Informationen für
Ärztinnen und Ärzte

# Schweigepflicht und Datenschutz in der Arztpraxis

(Stand: April 2004)

**Landesärztekammer**
**Baden-Württemberg**
Körperschaft des öffentlichen Rechts

## Inhalt

Im nachstehenden Text wird die Berufsbezeichnung „Arzt“ („Ärzte“) einheitlich und neutral für Ärztinnen und Ärzte verwendet.

Die hier abgedruckten Informationen sind auch im Internet über die Homepage der Landesärztekammer Baden-Württemberg abrufbar:

www.aerztekammer-bw.de

Herausgeber:

Landesärztekammer Baden-Württemberg,
Jahnstraße 40, 70597 Stuttgart

Redaktion:

Arbeitskreis „Vernetzung und Telemedizin“
Juristische Geschäftsführung
Ärztliche Pressestelle

# 1. Ärztliche Schweigepflicht

Die Schweigepflicht des Arztes dürfte so alt sein wie der Arztberuf selbst. Medizingeschichtlich erstmalig erwähnt wird die ärztliche Schweigepflicht wohl in indischen Sanskritschriften um 800 v. Chr. Weltweit bekannt geworden ist die Verpflichtung für Ärzte zu schweigen im hippokratischen Eid der griechischen Medizin, dessen Herkunft unbekannt ist, der aber ca. 2400 Jahre alt sein dürfte. Unter Strafe gestellt wurde der Bruch der ärztlichen Schweigepflicht erstmalig im Preußischen Allgemeinen Landrecht von 1794.

Heute schützt § 203 Strafgesetzbuch (StGB) vor der Verletzung von Privatgeheimnissen durch Ärzte und Angehörige anderer Berufsgruppen, die in einem besonderen Vertrauensverhältnis zum Patienten/Kunden stehen. Mit Freiheitsstrafe bis zu 1 Jahr oder mit Geldstrafe wird bestraft, wer ein Patientengeheimnis, das ihm anvertraut oder sonst bekannt geworden ist, unbefugt offenbart. Der Arzt handelt nicht unbefugt, wenn sein Sprechen gerechtfertigt ist. Wichtig für den Arzt sind daher die vier Offenbarungsbefugnisse:

a) die Einwilligung des Patienten,

b) die mutmaßliche Einwilligung des Patienten,

c) die gesetzlichen Offenbarungspflichten und -rechte

d) das Offenbarungsrecht aufgrund des sog. rechtfertigenden Notstandes gemäß § 34 StGB.

Zu a) Seine Einwilligung erklärt der Patient, wenn er seinen Arzt von der Schweigepflicht entbindet. Diese Erklärung sollte sich der Arzt immer schriftlich geben lassen, da das Datenschutzrecht dies verlangt (Näheres siehe unten 5.). Der Patient kann seine Einwilligung auch konkludent erteilen, z.B. bei der Mitbehandlung durch einen Praxisassistenten.

Zu b) Kein Verstoß gegen die ärztliche Schweigepflicht liegt ferner vor, wenn der Arzt die Einwilligung des Patienten vermuten kann. Hieran werden allerdings hohe Anforderungen gestellt. Die Einwilligung darf der Arzt daher in der Regel nur vermuten, wenn er den Patienten nicht oder nur unter großen Schwierigkeiten befragen kann.

Die Weitergabe von Patientendaten an privatärztliche Verrechnungsstellen und die Übergabe der Patientenkartei bei Aufgabe der Praxis ist nur mit schriftlicher Einwilligung der Patienten zulässig.

Zu c) Gesetzliche Offenbarungspflichten und -rechte finden sich in großer Zahl im Sozialgesetzbuch, aber z.B. auch im Infektionsschutzgesetz und in der Röntgenverordnung (siehe unter 4.).

Zu d) Gestattet ist die Weitergabe von Patientengeheimnissen schließlich in rechtfertigenden Situationen des Notstands. Eine solche Notstandssituation ist beispielsweise gegeben, wenn ein stark sehbehinderter Patient trotz der Überzeugungsbemühungen des Arztes uneinsichtig bleibt und ohne Sehhilfe, die für seine sichere Teilnahme am Straßenverkehr unabdingbar ist, am Verkehr teilnehmen will. Hier werden bei der Meldung des Arztes an die Führerscheinbehörde Patientengeheimnisse offenbart, die der ärztlichen Schweigepflicht unterliegen, jedoch erfolgt dies zum Schutz eines anderen höherwertigen Rechtsguts, nämlich der Sicherheit anderer Verkehrsteilnehmer.

Weitere Beispiele für das Offenbarungsrecht auf Grund des rechtfertigen Notstands sind die Kenntnis von Misshandlungen oder entwürdigenden Behandlungen von Kindern durch Eltern. Auch hier spricht die Interessenabwägung für die Offenbarung gegenüber Dritten / Polizei. – Die Bekanntgabe der AIDS-Infektion eines Patienten an dessen Lebensgefährtin kann gemäß § 34 StGB gerechtfertigt sein. Allerdings verlangt die Rechtsprechung immer, dass der Offenbarung ein (erfolgloser) Versuch des Arztes vorausgeht, den Patienten dazu zu bewegen, selbst entsprechend tätig zu werden.

### *Schweigepflicht in strafrechtlichen Verfahren*

Bei strafrechtlichen Ermittlungsverfahren gegen einen Arzt dürfen Patientenunterlagen, die als Beweismittel von Bedeutung sein können, beschlagnahmt werden, wenn der Arzt sie nicht freiwillig herausgibt. Die Beschlagnahme muss in der Regel ein Richter anordnen, der das Interesse an der Wahrheitsermittlung mit dem Datenschutzinteresse des Patienten abwägen muss. Ist dagegen der Patient der Beschuldigte oder das Opfer einer Straftat, hat der Arzt ein Zeugnisverweigerungsrecht. Er darf die Unterlagen nicht herausgeben, solange der Patient ihn nicht von der Schweigepflicht entbindet. Das Zeugnisverweigerungsrecht des Arztes (§ 53 der Strafprozessordnung, StPO) und das Beschlagnahmeverbot der Patientenakten ( § 97 StPO) haben ihre Begründung in der ärztlichen Schweigepflicht.

### *Ärztliche Schweigepflicht als Berufspflicht*

Neben die Strafandrohung durch § 203 StGB tritt für Ärzte die in den Berufsordnungen der Ärztekammern verankerte Berufspflicht, über all das zu schweigen, was sie in Ausübung ihres Berufs über den Patienten und seine Krankheiten erfahren haben. Jeder Arzt kann sich also nicht nur straf-

bar machen, sondern vom Berufsgericht auch mit einer berufsgerichtlichen Maßnahme (Warnung, Verweis, Geldbuße) belegt werden, wenn er gegen die ärztliche Schweigepflicht verstößt. Die ärztliche Schweigepflicht schützt Patientendaten in jeder Form (Karteikarte, Patientenakte, Computerdatei). – Sie gilt auch gegenüber anderen Ärzten und bindet den Arzt über den Tod des Patienten hinaus.

***Datenschutz***

Neben die Strafandrohungen des Strafrechts und der ärztlichen Berufsgerichtsbarkeit treten seit 1980 die datenschutzrechtlichen Verpflichtungen aus dem Bundesdatenschutzgesetz und den Datenschutzgesetzen der Bundesländer.

Zu unterscheiden ist zwischen dem öffentlichen und dem nichtöffentlichen Bereich: Für Krankenhausärzte (öffentlicher Bereich) gelten in der Regel die Datenschutzbestimmungen in den Landeskrankenhausgesetzen. Niedergelassene Ärzte haben hingegen die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) im nichtöffentlichen Bereich zu beachten.

Nach dem novellierten Bundesdatenschutzgesetz gehören Gesundheitsdaten zu den besonderen Arten personenbezogener Daten. Dies ist für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von besonderer Bedeutung (vgl. §3 Abs. 9 und § 28 Abs. 6 bis 8 BDSG). Dabei ist es einerlei, ob die Daten unter Einsatz von Datenverarbeitungsanlagen oder in oder aus nicht automatisierten Dateien verarbeitet werden. Das Bundesdatenschutzgesetz erfasst daher mittlerweile sämtliche automatisierten Computer-Daten und sämtliche nicht-automatisierten und manuell geführten Patientenakten. Das Bundesdatenschutzgesetz bezieht sich auf alle „personenbezogenen Daten“, nämlich alle Einzelangaben über sämtliche persönlichen oder sachlichen Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Es beschränkt sich weder auf medizinische oder persönliche „geheime“ Daten, noch auf den Personenkreis der Patienten als Betroffene.

Im Anhang sind die wichtigsten Rechtsvorschriften für Ärzte aus dem Bundesdatenschutzgesetz (in der Fassung vom 14.01.2003) abgedruckt. Die jeweils aktuelle Fassung ist im Internet abrufbar unter www.im.baden-wuerttemberg.de (Rubrik „Datenschutz“, Unterrubrik „Infomaterial“).

