Hinweise des Innenministeriums zum Datenschutz für private Unternehmen und Organisationen (Nr. 40)

Bekanntmachung des Innenministeriums vom 18. Februar 2002 Az. 2-0552.1/17,
bereitgestellt im Internet unter www.im.bwl.de,
Rubrik Datenschutz/Hinweise

Am 2. Dezember 1977 erschien die erste Nummer der Hinweise zum Datenschutz für private Unternehmen und Organisationen des Innenministeriums Baden-Württemberg. Daran wird deutlich, dass dem Datenschutz in Baden-Württemberg schon in dessen Anfangszeiten auch für den nichtöffentlichen Bereich ein hoher Stellenwert eingeräumt wurde.

Seither erschienen zu Beginn eines jeden Jahres neue Ausgaben der Hinweise, die nicht nur in den Unternehmen der privaten Wirtschaft auf breite Resonanz stießen. Auch in der Fachliteratur wurden diese Hinweise immer wieder aufgegriffen und der Beurteilung von datenschutzrechtlichen Fragestellungen zugrundegelegt. Damit war es gelungen, nicht nur den Praktikern eine Art Handlungsanleitung für die Beantwortung vieler im Alltag auftretenden Probleme im Datenschutz zur Verfügung zu stellen, sondern zugleich die allgemeine datenschutzrechtliche Diskussion durch Beiträge zu den verschiedensten Themen anzustoßen und zu vertiefen.

Mit dieser Ausgabe gibt das Innenministerium die 40. Ausgabe dieser Hinweise heraus. Diese runde Zahl ist für uns Anlass, künftig von einer regelmäßigen jährlichen Herausgabe zum jeweiligen Jahresanfang abzusehen und statt dessen je nach Bedarf gezielt zu einzelnen datenschutzrechtlichen Themen und Fragestellungen Hinweise zu veröffentlichen. Die Änderung der langjährigen Praxis erfolgt insbesondere vor dem Hintergrund, dass das Innenministerium seit 2001 alle zwei Jahre einen Tätigkeitsbericht vorzulegen hat, in dem ebenfalls zu einer Vielzahl von datenschutzrechtlichen Themen ausführlich Stellung genommen wird. Anhand dieses Berichts lässt sich jeweils umfassend die aktuelle Entwicklung im Datenschutz im nichtöffentlichen Bereich in Baden-Württemberg nachvollziehen. Die positive Resonanz, die der Tätigkeitsbericht 2001 gefunden hat, belegt, in welchem Maße solche Berichte geeignet sind, gerade auch die Öffentlichkeit über das Datenschutzrecht im nichtöffentlichen Bereich zu informieren.

A Die neue datenschutzrechtliche Regelung zur Videoüberwachung

Mit dem Gesetz zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze vom 18. Mai 2001 (BGBl. S. 904) wurde erstmalig in § 6b BDSG eine Regelung zur Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen – Videoüberwachung – aufgenommen.
Die Neuregelung wirft Fragen nach ihrem Anwendungsbereich und ihren Zulässigkeitsvoraussetzungen auf, mit denen sich die Aufsichtsbehörde im Rahmen ihrer Kontrolltätigkeit bereits in wesentlichen Teilen befasst hat.

1 Der Anwendungsbereich

1.1 Der Anwendungsbereich des Gesetzes

Nach § 1 Abs. 2 Nr. 3 BDSG gilt das Gesetz für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nichtöffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, es sei denn, die Erhebung, Verarbeitung und Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Das Beobachten öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen beinhaltet eine Erhebung personenbezogener Daten, wenn dabei jedenfalls auch Daten über natürliche Personen beschafft werden sollen. Daran fehlt es, wenn die Beobachtung zu einem anderen Zweck erfolgt, beispielsweise zur Überwachung des Ablaufs eines technischen Vorgangs, und dabei Personen, die sich zufällig in einem öffentlich zugänglichen Raum aufhalten, in den Blickwinkel der Videokamera gelangen können, ohne dass insoweit eine weitere Datenverarbeitung erfolgt. Ein Beispiel dafür ist die Überwachung eines Bahnsteigs durch den Zugführer über einen neben seinem Steuerstand auf dem Bahnsteig aufgestellten Monitor zu dem Zweck, vor der Abfahrt überprüfen zu können, ob alle Türen geschlossen sind. Die ein- und aussteigenden Personen werden bei dieser Verarbeitung nicht beobachtet. Hier ist schon der Schutzzweck des Gesetzes, das Persönlichkeitsrecht des Einzelnen zu schützen, nicht tangiert.

Eine Videoüberwachungsanlage ist, zumindest bei analoger Aufnahmetechnik, keine Datenverarbeitungsanlage. Da der Gesetzgeber die Videoüberwachung nichtöffentlicher Stellen nicht vom Anwendungsbereich des BDSG ausschließen wollte (sonst wäre § 6b BDSG auf nichtöffentliche Stellen nicht anwendbar, was nicht dem Sinn der Vorschrift entspricht), muss § 1 Abs. 2 Nr. 3 BDSG auf Videoüberwachungsanlagen insoweit analog angewandt werden.

Im Übrigen müssen die sonstigen Voraussetzungen für die Eröffnung des Anwendungsbereichs des BDSG erfüllt sein. Daran fehlt es, wenn die Videoüberwachung ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt.

1.2 Der Anwendungsbereich des § 6b BDSG

Voraussetzung für die Anwendbarkeit des § 6b BDSG ist, dass öffentlich zugängliche Räume mit optisch elektronischen Einrichtungen beobachtet werden, wobei eine anschließende Speicherung des Bildmaterials nicht erforderlich ist.

