BIVA

Bundesinteressenvertretung für alte
und pflegebetroffene Menschen e.V.

Überwachungskameras in Heimen

Welche Überwachungsmaßnahmen
sind zulässig, welche nicht?

BIVA

Impressum

Herausgeberin:

Bundesinteressenvertretung für alte und pflegebetroffene Menschen (**BIVA**) e.V.
Siebenmorgenweg 6-8
53229 Bonn

Tel.: 0228– 9090480
Fax: 0228– 90904822
E-Mail: info@biva.de
Internet: www.biva.de

Verantwortlich i.S.d.P.:
Der Vorstand der BIVA e.V. vertreten durch den Vorstandsvorsitzenden
Dr. Manfred Stegger

Text: Guido Steinke, Rechtsanwalt
Redaktion: Katrin Markus
Ersterscheinungsdatum: Juli 2007

2. Auflage April 2016
Aktualisierung: Ulrike Kempchen

Liebe Leserin, lieber Leser,

in Kaufhäusern, auf Bahnhöfen, an Tankstellen, Kiosken, Hauseingängen und in Verkehrsmitteln, überall sind heutzutage Videokameras zu finden.

Mit dem Anstieg der Zahl der von Demenz betroffenen Bewohnerinnen und Bewohnern halten auch in Wohn- und Betreuungseinrichtungen diese „Sicherungsvorkehrungen“ zunehmend Einzug. Sie sollen helfen, die demenziell Erkrankten besser zu schützen, damit z.B. bei Stürzen sofort jemand zu Hilfe eilen kann.

Was von den einen als Gewinn an Sicherheit geschätzt wird, bewerten andere als den ersten Schritt zur totalen Überwachung. Wie die Rechtslage ist und was man tun kann, wenn man sich unrechtmäßig überwacht fühlt, dazu soll dieser kleine Ratgeber einen Überblick geben.

Wir würden uns freuen, wenn wir Ihnen damit ein wenig Sicherheit geben können im Umgang mit diesen neuen Technologien!

Dr. Manfred Stegger, Vorstandsvorsitzender BIVA e.V.

Die **BIVA** setzt sich seit 1974 bundesweit für die Rechte und Interessen von Menschen ein, die Hilfe oder Pflege benötigen und daher in betreuten Wohnformen leben. Sie ist damit die einzige bundesweite Interessenvertretung für Bewohnerinnen und Bewohner von Pflegeheimen und für von Pflege Betroffene. Das schließt sowohl alle Menschen ein, die im Alter und bei Behinderung selbst Wohn- und Pflegeangebote in Anspruch nehmen, als auch deren Angehörige, die sich in der schwierigen Situation von Pflege und Betreuung befinden.

Die **BIVA** leistet bundesweit Hilfe und berät in persönlichen Angelegenheiten bei sämtlichen Fragen zum

- Leben im Heim sowie in stationär und ambulant betreuten Wohnformen,

insbesondere bei

- Fragen zum Heimvertrag, Mietvertrag, Betreuungsvertrag
- Fragen zu Entgelterhöhungen,
- Ärger mit der Heimleitung,
- Art und Umfang der Mitwirkungsrechte von Heimbeirat, Heimfürsprecher,
- Fragen zu den Aufgaben der Heimaufsicht.

Inhaltsverzeichnis

1. Einleitung

Im öffentlichen Bereich gehören sie fast schon zum Standard, in den stationären Einrichtungen halten sie mehr und mehr Einzug: Überwachungskameras.

Die Technik macht so rasante Fortschritte, dass einem die kleinen „Sicherheitshelfer“ fast gar nicht mehr auffallen. Wer erkennt schon, dass er an jedem Geldautomaten gefilmt wird?

Zur Gefahrenabwehr mögen Überwachungsapparate ihre Berechtigung haben. In Einrichtungen können sie z.B. das Personal unterstützen bei der Betreuung weglaufgefährdeter Menschen. Dort gibt es aber auch private, intime Bereiche, in denen der Einzelne allein und unbeobachtet bleiben muss. Wie kann man da den Einsatz von Überwachungskameras gestalten? Ist er überhaupt zulässig? Diese und andere Fragen sollen auf den folgenden Seiten geklärt werden.

2. Was ist Videoüberwachung?

Videoüberwachung fällt in den Bereich des Datenschutzes. Das BDSG definiert die Videoüberwachung als „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen“ (§ 6b Abs.1 BDSG). Damit stellt sich die Frage des Datenschutzes nicht erst dann, wenn Bilder aufgezeichnet oder gespeichert werden, sondern schon, sobald durch technische Vorrichtungen die tatsächliche **Möglichkeit der Beobachtung durch Menschen** gegeben ist.

Die Überwachung setzt also bereits mit der Installation von Kameras ein, auch wenn die Geräte nur im Bedarfs- oder Alarmfall aufzeichnen oder wenn sie zur bloßen Beobachtung genutzt werden, so wie dies in der Regel in den Einrichtungen der Fall ist!

3. Warum sollte mich eine Überwachungskamera stören?

Viele Menschen schätzen den vermeintlichen Sicherheitsgewinn durch Videoüberwachung höher ein als die eigenen Persönlichkeitsrechte. „Ich habe nichts zu verbergen“, denken einige, und wenn man manche Sendungen im Fernsehen sieht, bekommt man den Eindruck, dass die Schamgrenze der Menschen sehr niedrig ist - sofern sie überhaupt noch existiert.

Wer möchte aber schon gerne dabei gefilmt werden, wenn er in der Nase bohrt oder einen Streit mit seiner Begleiterin oder seinem Begleiter ausficht. Videokameras beobachten uns an vielen Stellen. Manche denken über das Überwachungsauge gar nicht nach, andere aber passen ihr Verhalten der Überwachungssituation an.