# 2. Organisation des Empfangsbereichs

Im normalen Praxisablauf treffen meist mehrere Personen zusammen, was Konsequenzen für den Datenschutz hat. Es muss daher klar sein, dass die Einhaltung des Datenschutzes vorrangig dem Schutz der Identität des Patienten gelten muss. Hierbei werden allerdings auch die Grenzen offenbar, wenn zum Beispiel im Eingangs- und Wartebereich verschiedene Patienten zeitgleich aufeinandertreffen.

### *Verpflichtung auf Schweigepflicht und Datengeheimnis*

Der Arzt ist nach der Berufsordnung der Landesärztekammer Baden-Württemberg vom 10.04.03 dazu verpflichtet, alle Praxismitarbeiter/innen über ihre Verschwiegenheitspflicht zu belehren und dies schriftlich im Arbeitsvertrag festzuhalten. Diese Verpflichtung zur Verschwiegenheit umfasst alle in einer Arztpraxis erhobenen personenbezogenen Daten.

### *Trennung von Empfangs-, Warte- und Behandlungsbereich*

Um die Zahl der Personen möglichst gering zu halten, die personenbezogene Informationen im Empfangsbereich ggf. mithören können, sollte dieser Bereich entsprechend den räumlichen Möglichkeiten vom eigentlichen Wartezimmer durch eine Tür getrennt sein. Eine solche Trennung durch eine Tür ist erst recht geboten zwischen einzelnen Behandlungsräumen. Es reicht nicht aus, Besprechungs- oder Behandlungsräume, in denen Patienten auf den Arzt warten oder eine Anwendung erhalten, von anderen Räumen, in denen gleichzeitig patientenbezogen medizinische Fragen bei einer Untersuchung oder Behandlung besprochen werden, nur durch Sichtblenden oder Vorhänge voneinander abzugrenzen.

### *Gespräche, Telefonate*

Das Praxispersonal muss Gespräche mit Patienten im Empfangsbereich möglichst so führen, dass nur die Betroffenen selbst medizinische Sachverhalte zusammen mit ihrem Namen den mithörenden Anwesenden offenbaren. Bei Telefongesprächen mit Dritten, die Anwesende – notgedrungen – mithören, sollte auf eine namentliche Anrede verzichtet werden, wenn es um die Übermittlung persön-

licher Daten mit medizinischen Inhalten geht. Derartige Telefongespräche sollten von der Anmeldung an einen anderen Anschluss weiterverbunden werden. Generell muss bei Auskünften am Telefon die Identität des Anrufers gesichert werden. Dies kann beispielsweise durch Rückruf oder Nachfrage von ausschließlich dem berechtigten Anrufer bekannten Daten geschehen. Besondere Vorsicht muss bei Anfragen und Anrufen von Familienangehörigen angewandt werden. Jede Möglichkeit der unbefugten Einsicht in fremde Krankenunterlagen durch Dritte muss verhindert werden. Dies gilt auch für EDV-Bildschirme oder das Telefaxgerät der Praxis. Beim Versenden der Patientendaten per Telefax muss sichergestellt sein, dass nur der Empfänger selbst oder ausdrücklich dazu ermächtigte Dritte Kenntnis vom Inhalt des Schreibens erhalten. Diese Sicherung kann nur durch Ankündigung der Übersendung beim Empfänger und regelmäßige Überprüfung der gespeicherten Rufnummern erreicht werden.

# 3. Die Patientenakte

### *Funktion*

Jeder Arzt hat die Behandlung eines Patienten umfassend zu dokumentieren. Er ist dazu sowohl zivil- als auch berufsrechtlich verpflichtet. Die früher meist handschriftliche Dokumentation ist heute in aller Regel der elektronischen Karteikarte gewichen. In beiden Fällen dient die Dokumentation dem Arzt als Gedächtnisstütze und als Nachweis seiner Tätigkeit. Dem Patienten dient sie zur Information. Die Patientenakte muss für beide Seiten verfügbar sein und vor dem Zugriff Dritter sicher verwahrt werden. Bei der elektronischen Karteiführung müssen nachträgliche Veränderungen erkennbar sein.

### *Inhalt*

Die Dokumentation muss alle objektiven Sachverhalte enthalten. Mindestens folgende:

- Anamnese
- Befunderhebungen/Beschreibung des Krankheitsverlaufes
- Therapien (Medikamente, physikalische Therapie u.a.m.)
- Diagnosen

Darüber hinaus können subjektive Wertungen Bestandteil der Dokumentation sein.

### *Behandlungsvertrag*

Arzt und Patient schließen – in der Regel mündlich, eher im Ausnahmefall schriftlich – einen Vertrag über das ärztliche Tätigwerden. In aller Regel bildet dabei die Behandlung, ggf. aber auch nur die Untersuchung (z.B. für Eignungsprüfungen), den Inhalt und Zweck des Arzt-Patienten-Verhältnisses. Dieser Zweck rechtfertigt und begrenzt zugleich die dazu „erforderliche“ Datenverarbeitung. Daher dürfen Patientendaten ohne gesonderte Einwilligung z.B. an außenstehende Rehabilitationsgruppen nicht weitergegeben werden.

Die Nutzung und Übermittlung von Patientendaten zu Forschungszwecken ist vom Behandlungsvertrag in aller Regel ebenfalls nicht gedeckt. Hier lässt aber das Bundesdatenschutzgesetz eine Zweckdurchbrechung zu. Voraussetzung ist, dass aber das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausmaß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Nach § 15 Abs. 2 der Berufsordnung der Landesärztekammer Baden-Württemberg dürfen der Schweigepflicht unterliegende Tatsachen und Befunde zum Zwecke der wissenschaftlichen Forschung und Lehre grundsätzlich nur soweit offenbart werden, als dabei die Anonymität des Patienten gesichert ist oder der Patient dem ausdrücklich zustimmt.

### *Anamnese-Fragebogen*

In vielen Arztpraxen werden die Patienten gebeten, vor einem ersten Kontakt mit dem Arzt einen Fragebogen auszufüllen. Da es sich um standardisierte Fragen für alle Patienten handelt, dürfen die Fragebogen nur solche Punkte enthalten, die für die Behandlung der allermeisten Patienten von Bedeutung sind. Der Patient ist bei der Aushändigung eines solchen Fragebogens dahingehend aufzuklären, dass er nur die Fragen beantworten muss, die er als Information für den Arzt für notwendig erachtet. Bei Unklarheiten ist das Ausfüllen des Fragebogens gemeinsam mit dem behandelnden Arzt im Sprechzimmer vorzunehmen.

### *Aufbewahrung*

Der Arzt ist Eigentümer der Patientenunterlagen. Er hat nach der Berufsordnung für sie eine öffentlich-rechtliche Aufbewahrungspflicht. Die Patientenunterlagen sind „in gehörige Obhut“ zu nehmen, auch nach Aufgabe der Praxis. Sie dürfen nicht unverschlossen in Räumen gelagert werden, die für Patienten ohne Aufsicht durch das Praxispersonal zugänglich sind. Während der Sprechstunden sind sie auch im Sprech- und Behandlungszimmer so zu legen bzw. zu verschließen, dass andere Patienten sie nicht einsehen können. Die Dauer der Aufbewahrung beträgt regelmäßig 10 Jahre nach Abschluss der Behandlung. Sie kann länger sein, wenn spezielle Rechtsvorschriften dies vorsehen. Bei Arzt- oder Wohnortwechsel sollte sichergestellt sein, dass auf Wunsch des Patienten seine Krankenakte dem weiterbehandelnden Arzt übersandt wird.

***Akteneinsicht***

Jeder Patient hat das Recht, die über ihn geführte Krankenakte beim Arzt einzusehen. Das Einsichtsrecht bezieht sich auf die dokumentationspflichtigen objektiven Sachverhalte und medizinische Feststellungen, nicht auf persönliche Bemerkungen des Arztes. Soweit die Patientenunterlagen Angaben über Dritte enthalten, sind diese abzudecken oder vor der Einsicht herauszunehmen. Ein sog. „therapeutisches Privileg“, das den Arzt berechtigen würde, dem Patienten zu seinem Schutz eine Einsichtnahme in seine Akte zu verwehren, gibt es im allgemeinen nicht. Der Patient kann anstelle der Einsichtnahme auch eine Kopie der Aufzeichnungen verlangen. Der Arzt darf ihm Originale nicht überlassen. Das Akteneinsichtsrecht kann der Patient auch auf Dritte übertragen. Dazu bedarf es in der Regel einer schriftlichen Vollmacht und einer Schweigepflichtentbindungserklärung. Nach dem Tod des Patienten darf der Arzt die Patientenunterlagen nur dann den Angehörigen zeigen, wenn der vor dem Tod geäußerte oder der mutmaßliche Wille des Verstorbenen dem nicht entgegensteht.

***Aktenvernichtung***

Wenn nach Ablauf der vorgeschriebenen Aufbewahrungsfristen die Patientendaten nicht mehr gebraucht werden, z.B. weil keine weitere Behandlung des Patienten zu erwarten ist, sind die Unterlagen ordnungsgemäß zu vernichten. Sie müssen daher entweder in einem eigenen Shredder zerkleinert (nach DIN-Norm 32 757, Sicherheitsstufe 3-4) oder einem Aktenvernichtungsunternehmen übergeben werden. Wenn zur Aktenvernichtung ein Unternehmen eingeschaltet wird, findet datenschutzrechtlich gesehen eine Datenverarbeitung im Auftrag statt. Hierbei sind die Anforderungen des § 11 BDSG (schriftlicher Auftrag mit Regelung, wie zu vernichten ist) zu beachten. Der Arzt bleibt die verantwortliche Stelle. Ihm obliegt es zu kontrollieren, ob der Auftrag datenschutzgerecht erledigt wurde. Um die Einhaltung der ärztlichen Schweigepflicht zu gewährleisten, sollten die Patientendaten in einem abgeschlossenen Behältnis, das in der Regel vom Unternehmen zur Verfügung gestellt wird, zur Vernichtung abgegeben werden.