Die Gesetzesbegründung nennt als öffentlich zugängliche Räume beispielhaft „Bahnsteige, Ausstellungsräume eines Museums, Verkaufsräume oder Schalterhallen“, also Räume, die nach dem Willen des oder der Berechtigten, gegebenenfalls nach Herbeiführung einer für jeden möglichen Zugangsberechtigung wie das Lösen einer Eintrittskarte, grundsätzlich jedermann zugänglich sind beziehungsweise betreten werden können.
Wie bereits in den Hinweisen des Innenministeriums zum Datenschutz für private Unternehmen und Organisationen Nr. 39 vom 25. Januar 2001 unter Buchstabe C Ziffer 2 ausgeführt, kann der öffentlich zugängliche Raum innerhalb oder außerhalb von Gebäuden liegen, wobei es nicht darauf ankommt, ob die Räumlichkeit im privaten oder öffentlichen Eigentum steht. Im Zusammenhang mit der dort erörterten Fallkonstellation war es ausreichend, für das Merkmal der öffentlichen Zugänglichkeit auf das Betreten–Können des Raumes abzustellen. Allein die faktische Möglichkeit für jedermann, einen Raum betreten zu können, beispielsweise weil die Haustüre offen steht, ist für sich allein aber nicht ausreichend, um einen Raum als öffentlich zugänglich qualifizieren zu können. Der Raum muss auch von jedermann betreten werden dürfen. Daran fehlt es, wenn nach dem Willen des oder der Berechtigten der Zugang nur bestimmten Personen oder bestimmten Personengruppen offen steht. Deshalb sind öffentlich zugängliche Räume nur solche, die nach dem erkennbaren oder mutmaßlichen Willen des oder der Berechtigten von jedermann betreten werden dürfen. Nicht öffentlich zugänglich in diesem Sinne sind Ein- und kleinere Mehrfamilienhäuser einschließlich deren Grundstücken, aber in der Regel auch Firmen- und Werksgelände sowie Flure, Aufzüge oder Tiefgaragen auch von größeren Mietshäusern. Etwas anderes kann bei großen Wohnanlagen gelten, wenn ausnahmsweise keinerlei Zugangsbeschränkungen bestehen.

Wird ein nicht öffentlich zugänglicher Raum videoüberwacht, so richtet sich die Zulässigkeit nach den gegebenenfalls einschlägigen allgemeinen datenschutzrechtlichen Regelungen sowie nach der hierzu ergangenen zivilgerichtlichen Rechtsprechung, auf die hier nicht gesondert eingegangen wird.

2 Fallbeispiele zur Videoüberwachung von Grundstücken, Gewerbeobjekten und öffentlich zugänglichen Räumen

Hier können verschiedene Fallgruppen gebildet werden:

2.1 Beobachtung öffentlich zugänglicher Räume durch eine Privatperson zum Zweck der Zugangskontrolle zum Privatwohnhaus

Der Anwendungsbereich des Gesetzes ist nicht eröffnet, denn die private Videoüberwachung privater Wohnhäuser durch den Eigentümer oder Besitzer ist ohne Weiteres als persönliche Tätigkeit zu qualifizieren. Werden bei dieser persönlichen Tätigkeit auch Bereiche des Gehwegs oder der Straße erfasst, ist dies unerheblich. Eine andere Auslegung würde den Anwendungsbereich über Gebühr entgegen § 1 Abs. 2 Nr. 3 BDSG und gegen Sinn und Zweck der Vorschrift des § 6b BDSG erweitern. Zu beachten ist das Erfordernis der Ausschließlichkeit. Die Videoüberwachung darf nicht noch für eine über die persönliche oder familiäre Tätigkeit hinausgehende Sekundärnutzung eingesetzt werden.

Sind private Sicherheitsdienste mit der Videoüberwachung beauftragt, muss differenziert werden. Ist die Videoüberwachung des konkreten privaten Objekts durch Sicherheitsdienste als Funktionsübertragung zu qualifizieren, so liegt keine Überwachung für persönliche oder familiäre Tätigkeiten vor. Verantwortliche Stelle ist dann der Sicherheitsdienst. Bei der Videoüberwachung als Datenverarbeitung im Auftrag bleibt dagegen der Auftraggeber verantwortlich, bei dem das Kriterium einer ausschließlich persönlichen oder familiären Tätigkeit zu beachten ist.

Grundsätzlich werden bei der Videoüberwachung eines Privathauses von der Aufsichtsbehörde persönliche oder familiäre Tätigkeiten vermutet, sofern keine anderen Anhaltspunkte vorliegen.

2.2 Beobachtung öffentlich zugänglicher Räume durch eine Privatperson (Videofilm zu sonstigen Zwecken)

Auch hier ist der Anwendungsbereich des Gesetzes grundsätzlich nicht eröffnet, wenn die Erhebung, Verarbeitung und Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Das Gesetz ist jedoch dann anwendbar, wenn die Grenze der persönlichen oder familiären Tätigkeiten überschritten wird oder die gewonnenen Daten einer unbestimmten Anzahl von Personen zur Kenntnis gegeben werden (Dammann/Simitis, EG-Datenschutzrichtlinie, Rdnr. 8 zu Art. 3).

2.3 Beobachtung öffentlich zugänglicher Räume zum Zweck der Zugangskontrolle zu einem öffentlich zugänglichen Gewerbeobjekt

Bei einer gewerblichen Nutzung des überwachten Objekts, auch durch Einzelgewerbetreibende oder Selbständige, liegt keine persönliche oder familiäre Tätigkeit vor. Das BDSG ist anwendbar, die Videoüberwachung muss den Anforderungen des § 6b BDSG entsprechen.

2.4 Beobachtung öffentlich zugänglicher Räume zum Zweck der Zugangskontrolle zu einem nicht öffentlich zugänglichen Gewerbeobjekt (Klingelkamera)

Auch hier liegt keine persönliche oder familiäre Tätigkeit vor. Die Videoüberwachung unterliegt jedoch dann nicht § 6b BDSG, wenn sich der Kamerablickwinkel auf den Zugangs- oder Einfahrtsbereich beschränkt. In diesem Fall steht nicht die Beobachtung des öffentlich zugänglichen Raums im Vordergrund. Vielmehr wird dieser nur bei Gelegenheit im Zuge eines konkreten Zugangs einer bestimmten Person oder einer konkreten Einfahrt eines bestimmten Fahrzeugs mit erfasst. Schaltet sich die Videokamera bei Türöffnungssystemen zudem nur dann ein, wenn geklingelt wird, und danach wieder selbsttätig ab, fehlt es erst recht an dem Merkmal der Beobachtung des öffentlichen Raums und damit an der Erhebung personenbezogener Daten.

Ist die Kamera im Türöffnungssystem jedoch so eingestellt, dass sie über den Zugangsbereich hinaus größere Flächen von Gehweg und Straße erfasst, so dass erkannt werden kann, ob und gegebenenfalls wer sich in der weiteren Umgebung des Objekts befindet, und ist sie unabhängig von der Betätigung der Türklingel in Betrieb, kann nicht mehr davon ausgegangen werden, dass die Erfassung nur zum Zwecke der Zugangskontrolle erfolgt. § 6b BDSG ist dann zu beachten.