Gleiches gilt für Wohn- und Betreuungseinrichtungen. Sind die Verwandten zu Besuch, kann es schon einmal zu Auseinandersetzungen kommen. Auch kommen in Einrichtungen romantische Momente vor, die unüberwacht zu bleiben haben. Auch die Bereiche, in denen Stürze am ehesten auftreten – in Bad und WC – sind zugleich diejenigen mit dem größten Schampotential.

Es ist wissenschaftlich erwiesen, dass Menschen sich nicht mehr frei und selbstbestimmt verhalten, wenn sie meinen, von einer Kamera beobachtet zu werden, selbst wenn dies eine Attrappe ist.

Dort, wo Überwachungstechnik einen effektiven Nutzen bringt, mag sie gerechtfertigt sein. Doch darf sie im Interesse der Privatsphäre der Menschen nicht unbedacht eingesetzt werden. Damit dies sichergestellt wird, müssen die für die Videoüberwachung geltenden Datenschutzvorschriften beachtet werden.

4. Welche Grundsätze gibt es für die Zulässigkeit von Videoüberwachungen?

Videoüberwachung ist prinzipiell überall möglich, aber nur unter ganz bestimmten Voraussetzungen zulässig. Immer muss eine Abwägung zwischen dem Schutzzweck auf der einen Seite und dem aus der Menschenwürde abgeleiteten Recht auf „informationelle Selbstbestimmung“ auf der anderen Seite erfolgen.

Dieses Recht ist ein Oberbegriff dessen, was auch das Recht am eigenen Bild erfasst. Das Recht auf informationelle Selbstbestimmung wird definiert als „die Befugnis des Einzelnen, selbst zu bestimmen, wer was wann und bei welcher Gelegenheit über einen weiß“. Im Computerzeitalter umfasst dieses Recht den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten. Der Betroffene soll grundsätzlich selbst über die Preisgabe und Nutzung seiner persönlichen Daten bestimmen. **(„Meine Daten gehören mir!“)**

5. Unter welchen Voraussetzungen ist eine Überwachung per Videokamera in Einrichtungen zulässig?

Das BDSG bestimmt in § 6b für öffentlich zugängliche Räume:

> Videoüberwachung ist nur zulässig, soweit sie
> 1. zur Aufgabenerfüllung öffentlicher Stellen,
> 2. zur Wahrnehmung des Hausrechts oder
> 3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke
>
> erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Öffentlich zugängliche Räume sind Bereiche innerhalb oder außerhalb von Gebäuden, die frei oder nach allgemein erfüllbaren Voraussetzungen (z.B. mit Eintrittskarte) betreten werden können. Hierzu gehören Bahnhofshallen, Bahnsteige, Tankstellen, Publikumsbereiche von Banken, Cafés, Verkaufsräume eines Warenhauses, Hotelfoyers sowie Museen und Kinos nach Lösen einer Eintrittskarte.

Öffentlich zugängliche Gemeinschaftsflächen von großen Wohnanlagen wie Eingänge oder Wege zwischen Gebäuden können solche Bereiche sein, wenn die Berechtigten sie erkennbar der Allgemeinheit zugänglich machen wollen. In Heimen könnte dies z.B. für den Eingangsbereich oder den Innenhof, den Garten etc. zutreffen.

Im Gegensatz dazu stehen Bereiche, die nur ganz bestimmten Personenkreisen zugänglich sind. Diese sind entweder als solche gekennzeichnet (z.B. umzäuntes oder durch Hinweisschilder kenntlich gemachtes Firmen- oder Werksgelände) oder es ist aufgrund allgemein anerkannter Gewohnheiten bekannt, dass sie nicht allgemein zugänglich sind (z. B. privater, nicht eingezäunter Vorgarten).

Bei den Eingangsbereichen von reinen Wohngebäuden wird man in der Regel nicht davon ausgehen können, dass es sich um öffentlich zugängliche Räume handelt, weil lediglich Bewohnerinnen und Bewohner sowie Besucher Zutrittsrechte haben. Das gilt auch bei nicht verschlossenen Gebäudeeingangstüren.

Der private Bereich einer Einrichtung, der erkennbar nur bestimmten Personen vorbehalten ist wie z.B. der Wohnbereich einer Wohngruppe einer Einrichtung, Flure, Treppenhäuser etc. ist daher nicht „öffentlich zugänglich“ i.S.d. § 6b BDSG, ebenso wenig wie der private Wohnraum der Bewohnerinnen und Bewohner.

Das heißt jedoch nicht, dass in öffentlich zugänglichen Räumen eine Videoüberwachung uneingeschränkt zulässig wäre. Das Recht des Menschen auf informationelle Selbstbestimmung gilt überall, nicht nur im privaten Bereich. Videoüberwachungen können daher Verstöße gegen allgemeine Grundsätze des Datenschutzes bedeuten und zivilrechtliche Abwehransprüche nach sich ziehen.

Für die nicht öffentlich zugängliche Räume (Eingangsbereiche, Treppen, Flure, Wohnbereiche, Gemeinschaftsräume) kommt es ebenfalls auf die Zweck-Mittel-Relation und die Abwägung der Interessen der Beteiligten (Überwacher und Betroffene) an. Dies ergibt sich aus den allgemeinen Grundsätzen zum Datenschutz und der Rechtsprechung des Bundesverfassungsgerichts.

Im Wesentlichen sind drei Kriterien zu prüfen:

a) Zweck

Die Videoüberwachung muss der Wahrung des Hausrechts oder eines anderen berechtigten Interesses für konkret festgelegte Zwecke dienen, s. dazu § 28 BDSG. Ein berechtigtes Interesse kann ideeller, wirtschaftlicher und rechtlicher Natur sein. Der Schutz vor Dieben kann ebenso eine Videoüberwachung rechtfertigen wie das Vermeiden von Vandalismus und das Verhindern sonstiger Straftaten. Das Interesse kann auch darin bestehen, die vorgenannten Verstöße vor Gericht nachweisen zu können. Der konkrete Zweck der Überwachung muss vorher schriftlich festgelegt worden sein.