Einen Sonderfall stellt der Austausch von Festplatten aus dem Praxiscomputer, auf denen sich unverschlüsselte Patientendaten befinden, dar. Hier muss vom Arzt dafür Sorge getragen werden, dass die Festplatte so vernichtet wird, dass die Daten nicht wiederhergestellt werden können. Dies ist auch bei einem Festplattenaustausch während der Gewährleistungsfrist zu beachten, da die Datenträger meist ausgetauscht, vom Hersteller repariert und von den Serviceunternehmen als Austausch-

festplatten oftmals mit dem noch vorhandenen ursprünglichen Datenbestand wieder eingesetzt werden.

Das oben Gesagte gilt auch für den Fall, dass der PC insgesamt beseitigt oder verkauft wird.

***Herrenlose Patientenunterlagen***

Probleme bereitet häufig die Aufbewahrung von Patientenunterlagen nach Praxisaufgabe ohne Praxisnachfolger. Der Arzt bleibt gem. § 10 Abs. 4 der Berufsordnung der Landesärztekammer Baden-Württemberg auch nach Praxisaufgabe verpflichtet, die Patientenunterlagen aufzubewahren oder dafür Sorge zu tragen, dass sie in gehörige Obhut gegeben werden. Die gleiche Verpflichtung betrifft die Erben nach dem Tod des Arztes, da die Erben im Rahmen der Gesamtsrechtnachfolge in die Pflichtenstellung des Arztes eintreten.

Wenn der Arzt ohne Erben verstirbt, wird der Staat Zwangserbe mit der Folge, dass er die Pflichten in Bezug auf die Patientendokumentation miterbt. Die herrenlose Patientenkartei stellt einen polizeirechtswidrigen Zustand dar, der ein Tätigwerden der Ortspolizeibehörde erforderlich macht. Die Ortspolizeibehörde muss deshalb die herrenlose Patientenkartei in ihre Obhut nehmen.

Die bisweilen vertretene Auffassung, dass die Ärztekammern eine Verpflichtung zur Übernahme von herrenlosen Patientenkarteien hätten, ist rechtlich nicht zutreffend.

# 4. Übermittlungen von Patientendaten aufgrund gesetzlicher Bestimmungen

Kern der ärztlichen Schweigepflicht ist es, dass der Patient darauf vertrauen kann, dass sein Arzt die ihm anvertrauten persönlichen, intimen Dinge Dritten nicht weitergibt. Dieses Vertrauen wird durchbrochen, wenn der Arzt zur Offenbarung von Patientendaten gegenüber Dritten durch ein Gesetz verpflichtet wird oder ein Gesetz ihm dies erlaubt. Die gesetzlichen Übermittlungspflichten und -rechte sind dem Patienten oft nicht bekannt. Der Arzt braucht sie dem Patienten auch nicht mitzuteilen. Erhalten andere Stellen zulässigerweise Patientendaten vom Arzt, dürfen diese Stellen die Daten nur für den jeweiligen Zweck nutzen, für den sie die Daten erhalten haben.

***Übermittlung an die Kassenärztliche Vereinigung***

Das Sozialgesetzbuch sieht die regelmäßige Datenübermittlung vom Vertragsarzt an die Kassenärztliche Vereinigung und an die gesetzlichen Krankenkassen vor. Der Vertragsarzt rechnet seine zur Behandlung des gesetzlich Krankenversicherten erbrachten Leistungen mit der Kassenärztlichen Vereinigung ab. Er hat deshalb der KV gemäß §§ 294 ff. Sozialgesetzbuch (SGB) V den Namen, die Anschrift und das Geburtsdatum des Patienten, dessen Krankenkasse und Versichertennummer sowie die ärztlichen Leistungen einschließlich der Diagnose(n) (verschlüsselt nach der ICD 10) maschinenlesbar zu übermitteln. Diese Daten dienen einerseits dazu, dass die Kassenärztliche Vereinigung die Abrechnung durchführen und kontrollieren kann. Andererseits stehen sie nach Bearbeitung durch die Kassenärztliche Vereinigung dieser und den Krankenkassen für die Überprüfung der Wirtschaftlichkeit des Vertragsarztes zur Verfügung (§§ 12, 106 SGB V). Darüber hinaus ist der Vertragsarzt verpflichtet, auf Verlangen seiner KV für Plausibilitätsprüfungen gemäß § 106 a SGB V einzelne Befunde vorzulegen. Die von der Kassenärztlichen Bundesvereinigung und den Bundesverbänden der Krankenkassen vereinbarten Abrechnungsvordrucke tragen dem Rechnung. Wer noch manuell abrechnet und diese Vordrucke verwendet, verstößt nicht gegen die ärztliche Schweigepflicht und den Datenschutz. Ebenso wenig handelt rechtswidrig, wer seine Abrechnungsdaten auf Datenträger oder über eine Datenleitung, verschlüsselt nach dem Kryptomodul der KBV, an seine KV übermittelt.

***Übermittlung an gesetzliche Krankenkassen***

Wie sich aus § 100 SGB X ergibt, ist jeder Arzt und jeder Angehörige eines anderen Heilberufs verpflichtet, den Leistungsträgern in der gesetzlichen Sozialversicherung im Einzelfall auf Verlangen Auskunft zu geben, soweit es für die Durchführung seiner Aufgaben nach dem Sozialgesetzbuch erforderlich und 1. gesetzlich zugelassen ist oder 2. der Betroffene im Einzelfall eingewilligt hat (i.d.R. schriftlich). Fehlt es an diesen Voraussetzungen, muss der (Vertrags-)Arzt schweigen. Er darf schweigen, wenn er durch Offenbarung/Übermittlung eine Straftat oder eine Ordnungswidrigkeit begeht (§ 100 Abs. 2 SGB X). Schweige- und auskunftspflichtig ist jeder Arzt und nicht nur jeder Vertragsarzt, denn der Privatarzt darf im Notfall auch Versicherte einer gesetzlichen Krankenversicherung behandeln (§ 76 Abs. 1 Satz 2 SGB V).

Ärzte müssen den gesetzlichen Krankenkassen nur Auskunft geben, soweit es für die Durchführung ihrer Aufgaben nach dem Sozialgesetzbuch erforderlich und gesetzlich zugelassen ist. Die gesetzlichen Krankenkassen haben insbesondere die Aufgabe, die Beiträge der Versicherten zu verwalten, die Leistungspflicht gegenüber ihren Versicherten mit und ohne den Medizinischen Dienst der Krankenversicherungen (MDK) zu überprüfen, sowie an der Zulassung der Vertragsärzte und Psychotherapeuten und an Wirtschaftlichkeitsprüfungen mitzuwirken. Im Rahmen dieser Aufgaben bedarf es ferner der jeweiligen gesetzlichen Zulassung zur Auskunftserteilung. Derartige Auskunftspflichten ergeben sich u. a. aus den §§ 294 ff. SGB V. Danach sind die Vertragsärzte verpflichtet, die für die Erfüllung der Aufgaben der Krankenkassen notwendigen Angaben, die aus der Erbringung, der Verordnung sowie der Abgabe von Versicherungsleistungen entstehen, aufzuzeichnen und den Krankenkassen mitzuteilen (§ 295 Abs. 2 a SGB V). Diese Übermittlungsbefugnisse haben die KBV und die Spitzenverbände der Krankenkassen in den §§ 36, 18 Bundesmantelvertrag Ärzte / Ersatzkassen (BMVÄ/EKV) präzisiert. Der Vertragsarzt ist verpflichtet, auf Wunsch einer Primär- oder Ersatzkasse dieser eine Auskunft auf dem vereinbarten Vordruck zu erteilen. Die wichtigsten vereinbarten Vordrucke sind: Bericht für den MDK, Wiedereingliederungsplan, Bericht des behandelnden Arztes, Anfrage zur Zuständigkeit einer anderen Krankenkasse oder eines sonstigen Kostenträgers, Anfrage bei Fortbestehen der Arbeitsunfähigkeit und Ärztliche Bescheinigung zur Feststellung des Erreichens der Belastungsgrenze.