3 Die Voraussetzungen der Videoüberwachung am Beispiel von Kaufhäusern und Verkaufsräumen

Die Verkaufsfläche eines Kaufhauses oder eines Ladengeschäfts ist, soweit Kunden freien Zutritt haben, ein öffentlich zugänglicher Raum im Sinne des § 6b Abs. 1 BDSG.

3.1 Die Zwecke der Videoüberwachung

Die Videoüberwachung durch nichtöffentliche Stellen ist nach § 6b Abs. 1 Nr. 2 und 3 BDSG nur zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhalts

punkte für das Vorliegen überwiegender schutzwürdiger Interessen des Betroffenen bestehen.

Die Vorschrift legt den Umfang des Hausrechts nicht fest. Zivilrechtlich gesehen ist das Hausrecht die Befugnis, über die Benutzung eines geschützten Raums zu verfügen und gegebenenfalls ein Hausverbot auszusprechen. Eine Videoüberwachung, die nicht unter das Hausrecht im engeren Sinn fällt (zum Beispiel eine Videoüberwachung zum Schutz des Eigentums), muss deshalb mit einem berechtigten Interesse nach § 6b Abs. 1 Nr. 3 BDSG begründet werden.
Berechtigt ist jedes Interesse, das nach vernünftiger Erwägung durch die Sachlage gerechtfertigt ist, also ein tatsächliches Interesse, das wirtschaftlicher oder ideeller Natur sein kann (Gola/Schomerus, Kommentar zum BDSG, Anm. 7.1 zu § 28 BDSG). Nach diesen Kriterien kann beispielsweise am Schutz des Eigentums oder an der Vermeidung von Inventurdifferenzen ein berechtigtes Interesse bestehen.
Weitere gesetzliche Voraussetzung ist die Erforderlichkeit. Sie ist dann gegeben, wenn der verfolgte beabsichtigte Zweck nicht mit einem anderen zumutbaren Mittel, das weniger in die Rechte der Betroffenen eingreift, erreicht werden kann.

Bei einer Videoüberwachung in einem Kaufhaus zum Schutz vor konkreten Straftaten wie Diebstahl, hält die Aufsichtsbehörde ein berechtigtes Unternehmensinteresse und die Erforderlichkeit für gegeben. So hält das LG Stuttgart die Videoüberwachung im Kaufhaus im Sinne eines effektiven Eigentumsschutzes für geradezu geboten.

Der konkrete Zweck der Videoüberwachung muss jedoch vor der Inbetriebnahme der Überwachung festgelegt, d.h. dokumentiert werden (siehe Ziff. 3.7). Bei der Festlegung des Zwecks ist zu beachten, dass bei der Videoüberwachung in einem Objekt gegebenenfalls mehrere unterschiedliche Zwecke bestehen können. So kann beispielsweise die Überwachung der Frauenparkplätze im kaufhauseigenen Parkhaus nicht mit dem Schutz vor Inventurdifferenzen, der für die Verkaufsräume zutreffend ist, begründet werden. Bei der Festlegung der Zwecke ist sehr sorgfältig vorzugehen, da mittels der Videoüberwachung gewonnene Erkenntnisse für andere als die festgelegte Zwecke, mit Ausnahme der Strafverfolgung, nicht verwendet werden dürfen.

Vor dem Beginn der Überwachung ist zu prüfen, ob Anhaltspunkte für ein überwiegendes schutzwürdiges Interesse der Betroffenen bestehen. Wenn Personen so videoüberwacht werden, wie ein aufmerksamer Beobachter dies mit bloßem Auge auch tun könnte, so liegt im Regelfall keine Verletzung eines schutzwürdigen Interesses vor. Geht die Videoüberwachung jedoch über die „normale“ Beobachtung hinaus, wird beispielsweise durch eine Beobachtung in der Umkleidekabine in die Privat- und Intimsphäre des Kunden eingegriffen, so werden schutzwürdige Interessen verletzt.

Da auch die Mitarbeiter von der Videoüberwachung betroffen sind, sind auch ihre schutzwürdigen Interessen zu berücksichtigen.

3.2 Die Besonderheit bei einer Funktionsübertragung

Werden die Verkaufsräume durch Dritte, z.B. durch eine Detektei überwacht, ist zu prüfen, ob eine Datenverarbeitung im Auftrag oder eine Funktionsübertragung vorliegt. Bei der Datenverarbeitung im Auftrag ist das Kaufhaus die verantwortliche Stelle und bei der Zulässigkeitsüberprüfung sind seine berechtigten Interessen relevant. Bei einer Funktionsübertragung dagegen liegt die datenschutzrechtliche Verantwortung bei der Detektei. Beim berechtigten Interesse zählt nur das Interesse der Detektei und nicht das des Kaufhauses, was zu Einschränkungen führen kann. Es kann zweifelhaft sein, ob eine Detektei auf Grund einzuhaltender vertraglicher Verpflichtungen gegenüber dem Kaufhaus ein eigenes berechtigtes Interesse an der Vermeidung von Inventurdifferenzen geltend machen kann. Um eine Funktionsübertragung auszuschließen, sind die Kriterien für die Auftragsdatenverarbeitung, insbesondere § 11 BDSG, einzuhalten.

3.3 Die Kenntlichmachung der Videoüberwachung

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

Auf die Überwachung kann durch Schilder, aber auch durch das Aufstellen von Monitoren im Eingangsbereich, die Ausschnitte der Überwachungsbilder zeigen, hingewiesen werden. In Verkaufsräumen, in denen auch Monitore zur Verkaufsförderung aufgestellt sind, wird zur Vermeidung von Verwechslungen empfohlen, keine Monitore als Hinweis zu verwenden.

Ein Hinweis auf die verantwortliche Stelle ist bei jeder Darstellungsform zu geben. Es liegt zwar nahe, dass die Überwachung eines Kaufhauses durch das Kaufhaus selbst durchgeführt wird, der Gesetzgeber verlangt aber ausdrücklich die Benennung der verantwortlichen Stelle, damit der Betroffene seine Rechte geltend machen kann (Gesetzesbegründung zu § 6b BDSG). Der Kunde kennt meist die konkrete Rechtsform des Unternehmens nicht. Beispielsweise ist in einem Filialunternehmen die verantwortliche Stelle aus Sicht des Kunden nicht selbsterklärend. Er weiß nicht, bei wem er seine Rechte geltend machen kann, in der Filiale vor Ort oder in der Konzernzentrale. Er weiß auch nicht, ob die Überwachung durch das Kaufhaus selbst oder im Wege der Funktionsübertragung von einem Dritten durchgeführt wird. Diese Unsicherheit besteht insbesondere in sogenannten Einkaufsmärkten mit verschiedenen Einzelhandelsgeschäften in einem Objekt. Da die Nennung der verantwortlichen Stelle der Geltendmachung der Ansprüche des Betroffenen dient, sollte

als verantwortliche Stelle die für die Durchführung verantwortliche Stelle vor Ort, also die Stelle, an die sich der Kunde wenden kann, benannt werden.