Für stationäre Einrichtungen bedeutet das: Der Schutz der z.B. dementiell erkrankten Bewohnerinnen und Bewohner kann ein rechtlich zulässiger Zweck sein. Die Betreiber müssen diesen Zweck schriftlich darlegen. Hierbei sind Beirat und Aufsichtsbehörde einzubeziehen (vgl. §§ 10 Abs. 1, 11 und 15 HeimG, § 30 Nr. 2 HeimmwV, s. auch unten Ziff. 6.).

b) Erforderlichkeit

Erforderlich ist die Videoüberwachung nur, wenn das festgelegte Ziel nur mit einer Überwachung erreicht werden kann und es dafür kein weniger einschneidendes Mittel gibt. Im Einzelfall müssen deshalb weniger belastende Möglichkeiten auf ihre Tauglichkeit hin überprüft werden, wie regelmäßige bzw. häufige Kontrollgänge durch das Personal. In diesem Zusammenhang ist auch zu prüfen, ob eine flächendeckende Einführung der Überwachungstechnik erforderlich ist oder ob ein Einsatz an bestimmten Schwerpunkten zu bestimmten Zeiten ausreicht. Bei der Prüfung des Merkmals der Erforderlichkeit kommt es auf wirtschaftliche Erwägungen nicht an.

c) Interessenabwägung

Eine erforderliche Videoüberwachung ist dennoch unzulässig, wenn die Betroffenen ein schutzwürdiges Interesse haben, das höher zu bewerten ist, als das Erreichen des mit der Beobachtung verfolgten Zwecks. Ein schutzwürdiges Interesse der Betroffenen ist in der Regel aufgrund des grundrechtlich garantierten Persönlichkeitsrechts gegeben. Dieses umfasst sowohl das Recht auf Schutz der Privat- und Intimsphäre als auch das Recht am eigenen Bild, das durch die Videoüberwachung berührt wird.

Die schutzwürdigen Interessen überwiegen nahezu immer, wenn die Intimsphäre verletzt wird. Die Überwachung von Toiletten oder Umkleidekabinen ist daher nicht erlaubt, ebenso nicht die Überwachung von Wohnräumen. Nur in besonderen Ausnahmefällen, z.B. bei Gefahr von Leib und Leben, kann eine eingeschränkte Überwachung zulässig sein (z.B. mit Filtern, auf denen man keine Details erkennt, sondern nur, ob jemand gestürzt ist). Vorher muss aber eine ausführliche Interessenabwägung erfolgen (s.u.). Wenn es weniger einschneidende Mittel gibt, wie z.B. Notrufsysteme, Sensormatten etc., ist eine Videoüberwachung unzulässig.

Die schutzwürdigen Interessen überwiegen meist auch dort, wo die Entfaltung der Persönlichkeit von wesentlicher Bedeutung ist, wie z.B. in Caféterien, Gemeinschaftsräumen, in denen Leute kommunizieren, essen, trinken oder sich erholen. Sie überwiegen i.d.R. nicht, wenn derartige Aktivitäten nicht im Vordergrund stehen wie in Eingangsbereichen oder auf Zufahrten.

Bei der Interessenabwägung ist weiter zu berücksichtigen, ob es sich um eine dauerhafte und flächendeckende Videoüberwachung handelt, der sich Betroffene nicht entziehen können. Diese greift stärker in das allgemeine Persönlichkeitsrecht ein als eine nur gelegentliche oder punktuelle Überwachungen. Die Konsequenz hieraus kann in überwachten Bereichen die Einrichtung nicht überwachter Zonen sein.

Man muss in Wohn- und Betreuungseinrichtungen daher genauestens prüfen, wo und wann die Überwachung stattfinden soll und wer davon betroffen sein könnte (z.B. Bewohnerinnen und Bewohner, Besucher, Personal).

Es bietet sich an, für die Interessenabwägung eine Matrix zu erstellen:

Schutzinteresse der betroffenen Personen	Wertung:	sehr hoch hoch mittel gering sehr gering	***** **** *** ** *
Betroffener Raum	Bewohner	Besucher	Personal
Privaträume			
Bad, WC			
Flure			
Eingangsbereich			
Küche			
Gemeinschaftsräume			
Garten			
Zugänge/Zufahrten			
…			

Vorteile der Überwachung	Wertung:	sehr hoch hoch mittel gering sehr gering	***** **** *** ** *
Betroffener Raum	Bewohner	Besucher	Personal
Privaträume			
Bad, WC			
Flure			
Eingangsbereich			
Küche			
Gemeinschaftsräume			
Garten			
Zugänge/Zufahrten			
…			

Die Rechtsprechung und die Datenschutzexperten haben sich bislang vor allem mit den folgenden Fällen beschäftigt:

- **Videoüberwachung am Arbeitsplatz**

  Eine Videoüberwachung von Beschäftigten an ihrem Arbeitsplatz kann nur ausnahmsweise durch „überwiegende schutzwürdige Interessen“ des Unternehmens gerechtfertigt sein. Bei der dabei stets vorzunehmenden Abwägung der Interessen im Einzelfall kommt es entscheidend auf den Grund für die Überwachung an. Wird die Videoüberwachung allein zu dem Zweck eingesetzt, die Sorgfältigkeit oder Effizienz der Arbeitstätigkeit der Beschäftigten zu überprüfen, so ist dies unzulässig.

  Es liegt auf der Hand, dass die Überwachung bestimmter betrieblicher Bereiche aus Sicherheitsgründen geboten sein kann, etwa bei Tresorräumen oder technischen Anlagen. Dort ist daher die offene, also für die Beschäftigten erkennbare Überwachung in der Regel zulässig. Selbstverständlich sind besonders sensible Bereiche wie Umkleidekabinen oder der Sanitärbereich von der Beobachtung auszunehmen.