Anders stellt sich die Rechtslage dagegen für ein Auskunftsbegehren einer gesetzlichen Krankenkasse auf einem nicht vereinbarten Vordruck dar. Hier muss die Krankenkasse im Einzelfall nachweisen, warum sie die Auskunft benötigt und aufgrund welcher Rechtsgrundlage sie diese fordert. Wenn diese Rechtsgrundlage der Krankenkasse kein gesetzliches Auskunftsrecht gibt, wie etwa bei § 66 SGB V, wonach die Krankenkasse den Versicherten bei der Geltendmachung von Schadenser-

satzansprüchen unterstützen kann, und das Auskunftsbegehren nur auf §100 SGB X basiert, hat die Krankenkasse eine aktuelle Entbindungserklärung des Versicherten von der Schweigepflicht beizufügen. Die allgemeine Aussage, Vertragsärzte seien verpflichtet, den Krankenkassen die für die Erfüllung ihrer Aufgaben notwendigen Angaben mitzuteilen, genügt in der Regel nicht. Das Ausstellen von Bescheinigungen ohne Wissen und Wollen des Patienten ist von daher aus datenschutzrechtlicher Sicht problematisch.

***Übermittlung an den MDK***

Ob der (Vertrags-)Arzt problemlos Patientendaten an den MDK weitergeben darf, ist bis heute umstritten. Vom Grundsatz her gilt, dass der (Vertrags-)Arzt auch gegenüber dem MDK schweigepflichtig ist, es sei denn, ihm steht eine der vier o. g. Offenbarungsbefugnisse zu. Der (Vertrags-) Arzt ist gesetzlich zur Auskunft gegenüber dem MDK verpflichtet, wenn eine gesetzliche Krankenkasse eine gutachtliche Stellungnahme oder Prüfung durch den MDK veranlasst hat und die Übermittlung für die gutachtliche Stellungnahme und Prüfung des MDK im Einzelfall erforderlich ist. Der Vertragsarzt hat nach Auffassung des LSG Baden-Württemberg beispielsweise auch die Pflicht, für die substantiierte Prüfung wegen eines Schadensregresses seine Abrechnungsunterlagen der Krankenkasse zur Weiterleitung an den MDK vorzulegen (Urt. vom 11.12.1996, in: MedR 1997, S. 331, 333). Datenschutzrechtlich akzeptabel ist auch die Praxis, wonach die Krankenkasse Unterlagen zur Vorlage an den MDK anfordert, vorausgesetzt, diese Unterlagen werden in einem verschlossenen und an den MDK (zur Weitergabe an diesen) adressierten Umschlag übersandt. Hinzuweisen ist aber – nochmals – darauf, dass sich die Vorlagepflicht an den MDK auf die „erforderlichen“ Daten beschränkt. Im Zweifel sollte der ersuchte Arzt eine Darlegung des MDK zur Frage der Erforderlichkeit fordern und nicht unbesehen alle vorhandenen Unterlagen aus der Hand geben.

***Übermittlung an Berufsgenossenschaften***

Im Recht der Unfallversicherung (SGB VII) ist der Arzt gem. §§ 201, 203 SGB VII gesetzlich verpflichtet, den Berufsgenossenschaften (BGen) Auskunft zu erteilen. (Vertrags-)Ärzte, die an einem Unfallheilverfahren beteiligt sind, müssen daher Patientendaten, die für ihre Entscheidung, eine Unfallheilbehandlung durchzuführen, maßgeblich waren, an die zuständige BG übermitteln. Soweit es für Zwecke der Heilbehandlung und der Erbringung sonstiger Leistungen erforderlich ist, müssen auch Daten über die Behandlung und den Zustand des Unfallversicherten sowie andere personenbezogene Daten an die BG weitergeleitet werden, selbst wenn der Patient widerspricht. Dem Patienten gegenüber besteht lediglich eine Informationspflicht. Haben BGen einen überbetrieblichen arbeitsmedizinischen Dienst eingerichtet, sind personenbezogene Arbeitnehmerdaten an diesen weiterzuleiten. Eine Übersendung der Patientendaten an die nicht ärztliche Geschäftsführung der BG ist nur

erlaubt, wenn der Patient zustimmt oder es um eine Beschwerde Dritter gegen einen Arzt des überbetrieblichen arbeitsmedizinischen Dienstes geht.

***Übermittlung an BfA und LVA***

Im Recht der Rentenversicherung (SGB VI) besteht gegenüber der BfA und den Landesversicherungsanstalten (LVAen) keine gesetzliche Pflicht des (Vertrags-)Arztes zur Auskunftserteilung. Zwar wird die Auffassung vertreten, dass dann, wenn ein Versicherter einen Rentenantrag stellt, er konkludent in die Beiziehung medizinischer Unterlagen einwilligt, die zur Prüfung der Rentenbewilligung notwendig sind. Da dies aber streitig ist und die Landesärztekammer Baden-Württemberg die Meinung vertritt, es müsse immer eine ausdrückliche Einwilligungserklärung eingeholt werden, sollten (Vertrags-)Ärzte an die BfA und die LVA nur Auskünfte erteilen, wenn sie zuvor eine aktuelle Entbindungserklärung von der Schweigepflicht erhalten haben.

***Übermittlung in weiteren Fällen (Auswahl)***

- bei ansteckenden Krankheiten

  Im Falle von bestimmten ansteckenden Krankheiten, insbesondere von Geschlechtskrankheiten, verpflichtet das Infektionsschutzgesetz vom 20.07.2000 (BGBl. I S. 1045) Ärzte dazu, den Krankheitsfall dem Gesundheitsamt mitzuteilen. Unterschieden wird zwischen der namentlichen und der nicht namentlichen Meldung. Die namentliche Meldung muss neben der konkreten Krankheit mindestens den Namen, die Anschrift, das Alter und das Geschlecht des Patienten enthalten. Formulare für die meldepflichtigen Krankheiten können bei den örtlichen Gesundheitsämtern angefordert oder von der Homepage des Robert-Koch-Instituts unter *www.rki.de* heruntergeladen werden.

- bei Röntgenaufnahmen

  Zum Schutz vor unnötigen Strahlenbelastungen bestimmt die Röntgenverordnung, dass der Arzt der Ärztlichen Stelle bei der Landesärztekammer Röntgenaufnahmen, auf denen ja regelmäßig der Patientenname vermerkt ist, zur Prüfung zugänglich macht (§§ 16 Abs. 3, 17 Abs. 4 Röntgenverordnung RöV). Außerdem hat der Arzt die Röntgenaufnahmen einem nachbehandelnden Arzt auf dessen Verlangen vorübergehend zu überlassen (§ 28 Abs. 8 RöV).

- bei Drogen-Substitution

  Nach der Betäubungsmittel-Verschreibungsverordnung ist die Substitutionsbehandlung eines Drogensüchtigen mit einem Betäubungsmittel (z.B. Methadon) dem Bundesinstitut für Arzneimittel und Medizinprodukte in Berlin in Form eines achtstelligen Patientencodes schriftlich oder kryptiert zu melden (§ 5 a Betäubungsmittelverschreibungsverordnung BtmVV). Der Nachweis und der Bestand von Betäubungsmitteln, wenn sie in der Arztpraxis vorgehalten werden, ist in einem amtlichen Formblatt zu führen. Wird einem Süchtigen ein Substitutionsmittel zum unmittelbaren Verbrauch überlassen, ist der Verbleib patientenbezogen nachzuweisen. Auf Verlangen der zuständigen Landesbehörde, in Baden-Württemberg dem Sozialministerium, ist dieser die vollständige Behandlungs-Dokumentation vorzulegen. Ein anderes oder ein darüber hinausgehendes Offenbarungsrecht ergibt sich aus den Richtlinien des Bundesausschusses der Ärzte und Krankenkassen über ärztliche Untersuchungs- und Behandlungsmethoden (BUB-Richtlinien) nicht. Allerdings muss der substituierende Vertragsarzt für gesetzlich krankenversicherte Patienten im Einzelfall eine Bewilligung zur Substitution bei der Substitutionskommission seiner KV beantragen. Hierzu hat er eine schriftliche Begründung zu übermitteln, aus der neben der medizinischen Indikation hervorgeht, für welchen Zeitraum die Substitution vorgesehen ist, welche Ziele angestrebt werden und welche medizinischen Maßnahmen im Rahmen eines umfassenden Therapiekonzepts vorgesehen sind.

- bei Krebskrankheiten

  Landesrechtlich kann das Krebsregistergesetz Baden-Württemberg den Arzt berechtigen, im einzelnen festgelegte persönliche und medizinische Daten an das Krebsregister zu übermitteln. Eine ausdrückliche Einwilligung des Patienten in die Datenübermittlung ist nach dem Landeskrebsregistergesetz Baden-Württemberg nur dann erforderlich, wenn die Meldung nicht rechnergestützt und unverschlüsselt erfolgt (§ 4 Abs. 1 LKrebsRG). Erfolgt sie dagegen rechnergestützt und verschlüsselt, sind die Daten anonymisiert, so dass es keiner Einwilligung bedarf (§ 3 Abs. 1 LKrebsRG). Ist der Patient verstorben, darf der Arzt auch ohne vorheriges Einverständnis des Patienten melden, „sofern kein Grund zu der Annahme besteht, dass er die Einwilligung verweigert hätte." (§ 4 Abs. 2 Landeskrebsregistergesetz LKRG)

- bei Geburten

  Neben anderen Personen ist auch der anwesende Arzt verpflichtet, die Geburt eines Kindes beim Standesbeamten mündlich anzuzeigen (§§ 16, 17 Personenstandsgesetz). Mitzuteilen sind Namen, Beruf, Wohnort und Staatsangehörigkeit der Eltern, die Zeit der Geburt und der Name sowie das Geschlecht des Kindes.