Vereinzelt sind Hinweise aufgestellt mit der Mitteilung, dass die Videoüberwachung zur Sicherheit der Kunden erfolgt. Von dieser Begründung wird abgeraten, da sie als festgelegter Zweck angesehen werden kann, der, da er öffentlich bekannt gemacht wird, die eigentlichen festgelegten Zwecke unwirksam machen könnte. Dies könnte zur Folge haben, dass die Videoüberwachung dann nur noch zur Sicherheit der Kunden genutzt werden kann. Es ist im Übrigen nicht erforderlich, den Hinweis auf die Videoüberwachung mit einer Begründung zu versehen.

Ein Hinweis auf die Videoüberwachung könnte z.B. lauten:
„Dieses Gebäude wird von der „Firma“ (alternativ: „*uns*“) *videoüberwacht. Bei Fragen hierzu wenden Sie sich bitte an ... (beispielsweise: unsere Kundeninformation im EG).“*

Der Hinweis ist deutlich sichtbar anzubringen. Was deutlich sichtbar ist, hängt von der Größe und Gestaltung des Hinweises, aber auch vom Umfeld und dem Hintergrund ab. Die räumliche Anordnung hat so zu erfolgen, dass der Kunde den Hinweis beim Betreten des Hauses beziehungsweise beim Eintritt in den überwachten Bereich im normalen Blickwinkel hat. Ein Hinweis erfüllt nur dann seinen Zweck, wenn er für den Kunden ohne Weiteres wahrnehmbar ist und von ihm nicht erst gesucht werden muss.

3.4 Die Verarbeitung und Nutzung der Daten

Bei der Verarbeitung, wie der Speicherung und Übermittlung, oder der Nutzung der durch die Videoüberwachung gewonnenen Daten ist nach § 6b Abs. 3 BDSG zu prüfen, ob die Verarbeitung und Nutzung des Beobachtungsergebnisses zum Erreichen des festgelegten Zwecks erforderlich ist und keine Anhaltspunkte für überwiegende schutzwürdige Interessen des Betroffenen bestehen. Die Übermittlung der Videoaufzeichnung an die Strafverfolgungsbehörden beziehungsweise die Nutzung als Beweismittel zur Erlangung von Schadenersatz kann zum Erreichen eines festgelegten Zwecks erforderlich sein. Bei einer Person, die einer Straftat verdächtigt wird, halten wir keine Anhaltspunkte überwiegender schutzwürdiger Interessen am Ausschluss der Nutzung als Beweismittel für gegeben.

3.5 Die Benachrichtigungspflicht

Nach § 6b Abs. 4 BDSG besteht eine Verpflichtung zur Benachrichtigung des Betroffenen entsprechend §§ 19a und 33 BDSG, wenn durch die Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet werden können. Darunter fällt immer der Verdächti

ge, beispielsweise aber auch das Opfer eines Taschendiebstahls oder sonstige namentlich bekannte Personen.

3.6 Die Pflicht zur unverzüglichen Löschung

Die unverzügliche Löschung der Aufnahmen nach der Erreichung des Aufnahmezwecks ist in § 6b Abs. 5 BDSG vorgeschrieben. Bei einer vollständigen Aufzeichnung eines Geschäftstags (z.B. in einer Black Box) muss die Aufzeichnung innerhalb von ein bis zwei Arbeitstagen ausgewertet werden (Gesetzesbegründung zu § 6b BDSG). Aufzeichnungen, die dann nicht entsprechend dem Zweck genutzt werden, sind unverzüglich, das heißt ohne schuldhaftes Zögern, zu löschen, beispielsweise durch Überspielen in einem zweiten Recorder ohne Aufnahmesignal. Wird eine Videokassette nicht nach dem Erreichen des Aufnahmezwecks, sondern erst bei ihrer nächsten Verwendung durch Überspielen gelöscht, so erfolgt die Löschung nicht unverzüglich. Die rechtzeitige Löschung ist deshalb unbedingt durch organisatorische Maßnahmen sicherzustellen.

3.7 Das Verfahren automatisierter Verarbeitung

Die Videoüberwachung ist einem automatisierten Verfahren gleichzusetzen, mit der Folge, dass bei Bestehen einer Meldepflicht die Angaben nach § 4e Satz 1 BDSG, die nach Nr. 4 auch die Angabe der Zweckbestimmungen der Datenerhebung, -verarbeitung oder –nutzung erfasst, der Aufsichtsbehörde zu melden sind. Besteht keine Meldepflicht, so muss der Datenschutzbeauftragte oder, wenn ein Datenschutzbeauftragter nicht bestellt ist, die verantwortliche Stelle nach § 4g Abs. 2 BDSG die Angaben nach § 4e Satz 1 Nr. 1 bis 8 BDSG auf Antrag jedermann in geeigneter Weise verfügbar machen.

Das nachfolgende Muster einer Dokumentation der Angaben – beschränkt auf die Angaben nach § 4e Satz 1 Nr. 1 bis 7 BDSG – soll dazu eine Hilfestellung bieten.

Muster einer Dokumentation der Angaben nach § 4e Satz 1 Nr. 1 bis 7 BDSG

Verfahren: Videoüberwachung im Objekt Anschrift, Stand 00.00.2002:

1. *Firma und Anschrift der verantwortlichen Stelle:*
   Firma:
   Anschrift:
   Filiale:
   Filialanschrift:

2. *Vorstand und für die Datenverarbeitung (Videoüberwachung) verantwortliche Personen:*
   Vorstand bzw. Geschäftsführer des Gesamtunternehmens:
   Datenschutzbeauftragter:
   Für die Durchführung der Videoüberwachung verantwortlicher örtlicher Geschäftsführer oder Beauftragter (Auskunftgeber):

3. *Festgelegte Zwecke der Videoüberwachung (§ 6b Abs. 1 Nr. 3 BDSG) und betroffene Personen(gruppen):*

   Verkaufsräume, die Videoüberwachung erfolgt zur:
   -Dokumentation begangener Straftaten,
   -Senkung von Inventurdifferenzen,
   -Geltendmachung von Schadenersatzansprüchen,
   -Feststellung und Abwehr von Störungen,
   -Koordinierung des Einsatzes von Sicherheitskräften bei akuten Gefahrensituationen.
   Betroffene Personen: Mitarbeiter und Kunden.