- **Videoüberwachung in einer Wohnanlage**

  Bewertet wurde vom Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein ein Fall, bei dem die Videoüberwachung nicht auf die einzelnen Hauseingänge der Wohnanlage ausgerichtet war, sondern auf die Hauptzufahrt. Da eine dauernde Beobachtung von Haus- oder Wohnungseingängen nicht vorlag und außerdem die Hauptzufahrt mit einem entsprechenden Hinweisschild "Dieses Gelände wird videoüberwacht. Wohnungsbaugesellschaft XYZ" versehen war, sahen die

Landesdatenschützer in der Videoüberwachung keinen datenschutzrechtlichen Verstoß.

Anders ist die Rechtslage, wenn Haus- oder Wohnungseingänge dauerhaft beobachtet werden. In diesem Fall liegt nach der Rechtsprechung ein unzulässiger Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen vor. Entscheidend ist, dass die Mieter Ihre Wohnungen jederzeit unbeobachtet erreichen können.

Aus diesen von der Rechtsprechung und den Datenschutzexperten entwickelten Grundsätzen für die sonstigen Lebensbereiche können **Grundsätze für den Einsatz von Überwachungstechnik in Wohn- und Betreuungseinrichtungen** abgeleitet werden.

6. Welche Maßnahmen muss der Betreiber vor Einrichtung einer Videoüberwachung ergreifen?

Wenn ein Betreiber sich bereits mit den genannten Punkten **Zweckbestimmung, Erforderlichkeit und Interessenabwägung** auseinandergesetzt hat und zu dem Schluss gekommen ist, eine Videoüberwachung einzurichten, sollte er die folgenden, weiteren Schritte beachten:

Unterrichtung der Beteiligten und Betroffenen
Vor der Installation einer Überwachungsanlage sollte der Betreiber die Bewohnerinnen und Bewohner, d.h. auch deren Betreuer, Bevollmächtigte und Interessenvertreter – also den Beirat – schriftlich über das Vorhaben informieren, damit gegebenenfalls noch Einwände behandelt und berücksichtigt werden können.

Eine schriftlich erteilte Zustimmung ist wünschenswert, aber nicht alleine ausschlaggebend. Die Überwachungsmaßnahme muss immer der o.g. Interessenabwägung unterzogen werden. Dabei spielt eine Zustimmung natürlich eine entscheidende, aber nicht die alleinige Rolle. Es könnten auch noch andere Personen betroffen sein oder die Zustimmung auf falschen Informationen oder Vorstellungen fußen. Außerdem ist eine Zustimmung jederzeit frei widerrufbar.

Dokumentationspflicht, Vorabkontrolle und betriebliche Datenschutzbeauftragte

Vor Beginn der Videoüberwachung ist der Zweck der Überwachung schriftlich festzulegen. Dies muss spätestens im Rahmen der Vorabkontrolle (s. § 4d Abs. 5 BDSG) durch die verantwortliche Stelle erfolgen. Die Vorabkontrolle ist regelmäßig erforderlich, weil die Videoüberwachung mit besonderen Gefahren für das Persönlichkeitsrecht der Betroffenen verbunden ist. Sie ist in größeren Betrieben von einer oder einem **betrieblichen Datenschutzbeauftragten** durchzuführen und zu dokumentieren.

Wenn mehr als 9 Personen in einer Einrichtung oder bei einem Träger ständig mit der Datenverarbeitung betraut sind, hat auch diese einen Datenschutzbeauftragten zu benennen, s. § 4f. BDSG. In den meisten Einrichtungen dürfte dies jedoch nicht der Fall sein, eher bei bundesweit agierenden Trägern.

Hinweispflicht

Die Videoüberwachung und der Ansprechpartner sind gemäß § 6b Abs. 2 Bundesdatenschutzgesetz (BDSG) durch geeignete Maßnahmen erkennbar zu machen. Der Hinweis muss deutlich erkennbar und vor Betreten des überwachten Bereiches problemlos wahrnehmbar sein, damit die freie Entscheidung für oder gegen das Betreten möglich ist. Ob etwa ein Schild mit dem Text: „Achtung, hier Videoüberwachung“ oder ein eindeutiges Kamerasymbol gewählt wird, bleibt freigestellt.

Ein Hinweis auf die verantwortliche Stelle ist bis auf wenige Ausnahmefälle immer erforderlich. In jedem Fall müssen die Betroffenen zweifelsfrei erkennen können, an wen sie sich in Sachen Videoüberwachung wenden können. Ein ausdrücklicher Hinweis auf die verantwortliche Stelle kann deshalb in einem Heim oder einer Einrichtung entbehrlich sein, wenn – wie in vielen Wohn- und Betreuungseinrichtungen – im Eingangsbereich die Ansprechpartner genannt werden.

Das Gesetz verlangt keinen Hinweis darauf, ob die Aufnahmen gespeichert werden. Gleichwohl wäre ein entsprechender Hinweis wünschenswert.

Datensparsamkeit, Anonymisierung und Pseudonymisierung

Als neues Instrument findet sich in modernen Datenschutzgesetzen der Grundsatz der Datensparsamkeit. Auch auf Bundesebene soll dieser über § 3a BDSG für sämtliche privaten Stellen verbindlich sein. Er verpflichtet die Betreiber von Videosystemen bei deren Gestaltung und Auswahl darauf zu achten, dass beim Einsatz so wenige personenbezogene Daten wie möglich entstehen. Insbesondere ist von der Möglichkeit der Anonymisierung und Pseudonymisierung (§ 3 Abs. 6, 6a BDSG) Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

