarbeitung“ aufgeführt sein. Dabei sind die Empfänger einer Datenübermittlung so konkret wie möglich zu nennen.

f) § 4a BDSG lässt es zu, dass eine Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden kann. Sein Wortlaut lässt zwei Möglichkeiten offen:

   (1) Die Einwilligung ist gesondert zu unterschreiben (Opt in). Auf diese Weise wird dem Unterzeichnenden in jedem Fall bewusst, dass er eine zusätzliche Erklärung abgibt.

   (2) Die Erklärung für das Hauptgeschäft kann auch zusammen mit der datenschutzrechtlichen Einwilligungserklärung durch eine einheitliche Unterschrift abgedeckt werden.
   Dabei kann eine Streichmöglichkeit (Opt out) angeboten werden.

g) Soweit sich die Einwilligung auf besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) beziehen soll, ist bei der formularmäßigen Gestaltung der Erklärung § 4a Abs. 3 BDSG zu beachten.

4.2 Die Gestaltung von datenschutzrechtlichen Einwilligungen auf elektronischen Formularen im Internet

Häufiger Gegenstand telefonischer und schriftlicher Anfragen sowie Anlass von Beanstandungen bei Datenschutzprüfungen vor Ort ist die datenschutzgerechte Gestaltung von Einwilligungserklärungen auf elektronischen Formularen im Internet.

Nach § 4 Abs. 2 Teledienstedatenschutzgesetz hat der Diensteanbieter sicherzustellen, dass die elektronische Einwilligung

- nur durch eine eindeutige und bewusste Handlung des Nutzers erfolgen kann,
- sie protokolliert wird und
- ihr Inhalt jederzeit vom Nutzer abgerufen werden kann.

Für den Nutzer muss dabei erkennbar sein, auf welche Daten sich die Einwilligungserklärung bezieht und zu welchen Zwecken diese Daten verwendet werden sollen.

Typisch ist folgender Einzelfall:

Ein Telediensteanbieter beabsichtigte, die personenbezogenen Daten seiner Nutzer nicht nur für die Erfüllung des Vertragsverhältnisses mit dem Nutzer zu verwenden, sondern diese auch an "ausgewählte Partnerunternehmen" zu Werbezwecken zu übermitteln. Da diese Datenübermittlung nicht mehr der Zweckbestimmung des Vertragsverhältnisses dient, soll sie durch eine elektronische Einwilligung des Nutzers legitimiert werden.

In dem folgenden **Negativbeispiel** kommt nicht zum Ausdruck, dass der Betroffene eine eigene Einwilligungserklärung abgibt. Das von ihm abverlangte „Einverständnis mit den Datenschutzrichtlinien“ zielt in eine andere Richtung. Die Datenschutzrichtlinien werden dem Teledienstanbieter zugeordnet.

☐ *Die AGB habe ich gelesen und akzeptiere sie.*
Durch das Absenden des Formulars erkläre ich mich mit den ***Datenschutzrichtlinien*** *einverstanden.*

Absenden

Dagegen wird im folgenden **Positivbeispiel** für den Betroffenen der Erklärungscharakter deutlich:

☐ *Die AGB habe ich gelesen und akzeptiere sie.*

☐ *In die Übermittlung meiner gespeicherten personenbezogenen Daten (Adresse, Telefonnummer) an dritte Unternehmen für die Verwendung zu werblichen Zwecken willige ich ein. Näheres hierzu finden Sie in § … der AGB (Link).*

Registrierung abschicken

* * *

5 Internationaler Datenverkehr

5.1 Erweiterung der Europäischen Union

Die Europäische Union ist am 01. Mai 2004 um 10 Länder erweitert worden: Estland, Lettland, Litauen, Malta, Polen, Slowakei, Slowenien, Tschechien, Ungarn und Zypern. Datenübermittlungen in diese Staaten wie auch in die übrigen EU- und EWR-Staaten sind datenschutzrechtlich den Datenübermittlungen im Inland gleichgestellt (§ 4b Abs. 1 Nr. 1 und Nr. 2 BDSG). Die Prüfung auf der sog. zweiten Stufe (§§ 4b und 4c BDSG), wie sie sonst bei Datenübermittlungen ins Ausland nötig ist, findet hier demnach nicht statt.

5.2 Alternative Standardvertragsklauseln

Bisher gab es bei Datenübermittlungen in Drittländer die Möglichkeit, ein angemessenes Datenschutzniveau beim Datenempfänger dadurch zu gewährleisten, dass man die Standardvertragsklauseln für die Datenübermittlung in Drittländer vom 15.06.2001 bzw. die Standardvertragsklauseln für die Datenübermittlung an Auftragsdatenverarbeiter in Drittländern vom 27.12.2001 verwendete.

Seit 01.04.2005 stehen nun zusätzlich die so genannten „alternativen Standardvertragsklauseln“ zur Verfügung. Sie wurden von Wirtschaftsverbänden entworfen und mit der Europäischen Kommission mit der Absicht ausgehandelt, die Unternehmen zur intensiveren Nutzung von Vertragsklauseln zu veranlassen. Einige Klauseln wurden unternehmensfreundlicher gestaltet. Dafür erhielten die Datenschutzaufsichtsbehörden umfangreichere Eingriffs- und Sanktionsmöglichkeiten, um Datenmissbrauch vorzubeugen.

5.3 Übermittlung von Mitarbeiterdaten innerhalb eines internationalen Konzerns

Häufig werden Fragen zu der Fallkonstellation gestellt, dass ein deutsches Unternehmen Mitarbeiterdaten in einen Drittstaat übermittelt, weil dort die Personal-

verwaltung oder das Personalmanagement des Konzerns, dem das deutsche Unternehmen angehört, konzentriert wird.

In einem konkreten Fall sollten bestimmte Mitarbeiterdaten zu den genannten Zwecken an die Konzernmutter in den USA übermittelt werden. Übermittelt werden sollten: Name, Anschrift, Telefonnummer, E-Mail-Adresse, Position, Standort, Gehalt, Arbeitsleistung, bewertende Informationen, Ausbildung und berufliche Fähigkeiten.

Bei Datenübermittlungen in Drittländer muss immer eine zweistufige Prüfung erfolgen. Die erste Stufe betrifft die Voraussetzungen, die auch bei Übermittlungen innerhalb Deutschlands bzw. des EU/EWR-Raums zu beachten sind, d. h. es muss entweder eine gesetzliche Rechtsgrundlage vorliegen (§ 28 BDSG) oder eine Einwilligung der Betroffenen eingeholt werden.

Die Datenübermittlung kann hier unter den Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig sein. Das ist dann der Fall, wenn die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung überwiegt. Ein berechtigtes Interesse kann auch ein wirtschaftliches sein, so dass die hier genannten Gesichtspunkte ein berechtigtes Interesse begründen dürften.

Bei der durchzuführenden Abwägung ist zunächst davon auszugehen, dass die Interessen der betroffenen Mitarbeiter einer Übermittlung an sich entgegenstehen. Dies kann sich aber dann ändern, wenn die beteiligten Konzernunternehmen besondere Maßnahmen zugunsten der schutzwürdigen Interessen der Arbeitnehmer treffen. Welche Maßnahmen dies sind, kann nur im Einzelfall entschieden werden. In Betracht kommt die Schaffung eines Datenschutzkonzepts, das einheitliche Standards zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen und koordinierte Sicherheitsmaßnahmen sowie eine datenschutzkoordinierende Konzernstelle mit entsprechenden Weisungsrechten gegenüber den beteiligten Konzernunternehmen festschreibt. Der Verarbeitungsverlauf muss für die Betroffenen transparent sein. Schließlich muss der Arbeitgeber für die betroffenen Mitarbeiter Ansprechpartner bleiben, d. h. auch für deren datenschutzrechtliche Rechte auf Auskunft, Berichtigung, Löschung, Sperrung und Schadensersatz einstehen, zusätzlich zu dem Unternehmen, an das die

Daten übermittelt werden. Entsprechende Regelungen müssen zwischen den beteiligten Konzernunternehmen verbindlich getroffen werden, sei es durch Verträge oder in Form von verbindlichen Unternehmensregelungen.

Da die Daten in die USA gehen, ist auf der zweiten Stufe zu prüfen, ob beim Datenempfänger ein angemessenes Datenschutzniveau gegeben ist. Das angemessene Datenschutzniveau ist ohne weiteres dann zu bejahen, wenn der Empfänger sich den Regelungen des "Safe Harbor" unterworfen hat, ein Regelwerk, das von der Europäischen Kommission und der US-Regierung ausgehandelt wurde (Amtsblatt der Europäischen Gemeinschaften vom 25.08.2000, L 215/7; Fundstellen im Internet: http://www.export.gov/safeharbor/ bzw. http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list .

Ansonsten stellen die von der Europäischen Kommission erarbeiteten Standardvertragsklauseln vom 15.06.2001 und vom 27.12.2004 ("alternative Standardvertragsklauseln") eine praktikable Lösung dar, das angemessene Datenschutzniveau herzustellen. Werden sie vollständig und unverändert übernommen, bedarf es keiner behördlichen Genehmigung.

* * *

6 Versicherungen

6.1 Funktionsausgliederungen

Es kommt immer wieder vor, dass innerhalb von Versicherungskonzernen die gesamte Geschäftstätigkeit von einer Gesellschaft auf eine andere Gesellschaft übertragen wird. Die abgebende Gesellschaft hält dann überhaupt kein Personal mehr vor. Vielmehr wird die gesamte Geschäftstätigkeit von den Beschäftigten der „aufnehmenden Gesellschaft“ abgewickelt. Für die Versicherten ist dies nicht erkennbar, da die ihnen zugehenden Schreiben den Briefkopf der Versicherung aufweisen, mit der sie den Versicherungsvertrag abgeschlossen haben. Tatsächlich ist jedoch allein die aufnehmende Gesellschaft tätig geworden.

Aus der Sicht des Zivilrechts handelt die aufnehmende Gesellschaft “unter fremdem Namen“ für die abgebende Gesellschaft. Die Vorschriften über die Vertretung sind entsprechend anzuwenden.

Für die datenschutzrechtliche Bewertung ist festzustellen, dass die personenbezogenen Daten der Versicherungsnehmer jeweils von der abgebenden Gesellschaft an die aufnehmende übermittelt werden. Dort werden sie erhoben, verarbeitet und genutzt. Es beginnt mit der Erhebung der Stammdaten, die in einem Versicherungsantrag enthalten sind, und setzt sich mit der Abwicklung der Leistungsanträge im laufenden Versicherungsverhältnis fort.

Die datenschutzrechtliche Zulässigkeit dieser Vorgänge wurde bisher wohl überwiegend bejaht. Zum Teil berief man sich auf § 5 Abs. 3 Nr. 4 Versicherungsaufsichtsgesetz, der eine Funktionsausgliederung als Geschäftsmodell zumindest anspricht. Daneben wurde der § 28 Abs. 1 Satz 1 Nr. 2 BDSG als Zulässigkeitstatbestand herangezogen.

Gegen diese Ansicht bestehen erhebliche Bedenken. Denn es ist derzeit weder im BDSG noch in einer sonstigen Rechtsvorschrift eine Rechtsgrundlage für eine Funktionsausgliederung vorhanden.

So kann die Übermittlung der Stammdaten nicht auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden. Es ist schon sehr fraglich, ob dafür ein berechtigtes Inte-

resse der abgebenden Versicherung anerkannt werden kann. In jedem Fall sind die schutzwürdigen Interessen der Versicherungsnehmer an dem Ausschluss einer Datenübermittlung an eine Gesellschaft, mit der man keinen Vertrag abgeschlossen hat, und einer dortigen Datenverwendung gerade im Versicherungsbereich in aller Regel höher einzustufen.

Für die Gesundheitsdaten liegen die besonderen tatbestandlichen Voraussetzungen des § 28 Abs. 6 Nr. 3 BDSG ebenfalls nicht vor. Vor allem würden gerade hier die schutzwürdigen Interessen der Versicherungsnehmer entgegenstehen.

Auch § 5 Abs. 3 Nr. 4 Versicherungsaufsichtsgesetz (VAG) kann nicht als Zulässigkeitsvorschrift bezüglich der Datenverwendungen herangezogen werden. Nach dieser Bestimmung bedürfen Versicherungsunternehmen für den Geschäftsbetrieb der Erlaubnis der Aufsichtsbehörde. Als Bestandteil des mit dem Antrag einzureichenden Geschäftsplanes ist u. a. auch ein etwaiger Funktionsausgliederungsvertrag vorzulegen.

Diese Vorschrift kann nicht als zulässigkeitsbegründende bereichsspezifische Vorschrift im Sinne des Datenschutzrechts angesehen werden. Das heißt, die Zulässigkeit der mit einer Funktionsausgliederung zusammenhängenden Datenverwendungen beurteilt sich nach den Vorschriften des BDSG.

Als Rechtsgrundlage für eine Funktionsausgliederung kommt somit nur eine gemäß § 4a BDSG rechtswirksam erklärte datenschutzrechtliche Einwilligung der betroffenen Versicherungsnehmer, die auch bei bestimmten Versicherungssparten die Entbindung von der Schweigepflicht (!) beinhalten muss, in Betracht. In jedem Fall ist auf eine Transparenz dieser Vorgänge zu achten.

Dieser Rechtsauffassung hat sich zwischenzeitlich auch die Arbeitsgruppe "Versicherungswirtschaft" des „Düsseldorfer Kreises“ der Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich (vgl. 2.5.1) grundsätzlich angeschlossen.

Die bisher von der Versicherungswirtschaft in Absprache mit den Datenschutzaufsichtsbehörden verwendete Einwilligungserklärung bezieht die mit einer Funktionsausgliederung zusammenhängenden Datenverwendungen nicht mit ein. Eine Datenweitergabe zur Geschäftsabwicklung ist dort weder unmittelbar noch

mittelbar angesprochen. Auch im Merkblatt ist diese vom Normalfall nicht unwesentlich abweichende Art einer Vertragserfüllung auf Seiten der Versicherung nicht erwähnt.

Im Rahmen der derzeitigen gemeinsamen Bemühungen der Versicherungswirtschaft und der Datenschutzaufsichtsbehörden um eine Neugestaltung der datenschutzrechtlichen Einwilligungserklärung in Versicherungsanträgen haben wir den Vorschlag eingebracht, auch eine Einwilligung in bereits bestehende oder künftige Funktionsausgliederungen aufzunehmen. Einige Versicherungsgesellschaften haben dies inzwischen schon von sich aus getan.