# 5. Übermittlung aufgrund einer Schweigepflichtentbindungserklärung

Wo ein gesetzliches Offenbarungsrecht fehlt, darf der Arzt Patientendaten nur weitergeben, wenn und soweit der Patient ihn von der Schweigepflicht entbunden hat Dies geschieht häufig formularmäßig und oft nicht direkt gegenüber dem Arzt, sondern gegenüber der Institution, die die Patientendaten benötigt.

***Übermittlung an private Versicherungsgesellschaften***

Schon bei Vertragsschluss lassen sich private Kranken-, Unfall-, Lebens- und andere Versicherungsgesellschaften in der Regel eine Schweigepflichtentbindungserklärung unterschreiben, die mit dem Bundesdatenschutzbeauftragten und/oder den Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich abgestimmt ist. Denn gesetzliche Offenbarungspflichten oder -rechte bestehen für den Arzt nicht. Diese Erklärung erlaubt der Versicherungsgesellschaft, sich auch bei Ärzten über mögliche Versicherungsrisiken des zukünftigen Versicherungsnehmers zu informieren. Im Versicherungsfalle (Krankheit, Unfall) berechtigt sie, bei Ärzten und Krankenhäusern alle Daten abzufragen, die zur Beurteilung der Leistungspflicht erforderlich sind. Dem Arzt teilt die Versicherung häufig nur mit, dass ihr eine Schweigepflichtentbindungserklärung vorliegt. Da der Arzt jedoch für die Offenbarung der Patientendaten verantwortlich bleibt, wird empfohlen, sich von der Versicherungsgesellschaft immer eine aktuelle Entbindungserklärung vorlegen zu lassen. Schließlich kann der Patient ein ernsthaftes Interesse daran haben, dass seine Versicherung über seine Krankheit, etwa im Bereich der Psychiatrie, nichts erfährt. Gegenüber Lebensversicherungsgesellschaften ist ebenfalls eine gewisse Vorsicht anzuraten, insbesondere dann, wenn eine Lebensversicherung aufgestockt werden soll und die Versicherungsgesellschaft auf eine frühere Entbindungserklärung von der Schweigepflicht verweist. Auch hier wird empfohlen, sich noch einmal eine aktuelle Entbindungserklärung von der Schweigepflicht vorlegen zu lassen. Es ist ferner ein guter Weg, dem Patienten die Antwort an die Versicherung zur Überprüfung und eigenständigen Weiterleitung zuzusenden. Da ein Antrag auf Abschluss eines Versicherungsvertrags inzwischen auch über das Internet gestellt werden kann, muss ein Arzt darauf achten, dass ihm eine vom Patienten eigenhän-

dig unterschriebene Erklärung über die Entbindung von der Schweigepflicht und nicht lediglich der Ausdruck eines Computerformulars vorgelegt wird.

### *Übermittlung an das Versorgungsamt*

Im Verhältnis des Arztes zu den Versorgungsämtern (Recht der sozialen Entschädigung bei Gesundheitsschäden sowie Feststellungen nach dem Schwerbehindertenrecht) gilt insbesondere § 12 Abs. 2 des Gesetzes über das Verwaltungsverfahren der Kriegsopferversorgung. Hiernach muss immer das Einverständnis des Antragstellers/Patienten eingeholt werden, wenn das Versorgungsamt vom Arzt Auskünfte einholt oder Untersuchungsunterlagen zur Einsicht beiziehen will.

Der Patient, der beim Versorgungsamt die Feststellung einer Gesundheitsstörung und ihres Grades beantragt, muss deshalb gegenüber dem Versorgungsamt eine Schweigepflichtentbindungserklärung unterschreiben. Sie umschreibt, wen (z.B. Ärzte), was und für welchen Zweck das Versorgungsamt fragt. Sie enthält einen „Raum für etwaige Einschränkungen der Einwilligung“ für den Fall, dass der Antragsteller/Patient dem Versorgungsamt einen bestimmten Sachverhalt nicht offenbaren will. Hat der Antragsteller/Patient seinen behandelnden Arzt ohne Einschränkungen von der Schweigepflicht entbunden, weist das Versorgungsamt den Arzt im jeweiligen Vordruck darauf hin. Ebenso ist das Versorgungsamt verpflichtet, den Arzt auf Einschränkungen hinzuweisen. Eine Pflicht des befragten Arztes, sich selbst davon zu überzeugen, dass er nicht durch eine Beschränkung der Einwilligung an der Offenbarung von Patientendaten gegenüber dem Versorgungsamt gehindert ist, besteht nicht.

### *Übermittlung an Arbeitgeber*

Gegenüber Arbeitgebern hat der Arzt grundsätzlich die Pflicht, über ihm anvertraute Patientengeheimnisse zu schweigen. Dies gilt auch für die Information über eine Arbeitsunfähigkeit. Zwar ist im Recht der gesetzlichen Krankenversicherung nach der Vordruckvereinbarung ein dreiteiliger Durchschreibevordruck zur Arbeitsunfähigkeit vereinbart, in dem auch ein Exemplar für den Arbeitgeber bestimmt ist. Dennoch darf der Vertragsarzt dieses Durchschriftsexemplar für den Arbeitgeber nicht an diesen weiterleiten, denn die Partner des Bundesmantelvertrages, die KBV und die Spitzenverbände der Krankenkassen, haben kein Recht, eine Offenbarungsregelung zwischen Vertragsarzt und Arbeitgeber des gesetzlich Krankenversicherten zu vereinbaren. Der Vertragsarzt hat die Pflicht zur Ausstellung einer Arbeitsunfähigkeitsbescheinigung aus einer Nebenpflicht des Behandlungsvertrages. Es liegt daher in der Hand des Patienten, ob er die AU-Bescheinigung an seinen Arbeitgeber weitergibt oder nicht. Sollte der Arbeitnehmer und Patient den Vertragsarzt dage-

gen bitten, das für den Arbeitgeber bestimmte Exemplar an diesen weiterzuleiten, ist diese Auskunft durch das Einverständnis des Patienten gedeckt.

Geht es um Beschäftigte bei Arbeitgebern, die von Gesetzes wegen mit Abrechnungsscheinen von Versicherten, Arbeitsunfähigkeitsbescheinigungen etc. umgehen müssen, wie z.B. Kassenärztliche Vereinigungen und Krankenkassen, wird empfohlen, kritische Diagnosen mit dem Patienten zu besprechen. Die genannten Arbeitgeber sind oft damit einverstanden, dass man bei ihren Arbeitnehmerinnen und Arbeitnehmern auf die gesetzlich an sich erforderliche Mitteilung der Diagnose(n) verzichtet.

Bei der Ausstellung von Arbeitsunfähigkeitsbescheinigungen für Privatpatienten gilt das Gleiche wie bei der AU-Bescheinigung für gesetzlich Krankenversicherte.

### *Übermittlung bei Praxisverkauf*

Die Patientenkartei hat einen wirtschaftlichen Wert, der beim Verkauf einer Praxis eine erhebliche Rolle spielt. Die Offenbarung der Patientendaten durch den verkaufenden Arzt gegenüber dem Praxisnachfolger ist nach einer Entscheidung des Bundesgerichtshofes jedoch nur mit Einverständnis des Patienten zulässig. Ist ein Verkauf beabsichtigt und steht ein Käufer fest, so ist der in Behandlung befindliche Patient nach seiner Zustimmung zur späteren Weitergabe seiner Daten an den Praxisnachfolger zu fragen. Eine vorsorgliche formularmäßige Einwilligung für den Fall, dass die Praxis irgendwann einmal an einen anderen Arzt übergeben wird, ist unwirksam, weil sie zu unbestimmt ist. Möglich ist, die früheren Patienten anzuschreiben und sie um ihre Einwilligung zur Übergabe der Patientenunterlagen an den Nachfolger zu bitten. Bei größeren Praxen ist dieser Weg allerdings sehr aufwändig. Als Alternative kommt in Betracht, einerseits aktuell die Patienten zu befragen und um ihr Einverständnis zu bitten, wenn der Name des Übernehmers feststeht und andererseits zwischen dem Praxisabgeber und dem -übernehmer einen Verwahrungsvertrag mit Androhung einer Vertragsstrafe abzuschließen, aufgrund dessen der Übernehmer die Krankenakten der früheren Patienten aus dem Altkarteischrank oder dem Alt-PC nur entnehmen darf, wenn der Patient dem aktuell zustimmt (sog. Zwei-Schrank-Modell). Möglich ist ferner, die alten Krankenakten nur von einer Arzthelferin betreuen zu lassen, die schon bei dem Praxisabgeber gearbeitet hat. Sie entnimmt Akten aus dem Altkarteischrank oder dem Alt-PC ebenfalls nur, wenn der Patient dem zuvor zugestimmt hat (sog. Zwei-Schrank-Modell mit Arzthelferin). In den Praxisübergabevertrag sollte selbst dann, wenn der übernehmende Arzt schon längere Zeit als Assistent in der Praxis gearbeitet hat, eine Aktenübergaberegelung vereinbart werden, weil Krankenakten von Patienten, die

lange nicht in der Praxis waren, auch in diesem Fall nur mit Einverständnis an den übernehmenden Arzt übergeben werden dürfen.