So ist der Dauerbeobachtung ein Verfahren vorzuziehen, das erst dann Bilder erfasst, wenn es z.B. durch eine Lichtschranke ausgelöst wird. Systeme mit reinen Übersichtsaufnahmen, bei denen es für die personenbezogene Erfassung eines selbst ausgelösten Zoom- und Aufzeichnungsvorgangs bedarf, haben Vorrang vor Systemen, die mit Dauervergrößerungen arbeiten. Monitorsysteme, die bzgl. nicht sicherheitsrelevanten und von Personen frequentierten Bereichen eine Verschleierung vorsehen, sind datenschutzgerechter als solche, die rundum scharfe Bilder liefern. Es sind viele interessante technische Entwicklungen denkbar, die die Risiken der Videoüberwachung für das Per-

sönlichkeitsrecht eingrenzen.
Das **Verwaltungsgericht in Minden** regte in einem Verfahren, bei denen ein Betreiber einer Einrichtung und die zuständige Aufsichtsbehörde um den Einsatz von Videokameras stritten (Az. 6 K 552/06, Vergleich vom 31.10.2006, s. Anhang) den folgenden Vergleich an:

1. Die Videoüberwachung ist zum Schutze der Bewohner zulässig, aber mit den folgenden Einschränkungen:
2. Sie erstreckt sich nur auf weniger sensible Bereiche wie Eingänge, Flure, Treppenhäuser (und nicht z.B. auf den Aufenthaltsraum).
3. Die Aufnahmen werden nicht länger als 72 Stunden gespeichert.

Merke: Aus der Rechtsprechung des Bundesverfassungsgerichts ergibt sich: Nicht die Betroffenen bzw. die Datenschützer müssen die Unzulässigkeit einer Videoüberwachungsmaßnahme nachweisen, sondern die Betreiber der Anlagen haben die Beweislast für die Notwendigkeit jeden Eingriffs in die Rechte der Menschen.

7. Welche Rechte habe ich als Betroffene oder Betroffener?

Auskunftsrecht

Nach § 34 Abs. 1 BDSG kann ein Betroffener über die zu seiner Person gespeicherten Daten, über die Empfänger und den Zweck Auskunft verlangen. Dies gilt auch für die Datenspeicherung von Videobildern. Aus praktischen Gründen kommt bei Videoaufzeichnung vorrangig die Auskunftserteilung durch Vorführen der jeweiligen Sequenz in Betracht.

Widerspruch

Das Recht, der Erhebung, Speicherung und Verwertung von Daten – also auch Bildern – zu widersprechen, ergänzt das Kriterium der Zustimmung. Selbst wenn man einmal der Videoüberwachung zugestimmt haben sollte, kann man dies jederzeit frei widerrufen. Ausdrücklich geregelt ist das Widerspruchsrecht in § 20 BDSG.

Berichtigung, Löschung und Sperrung

Ein Widerspruch macht nur dann Sinn, wenn die datenerhebende Stelle auch gezwungen werden kann, die Daten zu korrigieren oder sogar zu löschen bzw. zu sperren (falls z.B. gesetzliche Aufbewahrungspflichten dem nicht entgegenstehen). § 35 BDSG enthält diese Betroffenenrechte für den Fall der Datenerhebung durch nicht-öffentliche Stellen, also z.B. durch die Heimbetreiber. Bei kommunalen Einrichtungen gilt § 20 BDSG mit den entsprechenden Rechten und Pflichten.

Allerdings können diese Rechte eingeschränkt sein, wenn besondere Umstände vorliegen und eine Interessenabwägung ergibt, dass andere Rechtsgüter Vorrang haben.

Beispiel: Auf den Videoaufnahmen ist ein Diebstahl zu erkennen. Die entsprechenden Aufzeichnungen dürfen der Polizei zu Ermittlungszwecken übergeben werden. Sollte auch ein Bewohner auf den Bildern zu sehen sein, muss er sich mit der Löschung gedulden, bis die Ermittlungen abgeschlossen sind und das Material nicht mehr benötigt wird.

8. Wie lange dürfen die Aufzeichnungen gespeichert werden?

Wenn aufgezeichnet wird, ist das Videomaterial nach der Verwirklichung des Aufzeichnungszwecks ohne schuldhaftes Verzögern (unverzüglich) zu löschen, s. § 6b Absatz 5 und § 35 BDSG. Am Sinnvollsten erscheint es, das Videomaterial automatisiert, etwa durch Selbstüberschreiben zurückliegender Aufnahmen, unkenntlich zu machen.

Videoaufzeichnungen zum Beweis von Diebstählen werden nicht mehr benötigt, wenn kein Diebstahl festgestellt wurde. Die zur allgemeinen Kriminalitätsbekämpfung gefertigten Aufzeichnungen eines Tages sollten möglichst am nächsten Tag überprüft und überspielt werden, spätestens aber nach Ablauf von zwei weiteren Arbeitstagen.

Sofern in Einrichtungen überhaupt Bilder (und Töne) aufgezeichnet werden sollten, sind diese sofort zu löschen, wenn keine Gefahr mehr besteht. Siehe dazu auch den Vergleich vor dem Verwaltungsgericht Minden, oben Ziff. 6.

Beispiel: Es werden Videokameras in den Fluren und im Eingangsbereich installiert, zum Schutze von sog. „Wegläufern“. Nach gründlicher Interessenabwägung – vor allem auch mit den Interessen der übrigen Bewohnerinnen und Bewohnern und der Besucher – kommt der Einrichtungsträger zu dem Schluss, die Aufzeichnungen max. 24h zu speichern. Bis dahin sollte dem Pflegepersonal aufgefallen sein, ob sich ein schutzbedürftiger Mensch unbemerkt entfernt.

9. Was gilt bei anderen Formen der Überwachung?

Tonaufzeichnungen

Für solche Überwachungsmaßnahmen ist im Strafgesetzbuch (StGB) mit § 201 (Ver-

letzung der Vertraulichkeit des Wortes) eine Regelung enthalten, die es sogar unter Strafandrohung verbietet, das nicht öffentlich gesprochene Wort aufzuzeichnen oder abzuhören!