Unabhängig davon sollte der Gesetzgeber prüfen, ob man den mit einer Funktionsausgliederung verbundenen Umgang mit personenbezogenen Daten von Versicherungsnehmern einmal auf eine gesetzliche Grundlage stellen könnte.

6.2 Zentrale Wahrnehmung interner Funktionen im Konzern

In Versicherungskonzernen sind interne Funktionen der Konzerntöchter häufig zentral bei der Muttergesellschaft angesiedelt. Dies gilt z. B. für die Revision und die Rechtsabteilung. Soweit dieses Personal interne Aufgaben einer Tochtergesellschaft erfüllt, kommt es dort auch mit personenbezogenen Daten der jeweiligen Versicherungsnehmer in Berührung.

Das Vorliegen einer rechtlichen Grundlage ist dann in den einzelnen Fällen entweder gar nicht, z. B. bei den besonderen Arten personenbezogener Daten, oder nur sehr schwer zu begründen. Meistens fehlt es auch an der Transparenz dieser Vorgänge. Darüber hinaus ist ggf. eine strafbewehrte Verschwiegenheitspflicht zu beachten.

Gerade deshalb empfiehlt sich auch insoweit die Einholung von entsprechenden Einwilligungserklärungen. Auf die Ausführungen unter 6.1 am Ende wird verwiesen.

6.3 Entbindung eines Arztes von der Schweigepflicht

In vielen Verträgen mit privaten Krankenversicherungen entbindet der Versicherungsnehmer die ihn behandelnden Ärzte für Rückfragen der Krankenversicherung von der Schweigepflicht. Diese Erklärung beinhaltet auch eine entsprechende datenschutzrechtliche Einwilligung. Sie soll pauschal für die gesamte Laufzeit des Vertrages gelten.

Schweigepflichtentbindungserklärungen mit diesem Inhalt entsprechen nicht mehr der Rechtslage seit Umsetzung der EG-Datenschutzrichtlinie durch die BDSG-Novelle im Jahr 2001. Im Hinblick auf die sich aus § 4a Absätze 1 und 3 BDSG ergebenden Anforderungen kann eine derartige pauschale Einwilligungserklärung nicht mehr als rechtswirksam angesehen werden. Es reicht nicht aus, wenn sie „sozusagen ins Blaue hinein“ für Fälle abgegeben wird, bei denen gar nicht absehbar ist, wie sie ausgestaltet sind.

Vielmehr muss der Versicherungsnehmer wissen, wen er für welchen Zweck von der Schweigepflicht gegenüber der Versicherung entbindet. Nur wenn er entsprechend informiert ist, kann er frei über die Abgabe der Erklärung entscheiden.

Deshalb genügt es nach unserer Auffassung auch nicht, wenn der Versicherungsnehmer mit jedem Leistungsantrag die Entbindung von der Schweigepflicht für alle Ärzte erklärt, deren Rechnungen er einreicht. Auch hier handelt es sich um eine pauschale und deshalb mit dem § 4a BDSG nicht vereinbare Erklärung. Es fehlt an dem für den Erklärenden unabdingbaren konkreten Einzelfallbezug. Bei einer Nachfrage durch die Versicherung ist er hier nicht informiert, bei welchem Arzt und zu welchem Zweck die Nachfrage erfolgt.

Wir gehen davon aus, dass die Entscheidung des Bundesverfassungsgerichts vom 23.10.2006 - BVerfG, 1 BvR 2027/02 - unsere Rechtsauffassung bestätigt hat.

6.4 Konkludente Schweigepflichtentbindung durch Vorlage der Klinik-Card im Krankenhaus?

Eine private Krankenversicherung hatte ihrem Versicherungsnehmer im Zusammenhang mit dem Versicherungsvertrag eine sog. Klinik-Card ausgehändigt. Diese Karte gab der Versicherungsnehmer im Rahmen eines Krankenhausaufenthaltes bei der Verwaltung ab, damit diese direkt mit dem Privatversicherer abrechnen konnte.

Nach Erhalt der Rechnung hatte die Krankenversicherung einige Rückfragen und forderte zu diesem Zweck direkt vom Krankenhaus ergänzende Informationen über die Behandlung, Erkrankung etc. des Patienten an. Sie stellte sich auf den Standpunkt, dass der Patient allein mit der Vorlage der Klinik-Card durch schlüssiges Verhalten in die Übermittlung seiner Behandlungsdaten an die Krankenversicherung eingewilligt und damit gleichzeitig die Ärzte von der Schweigepflicht entbunden hätte.

Das Krankenhaus hat mit Recht die Herausgabe der gewünschten Daten wegen fehlender Schweigepflichtentbindung durch den Patienten abgelehnt.

Gemäß § 4a Abs. 1 Satz 3 BDSG bedarf die datenschutzrechtliche Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Eine schriftliche Einwilligung in die Datenübermittlung lag hier unstreitig nicht vor.

Die Vorlage der Klinik-Card kommt als "andere Form" der Einwilligung zunächst einmal für die Datenübermittlung vom Krankenhaus an die Krankenversicherung im Rahmen der Einreichung der Abrechnung in Betracht. Der Patient möchte ja gerade durch die Vorlage der Card die Abrechnung auf dem "direkten Weg" vom Krankenhaus zur Krankenkasse ermöglichen.

Im Gegensatz dazu ist aber die Frage, ob sich diese Einwilligung auch auf die Übermittlung darüber hinaus gehender Daten bezieht, zu verneinen! Man kann nicht annehmen, dass jeder Patient, der durch Vorlage der Klinik-Card eine direkte Rechnungstellung des Krankenhauses gegenüber der privaten Krankenversicherung veranlasst, noch zusätzlich mit einer weitergehenden Datenübermittlung

einverstanden ist. In gleicher Weise kann man auch in dem Fall, in dem der Versicherungsnehmer die Rechnung selbst bei der Versicherung einreicht, nicht ohne weiteres von der konkludenten Abgabe einer derartigen Einverständniserklärung ausgehen.

Vielmehr muss der Betroffene in beiden Fällen für die Beantwortung von Nachfragen eine zusätzliche - in der Regel schriftliche - Einwilligungserklärung, die auch die Entbindung von der Schweigepflicht enthält, abgeben.

6.5 Zulässigkeit der Anforderung von Krankenhausentlassberichten, OP-Berichten und ähnlichen umfassenden medizinischen Berichten durch private Krankenversicherungen

Es handelt sich hier um die Erhebung und Verwendung von Gesundheitsdaten, d. h. von besonderen Arten personenbezogener Daten. Sie ist gemäß § 28 Abs. 6 Nr. 3 BDSG ohne Einwilligung des Betroffenen für eine private Krankenversicherung nur zulässig, wenn sie u. a. zur Ausübung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung überwiegt.

Für die vom Arzt durchzuführende Datenübermittlung muss dann noch eine gemäß § 4a BDSG rechtswirksame Einwilligungserklärung einschließlich der Schweigepflichtentbindung durch den Patienten hinzukommen.

Voraussetzung für die Zulässigkeit der Anforderung derartiger Berichte ist somit zunächst, dass diese Datenerhebung im Rahmen "der Ausübung eines Rechtsanspruches der Krankenversicherung erforderlich ist". Diese Frage ist anhand des § 34 VVG zu beantworten. Nach dieser Bestimmung hat der Versicherungsnehmer, der eine Leistung der Krankenversicherung beantragt, die erforderlichen Nachweise vorzulegen bzw. die Krankenversicherung kann sie von ihm einfordern.

Dabei müssen auch der Grundsatz der Verhältnismäßigkeit sowie das Gebot der Datenvermeidung und Datensparsamkeit beachtet werden. Das Versicherungsunternehmen darf nur die erforderlichen, d. h. die personenbezogenen Daten er-

heben, verarbeiten und nutzen, die es zur Überprüfung seiner Leistungspflicht benötigt. Stehen mehrere Alternativen von Datenerhebungen zur Verfügung, so ist diejenige zu wählen, die diesen Prinzipien am ehesten gerecht wird.

Wenn es beispielsweise um die Überprüfung einzelner Rechnungspositionen geht, muss man nach hiesiger Ansicht davon ausgehen, dass in vielen Fällen eine konkrete Einzelnachfrage bei dem Arzt für die Klärung der Leistungsverpflichtung ausreicht. Die Anforderung des gesamten Krankenhausentlassberichtes ist dann nicht erforderlich. Er enthält nämlich eine Vielzahl von Daten, die in den meisten Fällen weit über den konkreten Informationsbedarf der Krankenversicherung hinausgeht.

Sicher gibt es Ausnahmefälle, in denen die Versicherung nach sorgfältiger Prüfung zu dem Ergebnis kommt, dass die anstehende Frage allein durch die Einsichtnahme in den Entlassbericht beantwortet werden kann. Sie muss die Anforderung dann dem Betroffenen gegenüber besonders begründen. Gegebenenfalls sollte sie ihm die Möglichkeit einräumen, dem persönlichen Lebenskreis zurechenbare Teile zu schwärzen.

In Beschwerdefällen ist die Erforderlichkeit der Anforderung auch der Datenschutzaufsicht darzulegen.

* * *

7 Banken

7.1 Versendung eines Darlehensangebotes als Infobrief

Der Kunde einer bayerischen Bank erhielt das Angebot zur Verlängerung seines Darlehens als Infobrief zugesandt. Dieser Infobrief ist auf dem Postweg von der Deutschen Post AG zu Prüfzwecken geöffnet worden. Der Bankkunde sah sich dadurch in seinem Persönlichkeitsrecht verletzt und hat sich bei uns über diese Art der Versendung beschwert.

Die Deutsche Post AG bietet Unternehmen an, Infobriefe zu einem günstigeren Porto zu versenden. Dabei behält sie sich nach ihren AGB`s vor, Infobriefe zu Prüfzwecken zu öffnen.

Die Versendung eines Darlehensangebotes als Infobrief verstößt gegen die Verpflichtung zur Weitergabekontrolle gemäß Nr. 4 der Anlage zu § 9 Satz 1 BDSG. Nach dieser Bestimmung muss die verantwortliche Stelle u. a. gewährleisten, dass personenbezogene Daten während ihres Transports nicht unbefugt gelesen werden können.

Die Bank gab an, dass den Mitarbeitern, die mit dem Postversand beauftragt sind, die dabei zu beachtenden Erfordernisse des Datenschutzes bekannt sein mussten. Es habe sich im vorliegenden Fall um ein bedauerliches Versehen gehandelt. Die betreffenden Mitarbeiter seien durch den Datenschutzbeauftragten nochmals auf die maßgeblichen Kriterien und die Beachtung der ihnen obliegenden Sorgfaltspflicht hingewiesen worden.

Wir haben die Angelegenheit gegenüber der Bank datenschutzrechtlich beanstandet.

7.2 Legitimation des Betreuers eines Bankkunden

Eine Bank verlangte vom Betreuer eines Kunden zum Nachweis seiner Legitimation den entsprechenden Beschluss des Amtsgerichts. Der Betreuer lehnte dies

ab, da in der Begründung des Beschlusses auch Angaben über die Gesundheit des Betreuten enthalten waren.

Die Bank räumte zwar ein, an den Gesundheitsdaten kein Interesse zu haben, bestand jedoch gleichwohl auf ihrer Forderung. Der Betreuer bat uns deshalb um eine datenschutzrechtliche Überprüfung.

Wir kamen dabei zu dem Ergebnis, dass für die von der Bank geforderte Einsichtnahme in den Gerichtsbeschluss bezüglich der dort enthaltenen Angaben über die Gesundheit keine Rechtsgrundlage vorhanden war. Die Erhebung der im Betreuerausweis enthaltenen Daten reichte für die Zwecke der Bank völlig aus. Die Bestellung des Betreuers sowie seine Befugnisse können dort entnommen werden. Ein darüber hinaus gehender Informationsbedarf der Bank war nicht erkennbar.

Wir haben das Verhalten der Bank beanstandet.

7.3 Auskünfte über den Nachlass an ein nicht erbberechtigtes Kind

Der Sohn eines Verstorbenen ist von diesem testamentarisch zum Alleinerben bestimmt worden. Gleichwohl trat seine nicht erbberechtigte Schwester an das Kreditinstitut ihres Vaters heran, legte die Sterbeurkunde vor und bat um Herausgabe der Vermögensaufstellung des Verstorbenen. Dabei hat sie der Bank gegenüber versichert, sie sei von ihren Geschwistern beauftragt worden, sich einen Überblick über die Vermögensverhältnisse zu verschaffen.

Die Bank gab die gewünschten Informationen heraus. Dem Sachbearbeiter war die Tochter des Verstorbenen persönlich bekannt und er vertraute auf ihre Aussage.

Diese Datenübermittlung war unzulässig. Kreditinstitute dürfen Informationen über die Vermögensverhältnisse Verstorbener nur an Berechtigte herausgeben, die sich z. B. mit Erbschein ausweisen. Werden, wie es im vorliegenden Fall geschehen ist, Kontodaten ohne Vorlage des Erbscheins oder anderer schlüssiger

Unterlagen an eine unbefugte Person herausgegeben, stellt dies einen Datenschutzverstoß und einen Verstoß gegen das vertraglich zugesicherte Bankgeheimnis dar.

Wir haben diese Datenübermittlung beanstandet.

7.4 Unbefugte Übermittlung von Kontodaten

Eine Bankmitarbeiterin hat im privaten Umfeld Informationen weitergegeben, die ihr im Zusammenhang mit ihrer Tätigkeit bei der Bank bekannt geworden sind. So teilte sie einem Dritten mit, welches Konto ein Kunde mit Barabhebungen belastet und in welchen Ländern er Barabhebungen getätigt hat. Sie hatte diese Informationen aus der automatisierten Verarbeitung ihrer Bank entnommen.

Wir sahen darin einen eklatanten Verstoß gegen den Datenschutz. Der Mitarbeiterin war bekannt, dass sie zur Verschwiegenheit über bankinterne Angelegenheiten verpflichtet ist und dennoch hat sie mit Wissen und Wollen Informationen über den Kunden weitergegeben.

Gegen die Mitarbeiterin haben wir ein Bußgeldverfahren durchgeführt.