   Cafeteria, die Videoüberwachung erfolgt zum:
   -Schutz der Kunden vor Taschendiebstählen.
   Betroffene Personen: Kunden und Mitarbeiter.

   Parkhaus, die Videoüberwachung erfolgt zum:
   -Schutz der Benutzer vor Überfällen und vor Einbrüchen in die Fahrzeuge.
   Betroffene Personen: Parkhausbenutzer.

(Anm.: wenn fallbezogen aufgezeichnet wird)
Die Videoüberwachung erfolgt durch Beobachtung. Aufgezeichnet wird nur, wenn sich bei der Beobachtung ein den festgelegten Zwecken entsprechender Verdacht ergibt.

(Anm.: wenn immer aufgezeichnet wird)
Die Videoüberwachung erfolgt durch Beobachtung und Aufzeichnung.
Die Auswertung der Aufzeichnung erfolgt spätestens am übernächsten Arbeitstag.

4. *Empfänger der Überwachungsaufnahmen*
Die Aufzeichnungen können als Beweismittel an die Strafverfolgungsbehörden übermittelt oder zur Durchsetzung zivilrechtlicher Forderungen verwendet werden.

5. *Löschung*
Die Aufzeichnungen, die nicht entsprechend Ziff. 4 genutzt werden, werden unverzüglich gelöscht.

B Übermittlung personenbezogener Daten im internationalen Bereich

1 Die neuen Vorschriften zum internationalen Datenverkehr

In den Hinweisen des Innenministeriums zum Datenschutz für private Unternehmen und Organisationen Nr. 39 vom 25.01.2001 hat das Innenministerium unter Buchstabe A auf der Grundlage des Regierungsentwurfs des Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze die vorgesehenen Neuregelungen der §§ 4b und 4c BDSG-E für die Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen ausführlich dargestellt. Im Verlauf des Gesetzgebungsverfahrens des am 23.05.2001 in Kraft getretenen Änderungsgesetzes haben die §§ 4b und 4c BDSG zwar Änderungen erfahren, die die Ausführungen des Innenministeriums jedoch im Wesentlichen unberührt lassen.

Gegenüber dem Regierungsentwurf ergaben sich folgende Änderungen:

- In die Regelung des § 4b Abs. 1 BDSG sind nunmehr auch die Staaten des Europäischen Wirtschaftsraums – EWR-Staaten – (Liechtenstein, Norwegen und Island) sowie die Organe und Einrichtungen der Europäischen Gemeinschaften einbezogen. Diese Erweiterung trägt der zum 1. Juli 2000 wirksam gewordenen Übernahme der EG-Datenschutzrichtlinie 95/46 – im folgenden Richtlinie genannt – durch die EWR-Staaten sowie der durch Art. 286 des Vertrags zur Gründung der Europäi

schen Gemeinschaften (EGV) für die Organe und Einrichtungen der Gemeinschaften wirksam gewordenen Richtlinie Rechnung .

- Die in § 4b Abs. 6 BDSG enthaltene Hinweispflicht ist nunmehr auf die reine Mitteilung des Übermittlungszweckes – ohne zusätzliches Zweckbindungsgebot – beschränkt. Da die Daten im Rahmen des § 4b Abs. 1 BDSG innerhalb des Anwendungsbereichs der Richtlinie verbleiben und das Zweckbindungsgebot nach der Richtlinie nicht uneingeschränkt gilt, kann der Hinweis in deren Geltungsbereich nicht weiter gehen als die Richtlinie selbst.
- Im Übrigen wurden die §§ 4b und 4c BDSG nur redaktionell überarbeitet.

Die Europäische Kommission hat zwischenzeitlich weitere Entscheidungen getroffen, die von den Mitgliedstaaten zu beachten sind.
Mit Entscheidung vom 20. Dezember 2001 hat die Kommission ein angemessenes Datenschutzniveau auch für Kanada festgestellt, beschränkt jedoch auf diejenigen Bereiche, die dem kanadischen Personal Information Protection and Electronic Documents Act unterfallen (ABl.EG 2002 Nr. L 2 S. 13). Der kanadische Datenschutzbeauftragte berät auf Anfrage europäische Unternehmen, ob für die datenempfangende Stelle in Kanada dieses kanadische Gesetz gilt.
Bereits am 15. Juni 2001 hat die Europäische Kommission Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG (ABl.EG 2001 Nr. L 181 S. 19) und am 27. Dezember 2001 für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländer nach der Richtlinie 95/46/EG (ABl.EG 2002 Nr. L 6 S. 52) erlassen.

2 Genehmigung von Datenübermittlungen in Drittländer nach § 4c Abs. 2 BDSG

Nach § 4c Abs. 2 BDSG kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an Stellen in Drittländer genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist, wobei sich die Garantien insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben können.
Zu dem neu eingeführten Genehmigungstatbestand bestehen vielfältige Unsicherheiten und Unklarheiten, die in den letzten Monaten vermehrt an das Innenministerium herangetragen wurden und auch schon zu Erörterungen innerhalb des Düsseldorfer Kreises führten. Besonderer Klärungsbedarf besteht bei Unternehmensregelungen, da sie, insbesondere in großen weltweit tätigen Konzernen, ohne Bezugnahme auf konkrete Datenübermittlungen oder Arten von Datenübermittlungen abstrakt abgefasst werden, um möglichst

für alle bestehenden, aber auch alle künftig denkbaren Datenübermittlungen ausreichende Garantien im Sinne von § 4c Abs. 2 BDSG vorweisen zu können.
Nachfolgend soll auf immer wieder auftretende Fragestellungen Antwort gegeben werden.