Werden Bild und Ton gemeinsam aufgenommen, erhält die technische Überwachung eine besondere Qualität; es entsteht eine größere sog. „Eingriffstiefe“. Für den Bereich des nicht öffentlich gesprochenen Wortes z.B. in einer Privatwohnung gibt es diverse Regelungen (vgl. z.B. § 201 StGB, Art. 13 Abs. 3-6 GG).

In der Praxis kommen Tonaufzeichnungen bisher eher selten vor. Mit Fortschreiten der Technik wird sich dies zweifellos ändern. Des Nachts könnte in Einrichtungen zum Schutz der Bewohnerinnen und Bewohner neben der Kamera zusätzlich ein Mikrofon installiert werden. Auch verfügen immer mehr technische Hilfsmittel über eine Sprachsteuerung, d.h. die Möglichkeit, Stimmen und Geräusche aufzuzeichnen.

10. Was kann ich rechtlich gegen eine Videoüberwachung unternehmen?

Neben den im BDSG genannten Ansprüchen auf Vorabinformation, Benachrichtigung, Auskunft und Löschung, die oben näher beschrieben wurden, kann es noch Ansprüche auf Schadenersatz (§ 7 BDSG, § 823 BGB) und Unterlassung (§ 1004 BGB) geben.

Da es sich beim Recht am eigenen Bild bzw. dem allgemeinen Persönlichkeitsrecht um ein nach § 823 BGB geschütztes subjektives Recht handelt, können widerrechtliche und zumindest fahrlässige Verletzungen einen Schadensersatzanspruch auslösen. Bei schwerwiegenden Verletzungen kann auch der Ersatz eines immateriellen Schadens, ein sog. Schmerzensgeld nach § 847 BGB, in Frage kommen. Voraussetzung ist jedoch immer ein vorwerfbarer Verstoß, der im Einzelfall nachzuweisen ist.

Entsprechend § 1004 BGB steht einem Geschädigten bzw. potenziell Beeinträchtigten ein Beseitigungs- und Unterlassungsanspruch zu. Der Unterlassungsanspruch geht dahin, die weitere Erstellung von Videobildern zu beenden. Der Beseitigungsanspruch zielt auf die Vernichtung gespeicherter Bilder.

11. An wen kann ich mich mit meinen Fragen zur Videoüberwachung wenden?

Primäre Ansprechpartner bei Fragen zum Datenschutz sind (laut den Datenschutzgesetzen des Bundes und der Länder) die **Datenschutzbeauftragten**.

Wenn es in der Einrichtung einen Datenschutzbeauftragten gibt, sollte dieser ebenfalls einbezogen werden, genauso wie der Beirat, der für alle Belange der Bewohnerinnen und Bewohner die richtige Kontaktstelle ist.

Es gibt eine grobe Aufgabenverteilung unter den verschiedenen Datenschutzbeauftragten:

Man sollte sich an diejenige Datenschutzeinrichtung wenden, die auch die Kontrolle über die datenverarbeitende Stelle – in diesem Fall die Einrichtung oder den Einrichtungsträger – wahrnimmt:

- Hat das Haus einen **öffentlichen Träger**, sind der Datenschutzbeauftragte des Bundes oder die Datenschutzbeauftragten der Länder zuständig.
- Ist der **Träger privatrechtlich organisiert**, sind meist die Datenschutzbeauftragten der Länder zuständig.
- Für die Kontrolle der Verarbeitung personenbezogener Daten durch **kirchliche Einrichtungen** sind die Datenschutzbeauftragten der evangelischen und der katholischen Kirche zuständig.

TIPP: Weiter hilft zunächst einmal der Datenschutzbeauftragte „vor Ort“, d.h. der/die Landesdatenschutzbeauftragte. Er/sie hilft auch, den richtigen Ansprechpartner zu finden.

Die einzelnen **Datenschutzbehörden** finden Sie im Internet unter www.datenschutz.de und im Anhang.

Man kann sich natürlich auch jederzeit an die **BIVA** wenden!

Anhang

I. Gesetze (in Auszügen)

Bundesdatenschutzgesetz (BDSG)

§ 3 Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) [1]Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. [2]Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) [1]Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. [2]Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
a) die Daten an den Dritten weitergegeben werden oder
b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(7) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) [1]Empfänger ist jede Person oder Stelle, die Daten erhält. [2]Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. [3]Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

(9) - (10) …

§ 3a Datenvermeidung und Datensparsamkeit

[1]Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. [2]Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 4d Meldepflicht

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nichtöffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei höchstens neun Personen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient.

(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zweck der Übermittlung oder
2. zum Zweck der anonymisierten Übermittlung

gespeichert werden.

(5) [1]Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). [2]Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder
2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

(6) [1]Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. [2]Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. [3]Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu wenden.

§ 6b Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

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

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) [1]Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. [2]Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 7 Schadensersatz

[1]Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. [2]Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

§ 20 Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht

(1) [1]Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. [2]Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.

(2) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegen den Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit
(…)

§ 21 Anrufung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

[1]Jedermann kann sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. [2]Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten

durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

§ 28 Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke

(1) [1]Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

[2]Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Für einen anderen Zweck dürfen sie nur unter den Voraussetzungen des Absatzes 1 Satz 1 Nr. 2 und 3 übermittelt oder genutzt werden.

(3) [1]Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig:

1. soweit es zur Wahrung berechtigter Interessen eines Dritten oder
2. zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist, oder
3. für Zwecke der Werbung, der Markt- und Meinungsforschung, wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf

a) eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
b) Berufs-, Branchen- oder Geschäftsbezeichnung,
c) Namen,
d) Titel,
e) akademische Grade,
f) Anschrift und
g) Geburtsjahr
beschränken

und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

(…)

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder
4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche

Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) [1]Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. [2]Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. [3]Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuches genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) [1]Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. [2]Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) [1]Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. [2]Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. [3]Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. [4]Absatz 3 Nr. 2 gilt entsprechend.