* * *

8 Auskunfteien

Im Bereich der Auskunfteien sind die Anfragen, Eingaben und Beschwerden gegenüber den vorhergehenden Jahren etwas zurückgegangen. Vielleicht ist dies auch darauf zurückzuführen, dass wir den Auskunfteien bei unserer Prüfungstätigkeit seit vielen Jahren ein besonderes Augenmerk widmen.

8.1 Warndatei für Ärzte

Ein Verein fragte nach, unter welchen Voraussetzungen er für seine als freiberufliche Ärzte tätigen Mitglieder eine elektronische Warndatei zur Aufnahme von Patienten einrichten kann, die ihre Arztrechnungen ganz oder teilweise nicht bezahlt haben.

Bei diesem Vorhaben handelt es sich um den Betrieb einer Auskunftei im Sinne von § 29 BDSG. Die in der geplanten Datei enthaltenen Informationen sind zum Zweck der Übermittlung gespeichert und dienen der Tätigkeit einer Auskunftei. Mit der Datei wird der Zweck verfolgt, durch die Übermittlung von Informationen über negativ in Erscheinung getretene Personen die dem Verein angehörenden Ärzte vor finanziellen Verlusten zu schützen. Der Verein verfolgt daher denselben Zweck wie gewerbsmäßig arbeitende Auskunfteien. Auch wenn er kein Entgelt für sein Angebot verlangt, betreibt er die Tätigkeit geschäftsmäßig. Man versteht darunter jede auf eine gewisse Dauer hin angelegte Tätigkeit. Dabei kommt es nicht darauf an, ob die Tätigkeit mit Einnahmen verbunden ist.

Neben den üblichen datenschutzrechtlichen Anforderungen an Auskunfteien ist hier insbesondere zu beachten, dass mit der Einmeldung des Zahlungsrückstandes auch die Information übermittelt wird, dass die bestimmte Person in ärztlicher Behandlung war. Damit werden Daten offenbart, die einerseits der durch § 203 StGB sanktionierten ärztlichen Geheimhaltungspflicht unterliegen und an die andererseits auch das BDSG besondere datenschutzrechtliche Anforderungen stellt, weil Angaben über die Gesundheit als besondere Arten personenbezogener Daten gelten.

Da eine gesetzliche Rechtsgrundlage für die Übermittlung der Gesundheitsdaten in § 28 Abs. 6 bis 9 BDSG nicht enthalten ist, ist eine Einwilligung der Patienten erforderlich, die den Anforderungen des § 4a BDSG genügen muss. Diese Einwilligung muss wegen der ärztlichen Geheimhaltungspflicht darüber hinaus eine Entbindung von der Schweigepflicht enthalten.

Da die Verantwortung für die Zulässigkeit der Datenübermittlung an den Verein das einmeldende Mitglied trägt, muss dieses für eine wirksame Einwilligung des Patienten sorgen.

Die Auskunfteitätigkeit des Vereins richtet sich - wie bei allen anderen Auskunfteien - nach § 29 BDSG. Zwar gelten bei der Verarbeitung von besonderen Arten personenbezogener Daten durch Auskunfteien § 28 Abs. 6 bis 9 BDSG entsprechend (vgl. § 29 Abs. 5 BDSG). Diese besonderen Vorschriften waren hier jedoch nicht anzuwenden, da nach den Plänen des Vereins für die Auskunftserteilung, also zum Zweck der Übermittlung, keine Angaben zur Gesundheit gespeichert werden sollten. Zur Auskunftserteilung sollte neben den Angaben zur Identifikation (Name und Anschrift des Betroffenen) nur gespeichert werden, dass die konkrete Person mit der Zahlung einer Rechnung in Verzug geraten ist. Bei welchem Arzt sich der Betroffene im Zahlungsrückstand befindet, sollte nicht beauskunftet werden.

Da auch der abfragende Arzt an den Verein die Information weitergibt, dass der Betroffene dort Patient ist, muss er ebenfalls eine datenschutzrechtliche Einwilligung des Patienten einschließlich der Entbindung von der ärztlichen Schweigepflicht einholen.

Darüber hinaus muss er gegenüber der Auskunftei ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft darlegen (Durchführung der Behandlung auf offene Rechnung), denn eine Datenübermittlung durch die Auskunftei ist nach § 29 Abs. 2 BDSG nur dann zulässig, wenn der Datenempfänger ein berechtigtes Interesse dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Wie bei anderen Auskunfteien zum Schutz vor Zahlungsausfällen, sehen wir eine Information Dritter über einen Zahlungsrückstand des Betroffenen nur dann für zulässig an, wenn Zahlungsunfähigkeit oder Zahlungsunwilligkeit bei dem Betrof-

fenen zweifelsfrei festgestellt werden kann. Dies ist nach unserer Auffassung nur dann möglich, wenn es sich um eine unbestrittene Forderung handelt und der Schuldner insgesamt mindestens viermal gemahnt wurde, davon zweimal durch den Arzt und zweimal qualifiziert durch einen Anwalt oder ein Inkassounternehmen. Dem Schuldner muss jeweils ausreichend Zeit zur Reaktion bzw. zum Zahlungsausgleich eingeräumt worden sein.

Wir haben den Verein auch darauf hingewiesen, dass die für Auskunfteien geltenden datenschutzrechtlichen Rahmenbedingungen einzuhalten sind. Dazu gehört neben den Anforderungen des § 29 BDSG insbesondere die Wahrung der Rechte der Betroffenen (Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung), die Bestellung eines Datenschutzbeauftragten sowie die Meldung bei der Aufsichtsbehörde.

8.2 Datenerhebung einer Auskunftei beim Bauamt einer kreisangehörigen Gemeinde

Ein Betroffener bat uns um Unterstützung, weil er befürchtete, dass eine Auskunftei Daten zu seiner Person rechtswidrig erhoben hat. Unter anderem störte sich der Betroffene an der Speicherung der Angabe, dass die Immobilie im „Eigentum der Eheleute“ steht.

Die Auskunftei teilte uns mit, dass ihr das gemeindliche Bauamt die Information gegeben hatte, die Immobilie sei "von den Eheleuten" gekauft worden.

Ungeachtet der Tatsache, dass das Bauamt Informationen über den Betroffenen überhaupt nicht herausgeben durfte, sind wir bei unserer Überprüfung zu dem Ergebnis gekommen, dass schon die Nachfrage der Auskunftei beim Bauamt nicht zulässig war. Die von den Bürgern den Behörden mitgeteilten personenbezogenen Daten dürfen an private Dritte ohne Einwilligung der Bürger nur in Ausnahmefällen mitgeteilt werden, wenn nämlich eine Rechtsvorschrift dies erlaubt, wie z. B. bei Auskünften aus dem Melderegister oder dem Gewerberegister. Ein derartiger Ausnahmefall lag aber hier nicht vor. Es bestand somit Grund zu der Annahme, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Datenerhebung beim Bauamt hatte (§ 29 Abs. 1 Nr. 1 BDSG).

Zwar erheben Auskunfteien Daten ohne Kenntnis des Betroffenen auch bei Dritten. In Frage kommen insbesondere allgemein zugängliche Quellen wie z. B. das Handelsregister, Insolvenzveröffentlichungen, das Schuldnerverzeichnis, das Gewerberegister oder das Einwohnermeldeamt.

Eine Ausnahme von dem in § 4 Abs. 2 Satz 1 BDSG festgelegten Grundsatz der Direkterhebung ist aber nur in engen Grenzen möglich (vgl. § 4 Abs. 2 Satz 2 BDSG). Auch hier dürfen keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Aus diesem Grund stellte die Datenerhebung beim Bauamt gleichzeitig einen Verstoß gegen den Grundsatz der Direkterhebung dar.

Wir haben dem Betroffenen mitgeteilt, dass wir nur die Datenerhebung durch die Auskunftei überprüfen konnten. Wegen der Datenübermittlung vom Bauamt an die Auskunftei könne er sich an den behördlichen Datenschutzbeauftragten der Gemeinde oder an den für die Datenschutzkontrolle zuständigen Bayerischen Landesbeauftragten für den Datenschutz wenden.

8.3 Vermieteranfragen bei Auskunfteien

In den letzten Jahren wurde vermehrt die Frage aufgeworfen, wie Vermieter vor Abschluss eines Mietvertrages in datenschutzrechtlich zulässiger Weise die Bonität von Mietinteressenten überprüfen können.

Es sind folgende Möglichkeiten denkbar:

1. Spezielle, d. h. geschlossene Auskunftssysteme für Vermieter mit bonitätsrelevanten Negativdaten der Betroffenen nur aus Mietverhältnissen und mit Daten aus den öffentlichen Schuldner- und Insolvenzlisten sind bei entsprechender rechtlicher Ausgestaltung mit dem Datenschutzrecht vereinbar.

2. Wir halten es aber auch für zulässig, wenn eine Auskunftei an einen Vermieter vor Eingehung eines Mietverhältnisses unter Berücksichtigung der schutzwürdigen Interessen der potentiellen Mieter nur die im Folgenden genannten Daten übermittelt:

a) "Harte" Negativdaten zur Bonität jeder Art, insbesondere rechtskräftige Urteile, Vollstreckungsbescheide, Daten aus den Schuldnerverzeichnissen.

b) Unbestrittene offene Forderungen jeder Art in einer Höhe von mindestens 1500 € oder mehrere Forderungen in einer Gesamthöhe von mindestens 1500 €, wenn mindestens zweimal durch den Gläubiger und mindestens einmal durch ein Inkassobüro oder einen Anwalt gemahnt worden ist.
   Durch die Betragsbegrenzungen nach unten werden die bei der Interessenabwägung nach § 29 Abs. 2 BDSG zu beachtenden schutzwürdigen Belange der Betroffenen angemessen berücksichtigt. Für ein Mietverhältnis kaum relevante kleinere Beträge, z. B. aufgrund von Handyrechnungen, wirken sich damit für die Betroffenen nicht negativ aus.

c) Nicht gerechtfertigte Nichtzahlung von zwei Mieten während der ersten drei Monate des Mietvertrags und Erstattung einer Anzeige durch den geschädigten Vermieter wegen Einmietungsbetrugs ("Mietnomaden").

* * *

9 Handel, Dienstleistung

9.1 Kundenbindungsprogramme

9.1.1 Allgemeines

Kundenkarten, bei deren Einsatz Rabatte oder sonstige Vorteile gewährt sowie Rabattpunkte gesammelt werden können (Kundenbindungsprogramme), erfreuen sich nach wie vor großer Beliebtheit bei den Kunden. Offensichtlich stören sich nur wenige daran, dass sie beim Einkauf mit einer Karte ihre Anonymität als Käufer aufgeben.

Aus datenschutzrechtlicher Sicht ist dabei entscheidend, dass nur die für die Abwicklung des Kundenbindungsprogramms dienlichen Kundendaten erhoben werden. Die Kunden müssen umfassend und verständlich über die Datenerhebung und -verwendung informiert werden. Wenn von ihnen darüber hinaus eine Einwilligung in eine weitere Datenverwendung abverlangt wird, muss dies zusammen mit dem damit verfolgten Zweck klar und deutlich herausgestellt werden (vgl. 4.1).

Die in unserem ersten Tätigkeitsbericht empfohlene Modifizierung der Formulare für Kundenbindungsprogramme wurde inzwischen von den Unternehmen weitgehend umgesetzt. Neue Anbieter von Kundenkarten auf dem Markt werden von uns entsprechend beraten.

Wenn auch Kundenbindungsprogramme unter datenschutzrechtlichen Gesichtspunkten häufig diskutiert werden, so haben die meisten Kunden damit offensichtlich keine Probleme. Uns erreichten im Zeitraum 2004/2005 dazu nur neun Eingaben. Diese Zahl steht in keinem Verhältnis zu der im hohen zweistelligen Millionenbereich liegenden Gesamtzahl der in Deutschland ausgegebenen Kundenkarten.

Bei unseren Prüfungen der Einzelfälle haben sich bisher keine wesentlichen Datenschutzverstöße ergeben.

9.1.2 Teilnahmebedingungen einer nicht beantragten Rabattkarte

Ein Zeitungsverlag sandte seinen Abonnenten eine Rabattkarte zu. Nach einem Passus in den Teilnahmebedingungen erklären sich die Teilnehmer am Rabattprogramm damit einverstanden, dass ihre Daten auch für Werbe- und Marktforschungszwecke verwendet werden, wenn sie „ihre Einwilligung" nicht widerrufen.

Die betroffenen Abonnenten, die die Rabattkarte nicht beantragt hatten, störte, dass sie beim Einsatz der Karte selbst aktiv werden müssen, wenn sie mit der Nutzung ihrer Daten für Werbung nicht einverstanden sind.

Der Verlag hat uns auf Nachfrage mitgeteilt, dass für Werbe- und Marktforschungszwecke ausschließlich die im sog. Listenprivileg (§ 28 Abs. 3 Satz 1 Nr. 3 BDSG) aufgeführten Daten und auch nur für eigene Werbezwecke des Verlages, genutzt werden. Eine Weitergabe von Daten an Dritte sei in jedem Fall ausgeschlossen.

Wir haben den Verlag darauf hingewiesen, dass die von ihm in die Teilnahmebedingungen eingestellte „Einwilligungserklärung“ die Anforderungen des § 4a BDSG nicht erfüllt (vgl. 4.1.2) und deshalb schon aus diesem Grund keine Rechtswirkungen entfalten kann. Auf der anderen Seite bedürfen die vom Verlag beabsichtigten Datenverwendungen keiner Einwilligung, da sie sich im Rahmen des § 28 Abs. 3 Satz 1 Nr. 3 BDSG bewegen. Es genügt deshalb ein Hinweis gemäß § 4 Abs. 3 BDSG.