2.1 Wann ist eine Genehmigung nach § 4c Abs. 2 BDSG erforderlich?

Eine Genehmigung nach § 4c Abs. 2 BDSG ist nur erforderlich, wenn kumulativ folgende Voraussetzungen vorliegen:

- Es muss sich um Datenübermittlungen personenbezogener Daten an Stellen handeln, die sich nicht in den Mitgliedstaaten der EU oder den EWR-Staaten befinden.
- Für die datenimportierende Stelle im Drittland ist kein angemessenes Schutzniveau im Sinne des § 4b Abs. 3 BDSG gewährleistet, was von der datenexportierenden Stelle in eigener Zuständigkeit zu prüfen ist, ausnahmslos aber dann gewährleistet ist, wenn eine positive Entscheidung der Europäischen Kommission über ein angemessenes Datenschutzniveau für das betreffende Land vorliegt (derzeit für Ungarn, die Schweiz und in begrenztem Umfang für Kanada). Zur Rechtsfolge bei Verwendung der Standardvertragsklauseln der Europäischen Kommission siehe Ziff. 2.8.
- Es greift keiner der in § 4c Abs. 1 S. 1 Nr. 1 bis 6 BDSG aufgeführten Ausnahmetatbestände (unter anderem Vorliegen einer Einwilligung des Betroffenen, Durchführung von vorvertraglichen Maßnahmen, Erfüllung eines Vertrags, Wahrung lebenswichtiger Interessen des Betroffenen).

Nur wenn keiner dieser Punkte zutrifft, ist die Datenübermittlung für ihre Zulässigkeit nach § 4c Abs. 2 BDSG genehmigungsbedürftig und ein Antrag bei der zuständigen Aufsichtsbehörde zu stellen.

2.2 Was ist Genehmigungsgegenstand nach § 4c Abs. 2 BDSG?

Genehmigungsgegenstand sind nach dem klaren Wortlaut des § 4c Abs. 2 BDSG die einzelnen genehmigungsbedürftigen Übermittlungen oder die genehmigungsbedürftigen Arten von Übermittlungen personenbezogener Daten. Daraus ergibt sich, dass eine Unternehmensregelung selbst nicht Gegenstand einer Genehmigung sein kann. Die Begründung des Regierungsentwurfs ist insoweit unscharf. Eine Genehmigung von Unternehmensregelungen und damit die abstrakte Feststellung, dass bestimmte „Garantien“ ausreichend sind, wäre auch deshalb unzulässig, weil nach Art. 26 Abs. 4 der Richtlinie solche Feststellungen nur der Europäischen Kommission vorbehalten sind. Eine Unternehmensregelung ist jedoch, wenn sie verbindlich ist, bei der Prüfung der zu genehmigenden Übermittlungen zur Feststellung ausreichender Garantien heranzuziehen. Ergeben sich die einzelnen Übermittlungen oder Arten von Übermittlungen und deren Übermittlungszweck nicht

aus der Unternehmensregelung selbst, so sind diese Angaben zwingend im Genehmigungsantrag zu machen, damit der Gegenstand der Genehmigung feststeht. Die Erteilung einer „Blanko-Genehmigung“ ist aus verwaltungsverfahrensrechtlichen Gründen nicht möglich.

2.3 Kann die Genehmigung für jedes Drittland erteilt werden?

Da sich die Frage der ausreichenden Garantien für jedes Drittland gesondert stellt, muss sich eine Genehmigung nach § 4c Abs. 2 BDSG immer auf ein einzelnes konkretes Drittland beziehen, das deshalb im Antrag anzugeben ist. Dies bedeutet jedoch nicht, dass nicht in einer einheitlichen Genehmigung Übermittlungen in mehrere Drittländer zusammengefasst werden können. Ob dies möglich ist, hängt neben dem Inhalt der jeweiligen verbindlichen Unternehmensregelungen insbesondere davon ab, wie genau die genehmigungsbedürftigen Datenübermittlungen beschrieben werden können.

2.4 Umfasst die Genehmigung nach § 4c Abs. 2 BDSG auch die Übermittlungsvoraussetzungen der §§ 28 bis 30 BDSG?

Die Übermittlungsvoraussetzungen nach §§ 28 bis 30 BDSG sind von der Genehmigung nicht umfasst. Die Genehmigung nach § 4c Abs. 2 BDSG bezieht sich nur auf die zusätzlichen Anforderungen dieser Vorschrift, nämlich auf das Vorliegen ausreichender Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte. Die Übermittlungsvoraussetzungen der §§ 28 bis 30 BDSG sind für jede Datenübermittlung durch die verantwortliche Stelle selbst zu prüfen. Im Genehmigungsverfahren müssen sie nicht, sie können aber im Rahmen der allgemeinen Aufsichtstätigkeit überprüft werden. Eine Datenübermittlung in ein Drittland kann deshalb nach §§ 28 bis 30 BDSG unzulässig sein, obwohl eine Genehmigung nach § 4c Abs. 2 BDSG erteilt wurde. Treten im Rahmen des Genehmigungsverfahrens Zweifel am Vorliegen der Übermittlungsvoraussetzungen nach §§ 28 bis 30 BDSG auf, so kann diesen ohne Weiteres nachgegangen werden. Stellt sich die Unzulässigkeit der Datenübermittlung nach §§ 28 bis 30 BDSG heraus, ist für eine Genehmigung mangels Vorliegens dieser allgemeinen Übermittlungsvoraussetzungen kein Raum mehr. Auf die Erteilung einer Genehmigung für eine rechtswidrige Übermittlung besteht nämlich kein Anspruch.

2.5 Was muss eine verbindliche Unternehmensregelung beinhalten, um ausreichende Garantien im Sinne des § 4c Abs. 2 BDSG vorzuweisen?

Die größte Gewähr dafür, dass – insbesondere abstrakte – verbindliche Unternehmensregelungen ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweisen, besteht dann, wenn sie sich in

haltlich an den aus den Standardvertragklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten in Drittländer ableitbaren datenschutzrechtlichen Standards auch im Hinblick auf die Drittbegünstigtenklausel und die Haftungsregelung orientieren (siehe hierzu die Checkliste unter Ziff. 3). Inhaltliche Abweichungen von den Vorgaben der Standardvertragsklauseln können dann unschädlich sein, wenn sie durch sonstige verbindliche unternehmensinterne Regelungen oder organisatorische Maßnahmen hinreichend kompensiert werden können.

2.6 Aufnahme eines Widerrufsvorbehalts

Auch wenn die Genehmigungsvoraussetzungen für einzelne Datenübermittlungen oder Arten von Übermittlungen einschließlich deren Zwecke vorliegen, beispielsweise weil eine verbindliche Unternehmensregelung ausreichende Garantien vorweist, wird eine Genehmigung nach § 4c Abs. 2 BDSG nur unter Widerrufsvorbehalt erteilt. Der Grund dafür ist, dass die erteilte Genehmigung wegen der Pflicht zur Notifizierung nach § 4c Abs. 3 BDSG dem Bund und von diesem nach Art. 26 Abs. 3 der Richtlinie der Europäischen Kommission vorgelegt werden muss. Nach Art. 26 Abs. 3 i.V.m. Art. 31 Abs. 2 der Richtlinie besteht für andere Mitgliedstaaten oder die Europäische Kommission die Möglichkeit, Widerspruch gegen die erteilte Genehmigung einzulegen. Die Kommission kann geeignete Maßnahmen erlassen, die von den Mitgliedstaaten zu beachten sind. Der Widerspruchsvorbehalt sichert der Aufsichtsbehörde die Möglichkeit, die von der Europäischen Kommission gegebenenfalls beschlossenen Maßnahmen umsetzen zu können.