§ 33 Benachrichtigung des Betroffenen

(1) [1]Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. [2]Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. [3]Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

(2) [1]Eine Pflicht zur Benachrichtigung besteht nicht, wenn

der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

1. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,
2. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,
3. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,
4. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforder-

lich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,
5. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
6. die Daten für eigene Zwecke gespeichert sind und
a) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder
b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefähr den würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder
8. die Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert sind und
a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Per sonen beziehen, die diese Daten veröffentlicht haben, oder
b) es sich um listenmäßig oder sonst zusammengefasste Daten handelt (§ 29 Abs. 2 Nr. 1 Buchstabe b) und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.

[2]Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Satz 1 Nr. 2 bis 7 abgesehen wird.

§ 34 Auskunft an den Betroffenen

(1) [1]Der Betroffene kann Auskunft verlangen über

die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
den Zweck der Speicherung.

(…)

(3) Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(4) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.

(5) [1]Die Auskunft ist unentgeltlich. [2]Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann jedoch ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. [3]Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. [4]Ein Entgelt kann in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergibt, dass die Daten zu berichtigen oder unter der Voraussetzung des § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(6) [1]Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. [2]Er ist hierauf in geeigneter Weise hinzuweisen.

§ 35 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit

gelöscht werden. Personenbezogene Daten sind zu löschen, wenn
1. ihre Speicherung unzulässig ist,
2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,
3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder
4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit
1. im Falle des Absatzes 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn
(1) 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
(2) die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Bürgerliches Gesetzbuch (BGB)

§ 823 Schadensersatzpflicht

(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.

(2) [1]Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. [2]Ist nach dem Inhalt des Gesetzes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Ersatzpflicht nur im Falle des Verschuldens ein.

§ 1004 Beseitigungs- und Unterlassungsanspruch

(1) [1]Wird das Eigentum in anderer Weise als durch Entziehung oder Vorenthaltung des Besitzes beeinträchtigt, so kann der Eigentümer von dem Störer die Beseitigung der Beeinträchtigung verlangen. [2]Sind weitere Beeinträchtigungen zu besorgen, so kann der Eigentümer auf Unterlassung klagen.

(2) Der Anspruch ist ausgeschlossen, wenn der Eigentümer zur Duldung verpflichtet ist.

Strafgesetzbuch (StGB)

§ 201 Verletzung der Vertraulichkeit des Wortes

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt

1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder
2. eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.

(2) [1]Ebenso wird bestraft, wer unbefugt

1. das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder
2. das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.

[2]Die Tat nach Satz 1 Nr. 2 ist nur strafbar, wenn die öffentliche Mitteilung geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. [3]Sie ist nicht rechtswidrig, wenn die öffentliche Mitteilung zur Wahrnehmung überragender öffentlicher Interessen gemacht wird.

(3) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichteter die Vertraulichkeit des Wortes verletzt (Absätze 1 und 2).

(4) Der Versuch ist strafbar.

(5) Die Tonträger und Abhörgeräte, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden.

§ 201a Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

(1) Wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und

dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer eine durch eine Tat nach Absatz 1 hergestellte Bildaufnahme gebraucht oder einem Dritten zugänglich macht.

(3) Wer eine befugt hergestellte Bildaufnahme von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, wissentlich unbefugt einem Dritten zugänglich macht und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(4) Die Bildträger sowie Bildaufnahmegeräte oder andere technische Mittel, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden.

II. **Urteile** (in Zusammenfassung)

Bundesverfassungsgericht (BVerfG)

Volkszählungsurteil vom 15. Dezember 1983, Az.: 1 BvR 209, 269, 362, 420, 440, 484/83

Die Leitsätze dieser Grundsatzentscheidung zur informationellen Selbstbestimmung, die als Meilenstein des Datenschutzes gilt, lauten wie folgt:

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

3. Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymer Form erhoben und verarbeitet werden, und solchen, die für statistische Zwecke bestimmt sind.

Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. Der Informationserhebung und Informationsverarbeitung müssen aber innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen.

4. Das Erhebungsprogramm des Volkszählungsgesetzes 1983 (§ 2 Nr. 1 bis 7, §§ 3 bis 5) führt nicht zu einer mit der Würde des Menschen unvereinbaren Registrierung und Katalogisierung der Persönlichkeit; es entspricht auch den Geboten der Normenklarheit und der Verhältnismäßigkeit. Indessen bedarf es zur Sicherung des Rechts auf informationelle Selbstbestimmung ergänzender verfahrensrechtlicher Vorkehrungen für Durchführung und Organisation der Datenerhebung.

5. Die in § 9 Abs. 1 bis 3 des Volkszählungsgesetzes 1983 vorgesehenen Übermittlungsregelungen (unter anderem Melderegisterabgleich) verstoßen gegen das allgemeine Persönlichkeitsrecht. Die Weitergabe zu wissenschaftlichen Zwecken (§ 9 Abs. 4 VZG 1983) ist mit dem Grundgesetz vereinbar.

Verwaltungsgericht (VG) Minden,

Vergleich vom 31.10.2006, Az.: 6 K 552/06

Videoüberwachungen sind mit Einschränkungen zulässig, befand das VG Minden in einem Rechtsstreit zwischen der Betreiberin eines Seniorenheims und der Heimaufsichtsbehörde. Der Rechtsstreit endete mit einem Vergleich.

Die Heimaufsicht hatte beanstandet, dass die Einrichtung mit insgesamt zehn Videokameras ausgestattet worden war. Diese Kameras überwachten den Aufenthaltsraum, die Eingänge sowie Treppen und Flure des Heims. Der Heimbetreiber wollte dadurch den Schutz der Bewohner im Falle von Stürzen und vor unbemerkten Eindringlingen verbessern. Die Aufnahmen wurden in den Aufsichtsraum des Personals übertragen und dort für die Dauer von drei Wochen gespeichert. Die Heimaufsicht hielt dies aus datenschutzrechtlichen Gründen für nicht zulässig.