In Anlehnung an den bisherigen Text des Verlags haben wir dem Verlag in dem konkreten Fall für einen "Hinweis zum Datenschutz" folgende Formulierung vorgeschlagen:

> *"Die Firma ……., Anschrift, erhebt, verarbeitet und nutzt die Abonnentendaten (Name, Anschrift, Abonummer) und die beim Einsatz der Kundenkarte anfallenden Daten, soweit dies für die Durchführung des Bonusprogrammes erforderlich ist.*
> *Weiterhin können Name und Anschrift der Karteninhaber für Marktforschungs- und Marketingzwecke im Rahmen der gesetzlichen Bestimmungen genutzt werden. Eine Nutzung für Marketingzwecke erfolgt nur, soweit diese Vorteile, Vergünstigungen oder Ähnliches bieten. Eine Marktfor-*

schung muss zum Ziel haben, die Angebote im Rahmen der Kundenkarte zu verbessern. Gegen die Nutzung der Abonnentendaten für Marktforschungs- und Marketingzwecke kann bei der Firma ….. Widerspruch eingelegt werden.
Eine Übermittlung von Abonnentendaten an Dritte findet nicht statt.
Seine Rechte nach dem Bundesdatenschutzgesetz, insbesondere Auskunft (§ 34 BDSG) sowie Berichtigung, Löschung und Sperrung (§ 35 BDSG) kann der Teilnehmer durch schriftliche Erklärung gegenüber der Firma …… ausüben."

9.2 Anschriftenermittlung durch ein Inkassobüro

Die Bewohnerin eines Mehrfamilienhauses fand in ihrem Briefkasten ein Schreiben eines Inkassobüros. Erst nachdem sie es geöffnet hatte, erkannte sie, dass das Schreiben nicht an sie, sondern an die Hausverwaltung gerichtet war, die allerdings nicht in diesem Haus untergebracht ist. Vermutlich hat der Briefträger das an diese Hausnummer adressierte Schreiben in irgendeinen Briefkasten des Hauses eingeworfen.

In dem Schreiben ging es um eine Anschriftenermittlung. Das Inkassobüro wollte über die Hausverwaltung des Anwesens in Erfahrung bringen, wo eine Schuldnerin, die vor etlichen Jahren dort gewohnt hatte, verblieben ist.

Die Empfängerin des Briefes hat bei uns nachgefragt, ob derartige Recherchen und die gewählte Art und Weise zulässig sind.

Die Erhebung von personenbezogenen Daten muss nach dem BDSG grundsätzlich beim Betroffenen selbst erfolgen (Grundsatz der Direkterhebung, § 4 Abs. 2 Satz 1 BDSG). Abweichend davon kann eine Datenerhebung bei Dritten zulässig sein, wenn der Geschäftszweck der verantwortlichen Stelle eine Erhebung bei anderen Personen oder Stellen erforderlich macht und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden (§ 4 Abs. 2 Satz 2 Nr. 2a BDSG).

Das Inkassobüro hatte auf Grund eines Auftrages versucht, sich mit der Schuldnerin direkt in Verbindung zu setzen. Da ihre aktuelle Anschrift nicht bekannt war,

kann diese Information nur bei Dritten erhoben werden. Die Fortführung des Auftrages macht daher die Datenerhebung bei Dritten erforderlich.

Zwar berührt das hier in Rede stehende Schreiben des Inkassobüros das Persönlichkeitsrecht der Betroffenen, weil persönliche Lebenssachverhalte einem Dritten (hier der Hausverwaltung der letzten bekannten Anschrift) offenbart werden. Grundsätzlich muss aber – auch zum Schutz der Allgemeinheit – verhindert werden können, dass sich Schuldner durch Wechsel des Aufenthaltsortes ohne Unterrichtung der Gläubiger sowie ohne Ummeldung bei der Gemeinde der Eintreibung einer Forderung entziehen können.

Wir sind bei der hier im Rahmen des § 4 Abs. 2 Satz Nr. 2a und des § 28 Abs. 1 Satz 1 Nr. 2 BDSG durchzuführenden Interessenabwägung zu dem Ergebnis gekommen, dass schutzwürdige Interessen der Betroffenen dann zurückstehen müssen, wenn zur Feststellung des Aufenthaltsortes des Schuldners sämtliche andere Möglichkeiten (z. B. Einwohnermeldeamt) fruchtlos ausgeschöpft worden sind und dem Empfänger eines Anschriftermittlungsschreibens nur die für den Zweck der Anfrage unbedingt notwendigen Informationen mitgeteilt werden.

Das Inkassobüro konnte insoweit darlegen, dass vor dem Versenden des Anschriftenermittlungsschreibens sämtliche weniger beeinträchtigende Möglichkeiten zur Feststellung der aktuellen Anschrift fruchtlos ausgeschöpft wurden.

Allerdings war in dem Anschreiben an die Hausverwaltung der Name des Gläubigers enthalten. Da diese Information für die Ermittlung des Aufenthaltsortes irrelevant war, haben wir dies beanstandet.

Darüber hinaus haben wir die fehlerhafte Adressierung beanstandet. Das Inkassobüro hat nämlich nicht geprüft, ob die Hausverwaltung unter der angegebenen Hausnummer erreichbar ist. Damit hat das Büro es in Kauf genommen, dass unbefugte Dritte von personenbezogenen Daten Kenntnis erhalten.

9.3 Datenerhebung bei Zahlungen mit EC-Karte

Mehrere Eingaben bezogen sich darauf, dass Einzelhandelsunternehmen bei der Bezahlung mit EC-Karte im Lastschriftverfahren die Vorlage des Ausweises verlangen und z. B. die Adressdaten aus dem Ausweis entweder auf dem Zahlungsbeleg notieren oder in einem dafür vorgesehenen Formblatt festhalten.

Wir haben die Sachverhalte überprüft und sehen es als gerechtfertigt an, dass ein Händler zur Verhinderung/Aufklärung von Kartenmissbrauch bzw. zur Vorsorge für Fälle von Rücklastschriften die hierfür erforderlichen personenbezogenen Daten des Kunden erhebt. Zwar würde es für die Feststellung der Identität des Käufers ausreichen, Einsicht in den Ausweis zu nehmen. Die Datenerhebung aus dem Ausweis ist jedoch zur Wahrung der Interessen des Händlers erforderlich. Einerseits wird die Hemmschwelle für einen Kartenmissbrauch angehoben, weil ein unrechtmäßiger Besitzer auf diese Weise von einer missbräuchlichen Verwendung der EC-Karte abgehalten werden kann. Andererseits wird auch das Kassenpersonal dazu verpflichtet, die Vorlage eines Ausweises zu verlangen und ihn genau zu prüfen. Die Erhebung der Ausweisdaten dient auch den Interessen der Allgemeinheit, missbräuchliche Verwendungen von EC-Karten zu verhindern. Auf Grund der Adressenerhebung kann das Unternehmen bei Nichteinlösung der Lastschrift ohne Bankrückfrage sofort die anderweitige Einziehung der offenen Forderung in die Wege leiten.

Es dürfen allerdings aus dem Ausweis nur die Daten erhoben werden, die für den festgelegten Zweck erforderlich sind. Zur Verhinderung/Aufklärung von Kartenmissbrauch bzw. zur Eintreibung einer offenen Forderung sehen wir nur die Erhebung folgender Daten für erforderlich an: Name, Vorname, Straße, PLZ, Wohnort und Geburtsdatum. Für die Erhebung der Pass- bzw. Personalausweisnummer, des Ausstellungsdatums sowie der ausstellenden Behörde können wir keine Notwendigkeit erkennen.

Die Erhebung der Pass-/Personalausweisnummer, des Ausstellungsdatums sowie der ausstellenden Behörde wurde daher von uns beanstandet. In einem Fall, in dem für die Erhebung der Ausweisdaten ein Formular verwendet wurde, haben wir dem Unternehmen eine entsprechende Anpassung nahe gelegt.

Aus Gründen der Transparenz gegenüber den Kunden haben wir darüber hinaus gefordert, rechtzeitig z. B. durch ein Hinweisschild an der Kasse darüber zu informieren, dass bei Bezahlung mit EC-Karte ein Ausweis zur schriftlichen Erhebung der Adresse und des Geburtsdatums vorgelegt werden muss. Der Kunde kann sich dann überlegen, ob er mit der EC-Karte im Lastschriftverfahren oder bar zahlt. Das Kassenpersonal muss darüber hinaus Auskunft geben können, wofür die Daten benötigt werden und was mit den Daten weiterhin geschieht.

9.4 Datenerhebung bei Kauf auf Rechnung

Die Kundin eines Baumarktes beschwerte sich darüber, dass sie beim Kauf von Baumaterial auf Rechnung über die Adresse hinaus noch das Geburtsdatum und Daten zu Beruf und Arbeitgeber angeben musste. Der Kaufpreis belief sich auf etwas über 1000 €.

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben und Speichern personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient. Durch die Bestellung auf Rechnung schloss die Betroffene mit dem Baumarkt einen Vertrag mit kreditorischem Risiko.

Das Geburtsdatum dient vor allem der Identifizierung, um Verwechslungen bei Namensgleichen zu vermeiden. Der Baumarkt kann im vorliegenden Fall auch Angaben zu Beruf und Arbeitgeber abfragen, um sich vor Kreditbetrug und sonstigen Zahlungsausfällen zu schützen. Denn bekannterweise werden nicht alle Rechnungen ordnungsgemäß bezahlt. Die Unternehmen und auch die redlichen Teilnehmer am Wirtschaftsleben müssen solche Zahlungsausfälle zwangsläufig mittragen.

Wir haben deshalb die Forderung des Baumarkts nach den gewünschten Angaben bei Lieferung gegen Rechnung für zulässig erachtet.

Im Rahmen der Vertragsfreiheit halten wir die Festlegung derartiger Zahlungsbedingungen für vertretbar. Will ein Käufer darauf nicht eingehen, muss er eine andere Zahlungsart oder einen anderen Vertragspartner auswählen.

9.5 Automatenvideotheken mit biometrischer Kontrolle

Nach der Rechtsprechung dürfen Automatenvideotheken mit jugendgefährdenden Filmen nur dann betrieben werden, wenn sich die zutrittsberechtigten Personen mittels biometrischer Erkennung identifizieren (z. B. BGH, Urteil vom 22.05.2003, Bayer. Verwaltungsgerichtshof, Urteil vom 28.01.2003). Daraus ergibt sich die grundsätzliche Erforderlichkeit und die Zulässigkeit des Einsatzes biometrischer Verfahren im Bereich der Automatenvideotheken.

Bei einer Besichtigung vor Ort haben wir uns im Hinblick auf die Verwendung biometrischer Daten mit der Funktionsweise einer Automatenvideothek befasst.

Die Erfassung eines neuen Kunden läuft dort wie folgt ab:

- Nach dem Ausfüllen eines schriftlichen Antragsformulars wird ein Datensatz im System angelegt.

- Der Kunde erhält eine PIN, die bei der Ausleihe in der üblichen Videothek eingegeben wird, aber auch an den Automaten zur Anwendung kommen kann.

- Dem Kunden wird eine Chipkarte mit Geldkartenfunktion ausgehändigt, auf der die Kundennummer (zur Verknüpfung mit dem individuellen Datensatz im System) und der Betrag des Guthabenkontos gespeichert sind.

- Es werden die Referenzfingerabdrucke von einem Mitarbeiter der Videothek abgenommen. Der erfasste Fingerabdruck wird nicht als Bild gespeichert, sondern lediglich die Position charakteristischer Punkte der Fingerlinien, sog. Templates. Von jedem Kunden werden vier Templates genommen, wenn möglich von zwei verschiedenen Fingern (Zeige-/Mittelfinger), damit auch bei Verletzung eines Fingers die Funktion des Systems gewährleistet ist. Die Templates werden verschlüsselt gespeichert.

Bei der Filmausleihe führt der Kunde seine Chipkarte in den Automaten ein und identifiziert sich durch Auflegen von einem der registrierten Finger auf das dafür vorgesehene Feld. Der vom Kunden vorgelegte Fingerabdruck wird mit den vier

gespeicherten Templates verglichen. Bei Übereinstimmung wird der Zugriff gewährt. Bei Zweifeln an der Übereinstimmung erfolgt zusätzlich eine PIN-Abfrage.

Wir haben geprüft, ob die datenschutzrechtlichen Rahmenbedingungen bei der Verwendung biometrischer Daten eingehalten werden. Hierzu gehört in erster Linie eine ausreichende Information der Betroffenen über den Umgang mit ihren personenbezogenen Daten. Nur so kann der Betroffene entscheiden, ob er unter diesen Bedingungen von der Filmausleihe am Automaten Gebrauch macht oder lieber während der Geschäftszeiten von einem Mitarbeiter der Videothek bedient wird.

Bei der geprüften Videothek waren die Informationen der Kunden über die Erhebung, Verarbeitung und Nutzung biometrischer Merkmale nicht ausreichend. Es war lediglich ein Passus in den Geschäftsbedingungen enthalten, dass sich der Kunde mit der Erfassung der biometrischen Identifikationsmerkmale, wie z. B. einem Fingerabdruck, einverstanden erklärt. Weitere Informationen waren nicht vorgesehen. Wir haben daher gefordert, dass die Kunden über die Erhebung, Verarbeitung und Nutzung insbesondere ihrer biometrischen Daten besser informiert werden müssen.

Im Anschluss an die veröffentlichten Hinweise Nr. 41 des Innenministeriums Baden-Württemberg halten wir es für erforderlich, dass der Kunde zumindest darüber informiert wird,

- dass nur ein charakteristisches Muster seiner Fingerlinien als sog. Template gespeichert wird,

- dass diese Daten bei jedem Ausleihvorgang zum Vergleich und zur Bestätigung seiner Identität herangezogen werden,

- dass dies der einzige Zweck der Verarbeitung und Nutzung der biometrischen Daten ist und

- wann eine Löschung dieser Daten erfolgt.

Wir haben vorgeschlagen, diese Informationen entweder in die AGB`s aufzunehmen, in einem gesonderten Merkblatt dem Kunden an die Hand zu geben

oder den Kunden bei der Abgabe des Referenzfingerabdruckes mündlich zu informieren.

Zwischenzeitlich hat die Videothek zugesichert, dass die geforderten Informationen für den Kunden bzgl. Art und Nutzung der biometrischen Daten ab sofort bei jedem Vertragsabschluss gegeben werden.

Bei der geprüften Videothek wurden auch angemessene Löschungsfristen festgelegt. Eine Löschung der automatisiert gespeicherten Referenzdaten einschließlich der Templates erfolgt entweder nach einer Vertragskündigung oder in den Fällen, in denen ein Kunde ein Jahr lang inaktiv war.