2.7 Welche Behörde ist für die Erteilung der Genehmigung nach § 4c Abs. 2 BDSG zuständig?

Die Genehmigung ist bei der für das datenexportierende Unternehmen auch ansonsten nach § 38 Abs. 6 BDSG zuständigen Aufsichtsbehörde für den nichtöffentlichen Bereich zu beantragen. Ausschlaggebend dafür ist der Sitz der nichtöffentlichen verantwortlichen Stelle (§ 2 Abs. 4 und § 3 Abs. 7 BSDG). Ausnahmen hat das novellierte BDSG weder grundsätzlich für Konzerne noch im Zusammenhang mit dem Genehmigungsverfahren nach § 4c Abs. 2 BDSG vorgesehen. Für Konzernmütter und ihre Töchter bedeutet dies, dass Genehmigungen von allen rechtlich eigenständigen Unternehmen für ihre jeweiligen Übermittlungen oder Arten von Übermittlungen bei der jeweils zuständigen Aufsichtsbehörde zu beantragen sind und von der jeweils zuständigen Aufsichtsbehörde auch das Genehmigungsverfahren durchzuführen ist. Den Aufsichtsbehörden ist bewusst, dass die – insbesondere für Konzerne – häufig bestehende Genehmigungszuständigkeit mehrerer Aufsichtsbehörden in unterschiedlichen Bundesländern unbefriedigend ist, insbesondere dann, wenn sich die ausreichenden Garantien aus konzernweit geltenden Unternehmensregelungen oder zu verwendenden Vertragsklauseln ergeben sollen. Die Aufsichtsbehör

den sind deshalb in diesen Fällen bestrebt, sich untereinander abzustimmen, um zu einer möglichst einheitlichen Bewertung zu gelangen. Liegt der Sitz des Konzerns im Zuständigkeitsbereich einer Aufsichtsbehörde, so sollte dieser Aufsichtsbehörde intern die Federführung obliegen. In anderen Fällen wird die Federführung wohl diejenige Aufsichtsbehörde übernehmen, bei der der erste Genehmigungsantrag gestellt wird. Eine andere rechtlich unbedenkliche Lösung ist jedenfalls derzeit nicht ersichtlich.

2.8 Bedarf es bei der Verwendung der Standardvertragsklauseln zusätzlich noch einer Genehmigung nach § 4c Abs. 2 BDSG?

Erfolgt die Datenübermittlung in Drittländer auf der Grundlage der im Einzelnen vollständig ergänzten und im Übrigen unveränderten, vertraglich vereinbarten Standardvertragsklauseln der Europäischen Kommission, bedarf die Datenübermittlung keiner zusätzlichen Genehmigung. Es besteht auch grundsätzlich keine Verpflichtung zur Vorlage der Standardvertragsklauseln bei der Aufsichtsbehörde, damit diese überprüfen kann, ob diese auch tatsächlich vollständig und unverändert vereinbart wurden. Dies schließt jedoch nicht aus, dass die Aufsichtsbehörde im Rahmen ihrer Aufsichtstätigkeit nach § 38 BDSG die Vorlage der vereinbarten Standardvertragsklauseln zu Überprüfungszwecken verlangen kann. Dieser Aufforderung muss nachgekommen werden.

3 Checkliste
Inhalt der Standardvertragsklauseln der Europäischen Kommission vom 15.06.2001 in Stichworten

Die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG der Europäischen Kommission vom 15 Juni 2001 haben kurz zusammengefasst folgenden Regelungsinhalt:

3.1 Klausel 3-Drittbegünstigstenklausel

Dem Betroffenen muss das Recht eingeräumt sein, die Verletzung folgender Regelungen aus eigenem Recht geltend machen zu können:

3.1.1 Klausel 4 b

Pflicht des Datenexporteurs zur Information des Betroffenen darüber, wenn in die Datenübermittlung sensitive Daten einbezogen sind, die auch in ein Drittland ohne angemessenes Schutzniveau übermittelt werden könnten.

3.1.2 Klausel 4 c

Pflicht des Datenexporteurs, dem Betroffenen die Regelungen zugänglich zu machen. (siehe auch Ziff. 3.1.7).

3.1.3 Klausel 4 d

Pflicht des Datenexporteurs, Anfragen der Kontrollstellen oder der Betroffenen zur Datenverarbeitung des Datenimporteurs in angemessenem Zeitraum und zumutbarem Maß zu beantworten.

3.1.4 Klausel 5 a

Pflicht und Garantie des Datenimporteurs, dass ihm die Einhaltung der Regelungen durch nationales Recht möglich ist und dass er über nachträgliche, negative Gesetzesänderung informiert, mit Berechtigung des Datenexporteurs, in einem solchen Fall die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten.

3.1.5 Klausel 5 b

Pflicht des Datenimporteurs zur Einhaltung folgender Datenschutz-Grundsätze der Anlage 2:

a) Zweckbindung

- Verarbeitung der Daten nur im Rahmen des Zwecks für den sie übermittelt wurden.
- Löschung der Daten, wenn für die Zwecke nicht mehr erforderlich.

b) Datenqualität und –verhältnismäßigkeit

- Daten müssen sachlich richtig und wenn nötig aktuell sein.

- Daten müssen im Hinblick auf die Zweckbestimmung erforderlich sein.

c) Transparenz

Betroffene müssen über die Datenverarbeitung - soweit erforderlich - informiert sein.

d) Sicherheit und Vertraulichkeit

- Organisatorische und technische Maßnahmen müssen getroffen sein.
- Mit der Datenverarbeitung befasste Personen – auch Auftragsdatenverarbeiter – haben Anweisungen des für die Datenverarbeitung Verantwortlichen zu beachten.

e) Recht auf Zugriff, Berichtigung, Löschung und Widerspruch

- Zugriff (Auskunft),
- Berichtigung,
- Löschung,
- Sperrung und
- Widerspruch gegen eine rechtmäßige Datenverarbeitung aus zwingenden berechtigten Gründen, die mit der persönlichen Situation des Betroffenen zusammenhängen.

f) Beschränkung der Weiterübermittlung

(Achtung: wenn die Datenweiterübermittlung vom Datenimporteur an einen in einem Drittland ansässigen Dritten nicht vom Zweck der Übermittlung gedeckt ist, dann ist sie – es sei denn, es liegt eine Einwilligung vor – nach § 4c Abs. 1 Satz 2 BDSG unzulässig, da sich § 4c Abs. 2 nur auf § 4c Abs. 1 Satz 1 BDSG bezieht.)