### *Übermittlung an privatärztliche Verrechungsstellen*

Privatpatienten erhalten die Arztrechnung entweder vom Arzt direkt oder von einer ärztlichen oder gewerblichen Verrechnungsstelle. Nach einer Entscheidung des Bundesgerichtshofes darf der Arzt der Verrechnungsstelle die Abrechnungsdaten seiner Privatpatienten nur dann übermitteln, wenn diese vorher einwilligt haben. Dies geschieht zunehmend per Formular. Darauf **darf aber** die Widerruflichkeit der Einwilligung nicht ausgeschlossen werden. **Verboten** ist auch, die Einwilligung auf eventuelle Gläubiger der Verrechnungsstelle zu erweitern, denen die Arztforderung abgetreten werden könnte. Auch wenn es in der Regel keine Behandlungspflicht gibt, darf der Arzt die Weigerung des Patienten, zu Abrechnungszwecken seine Daten an eine Verrechnungsstelle weiterzugeben, nicht zum Anlass nehmen, die Behandlung des Patienten „mangels Vertrauensverhältnisses“ abzulehnen. Denn der Patient übt nur ein ihm ausdrücklich eingeräumtes Recht aus. Sollte die Verrechnungsstelle die Daten an Dritte für Subunternehmerleistungen weitergeben, z.B. an ein Druck- und Kuvertierzentrum für den Postversand, oder eine Bonitätsprüfung durchführen, so muss der Patient in der Einwilligungserklärung darüber informiert werden.

### *Übermittlung an ein Labor*

Bei Beauftragung eines Labors ist zu differenzieren. Übergibt der niedergelassene Arzt die Proben pseudonymisiert an seine Laborgemeinschaft oder an ein externes Labor, bedarf dies keiner Zustimmung des Patienten. Wird Körpermaterial des Patienten mit seinen Daten an einen Dritten weitergegeben, auch wenn es sich bei diesem Dritten um einen Arzt handelt, muss der Patient grundsätzlich einwilligen, da er in der Regel nicht davon ausgeht, dass Dritte an einem anderen Ort als dem Praxisort Kenntnis von seinem Körpermaterial und seinem Namen erhalten. Voraussetzung hierfür ist eine entsprechende Information des Patienten. Für die Annahme eines „konkludenten Einverständnisses“ ist grundsätzlich kein Raum, da der Patient im Zeitpunkt der Gewebeentnahme gefragt werden kann.

### *Übermittlung an einen weiterbehandelnden Arzt*

Gemäß § 73 Abs. 1b SGB V darf ein hausärztlich tätiger Vertragsarzt mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, bei anderen Vertragsärzten und Leistungserbringern

Behandlungsdaten und Befunde zum Zwecke der Dokumentation und der weiteren Behandlung erheben. Die Regelungen über die schriftliche Einwilligung des Patienten in die Datenübermittlung nach § 73 Absatz 1 b SGB V sollen die Dokumentationsbefugnis des vom Patienten gewählten Hausarztes bei Behandlungen durch andere Leistungserbringer stärken. Die Regelung betrifft somit nicht den Fall der eigenen Behandlung des Patienten durch den Hausarzt selbst. Wenn zum Zwecke der Behandlung und der Diagnose durch den Hausarzt andere Leistungserbringer einbezogen werden, z.B. Radiologen oder Laborärzte oder ein Notarzt eingeschaltet wird, ist von einer Einwilligung des hiervon betroffenen Patienten auszugehen. Die Herausgabe von Originalunterlagen an den Patienten darf nicht generell unterbleiben, auch wenn dies nicht der Regelfall ist. Das OLG München hält in einer Entscheidung vom 19.04.2001 unter bestimmten Voraussetzungen die Herausgabe von Röntgenaufnahmen im Original für erforderlich. § 28 Abs. 6 Satz 2 der RöV trifft Regelungen für eine Übergabe an den Patienten. Eigentümer der Krankenakten ist der Arzt. Er hat sie aufgrund der Berufsordnung der Landesärztekammer Baden-Württemberg öffentlich-rechtlich mindestens 10 Jahre aufzubewahren. Wenn Originalunterlagen weitergegeben werden, sollte dies nur von Arzt zu Arzt geschehen. Der abgebende Arzt sollte sich den Empfänger notieren.

***Übermittlung an Angehörige***

Auch gegenüber Angehörigen des Patienten ist die ärztliche Schweigepflicht zu beachten. Der Patient kann seinen Willen zur Entbindung von der Schweigepflicht ausdrücklich oder konkludent dadurch deutlich machen, dass er in Anwesenheit von Angehörigen mit seinem Arzt über die Krankheit spricht. Ist der Patient über die wahre Diagnose (z.B. Krebs) jedoch nicht aufgeklärt, ist dem Arzt auch eine Mitteilung darüber an Angehörige verboten. Die nicht selten anzutreffende Praxis, den Patienten nicht aufzuklären, aber die Angehörigen umfassend zu informieren, widerspricht der „informationellen Selbstbestimmung“ des Betroffenen. Anders ist es, wenn der Patient erklärt, er wolle es selbst zwar nicht wissen, wünsche aber eine Unterrichtung seiner Angehörigen. Der Arzt kann sich in diesem Sinne auch bei seinem Patienten nach dessen Auffassung erkundigen.

Die Schweigepflicht besteht auch gegenüber den Eltern/Personensorgeberechtigten eines Minderjährigen, wenn dieser selbst eine ausreichende Einsichtsfähigkeit zum Verständnis von Diagnose und Therapie besitzt. Das kann schon bei einer 14jährigen Jugendlichen der Fall sein, die den Arzt um ein Rezept für eine Anti-Baby-Pille bittet. Vorsorglich kann der Arzt den Minderjährigen um eine Schweigepflichtentbindungserklärung bitten. Nicht zulässig ist die Versendung der Arztrechnung mit den Leistungsdaten an den (allein verdienenden) Ehemann einer behandelten Ehefrau/Privatpatientin. Der privatärztliche Behandlungsvertrag, der die Zahlungspflicht auslöst, wird

ausschließlich mit der Patientin abgeschlossen. Es ist ihre Sache, die Zahlung sicherzustellen. Die sog. „Schlüsselgewalt“ der Hausfrau greift hier nicht.

Eine Offenbarung der Krankheitsdaten eines Verstorbenen gegenüber seinen Angehörigen ist wie die Akteneinsicht (s. o. Nr. 3.) vom erklärten oder mutmaßlichen Willen des Patienten abhängig. Im Normalfall – d. h. ohne besondere Anhaltspunkte für einen gegenteiligen Willen – wird man davon ausgehen können, dass der Verstorbene den nächsten Angehörigen eine Information über Krankheit und Todesursache nicht vorenthalten wollte.

# 6. Die Praxis-EDV

Bei der Anschaffung eines EDV-Systems für die Patientenverwaltung müssen auch datenschutzrechtliche Erwägungen berücksichtigt werden. Die folgenden Ausführungen dazu beziehen sich nicht auf bestimmte Systeme einzelner Hersteller. Sie formulieren vielmehr allgemeine datenschutzrechtliche Grundsätze und Anforderungen, die die gegenwärtig angebotenen EDV-Systeme nur zum Teil verwirklichen. Der Arzt ist für die Auswahl des Systems sowie dafür verantwortlich, dass nötigenfalls spezielle zusätzliche Sicherungs-Software eingesetzt wird. Der Erwerb eigener EDV-Kompetenz durch den Praxisinhaber ist empfehlenswert. Die nachfolgenden Problempunkte sollte der Arzt als Check-Liste gegenüber den Anbietern nutzen.

***Vorschriften***

Die rechtlichen Rahmenbedingungen für eine Praxis-EDV sind entweder sehr allgemein oder auf enge Spezialfragen beschränkt. Es fehlt eine umfassende systematische Regelung. Die Berufsordnung für Ärzte fordert für Aufzeichnungen auf elektronischen Datenträgern besondere Sicherungs- und Schutzmaßnahmen, um deren Veränderung, vorzeitige Vernichtung oder unrechtmäßige Verwendung zu verhindern. *Hierzu hat die KBV schon 1989 „Empfehlungen zu Datenschutz und Schweigepflicht beim EDV-Einsatz in der kassenärztlichen Praxis“ formuliert. Sie gehen besonders ein auf Zugriffsrechte von externem Wartungspersonal, auf Datenfernübertragung und die Vernichtung von Datenträgern. Für die Verwendung von EDV-Systemen zur Abrechnung mit der Kassenärztlichen Vereinigung gibt es darüber hinaus eine Vereinbarung zwischen der KBV und den Spitzenverbänden der Krankenkassen. Der Vertragsarzt hat die dortigen Regelungen zum Datenschutz zu beachten.*

***Datenschutzrechtliche Anforderungen: Grundsatz***

„Das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen“ (§ 28 BDSG). Der Arzt darf also die EDV im Rahmen des Behandlungsvertrages mit dem Patienten einsetzen. Für andere Zwecke oder zeitlich über die Behandlung hinaus darf er personenbezogene Patientendaten nur mit Zustimmung des Patienten verar-

beiten. Bei der elektronischen Verarbeitung müssen die Daten vor unbefugtem Zugriff Dritter geschützt werden. Für besondere Schutz- und Sicherungsmaßnahmen zählt das BDSG in einer Anlage verschiedene Kontrollbereiche auf - von der Zugangs- über die Übermittlungs- und Eingabe- bis zur Organisationskontrolle (die „8 Gebote"). Nachfolgend werden die allgemeinen Anforderungen für den Bereich der Arztpraxis konkretisiert