9.6 Liebes-SMS per unbefugter Datennutzung

Eine junge Frau kaufte in einem Laden ein Handy. Dabei wurden ihre Daten in die Kundendatenbank aufgenommen. Wegen eines Umtausches sprach sie wieder im Laden vor.

Kurz darauf erhielt sie auf ihrem Mobiltelefon, dessen Nummer nicht für das Telefonbuch freigegeben war, eine SMS von einem Mitarbeiter dieses Geschäfts mit folgender Botschaft:

> Hallo …. Du kennst mich aus dem Handy-Shop ☺. Leider hab ich dich am Freitag verpasst und ich hätte dich doch gerne gefragt, ob du mit mir mal auf einen Cocktail gehst? Würde mich freuen! Falls es da jemand anderen gibt, hab ich's ja versucht! Liebe Grüße …

Wir haben den Sachverhalt datenschutzrechtlich wie folgt beurteilt:

Die Kundin konnte darauf vertrauen, dass ihre Daten vertraulich behandelt und nur in geschäftlichem Zusammenhang genutzt werden. Die Handynummer wurde durch den Mitarbeiter für die privat motivierte Ansprache per SMS unbefugt genutzt.

Dies wurde von uns beanstandet.

Die Geschäftsführung wies ihre Mitarbeiter per Arbeitsanweisung nochmals ausdrücklich darauf hin, dass die Handynummern der Kunden nicht für private Zwecke genutzt werden dürfen.

9.7 Nutzung von gesperrten Daten

Der Abonnent einer Zeitung hat nach einem Jahr Pause diese Zeitung wieder abonniert und bei der Zahlungsart um eine Rechnung gebeten. Entgegen seinem Wunsch wurde der Betrag jedoch von seinem Konto abgebucht. Die Kontodaten hatte der Abonnent bei der Neubestellung gar nicht genannt. Sie waren bei der Tageszeitung noch aus dem vorhergehenden Abonnement gespeichert.

Der Abonnent erkundigte sich, ob eine solche Datenverwendung erlaubt ist.

Nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG sind personenbezogene Daten, die für eigene Zwecke (hier: Vertragsverhältnis) verarbeitet werden, zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. An die Stelle einer Löschung tritt eine Sperrung, soweit einer Löschung gesetzliche (insbes. Abgabenordnung, Handelsgesetzbuch), satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen (§ 35 Abs. 3 Nr. 1 BDSG).

Die Abonnementsdaten für den kostenpflichtigen Bezug einer Zeitung müssen nach Vertragsende gemäß den Vorschriften der Abgabenordnung aufbewahrt werden und sind deshalb zu sperren.

Gesperrte Daten dürfen nach § 35 Abs. 8 BDSG ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

- es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

- die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Diese engen gesetzlichen Voraussetzungen für eine Nutzung schon gesperrter Daten lagen bei dem gegebenen Sachverhalt zweifellos nicht vor.

Wenn also die Tageszeitung die personenbezogenen Daten eines früheren Abonnenten nach Vertragsende automatisiert mit Sperrvermerk aufgrund der Aufbewahrungsfristen gespeichert hat, ist eine Nutzung einzelner Daten für einen Neuvertrag unzulässig.

Wir haben die unzulässige Nutzung der früheren Abo-Daten beanstandet.

9.8 Vorlage einer Sterbeurkunde für eine Vertragskündigung?

Nach dem Tod ihrer Mutter kündigte die Tochter als Alleinerbin die noch bestehenden Verträge. Ein Unternehmen hat dabei von ihr zum Nachweis für den Tod der Mutter die Vorlage der Sterbeurkunde verlangt, was der Erbin wegen der darin enthaltenen Daten (z. B. Familienstand der Verstorbenen) zu weit ging.

Wir haben auf ihre Anfrage hin mitgeteilt, dass wir für die Kündigung eines Vertrages die Vorlage einer Sterbeurkunde nicht für notwendig erachten.

Vielmehr reicht als Nachweis ein Dokument aus, aus dem allein der Tod der Mutter hervorgeht, z. B eine Meldebescheinigung oder die Sterbeurkunde, auf der die nicht benötigten Daten geschwärzt sind. Bei dieser Vorgehensweise wird den Interessen beider Seiten ausreichend Rechnung getragen und der Datenschutz gewahrt.

* * *

10 Werbung, Adresshandel

10.1 Telefonische Wiederanwerbung eines Abonnenten

Ein Zeitschriftenverlag hatte einen Abonnenten nach dessen Kündigung zu einem "Nachbearbeitungsgespräch" angerufen, in dem der Betroffenen dazu bewegt werden sollte, die Zeitschrift weiterhin im Abo zu beziehen.

Die Nutzung von personenbezogenen Daten ist nach § 4 Abs. 1 BDSG zulässig, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Eine Einwilligung des Abonnenten in eine Telefonwerbung durch den Zeitschriftenverlag lag hier nicht vor.

Als gesetzlicher Zulässigkeitstatbestand für die Nutzung der Telefonnummer für Werbezwecke kam hier allenfalls § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Es war daher zu prüfen, ob die Nutzung der ehemaligen Abonnentendaten zur Wahrung berechtigter Interessen des Zeitschriftenverlages erforderlich war und kein Grund zu der Annahme bestand, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Datennutzung überwiegt.

Auch wenn der Verlag an der Neuaufnahme eines Abonnements ein wirtschaftliches Interesse geltend machen konnte, muss nicht zuletzt im Hinblick auf die Regelungen in § 7 Abs. 2 Nr. 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) davon ausgegangen werden, dass bezüglich der Nutzung der Telefonnummer die schutzwürdigen Interessen des Betroffenen überwiegen. Wird der ehemalige Abonnent ungebeten angerufen, bedeutet dies ein Eindringen in dessen Privatsphäre und - wie uns ständig geschildert wird - eine belästigende oder zumindest unerwünschte Störung. Da für den Angerufenen nicht ohne weiteres erkennbar ist, wer anruft und es sich durchaus um einen wichtigen Anruf handeln könnte, wird er gezwungen, das Gespräch entgegenzunehmen.

Auch bei dem hier vorliegenden Sachverhalt musste davon ausgegangen werden, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss einer

derartigen Datennutzung überwogen. Schließlich hatte er durch die Kündigung des Abonnements seinen Willen bereits klar zum Ausdruck gebracht.

Die Nutzung der für das Vertragsverhältnis gespeicherten Telefonnummer für Werbezwecke nach Beendigung des Vertrages haben wir deshalb als unzulässig angesehen und gegenüber dem Zeitschriftenverlag beanstandet.

10.2 Datenerhebung durch den Reparaturservice

Ein Unternehmen, das seine Produkte über den Einzelhandel vertreibt, versuchte über den Reparaturservice des Handels an die Daten der Käufer seiner Produkte zu gelangen, um sie für seine Werbung nutzen zu können.

Wir halten dieses Vorgehen nur mit Einwilligung des Kunden für zulässig. Zwischen dem Hersteller und dem Endkunden besteht weder eine vertragliche Beziehung noch ein vertragsähnliches Vertrauensverhältnis. Einer Datenübermittlung an das Unternehmen stehen schutzwürdige Interessen der Endkunden entgegen.

Die Einwilligung des Endkunden muss den datenschutzrechtlichen Anforderungen des § 4a BDSG entsprechen. Der Kunde ist insbesondere auf den vorgesehenen Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten (Weitergabe an den Hersteller für Werbezwecke) hinzuweisen.

Wir haben dem Hersteller empfohlen, dem Kunden durch den Reparaturservice vor Ort eine den Anforderungen des § 4a BDSG entsprechende Einwilligungserklärung zur freiwilligen Unterschrift vorlegen zu lassen (vgl. oben 4.1).

* * *

11 Arbeitnehmerdatenschutz

11.1 Weitergabe der Arbeitnehmerdaten durch ein Reinigungsunternehmen

Ein Auftraggeber hatte mit einem Reinigungsunternehmen einen Reinigungsvertrag geschlossen, der u. a. Folgendes vorsieht:

> *Das Reinigungsunternehmen darf grundsätzlich nur sozialversicherungspflichtiges Personal beschäftigen. Die Beschäftigung erfolgt ausschließlich nach den Bestimmungen des Lohn-, Gehalts- und Rahmentarifvertrages des Gebäudereiniger-Handwerks. Die Anmeldungen der im Reinigungsobjekt beschäftigten Arbeitskräfte zur Sozialversicherung und die dazugehörenden Lohn-/Gehaltsabrechnungen sowie die abgeschlossenen Arbeitsverträge sind der Verwaltung des Auftraggebers auf Verlangen vorzulegen. Ein abweichender Personaleinsatz mit sozialversicherungsfreiem Personal ist mit dem Auftraggeber abzustimmen. Ausländische Arbeitskräfte dürfen nur mit gültigen Arbeits- und Aufenthaltspapieren beschäftigt werden. Die aktuellen Personaleinsatzlisten sind in den einzelnen Einsatzbereichen auszuhändigen und auf Verlangen des Auftraggebers zu Einsicht vorzulegen.*

Als der Auftraggeber in die Lohn-/Gehaltsabrechnungen sowie in die Arbeitsverträge zu Kontrollzwecken Einsicht nehmen wollte, stellte sich die Frage, ob diese vom Reinigungsunternehmen vorzunehmenden Datenübermittlungen zulässig sind.

Wir äußerten uns dazu wie folgt:

Als gesetzliche Grundlage für eine derartige Datenweitergabe kommt § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Das berechtigte Interesse des Reinigungsunternehmens besteht in der Erlangung dieses Auftrages und in der Erfüllung seiner vertraglichen Verpflichtung.

Man kann nicht annehmen, dass schutzwürdige Interessen der Arbeitnehmer in diesem Fall überwiegen. Im Gegenteil, diese Datenübermittlung dient gerade ih-

rem fundamentalen Interesse an dem Erhalt ihres Arbeitsplatzes. Auftraggeber, die nicht nur auf dem Einsatz von sozialversicherten und tariflich bezahlten Arbeitnehmern bestehen, sondern dies auch nachprüfen, sind für diese Arbeitnehmer die beste Beschäftigungsgarantie.

Allerdings muss für die Datenübermittlung an die Kunden eine möglichst datenschutzverträgliche Lösung gesucht werden. Schließlich enthalten Arbeitsverträge und Lohnabrechnungen zahlreiche Daten, auf die sich die o. g. Vereinbarung nicht bezieht. Unter ihnen befinden sich auch sensible personenbezogene Daten über die Gesundheit, Religionszugehörigkeit usw. Eine „überschießende Datenübermittlung“ muss deshalb vermieden werden.

Die zulässigen Datenübermittlungen müssen für die Arbeitnehmer transparent sein. Die Arbeitnehmer sollten bereits vor Abschluss ihres Arbeitsvertrages darauf hingewiesen werden, dass derartige Datenübermittlungen vorkommen können. Darüber hinaus empfiehlt sich eine entsprechende Information vor der Annahme von Aufträgen, die diese Auflagen enthalten.

Soweit ein Arbeitnehmer dann doch einer Übermittlung widerspricht, gibt er zu erkennen, dass seine schutzwürdigen Interessen entgegenstehen. Die Übermittlung wäre dann in diesem Fall unzulässig.

11.2 Geburtstags- und Jubiläumslisten

In einem Unternehmen sollten am PC erstellte Geburtstagslisten der Mitarbeiter am schwarzen Brett ausgehängt werden. Darüber hinaus sollte diese Liste zusammen mit einer Jubiläumsliste in einem im Bistro aufgestellten PC gespeichert werden. Dieser PC könnte sowohl von Mitarbeitern als auch von Kunden und Lieferanten benutzt werden.

Wir gaben der anfragenden betrieblichen Datenschutzbeauftragten im Hinblick auf die datenschutzrechtliche Rechtslage den Rat, im Unternehmen darauf hinzuwirken, dass die beiden Vorhaben nicht verwirklicht werden.

Wenn im Unternehmen Geburtstagslisten intern verteilt oder ausgehängt werden, handelt es sich um ein "Nutzen" von personenbezogenen Daten. Die Veröffentli-

chung der Geburtstage/Jubiläen etc. in einem auch für externe Personen zugänglichen PC stellt beim Zugriff der Mitarbeiter ein "Nutzen", beim Zugriff der externen Personen ein "Übermitteln" dar.

Die Zulässigkeit der geschilderten Datenverwendungen ergibt sich weder aus einem Gesetz noch aus einer sonstigen Rechtsvorschrift. Sie dienen nicht der Zweckbestimmung des Arbeitsvertrages gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Im Rahmen der Nr. 2 dieser Vorschrift ist ein berechtigtes Interesse des Arbeitgebers nicht zu erkennen. Darüber hinaus wird man annehmen müssen, dass schutzwürdige Interessen zahlreicher Arbeitnehmer am Ausschluss dieser Datenverwendungen bestehen.

Ob die Zulässigkeit der genannten Veröffentlichungen auf eine Einwilligung der einzelnen Arbeitnehmer gestützt werden kann, ist umso fraglicher, je größer ein Unternehmen ist. Insbesondere sprechen das Abhängigkeitsverhältnis eines Arbeitnehmers und auch ein gewisser Gruppendruck in der Belegschaft gegen eine freie und damit rechtswirksame Einwilligung eines Arbeitnehmers (§ 4a Abs. 1 Satz 1 BDSG).

11.3 Kontrollmöglichkeit des Arbeitgebers bei erlaubter privater Nutzung von Internet und E-Mail am Arbeitsplatz

In unserem 1. Tätigkeitsbericht haben wir unter Nr. 10.1 darauf hingewiesen, dass es hier entscheidend darauf ankommt, ob der Arbeitgeber die private Nutzung dieser Dienste gestattet oder nicht. Wir haben dabei vor allem deutlich gemacht, dass die Kontrollen des Arbeitgebers nur unter sehr engen Voraussetzungen zulässig sind, wenn eine private Nutzung gestattet ist und keine flankierenden Regelungen getroffen sind.

Bei unseren Kontrollen stellten wir bei zahlreichen Unternehmen fest, dass die private Nutzung von Internet und E-Mail zwar nicht ausdrücklich geregelt ist, dass sie aber stillschweigend in geringem Umfang auf Vertrauensbasis erlaubt oder zumindest geduldet wird.