Die Datenweiterübermittlung setzt voraus,
- Einwilligung, Widerspruchsrecht nach vorheriger Aufklärung oder
- Erstreckung der Klausel auf neue Partner.

g) Besondere Datenkategorien

Für die Verarbeitung sensitiver Daten sollten zusätzliche Garantien, insbesondere angemessene Sicherheitsmaßnahmen, wie z.B. strenge Verschlüsselung für die Datenübermittlung oder Aufzeichnung über Zugriffe, vorliegen.

h) Direktmarketing

Ermöglichung eines „Opt-out“.

i) Automatisierte Einzelentscheidungen

- Grundsätzliches Verbot, wenn keine anderen Maßnahmen zur Wahrung berechtigter Interessen ergriffen werden.
- Wenn Datenübermittlung zum Zweck einer belastenden automatisierten Einzelentscheidung erfolgt, Recht des Betroffenen, die Gründe dieser Entscheidung zu erfahren.

3.1.6 Klausel 5c

- Pflicht des Datenimporteurs, Anfragen des Datenexporteurs oder von Betroffenen unverzüglich und genau zu bearbeiten.
- Pflicht des Datenimporteurs zur Kooperation mit der zuständigen Kontrollstelle bei dortigen Anfragen.
- Pflicht des Datenimporteurs, Feststellungen der Kontrollstelle zu respektieren.

3.1.7 Klausel 5e

- Pflicht des Datenimporteurs, dem Betroffenen die Regelungen zugänglich zu machen.
- Pflicht des Datenimporteurs, dem Betroffenen die Stelle zu benennen, die für Beschwerden zuständig ist.

3.1.8 Klausel 6

- Recht des Betroffenen, Schadenersatz gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend zu machen.
- Befreiung des Datenexporteurs und Datenimporteurs von der Haftung nur bei Beweis, dass keiner von ihnen für die Verstöße verantwortlich ist.
- Vereinbarung gesamtschuldnerischer Haftung von Datenexporteur und Datenimporteur.

3.1.9 Klausel 7

Schlichtungsverfahren und Zuständigkeit.

3.1.10 Klausel 9

Weitergeltung der Regelungen für die Verarbeitung der zuvor übermittelten Daten, d.h. Kündigung/Aufhebung ist nur für die Zukunft möglich.

3.1.11 Klausel 11

Pflicht, die Regelungen nicht zu ändern (kann bei Unternehmensregelungen in die Genehmigung aufgenommen werden).

3.2 Pflichten, die zusätzlich einzuhalten sind:

3.2.1 Klausel 4a

Pflicht und Garantie des Datenexporteurs, dass Datenverarbeitung einschließlich Datenübermittlung nach nationalem Recht rechtmäßig ist.

3.2.2 Klausel 5d

Pflicht des Datenimporteurs, Datenverarbeitungs-Einrichtungen zur Prüfung durch den Datenexporteur oder von Datenexporteur (mit Kontrollstelle) ausgewählten Prüfgremien zur Verfügung zu stellen.

3.2.3 Klausel 8

Pflicht, Regelungen bei der Kontrollstelle zu hinterlegen, wenn von ihr verlangt (entfällt bei Unternehmensregelungen, da sie mit dem Antrag vorzulegen sind).

3.2.4 Klausel 10

Für Regelungen gilt Recht des Staates, in dem der Datenexporteur ansässig ist.

C Einzug privatärztlicher Forderungen durch Rechtsanwälte und Inkassounternehmen

Bei der Abrechnung und der Eintreibung privatärztlicher Honorarforderungen durch Dritte unterscheiden sich die datenschutzrechtlichen Anforderungen an die Zulässigkeit der Datenübermittlung erheblich voneinander. Wie bereits in den Hinweisen des Innenministeriums zum Datenschutz für private Unternehmen und Organisationen Nr. 36 vom 13. Januar 1998 unter Ziffer 2 und Nr. 38 vom 18. Januar 2000 unter Buchstabe D ausgeführt, muss der Patient in die Weitergabe seiner Gesundheitsdaten einwilligen, wenn der Arzt seine erbrachten Leistungen über einen Dritten, beispielsweise über eine Verrechnungsstelle, abrechnen lassen will.

Anders sieht es jedoch aus, wenn der Arzt mit dem Patienten selbst abrechnet, der Patient aber säumig bleibt und der Arzt die offene Forderung durch einen Rechtsanwalt oder ein Inkassobüro eintreiben lassen möchte. Liegt eine Einwilligung des Patienten zur Weitergabe seiner Daten an einen Rechtsanwalt oder ein Inkassobüro nicht vor, wovon im Regelfall auszugehen ist, so darf der Arzt seine offene Forderung durch einen Rechtsanwalt oder ein Inkassobüro dann eintreiben oder einklagen lassen, wenn er vor der Weitergabe der Daten den Patienten gemahnt und auf die Folgen der weiteren Zahlungsverweigerung hingewiesen hat. Bei der Einschaltung eines Inkassounternehmens oder der Übergabe an einen Rechtsanwalt zum Zwecke des Forderungseinzugs handelt es sich im Regelfall um eine Funktionsübertragung und nicht um eine Datenverarbeitung im Auftrag. Daher liegt datenschutzrechtlich eine Datenübermittlung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG vor. Da dem Patienten durch die vorherige Information ermöglicht wurde, die Datenübermittlung durch Begleichung der Forderung abzuwenden, besteht hier kein Grund zur Annahme, dass das schutzwürdige Interesse des betroffenen Patienten am Ausschluss der Übermittlung seiner Daten das berechtigte Interesse des Arztes an der Übermittlung der zur Rechtsverfolgung erforderlichen Behandlungsdaten überwiegt. Der Arzt verletzt hierbei auch nicht seine Schweigepflicht nach § 203 StGB, denn die Wahrung seiner eigenen Inte

ressen an der Eintreibung seiner Honorarforderung rechtfertigt die Offenbarung der ansonsten geschützten Patientendaten.