***Zugangs- und Zugriffskontrolle***

Die EDV-Anlage ist durch geeignete Maßnahmen gegen unbefugten Zugang zu sichern. Um zu verhindern, dass Unbefugte innerhalb der Praxis auf das System zugreifen, ist ein Passwortschutz geboten. Dabei darf als Passwort nicht das vom System-Hersteller „mitgebrachte" übernommen werden. Das Passwort ist in bestimmten Zeitabständen zu ändern, dies soll von der Software unterstützt werden. Verlässt ein Mitarbeiter die Praxis nach einer Kündigung, ist die Zugriffsberechtigung sofort zu löschen bzw. zu ändern. Nach mehreren Versuchen, mit einem - falschen - Passwort in das System zu gelangen, sollte die Software den Zugriff automatisch ganz sperren. In großen Arztpraxen bietet es sich an, die Zugriffsrechte je nach Aufgabe des Mitarbeiters auf die tatsächlich erforderlichen Daten zu beschränken.. Auch ist zu prüfen, inwieweit einzelne Mitarbeiter nur zum Lesen der Daten, nicht aber auch zu ihrer Veränderung berechtigt werden sollten. Um einen Zugriff durch wartende Patienten zu vermeiden, sind Bildschirme so aufzustellen, dass sie nur vom Arzt und dem Praxispersonal eingesehen werden können. Verlassen diese – auch kurzzeitig – den Raum und bleibt der Patient mit Bildschirm und Tastatur allein, so muss der EDV-Arbeitsplatz gesperrt werden. Eine Aktivierung des Systems darf nur durch eine erneute Passworteingabe möglich sein.

Alternativ zur Sperrung des EDV-Arbeitsplatzes kommt die Verwendung eines passwortgeschützten Bildschirmschoners in Betracht. Dieser sollte entweder vom Arzt bei Verlassen des Computerbereiches aktiviert werden oder sich selbst nach kurzer Zeit einschalten und nur durch Eingabe eines dem Arzt bekannten Passwortes wieder ausschalten lassen. Jegliches verwendete Passwort sollte modernen Sicherheitsanforderungen genügen, d.h. aus mindestens acht Stellen, darunter Buchstaben, Zahlen und Sonderzeichen bestehen.

***Datensicherung („back up")***

Zum Schutz der Patientendaten vor Verlust sind täglich Sicherungskopien auf geeigneten externen Medien zu erstellen. Die Datensicherungsmedien müssen regelmäßig auf ihre Lesbarkeit überprüft

werden. Sie sind räumlich getrennt vom Server aufzubewahren und sollten physikalisch gelöscht werden, wenn ihre Schutzfunktion überholt ist.

### *Computerviren und andere destruktive Programme*

Bei jedem Einspielen von Datenträgern besteht die Gefahr, dass Computerviren und andere destruktive Programme in das EDV-System eindringen. Manche wurden entwickelt, um Datenbestände zu verändern oder zu zerstören.

Es sollten daher keine fremden Datenträger im System eingesetzt werden ohne vorherige Überprüfung mit einem aktuellen Virensuchprogramm. Dies gilt auch für Software-Datenträger renommierter Firmen, für CD' s und neuerdings auch für Datenträger, die nur Text- und Kalkulationsdokumente (vor allem WORD und EXCEL für Windows) beinhalten.

### *Fälschungssicherheit*

Soweit das EDV-System die konventionelle Karteikarte / Patientenakte ersetzt, muss es insbesondere die Anforderungen an die ärztliche Dokumentationspflicht erfüllen (s.o.). Aus diesem Grund sollten Ärzte die Hersteller von Praxis-Software dazu drängen, die Beweiskraft der elektronischen Dokumentation zu erhöhen.

### *Systemverwaltung und Wartung*

Im normalen Praxisbetrieb nutzen Arzt und Praxis-Personal die EDV menügesteuert durch festgelegte Verarbeitungsschritte. Bestimmte Aufgaben wie die Definition von Zugriffsrechten erfordern jedoch weitergehende Verarbeitungsrechte. Notwendig werden kann auch ein Zugang zum Betriebssystem. Diese erweiterten („privilegierten“) Rechte sollten einer Person, dem System- bzw. Netzverwalter, vorbehalten sein. Eine eigene Kennung für diese Funktion schützt vor unbefugter Inanspruchnahme der erweiterten Rechte durch andere Personen. Wird die Wartung bzw. die Systemverwaltung der EDV-Anlage von einer externen Firma übernommen, ist darauf zu achten, dass der Schutz der Patientendaten gewährleistet ist. Ähnliches gilt beispielsweise auch für Handwerker oder Reinigungskräfte, die in der Praxis tätig werden.

***Sicherheit im Internet***

Bei jedem Computer, der mit dem Internet verbunden ist, besteht grundsätzlich die Möglichkeit, dass Dritte versuchen, unbemerkt eine Verbindung aufzubauen, um Schaden stiftende Programme dort zu installieren oder den Datenbestand auszuspähen, zu verändern oder zu löschen. Damit wird bei Computern, die unverschlüsselte Patientendaten enthalten, der Reglungsbereich des § 9 Bundesdatenschutzgesetz, hier Ziffer 2 (Zugangskontrolle) und Ziffer 3 (Zugriffskontrolle) verletzt. Einen wirkungsvollen Schutz bietet nur eine hochwertige, regelmäßig gewartete und aktualisierte Firewall. Diese sichere Firewall wird in der Regel aus Kostengründen in der Arztpraxis nicht vorgehalten werden können, womit sich der Internetanschluss am Praxis-PC ausschließt.

Auch die alternierende Nutzung als Internet-PC, nachdem die Praxisanwendung geschlossen und der PC eventuell als reiner Internet-PC neu gestartet wurde, birgt Risiken in sich, da auch da unbemerkt die Festplatte kopiert werden kann oder Programme, die Schaden stiften oder zu einem späteren Zeitpunkt Daten sammeln, unbemerkt installiert werden können. Aus diesem Grund kann jeder Internetanschluss an einem Praxis-PC, ohne einen nachgewiesenen ausreichenden Schutz, zu einer datenschutzrechtlichen Beanstandung durch die Aufsichtsbehörde führen.

***Patientenrecht auf Auskunft und Berichtigung***

Nach dem Bundesdatenschutzgesetz kann jeder Patient Auskunft verlangen über 1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen, 2. den Zweck der Speicherung und 3. Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, wenn seine Daten automatisiert verarbeitet werden. Eine derartige Auskunftsfunktion sollte die Praxis-Software von vornherein mit vorsehen. Denn die schriftlich zu erteilende Auskunft muss für den Patienten „lesbar“ sein, d.h. Kürzel und Schlüssel müssen erklärt werden – entweder durch ein entsprechendes Verzeichnis oder eine eigene Langtext-Fassung als Auskunfts-Version des EDV-Ausdrucks. Während die Dokumentationspflicht sich nur auf medizinische Feststellungen und Bewertungen bezieht, erfasst die Auskunftspflicht nach dem Bundesdatenschutzgesetz alle zum Patienten gespeicherten Daten. Hinweise des Arztes auf Eigenheiten des Patienten ohne medizinische Bedeutung sind davon nicht ausgeschlossen. Eine Offenbarung solcher Hinweise kann der Arzt nur verhindern, wenn sie nicht (mehr) im EDV-System erfasst sind. „Die Auskunft ist unentgeltlich“. Diese Feststellung im Bundesdatenschutzgesetz geht jeder Gebührenordnung vor. Das Auskunftsrecht, versetzt den Patienten in die Lage, unrichtige Daten zu erkennen. Er hat einen gesetzlichen Anspruch auf eine entsprechende Berichtigung.

***Risiken und datenschutzrechtliche Anforderungen beim Einsatz mobiler Rechner***

Für die Zugriffssicherheit mobiler Rechner gilt das gleiche wie bei anderen Personal Computern, denn ohne zusätzliche Schutzmaßnahmen hat jeder, der das Gerät in die Hände bekommt, einen ungehinderten Zugriff auf die gespeicherten Daten. Es ist daher in besonderem Maße Sorge zu tragen, dass ein mobiler Rechner mit Patientendaten während des Einsatzes unter der ständigen Aufsicht des Arztes verbleibt!