Auch bei dieser Fallgestaltung ist der Arbeitgeber kraft Gesetzes Anbieter von Telekommunikations- bzw. Telediensten. Bezüglich der Kontrollen muss er die einschlägigen Vorschriften beachten. Es geht dabei insbesondere um das Fernmeldegeheimnis und die datenschutzrechtlichen Bestimmungen des Teledienstedatenschutzgesetzes.

Der Arbeitgeber unterliegt damit einem weitgehenden Kontrollverbot. Bei unvorhergesehenen Abwesenheitszeiten eines Mitarbeiters ist ein Zugriff auf das E-Mail-Postfach ohne Einwilligung auch aus dienstlichen Gründen nicht zulässig. Gestattet ist allein eine Auswertung der Protokolle über Verbindungs- und Inhaltsdaten im Hinblick auf Fragen der Datensicherheit, des Datenschutzes, der Sicherung des ordnungsgemäßen Betriebes und für die Abrechnung.

Im Hinblick auf diese Problematik empfehlen wir den Unternehmen, z. B. in einer Betriebsvereinbarung, schriftliche Regelungen zu treffen. Darin kann vorgesehen werden, dass nur denjenigen Mitarbeitern eine private Nutzung erlaubt ist, die im Gegenzug ihre Einwilligung zu den notwendigen Zugriffen erteilen.

11.4 Übermittlung von Mitarbeiterdaten innerhalb eines internationalen Konzerns

Auf den Beitrag unter 5.3 wird verwiesen.

* * *

12 Gesundheitswesen

Dem Datenschutz muss im Gesundheitswesen ein hoher Stellenwert eingeräumt werden. Schließlich geht man gerade hier mit sehr sensiblen personenbezogenen Daten um. Neben den Datenschutzvorschriften sind hier auch noch die speziellen, meist strafbewehrten Geheimhaltungsverpflichtungen wie z. B. das Arzt- und Apothekengeheimnis zu beachten.

12.1 Vertraulichkeit in Arztpraxen

Immer wieder wird über die fehlende Vertraulichkeit in Arztpraxen Beschwerde geführt. So halten sich oft mehrere Patienten im Eingangsbereich und am Empfang einer Praxis auf, die räumlich diesem Ansturm nicht gerecht wird. Eine vertrauliche Betreuung eines einzelnen Patienten durch die Arzthelferin ist in diesem Bereich nicht gewährleistet.

Entscheidend für die vertrauensvolle Beziehung zwischen Arzt und Patienten ist der verantwortungsvolle Umgang mit den persönlichen Daten des Patienten. Dazu gehören Daten wie Personalien, Krankenversicherung, Grund des Arztbesuches, Angaben über weitere Untersuchungen und Behandlung etc. Die Diskretion muss schon am Empfang beginnen. Patienten sollen ihr medizinisches Anliegen schildern und die dafür notwendigen Angaben machen können, ohne dass unberechtigte Dritte mithören.

Zu diesem Zweck hat der Arzt nach dem BDSG auch räumlich die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die unbefugte Kenntniserlangung von Patientendaten durch Dritte zu verhindern.

Beschwerdeführer verweisen wir auch an die zuständige Ärztekammer als fachliche Aufsichtsbehörde, um auf diese Weise zu erreichen, dass man sich auch von dort aus dieser Problematik vermehrt annimmt.

.

12.2 Praxisübergabe

Ein Arzt hat seine Praxis geschlossen und seinen Patientenstamm an eine andere Arztpraxis abgegeben. Dies hat er in einer Zeitungsanzeige bekannt gegeben. Seine Patienten baten uns um eine datenschutzrechtliche Überprüfung.

Grundsätzlich ist dazu zu sagen, dass die Übermittlung der Patientenunterlagen an den Praxisnachfolger nur mit der datenschutzrechtlichen Einwilligung und der Entbindung von der Schweigepflicht durch den betroffenen Patienten zulässig ist.

Die Ärzte sind nach ihren Berufsordnungen verpflichtet, die ärztlichen Unterlagen 10 Jahre lang aufzubewahren. Bei einer Praxisübergabe ist es naheliegend, mit dieser Aufgabe den Praxisnachfolger zu betrauen, da der bisherige Praxisinhaber dazu meist nicht mehr in der Lage ist. Auch bleibt ein Großteil der Patienten beim Praxisnachfolger, so dass es sinnvoll ist, dass dieser mit Einwilligung der Patienten die bisherigen Daten auswerten kann, um überflüssige Neuuntersuchungen zu vermeiden.

Sind diese Erklärungen aller Patienten mit vertretbarem Aufwand nicht zu erlangen, können zur Lösung dieses Problems die Patientenunterlagen dem Praxisübernehmer mit der Maßgabe übergeben werden, in die Daten nur mit dem Einverständnis des jeweiligen Patienten Einblick zu nehmen. Bei einer automatisiert erfolgten Verarbeitung von Patientendaten müssen bei Übergabe vergleichbare Vorkehrungen getroffen werden, z. B. eine Datenspeicherung je Patient auf Diskette oder CD-ROM.

* * *

13 Verbände, Vereine, Parteien

13.1 Nutzung von Mitgliederdaten eines Vereins für politische Wahlwerbung

Wir werden immer wieder mit der Frage der Verwendung von Mitgliederdaten z. B. eines Sportvereins für die Wahlwerbung politischer Parteien im Zusammenhang mit Bundestags-, Landtags- oder Kommunalwahlen konfrontiert.

Sowohl eine Versendung der Wahlwerbung durch den Verein im Rahmen einer sog. Adressmittlung als auch eine Übermittlung der Mitgliederdaten an eine Partei zu diesem Zweck ist in aller Regel unzulässig.

Diese Verwendungen dienen in der Regel nicht den in der Satzung festgelegten Zielen des Vereins und damit auch nicht dem vertragsähnlichen Vertrauensverhältnis zwischen den Mitgliedern und dem Verein (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG).

Auch die Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG liegen nicht vor. Fraglich ist schon, ob ein Verein ein berechtigtes Interesse an diesen Datenverwendungen haben kann. In jedem Fall ist aber ein überwiegendes schutzwürdiges Interesse der Mitglieder am Ausschluss der Nutzung oder der Übermittlung zu Zwecken der Wahlwerbung anzuerkennen. Die Mitglieder vertrauen regelmäßig darauf, dass der Verein ihre Daten nicht für politische Zwecke an Dritte übermittelt bzw. selbst zu diesem Zweck nutzt.

Schließlich lässt auch das sog. Listenprivileg des § 28 Abs. 3 Satz 1 Nr. 3 BDSG eine Übermittlung oder Nutzung zu dem genannten Zweck nicht zu. Die schutzwürdigen Interessen der Vereinsmitglieder stehen hier in gleicher Weise entgegen.

13.2 Werbung für einen Bürgerentscheid

Der Vorsitzende einer Bürgerinitiative, die ein Bürgerbegehren initiiert hat, fragte an, ob die Adressen der Unterstützer des Bürgerbegehrens für die Werbung für den sich anschließenden Bürgerentscheid verwendet werden dürfen.

Die Unterstützungsunterschriften werden bis zur Abgabe bei der Gemeinde von der Bürgerinitiative aufbewahrt. Solange die Liste lediglich in Papierform vorliegt, ist das BDSG nicht anwendbar. Bei der Liste handelt es sich nicht um eine nicht-automatisierte Datei i. S. d. § 3 Abs. 2 Satz 2 BDSG.

Sobald die Unterstützeradressen aber auf einem PC gespeichert werden, ist das BDSG zu beachten. Dies gilt dann auch für die Nutzung der Adressen für die Versendung von Werbebriefen an die Unterstützer.

Als mögliche gesetzliche Grundlage kommt hier § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Nach dieser Vorschrift ist die Speicherung und Nutzung der Unterstützeradressen bei der Bürgerinitiative zulässig, soweit dies zur Wahrung von deren berechtigten Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegen.

Das berechtigte Interesse der Bürgerinitiative an der Speicherung zum Zwecke der Versendung der Werbeschreiben für den Bürgerentscheid liegt darin, die Unterstützer des Bürgerbegehrens für eine Teilnahme an der Abstimmung und eine für sie positive Stimmabgabe zu gewinnen. Es ist für sie für die Erreichung ihrer Ziele erforderlich, gerade auch bei denen zu werben, die sie bereits beim Bürgerbegehren unterstützt haben.

Die schutzwürdigen Interessen der Betroffenen an einem Ausschluss dieser Verwendungen überwiegen in diesem Fall nicht. Man wird hier vielmehr annehmen können, dass diejenigen, die sich in die Unterschriftenliste für ein Bürgerbegehren eintragen, auch Interesse an der Sache zeigen und keine Einwände gegen eine weitere Kontaktaufnahme in einem angemessenen Rahmen haben.

Wir haben deshalb diese Datenverwendungen als zulässig angesehen.

Die Daten dürfen keinesfalls für andere Zwecke der Organisation verwendet werden. Sie sind vielmehr anschließend zu löschen.

13.3 Wiederholte Nutzung von Wählerdaten

Ein Ortsverband einer Partei hatte vor der Bürgermeisterwahl von der gesetzlichen Möglichkeit des Art 35 Abs. 1 Bayerisches Meldegesetz (MeldeG) Gebrauch gemacht und Adressen von Jungwählern von der Meldebehörde erhalten (sog. Gruppenauskunft).

Der Ortsverband hat die Adressen aber nicht, wie es die genannte Bestimmung des MeldeG vorschreibt, einen Monat nach der Wahl gelöscht, sondern im Hinblick auf eine Wahlanfechtung weiterhin gespeichert und für die später erforderliche Wiederholung der Wahl noch einmal verwendet. Dabei ist er davon ausgegangen, dass die der Gruppenauskunft zugrunde liegende Wahl wegen der Wahlanfechtung noch nicht abgeschlossen war und deshalb eine weitere Verwendung der Adressdaten möglich war.

Dies ist mit dem Art 35 Abs. 1 Satz 5 MeldeG nicht zu vereinbaren. Der Abschluss einer Wahl wird durch ihre Anfechtung nicht hinausgeschoben. Zum einen steht bei der Anfechtung einer Wahl noch nicht fest, ob eine Wiederholung stattfindet. Zum anderen beginnt für den Fall, dass eine Wahl im Anfechtungsverfahren für ungültig erklärt worden ist, ein neues Wahlverfahren. Im Rahmen des neuen Wahlverfahrens wird die Möglichkeit einer Gruppenauskunft erneut eröffnet.

Darüber hinaus ist die genannte Ausnahmebestimmung eng auszulegen. Es ist vom Gesetzgeber im Sinne des Datenschutzes gewollt, dass die Adressdaten von der Partei zeitnah wieder gelöscht werden. Auf diese Weise soll eine zweckwidrige Verwendung der Daten verhindert werden. Zweckwidrig ist auch die erneute Nutzung der Datensätze vor einer Nachwahl, die nach der Ungültigerklärung der ersten Wahl stattfindet. Denn die Liste ist dann nicht mehr aktuell. Insbesondere werden zwischenzeitlich eingelegte Widersprüche der Bürger gegen eine Weitergabe der Adressdaten durch die Meldebehörde an Parteien nicht berücksichtigt. Darüber hinaus werden auch durch Umzüge oder Sterbefälle ungültig gewordene Adressen verwendet.

Die Speicherung der Adressdaten über einen Monat nach der ersten Wahl hinaus und die erneute Verwendung durch die Partei bei der Wiederholungswahl waren daher unzulässig. Wir haben dies beanstandet.

13.4 Mitgliederdaten in der Festschrift eines Vereins

Ein Verein wollte in seiner Festschrift anlässlich des 125jährigen Gründungsjubiläums eine Mitgliederliste veröffentlichen. Die Liste sollte Name, Vorname und Status (aktives, passives oder förderndes Mitglied) enthalten.

Auf eine entsprechende Anfrage beurteilten wir die datenschutzrechtliche Zulässigkeit dieser Veröffentlichung wie folgt:

Soweit keine ausdrückliche Einwilligung der einzelnen Mitglieder vorliegt, ist die Veröffentlichung der Mitgliederliste in der Festschrift auch dann zulässig, wenn der Verein ein berechtigtes Interesse an der Veröffentlichung hat und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Mitglieder an einem Ausschluss der Veröffentlichung überwiegt (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG).

Das berechtigte Interesse des Vereins, die aufgezählten Daten seiner Mitglieder (Name, Vorname und Status) in einer Jubiläumsfestschrift zu veröffentlichen, kann grundsätzlich anerkannt werden. Es sollte durch einen Beschluss des zuständigen Gremiums festgestellt werden, in dem auch der Verbreitungsumfang der Festschrift angesprochen ist.

Im Allgemeinen ist nicht anzunehmen, dass überwiegende schutzwürdige Interessen der Mitglieder einer Veröffentlichung dieser Daten entgegenstehen. Um sicher zu gehen, sollte der o. g. Beschluss den Mitgliedern durch ein Schreiben oder einen auffälligen Hinweis in der Vereinszeitschrift bekannt gegeben und ihnen die Möglichkeit eingeräumt werden, innerhalb einer angemessenen Frist der Veröffentlichung ihrer personenbezogenen Daten zu widersprechen.

Bei Mitgliedern, die rechtzeitig Widerspruch erheben, ist von einem entgegenstehenden schutzwürdigen Interesse im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG auszugehen. Sie dürfen deshalb nicht in die Festschrift aufgenommen werden.

Ein anderer Verein wollte in seiner Festschrift zusätzlich auch das Geburtsdatum der Mitglieder abdrucken. In diesem Fall kann ein berechtigtes Interesse des Vereins an der Veröffentlichung des Geburtsdatums nur in geringem Maße anerkannt werden. Demgegenüber überwiegen die schutzwürdigen Interessen zahlreicher Mitglieder daran, dass das Geburtsdatum nicht veröffentlicht wird. Die Erfahrung zeigt, dass nicht wenige Menschen aus den verschiedensten Gründen mit der Veröffentlichung ihres Geburtsdatums Schwierigkeiten haben.

Für eine Veröffentlichung des Geburtsdatums in einer Festschrift wäre deshalb eine dem § 4a BDSG entsprechende ausdrückliche Einwilligung der Betroffenen erforderlich.