In der mündlichen Verhandlung widersprach das Gericht der Auffassung der Heimaufsichtsbehörde, hier seien die Bestimmungen für die Überwachung öffentlich zugänglicher Räume einschlägig. Die Videoüberwachung sei allerdings bedenklich, weil sie sich auch auf den Aufenthaltsraum erstrecke. Hier sei ein unzulässiger Eingriff in die Privatsphäre der Heimbewohner zu befürchten. Datenschutzrechtliche Zweifel bestünden auch an der Speicherung der Aufnahmen über einen Zeitraum von drei Wochen hinweg. Auf Vorschlag des Gerichts einigten sich die Parteien darauf, dass die Überwachung des Aufenthaltsraums zukünftig nicht mehr stattfindet. In den weniger sensiblen Bereichen wie Eingängen, Fluren und Treppenhäusern sollte die Überwachung zum Schutz der Bewohner jedoch fortgesetzt werden dürfen. Die Aufnahmen dürften allerdings nicht länger als 72 Stunden gespeichert bleiben.

III. Adressen

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Husarenstr. 30
53117 Bonn
Telefon: 0228 / 997799 - 0
Telefax: 0228 / 997799 - 550
E-Mail: poststelle@bfdi.bund.de

Der Landesbeauftragte für den Datenschutz in Baden-Württemberg

Königstraße 10a
70173 Stuttgart
Telefon: 0711 / 615541 - 0
Telefax: 0711 / 615541 - 15
E-Mail: poststelle@lfd.bwl.de

Der Bayerische Landesbeauftragte für den Datenschutz

Wagmüllerstraße 18
80538 München
Telefon: 089 / 212672 - 0
Telefax: 089 / 212672 - 50
E-Mail: poststelle@datenschutz-bayern.de

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit

Friedrichstr. 219
10969 Berlin
Telefon: 030 / 13889 - 0
Telefax: 030 / 2155050
E-Mail: mailbox@datenschutz-berlin.de

Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen

Arndtstraße 1
27570 Bremerhaven
Telefon: 0471 / 5962010
Telefax: 0471 / 49618495
E-Mail: office@datenschutz.bremen.de

Die Landesbeauftragte für den Datenschutz und für das Recht zur Akteneinsicht in Brandenburg

Stahnsdorfer Damm 77
14532 Kleinmachnow
Telefon: 033203 / 356 - 0
Telefax: 033203 / 356 - 49
E-Mail: poststelle@lda.brandenburg.de

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Klosterwall 6, Block C
20095 Hamburg
Telefon: 040 / 42854 - 4040
Telefax: 040 / 4279 - 11811
E-Mail: mailbox@datenschutz.hamburg.de

Der Hessische Datenschutzbeauftragte

Gustav-Stresemann-Ring 1
65189 Wiesbaden
Telefon: 0611 / 1408 - 0
Telefax: 0611 / 1408 - 900
E-Mail: poststelle@datenschutz.hessen.de

Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Kavalleriestr. 2 – 4
40102 Düsseldorf
Telefon: 0211 / 38424 - 0
Telefax: 0211 / 38424 - 10
E-Mail: poststelle@ldi.nrw.de

Der Landesbeauftragte für den Datenschutz in Niedersachsen

Prinzenstraße 5
30159 Hannover
Telefon: 0511 / 120 - 4500
Telefax: 0511 / 120 - 4599
E-Mail: poststelle@lfd.niedersachsen.de

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Hintere Bleiche 34
55116 Mainz
Telefon: 06131 / 208 - 2449
Telefax: 06131 / 208 - 2497
E-Mail: poststelle@datenschutz.rlp.de

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Saarland

Fritz-Dobisch-Str. 12
66111 Saarbrücken
Telefon: 0681 / 94781 - 0
Telefax: 0681 / 94781 - 29
E-Mail: poststelle@datenschutz.saarland.de

Landesbeauftragter für den Datenschutz Sachsen-Anhalt

Leiterstraße 9
39104 Magdeburg
Telefon: 0391 / 81803 - 0
Telefax: 0391 / 81803 - 33
E-Mail: poststelle@lfd.sachsen-anhalt.de

Der Sächsische Datenschutzbeauftragte

Bernhard-von-Lindenau-Platz 1
01067 Dresden
Telefon: 0351 / 493 - 5401
Telefax: 0351 / 493 – 5490
E-Mail: saechsdsb@slt.sachsen.de

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Holstenstraße 98
24103 Kiel
Telefon: 0431 / 988 - 1200
Telefax: 0431 – 988 -1223
E-Mail: mail@datenschutzzentrum.de

Der Landesbeauftragte
für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
Lennéstraße 1
Schloss Schwerin
19053 Schwerin
Telefon: 0385 / 59494 - 0
Telefax: 0385 / 59494 - 58
E-Mail: info@datenschutz-mv.de

Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
Häßlerstraße 8
99096 Erfurt
Telefon: 0361 / 3771900
Telefax: 0361 / 3771904
E-Mail: poststelle@datenschutz.thueringen.de

IV. Glossar

- AG = Amtsgericht
- Abs. = Absatz
- Art. = Artikel
- BDSG = Bundesdatenschutzgesetz
- BGB = Bürgerliches Gesetzbuch
- BGH = Bundesgerichtshof
- BSG = Bundessozialgericht
- BVerfG = Bundesverfassungsgericht
- BVerwG = Bundesverwaltungsgericht
- GG = Grundgesetz
- HeimMindBauV = Heimmindestbauverordnung
- HeimPersV = Heimpersonalverordnung
- LG = Landgericht
- LSG = Landessozialgericht
- OLG = Oberlandesgericht
- PangV = Preisangabenverordnung
- SGB V = Sozialgesetzbuch 5. Buch, Gesetzliche Krankenversicherung
- SGB XI = Sozialgesetzbuch 11. Buch, Soziale Pflegeversicherung
- SGB XII = Sozialgesetzbuch 12.Buch, Sozialhilfe
- StGB = Strafgesetzbuch
- VG = Verwaltungsgericht
- WEG = Wohneigentumsgesetz