13.5 Personenbezogene Daten in Stellenplänen für die Delegiertenversammlung eines Verbandes

Ein Delegierter einer Landesversammlung eines größeren Verbandes fragte bei uns an, ob der für die Beratung und Beschlussfassung zur Verfügung gestellte Stellenplan die Namen der jeweiligen Stelleninhaber ausweisen dürfe. Die Landesgeschäftsstelle habe dies erstmals abgelehnt und dabei auf das Datenschutzrecht hingewiesen.

Unsere Überprüfung hat ergeben, dass die Landesgeschäftsstelle die Nennung der Namen zu Recht abgelehnt hat. Es liegt nämlich weder eine Rechtsvorschrift noch eine Einwilligung der betroffenen Arbeitnehmer vor, die eine derartige Nutzung der personenbezogenen Daten in der Form der Weitergabe an die Delegierten erlauben würde.

Die Delegierten dürften diese Arbeitnehmerdaten gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG nur dann erfahren, wenn dies "der Zweckbestimmung der Arbeitsverträge dienen würde". Das wäre dann der Fall, wenn die Delegiertenversammlung innerhalb des Landesverbandes für Personalentscheidungen bzw. für die Personalverteilung zuständig wäre. Eine derartige Zuständigkeit ergab sich aber aus der Satzung des Landesverbandes nicht.

Als Bestandteil des Haushaltsentwurfs des Landesverbandes ist der Stellenplan vielmehr allein die Grundlage für die Mittelbewirtschaftung im Personalbereich. Wie schon die Bezeichnung "Stellenplan" zeigt, weist er die Zahl und die Beschaffenheit der einzelnen Stellen aus, die der Delegiertenversammlung zur Beschlussfassung für das jeweilige Haushaltsjahr vorzulegen ist. Die Benennung der Stelleninhaber ist dafür nicht erforderlich.

* * *

14 Videoüberwachung

Bei einer Videoüberwachung entsteht stets ein Konflikt zwischen den berechtigten Interessen des Beobachtenden und den schutzwürdigen Interessen derjenigen, die beobachtet werden. Diesen Konflikt bekam die Datenschutzaufsichtsbehörde im Berichtszeitraum immer wieder in der Form von Eingaben zu spüren, in denen Betroffene sich mit der Frage an uns wandten, ob eine Kameraüberwachung rechtmäßig ist.

14.1 Videoüberwachung in öffentlich zugänglichen Räumen

Der § 6b BDSG gibt die rechtlichen Vorgaben für die Videoüberwachung in öffentlich zugänglichen Räumen sowie für die Verarbeitung und Nutzung der auf diese Weise erhobenen Daten.

Nach dieser Bestimmung ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) für private Stellen nur zulässig, soweit sie zur Wahrnehmung

1. des Hausrechts oder
2. berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen (§ 6b Abs. 2 BDSG).

So klar der Tatbestand des § 6b BDSG auf den ersten Blick formuliert ist, so schwierig ist zuweilen seine Anwendung in der Praxis, wie die im Folgenden von uns bearbeiteten Fallbeispiele zeigen. Wir schildern die einzelnen Fragen und Probleme an Hand der Tatbestandsmerkmale der gesetzlichen Bestimmung.

14.1.1 Beobachtung mit optisch-elektronischen Einrichtungen

Unter den in § 6b Abs. 1 Satz 1 BDSG angesprochenen optisch-elektronischen Einrichtungen sind fest installierte Videokameras und Webcams zu verstehen.

Nicht erfasst werden mobile Geräte, wie Handykameras, Fotoapparate oder Ferngläser.

Kameraattrappen stellen keine optisch-elektronischen Einrichtungen dar. Mit ihnen kann nicht beobachtet werden, sondern die Attrappen dienen anderen Zwecken, nämlich der Abschreckung oder Einschüchterung. Da keine Bildübertragung zur Überwachung oder Aufzeichnung stattfindet und keine personenbezogenen Daten verarbeitet werden, wird das informationelle Selbstbestimmungsrecht der Betroffenen nicht berührt. Deshalb kommt weder eine direkte noch eine analoge Anwendung des § 6b BDSG in Betracht.

Eine Person kann sich allerdings auch von einer vermeintlichen Kamera in ihrem allgemeinen Persönlichkeitsrecht verletzt fühlen. Insoweit hat sie unter Umständen in entsprechender Anwendung der §§ 1004, 823 Abs.1 BGB einen zivilrechtlichen Beseitigungsanspruch.

Ausgeschaltete Kameras sind wie Attrappen zu behandeln. Erst wenn sie aktiviert werden, ist der § 6b BDSG auf sie anwendbar.

14.1.2 Öffentlich zugängliche Räume

Der § 6b BDSG bezieht sich nur auf die Videoüberwachung im öffentlich zugänglichen Raum innerhalb oder außerhalb von Gebäuden. Öffentlich zugänglich ist ein Raum, wenn sich seine Zugänglichkeit nach allgemeinen Merkmalen bestimmt, die von jeder Person erfüllt werden können (vgl. Simitis, RN 41 zu § 6b BDSG).

Dazu gehören z. B. nicht nur öffentliche Straßen, Wege und Plätze sowie öffentlich gewidmete Grundstücke, sondern auch Kaufhäuser, Gaststätten, der Schalterbereich von Banken und Tankstellenbetriebe. Öffentlich zugänglich sind auch Theater, Konzertsäle, Kinos oder Museen, da sie, unabhängig davon ob ein Ein-

trittsgeld verlangt wird, für die Nutzung durch die Allgemeinheit bestimmt sind. Auch private Zugangswege zu großen Wohnanlagen sind öffentlich zugänglich, weil hier der Kreis der zutrittsberechtigten Personen (Bewohner, Angehörige, Besucher usw.) noch nicht abgrenzbar ist.

Nicht öffentlich zugänglich sind dagegen Räume, die nur von einem bestimmten Personenkreis betreten werden dürfen, z. B. Privatwohnungen, Produktionshallen, Büros ohne Besucherverkehr sowie Treppenhäuser, deren Zugangstür verschlossen ist.

Im Fall der Überwachung des Flures in einer Senioren-Wohnanlage (vgl. 14.2.1) handelt es sich um einen nicht öffentlich zugänglichen Raum, da die Haustür der Wohnanlage stets verschlossen ist. Zutritt besteht nur für Bewohner sowie deren Besucher. Bewohner können mit ihrem Schlüssel die Eingangstüre öffnen, Besuchern muss Zutritt in die Wohnanlage durch einen Bewohner ausdrücklich gewährt werden. Externe können also nicht ungehindert das Gebäude betreten.

14.1.3 Abwägung

Zwischen der Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke einerseits und den schutzwürdigen Interessen derjenigen, die beobachtet werden, ist abzuwägen. Die Videoüberwachung ist nur zulässig, wenn keine Anhaltspunkte dafür bestehen, dass die schutzwürdigen Belange der Betroffenen überwiegen.

14.1.3.1 Überwachung des gesamten Straßenraumes in einem Rotlichtviertel

Die Betreiberin eines in einem Rotlichtviertel gelegenen Lokals hat auf dem Dach ihres Anwesens eine Kamera montieren lassen. Die Bilder wurden auf einen Monitor in ihre Wohnung übertragen, so dass sie von dort bequem die gesamte Straße einsehen konnte. Sie wollte auf diese Weise frühzeitig mögliche Störer erkennen, um ihnen den Zutritt zu ihrem Lokal verweigern zu können.

Die Zulässigkeit der Überwachung des gesamten Straßenraumes scheitert

hier zum einen daran, dass eine Kamera mit einer derartigen Reichweite für die Wahrnehmung des Hausrechts nicht erforderlich ist. Eine sog. Klingelkamera oder eine bloße Kamera im Bereich der Eingangstür könnte den angestrebten Zweck genauso gut erfüllen. Darüber hinaus überwiegen in jedem Fall die schutzwürdigen Interessen der Passanten daran, gerade in dieser Gegend nicht beobachtet zu werden.

14.1.3.2 Überwachung des Schließfachbereiches im Hallenbad

In einem Hallenbad wird der Bereich der Schließfächer mit Videokameras überwacht. Auf diese Weise will man einen Beitrag zur Sicherheit im Bad und zur Verhinderung bzw. Aufklärung von Diebstählen leisten. Die Bilder werden auf einen Monitor im Eingangsbereich - für jedermann einsehbar - übertragen. Manche Badegäste ziehen sich aus Zeitgründen nicht in den separaten Umkleidekabinen, sondern gleich vor den Schließfächern um, so dass die Videoübertragung auf den Monitor im Eingangsbereich von manchen Besuchern "mit einigem Interesse beobachtet" wird.

Hierzu ist festzustellen, dass für die genannten Zwecke zwar die Videoüberwachung als solche, nicht jedoch eine öffentliche Darstellung der Videoaufnahmen im Eingangsbereich erforderlich ist. Hier überwiegen die schutzwürdigen Interessen der Betroffenen, in diesem Bereich nicht öffentlich zur Schau gestellt zu werden.

Wir haben daher die öffentliche Darstellung der Videoaufnahmen beanstandet und gefordert, den Monitor in einem Raum aufzustellen, in dem nur solche Personen Einblick nehmen können, die für die Überwachung und die Gewährleistung der Sicherheit im Bad zuständig sind. Diese können über den Monitor die Vorgänge im Schließfachbereich verfolgen und bei entsprechenden Gefährdungssituationen schnell reagieren. Einer derartigen Videoüberwachung stehen die schutzwürdigen Interessen der Betroffenen nicht entgegen.

Im Bereich der Schließfächer muss auf die Videoüberwachung hingewiesen werden.

14.1.3.3 Überwachung einer Gaststätte

Mit der Überwachung von großen Teilen des Gastraumes wollte der Betreiber einer Gaststätte Straftaten dokumentieren, Diebstählen vorbeugen und Inventurdifferenzen senken. Eine besondere Gefahrensituation oder einen konkreten Anlass für diese Überwachungsmaßnahme hat er nicht vorgetragen.

Die allgemeinen Beobachtungsinteressen eines Gastwirts, wie sie gerade beschrieben wurden, können nicht als „berechtigte Interessen für konkret festgelegte Zwecke“ anerkannt werden. Dafür müssten stärkere Verdachtsmomente vorliegen. Das Interesse an der Wahrnehmung des Hausrechts ist unter diesen Umständen als gering einzustufen.

Demgegenüber überwiegen hier die schutzwürdigen Interessen der Gäste. Diese gehen in aller Regel davon aus und erwarten es auch, dass ihr Verhalten in einer Gaststätte weder beobachtet noch aufgezeichnet wird. Ihr Schutzbedürfnis ist gerade hier sehr hoch.

Darüber hinaus sind auch die Interessen der Mitarbeiter zu beachten. Sie sind bei ihrer Arbeit einem dauerhaften und zur Erfüllung der o. g. Zwecke unverhältnismäßigen Überwachungsdruck ausgesetzt, Dies gilt insbesondere für den Mitarbeiter hinter dem Tresen, denn eine Kamera ist direkt auf diesen Bereich gerichtet. Somit überwiegen auch die Interessen der Mitarbeiter, nicht ständig beobachtet zu werden, die in diesem Fall als geringer einzustufenden Interessen des Gastwirts.

Diese unzulässige Videoüberwachung haben wir beanstandet.

14.1.3.4 Überwachung eines Reisebüros am Flughafen

In einem offen zugänglichen Reisebüro in einem Flughafen wurde eine Kameraüberwachung nicht nur zur Verhinderung und Aufklärung von Diebstählen und sonstiger Straftaten, sondern auch gezielt zur Überwachung der Arbeitnehmer eingesetzt.

Eine Überprüfung vor Ort ergab, dass die Kamera die Mitarbeiter, die Kunden, aber auch die am Geschäft vorbeigehenden Passanten erfasste. Die Kamera

selbst war für die Betroffenen nicht erkennbar, sondern in einem an der Decke befindlichen Gegenstand versteckt, der wie ein üblicher Bewegungsmelder aussah. Ein Hinweis auf die Videoüberwachung war nicht vorhanden. Die Mitarbeiter sind zwar per Mail von der Unternehmensleitung über die Videoüberwachung informiert worden. Sie brachten bisher keine Einwände dagegen vor, wenngleich sie die Maßnahme als sehr unangenehm empfanden.

Es ist bereits zweifelhaft, ob in einem Reisebüro zur Wahrnehmung des Hausrechts oder sonstiger berechtigter Interessen, wie sie eingangs beschrieben wurden, gegenüber den Kunden, Mitarbeitern oder Passanten eine Videoüberwachung erforderlich ist. Selbst wenn man diese Frage bejaht, sind in diesem Fall die schutzwürdigen Interessen der Betroffenen höher zu gewichten.

Wir haben die Verantwortlichen des Unternehmens aufgefordert, die unzulässige Videoüberwachung einzustellen.

14.1.3.5 Überwachung von auf öffentlichem Grund abgestellten Gegenständen

Nachdem sein auf der Straße abgestellter PKW mehrfach beschädigt worden war, überwachte der Geschädigte sein Fahrzeug zur Aufklärung weiterer Sachbeschädigungen von seinem Wohnzimmerfenster aus mit einer Videokamera.

Das Interesse eines PKW-Eigentümers an der Überwachung seines Fahrzeuges, um auf diese Weise Personen, die den PKW stehlen oder beschädigen, der Tat überführen zu können, ist bei einer entsprechenden Gefahrenlage berechtigt.

Dies war hier der Fall. Da der PKW schon mehrfach beschädigt worden ist, kann die Erforderlichkeit einer Videoüberwachung solange anerkannt werden, als eine derartige Gefährdung gegeben ist.

Schutzwürdige Interessen der anderen Verkehrsteilnehmer werden allerdings nur dann nicht berührt, wenn vom Umgriff des überwachten Wagens so wenig wie möglich zu sehen ist. Da hier nur Personen aufgenommen werden konn-

ten, die sich unmittelbar am Auto zu schaffen machten, haben wir die Videoüberwachung als vertretbar angesehen.

In einem ähnlichen Fall überwachte ein Eisdielenbesitzer seine auf dem Gehsteig aufgestellten Tische und Stühle in den Nachtstunden, um Beschädigungen und Diebstähle zu verhindern bzw. aufdecken zu können, mit einer Videokamera und zeichnete die Aufnahmen für wenige Stunden auf.

Eine Gefahrenlage war auch hier gegeben. Beschädigungen sowie ein Diebstahl waren bereits vorgekommen. Wir haben den Besitzer der Eisdiele darauf hingewiesen, dass die Videoüberwachung nicht zu den Geschäftszeiten stattfinden darf und dass er die Kamera so anbringen muss, dass nur die überwachten Gegenstände, nicht jedoch die passierenden Fußgänger von der Kamera erfasst werden.

Unter diesen Umständen bestehen keine Anhaltspunkte dafür, dass schutzwürdige Interessen der Betroffenen überwiegen.

14.1.3.6 Videoüberwachung des EC-Karten-Terminals

Die Videoüberwachung in Tankstellen gehört mittlerweile zu dem gewohnten Bild. Das berechtigte Interesse der Tankstelle für eine derartige Maßnahme kann im Grundsatz anerkannt werden, da dieser Bereich besonderen kriminellen Risiken ausgesetzt ist.

Die schutzwürdigen Interessen der Betroffenen überwiegen allerdings in den Fällen, in denen die Videoüberwachungskamera das unverdeckte EC-Karten-Terminal erfasst und somit auch die PIN-Eingabe aufzeichnen kann. Da die PIN nur den jeweils Berechtigten selbst bekannt sein darf, ist es nicht vertretbar, wenn die Eingabe der PIN von dritter Seite beobachtet oder sogar aufgezeichnet wird.

Wir konnten bei keinem der uns vorgelegten Fälle die Möglichkeit einer Erkennbarkeit der PIN-Eingabe ausschließen. Die erzeugten Bilder hatten durchwegs gute Qualität, so dass die Führung der Hand und dadurch die Zif-

fernfolge nachvollzogen werden konnten, z. B. dann, wenn Kunden die PIN nur mit dem Zeigefinger eingeben.

Schwieriger und oft sogar unmöglich ist die Erkennbarkeit der Eingabe allerdings in den Fällen, in denen lediglich einzelne Bilder in größeren Zeitabständen aufgezeichnet werden.

Ein Betreiber einer derartigen Videoüberwachungsanlage hat vorgeschlagen, dass Kunden, die eine Überwachung der PIN-Eingabe ausschließen möchten, das Eingabegerät, das über ein ausreichend langes Kabel verfügt, aus dem Sichtbereich der Kamera entfernen können. Diese Maßnahme haben wir keinesfalls für geeignet angesehen, den erforderlichen Schutz zu gewährleisten. Manchen Kunden wird zwar bekannt sein, dass im Kassenbereich von Tankstellen Überwachungskameras angebracht sind. Es muss jedoch davon ausgegangen werden, dass nicht alle Kunden die Kameras tatsächlich wahrnehmen oder die Gefahr einer Aufzeichnung der PIN-Eingabe erkennen und deshalb von der angebotenen Schutzmöglichkeit keinen Gebrauch machen.

Wir haben daher gefordert, z. B. durch das Anbringen eines Sichtschutzes sicherzustellen, dass eine Beobachtung und Aufzeichnung der PIN-Eingabe verhindert wird.

14.2 Aufzeichnung von Videoaufnahmen in Räumen, die nicht öffentlich zugänglich sind

In einem nicht öffentlich zugänglichen Bereich, z. B. in einem abgeschlossenen Firmengelände, ist § 6b BDSG nicht anwendbar. Soweit jedoch eine digitale Aufzeichnung von Videoaufnahmen stattfindet, gelten die allgemeinen Vorschriften des BDSG. Es findet dabei nämlich eine automatisierte Datenverarbeitung statt (vgl. § 1 Abs. 2 Nr. 3 BDSG).

Wenn keine Einwilligung der Betroffenen nach § 4a BDSG vorliegt, kann sich eine Zulässigkeit aus § 28 BDSG ergeben. In der Regel kommt § 28 Abs. 1 Nr. 2 BDSG zur Anwendung, wonach die Erhebung und Speicherung personenbezo-

gener Daten zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich sein muss und entgegenstehende schutzwürdige Interessen der Betroffenen nicht überwiegen dürfen.

Bei dieser Abwägung spielen schwerpunktmäßig der Umfang der zu erhebenden Daten, der betroffene Personenkreis, die Speicherungsdauer, bisherige Problemfälle im überwachten Bereich und die allgemeine Sicherheitssituation des betroffenen Unternehmens eine wichtige Rolle.

Bei der Erhebung der Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen (§ 28 Abs. 1 Satz 2 BDSG).

Auch in den nicht öffentlich zugänglichen Räumen sind grundsätzlich Hinweise auf die Videoaufzeichnung anzubringen.

14.2.1 Videoüberwachung der Flure in einer Seniorenwohnanlage

Die Hausverwaltung einer Seniorenwohnanlage hat im nicht öffentlich zugänglichen Flur eine Kamera installiert, da die Bewohner mehrfach eine ihnen unbekannte Person im Gebäude beobachtet hatten und es in der letzten Zeit bereits zum Aufbruch einer Wohnungstür und zur Entwendung von Wertgegenständen gekommen war. Die Videobänder werden nach 48 Stunden automatisch überspielt.

Da die Hausverwaltung für die Sicherheit in der Wohnanlage und damit auch für den Schutz der Bewohner verantwortlich ist, dient die Videoüberwachung der Zweckbestimmung des Heimvertrages.

Die Maßnahme ist im Hinblick auf die geschilderten Vorkommnisse vertretbar. Sie verstößt nicht gegen den Grundsatz der Verhältnismäßigkeit. Gegenüber dem Interesse der Bewohner, nicht beobachtet zu werden, überwiegt ihr gleichzeitig bestehendes Sicherheitsinteresse.

Wir haben die Hausverwaltung darauf hingewiesen, dass sie diese Maßnahme nur so lange beibehalten darf, wie die Gefahrenlage besteht.

14.2.2 Videoüberwachung im Unterrichtsraum

In einer privaten Schule sollte der Computerhörsaal mit Kameras ausgestattet werden, um auf diese Weise die neu angeschafften Geräte vor Beschädigungen zu schützen. Der Hörsaal steht nicht nur für den Unterricht, sondern auch außerhalb der Unterrichtszeiten den Schülern für Übungszwecke zur Verfügung.

Während des Unterrichts ist eine Videoüberwachung unzulässig. Sie ist nicht erforderlich, weil ein Lehrer als Aufsicht anwesend ist, so dass es bereits an einem berechtigten Interesse der Schule im Sinne des § 28 Abs.1 Satz 1 Nr.2 BDSG fehlt. Darüber hinaus stehen auch die schutzwürdige Interessen der Lehrer und der Schüler, im Unterricht nicht von Videokameras beobachtet zu werden, entgegen.

Auch eine Einwilligung kommt hier nicht in Betracht. Sie ist nach § 4a Abs.1 Satz 1 BDSG nur wirksam, wenn sie auf der freien Entscheidung der Betroffenen beruht. Diese können jedoch für die Zeit der im Computerhörsaal abgehaltenen Unterrichtsstunden keine freie Entscheidung treffen, da sie gezwungen sind, sich dort aufzuhalten.

Etwas anders stellt sich die Rechtslage außerhalb des Unterrichtsbetriebes dar. Hier ist im Rahmen der Abwägung ein berechtigtes Interesse der Schule an der Überwachung der wertvollen Geräte zu bejahen, da sich außerhalb der Unterrichtszeiten keine Lehrer in dem Raum aufhalten. Ob jedoch die schutzwürdigen Interessen der Schüler, nicht einem ständigen Überwachungsdruck ausgesetzt zu sein, hier überwiegen, ist allerdings auch bei dieser Fallgestaltung fraglich.

Deshalb sollte die Einwilligung der Schüler eingeholt werden. Sie beruht jedoch nur dann auf deren freier Entscheidung und kann deshalb als wirksam erachtet werden, wenn den Schülern auch andere Möglichkeiten zum Üben zur Verfügung stehen und sie insoweit nicht auf den Lehrsaal angewiesen sind.

Die Schüler müssen in diesem Zusammenhang über die näheren Umstände der Überwachungsmaßnahme informiert werden (Wann und wie wird überwacht, wer speichert die Aufnahmen, wer kann unter welchen Umständen Auswertungen vornehmen, wie lange wird gespeichert?).

14.3 Übertragung von Webcam-Aufnahmen ins Internet

Ein Beschwerdeführer machte geltend, dass er sich durch eine auf einem hohen Gebäude angebrachte steuer- und zoombare Webcam, in deren Aufnahmefeld sich seine Wohnung befindet, beeinträchtigt fühlt.

In diesem Fall werden mit der Webcam Bilder mit personenbezogenen Daten i. S. d. § 3 Abs. 1 BDSG in das Internet übertragen. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Eine Bildübertragung erfüllt diese Voraussetzungen dann, wenn ein Betrachter eine abgebildete Person oder deren sachliche Verhältnisse identifizieren kann. Dabei ist nicht erforderlich, dass die Bildaufnahmen ein eindeutiges Erkennen einer bestimmten Person zulassen. Der Bezug zu einer bestimmten Person lässt sich vielmehr bereits dann herstellen, wenn der Beobachter eine großflächige Aufnahme eines Anwesens betrachtet und zusätzlich über das für eine Identifikation erforderliche Zusatzwissen verfügt, z. B. weiß, welche Person in welcher Wohnung wohnt, oder eine Person mit einem ihm bekannten besonderen Merkmal (z. B. Rollstuhlfahrer vor dem Hauseingang) erkennen kann. Es genügt dann auch, wenn die übertragenen Bilder einem kundigen Betrachter zeigen, ob sich jemand auf einem bestimmten Balkon aufhält oder ob in der bestimmten Wohnung Licht brennt. Er kann dann z. B. feststellen, ob die in der Wohnung allein lebende Person zuhause ist oder womit sie sich gerade beschäftigt. Bei all diesen möglichen Erkenntnissen handelt es sich um personenbezogene Daten. Das BDSG ist somit anwendbar.

Als Zulässigkeitstatbestand für die Übermittlung der personenbezogenen Daten in das Internet kommt allein § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht, soweit es um die Erfassung privater Bereiche geht. Eine Abwägung zwischen den niedrig einzuschätzenden berechtigten Interessen derjenigen, die diese Bilder im Internet verbreiten, einerseits und den schutzwürdigen Interessen der Beobachteten andererseits sind die letzteren in aller Regel stärker zu gewichten.

Zum selben Ergebnis kommt man in den Fällen, in denen die Kamera öffentlich zugängliche Bereiche (z. B. öffentliche Straßen und Plätze), aufnimmt. Die tatbestandlichen Voraussetzungen des § 6b Abs. 1 BDSG liegen meist nicht vor. Es fehlt bereits an einem berechtigten Interesse der Aufnehmenden. Darüber hinaus

überwiegen die schutzwürdigen Interessen der Betroffenen daran, nicht aufgenommen zu werden.

In beiden Fällen ist somit die Übermittlung personenbezogener Daten ins Internet unzulässig. Den Betreibern gegenüber bestehen wir darauf, die Zoomfunktion so weit zurückzunehmen, dass ein Personenbezug nur noch schwer herzustellen ist.

* * *

15 Medien- und Teledienste, Internet, Telekommunikation

15.1 E-Mail-Werbung

Viele Eingaben beziehen sich nach wie vor auf die Zusendung von unerwünschten E-Mails, sog. Spams. Dabei erhalten die Betroffenen von einer Firma, mit der sie bisher noch nicht in geschäftlichem Kontakt standen, Werbung per E-Mail. In vielen Fällen reagieren die Unternehmen auf ein Auskunftsersuchen überhaupt nicht oder nur unzureichend.

Bei der Zusendung von unerwünschter E-Mail-Werbung handelt es sich vorwiegend um ein verbraucherschutzrechtliches Problem. Daher weisen wir die Eingabeführer bei Anfragen stets auch auf die Möglichkeit hin, sich an den Verbraucherschutz zu wenden.

Der Verbraucherzentrale Bundesverband (vzbv) hat im September 2005 eine Spam-Beschwerdestelle eingerichtet.

An die Adresse beschwerdestelle@spam.vzbv.de können Betroffene bei ihnen eingegangene unerwünschte E-Mails übermitteln. Der vzbv hat angekündigt, dass er in geeigneten Fällen juristisch gegen die Versender der E-Mails und deren Auftraggeber vorgehen wird.

In den meisten Fällen konnten wir den Betroffenen dazu verhelfen, dass sie von den E-Mail-Versendern die ihnen gemäß § 34 BDSG zustehende Auskunft über die dort zu ihrer Person gespeicherten Daten erhalten.

Außerdem wurde durch den Versender der E-Mail meist schriftlich bestätigt, dass die E-Mail-Adresse des Betroffenen aus dem dortigen Datenbestand gelöscht bzw. in eine entsprechende Sperrdatei aufgenommen worden ist.

15.2 Internetveröffentlichungen über Bauhandwerker

Ein Internetauftritt hat Bauherrn die Möglichkeit geboten, ihre positiven und negativen Erfahrungen mit bestimmten Bauunternehmen zu schildern. Der verantwortliche Anbieter dieses Teledienstes stellte die übermittelten Berichte mit den Namen der Unternehmen in eine sog. "TOP 20 Liste“ ein. Darüber hinaus wählte man ein Unternehmen aus, das (angeblich) die größte Fehlleistung erbracht hat.

Auf diese Weise wurden personenbezogene Daten der einzelnen Handwerker in der Form von eingescannten Rechnungen, Äußerungen in Schreiben oder Bewertungen durch die Bauherrn über das Internet weltweit übermittelt.

Diese Datenübermittlungen im Internet können nicht auf den § 28 Abs. 1 Satz 1 Nr. 2 bzw. Abs. 3 Satz 1 Nr. 1 BDSG gestützt werden. Es ist schon sehr fraglich, ob man ein berechtigtes Interesse der Bauherrn an einer weltweiten Veröffentlichung ihrer schlechten Erfahrungen mit Handwerkern anerkennen kann. In gleicher Weise ist zweifelhaft, ob Dritte ein berechtigtes Interesse an derart einseitigen Berichten haben. In jedem Fall überwiegen jedoch die schutzwürdigen Belange der Handwerker dahingehend, dass über sie derartige Behauptungen veröffentlicht werden.

Da auch keine Einwilligungen der einzelnen Handwerker vorlagen, waren diese Veröffentlichungen unzulässig.

Der Anbieter hat nach unseren Hinweisen auf die Rechtslage diesen Internetauftritt eingestellt.

* * *