# 7. Datenschutz bei gemeinschaftlicher Berufsausübung

***Grundsatz***

Viele Ärzte praktizieren in Praxisgemeinschaften. Die Berufsordnung der Ärzte stellt dazu fest: „Bei allen Formen gemeinsamer Berufsausübung muss die freie Arztwahl gewährleistet bleiben." Das bedeutet datenschutzrechtlich: Wer sich einem bestimmten Arzt in einer Praxisgemeinschaft anvertraut, muss sich darauf verlassen können, dass andere Ärzte seine persönlichen und medizinischen Daten nicht erfahren, wenn er es nicht will. Dies gilt jedoch nicht für Gemeinschaftspraxen, die ja berufsrechtlich *eine* Praxis darstellen und deshalb auf dem Schild als solche gekennzeichnet werden müssen. Der Patient weiß damit, dass die ärztlichen Leistungen in Gemeinschaftspraxen austauschbar sind. Nutzen die Praxis-Partner ein gemeinsames EDV-System, so sollte dies ermöglichen, dass verschiedene Kennungen eingerichtet werden, die regelmäßig nur den Zugriff auf die Daten der „eigenen" Patienten ermöglichen (z.B. mandantenfähiges System). Der Umstand, dass das übrige Praxis-Personal in der Regel für alle Ärzte arbeitet und damit zumeist Zugriff auf alle Patientenakten und Dateien hat, schließt ein Zugriffsverbot für den nicht behandelnden Arzt rechtlich nicht aus.

***Auflösung einer Gemeinschaftspraxis***

Wurde in einer Gemeinschaftspraxis die Zuordnung der Patienten zu dem jeweils behandelnden Arzt konsequent durchgeführt, bereitet eine Trennung der Partner datenschutzrechtlich keine Probleme: Jeder Arzt verfügt über die Unterlagen „seiner" Patienten; er ist insoweit auch für die weitere Dokumentation verantwortlich. Bei einer gemeinsamen Praxis-EDV ist dem Arzt, der die Praxis verlässt, ein Ausdruck oder ein Datenträger mit den Daten „seiner" Patienten mitzugeben. Danach sind diese Daten im System physikalisch zu löschen, sofern nicht eine ähnliche Vorgehensweise wie beim Praxisverkauf vereinbart wird. Problematisch wird es dann, wenn die Praxis-Partner eine Zuordnung der Patienten unterlassen haben und insbesondere die EDV nur Patienten „der Gemeinschaftspraxis" kennt. Der Arzt, der – als bisher gleichberechtigter Partner – die Praxis und damit die EDV-Anlage verlässt und eine eigene Praxis eröffnen will, hat ein legitimes Wettbewerbsinteresse an den gemeinsamen Patientendaten. Datenschutzrechtlich hat er jedoch nur einen Anspruch auf die Daten derjenigen Patienten, die ihm aus der Gemeinschaftspraxis in seine neue Praxis folgen. In der

Regel ist damit erst eine nachträgliche Herausgabe der entsprechenden Patientenunterlagen bzw. Datenträger an den ausgeschiedenen Arzt und die Löschung in der Gemeinschaftspraxis-EDV vertretbar.

***Datenschutz in vernetzten Arztpraxen***

Das Thema „Datenschutz in vernetzten Arztpraxen“ ist äußerst komplex. Es wird daher empfohlen, soweit solche Kooperationen konkret geplant sind, in Zusammenarbeit mit der Datenschutzaufsicht ein individuelles Konzept zu erarbeiten, das den jeweils beteiligten Ärzten dann bekannt gegeben wird.

# 8. Datenschutz-Kontrolle

***Betrieblicher Datenschutzbeauftragter***

Bei der automatisierten Verarbeitung von Gesundheitsdaten muss ein betrieblicher Datenschutzbeauftragter bestellt und der Praxis-Leitung direkt unterstellt werden. Er hat die erforderliche Fachkunde und Zuverlässigkeit zu besitzen und ist bei der Anwendung seiner Fachkunde weisungsfrei. Jeder, der die erforderlichen Voraussetzungen erfüllt, kann mit dieser Aufgabe betraut werden. Die Bestellung des Datenschutzbeauftragten hat schriftlich zu erfolgen. Es kann auch eine externe Person zum Datenschutzbeauftragten bestellt werden, die dann der gleichen Verschwiegenheitspflicht unterliegt wie die Praxismitarbeiter und auch darüber zu belehren ist. Die Praxis-Leitung hat ihm Übersichten über die eingesetzte EDV, über die Art der gespeicherten Daten und Dateien, über Speicherungszwecke, regelmäßige Datenempfänger und zugriffsberechtigte Personen zur Verfügung zu stellen. Der Datenschutzbeauftragte wirkt nach § 4g Abs.1 BDSG auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften zum Datenschutz hin.

***Ärztekammer***

Von den externen Kontroll-Einrichtungen hat die Ärztekammer die umfassendsten Aufsichtsbefugnisse. Sie hat Beschwerden über mögliche Verletzungen der ärztlichen Schweigepflicht und des Datenschutzes nachzugehen. Als Selbstverwaltungseinrichtung der Ärzte vertritt sie allerdings zugleich die Interessen der Ärzteschaft insgesamt. Dies schließt jedoch die Aufklärung und ggf. Ahndung von Berufspflichtverletzungen ausdrücklich ein. Bei Patienten-Beschwerden an die Ärztekammer ist zu beachten, dass der betroffene Arzt ein Einsichtsrecht in die ihn betreffenden Aktenvorgänge bei der Ärztekammer hat. Er kann die Beschwerde und den Absender also zur Kenntnis nehmen.

***Polizei, Staatsanwaltschaft***

Verstöße gegen die ärztliche Schweigepflicht sind nicht nur Berufsvergehen, sondern Straftaten im Sinne des Strafgesetzbuches. Bußgeldbewährt oder strafbar nach dem BDSG ist die unbefugte

Speicherung, Veränderung, Übermittlung, Erschleichung, zweckwidrige Nutzung und Verknüpfung von nicht offenkundigen personenbezogenen (Patienten-)Daten in oder aus Dateien (§§ 43 und 44 BDSG)

### *Aufsichtsbehörde für den Datenschutz*

Im Bundesdatenschutzgesetz heißt es: „Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5." Die Aufgabe der Aufsichtsbehörde wird in Baden-Württemberg von der Aufsichtbehörde für den Datenschutz im Innenministerium Baden-Württemberg wahrgenommen. Für ein Tätigwerden der Aufsichtsbehörde fordert das Bundesdatenschutzgesetz keinen Anlass. Dieser kann neben einer konkreten Beschwerde auch in einer Pressenotiz oder einem anonymen Hinweis bestehen. Zur Aufklärung möglicher Datenschutzverstöße muss der niedergelassene Arzt der Aufsichtsbehörde unverzüglich die erforderlichen Auskünfte erteilen und Gelegenheit geben, seine Praxis zu betreten, Prüfungen durchzuführen und Unterlagen einzusehen. Die Aufsichtsbehörde kann Anordnungen zur Beseitigung festgestellter technischer oder organisatorischer Mängel treffen und nur in diesem Zusammenhang bei besonderer Gefährdung des Persönlichkeitsrechts Zwangsgelder verhängen. Als letztes Mittel kann sie auch den Einsatz einzelner Verfahren untersagen. Ferner darf sie die Abberufung des betrieblichen Datenschutzbeauftragten verlangen, wenn dieser die erforderliche Fachkunde und Zuverlässigkeit nicht besitzt. Nach § 43 BDSG können seitens Aufsichtsbehörde z.B. bei Nichtbestellung eines Datenschutzbeauftragten oder bei unbefugter Übermittelung personenbezogener Daten an Dritte Bußgelder verhängt werden.

# Anhang

In diesem Anhang sind die wichtigsten Rechtsvorschriften für Ärzte aus dem Bundesdatenschutzgesetz (in der Fassung vom 14.01.2003) abgedruckt.

Landesdatenschutzgesetz und Bundesdatenschutzgesetz sind in der jeweils vollständigen und aktuellen Fassung im Internet abrufbar unter www.im.baden-wuerttemberg.de (Rubrik „Datenschutz“, Unterrubrik „Infomaterial“).

**§ 1 Zweck und Anwendungsbereich des Gesetzes**

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,

2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
   a) Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,

3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zweck des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

**§ 2 Öffentliche und nicht-öffentliche Stellen**

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Son-

dervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn
1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.
Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

**§ 3 Weitere Begriffsbestimmungen**

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

(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. 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) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern: das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck 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) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. 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) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

(10) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,

1. die an den Betroffenen ausgegeben werden,

2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und

3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

**§ 3a Datenvermeidung und Datensparsamkeit**

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. 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.

**§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung**

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder

2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde
   und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,

2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und

3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

**§ 4a Einwilligung**

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

**§ 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen**

(1) Für die Übermittlung personenbezogener Daten an Stellen

1. in anderen Mitgliedstaaten der Europäischen Union,

2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder

3. der Organe und Einrichtungen der Europäischen Gemeinschaften

gelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, soweit die Übermittlung im Rahmen von
Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.

(2) Für die Übermittlung personenbezogener Daten an Stellen nach Absatz 1, die nicht im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, sowie an sonstige ausländische oder über- oder
zwischenstaatliche Stellen gilt Absatz 1 entsprechend. Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Satz 2 gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

(3) Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.

(4) In den Fällen des § 16 Abs. 1 Nr.. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.

(5) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(6) Die Stelle, an die die Daten übermittelt werden, ist auf den Zweck hinzuweisen, zu dessen Erfüllung die Daten übermittelt werden.

**§ 4c Ausnahmen**

(1) Im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, ist eine Übermittlung personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, sofern

1. der Betroffene seine Einwilligung gegeben hat,

2. die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,

3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,

4. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,

5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder

6. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden.

(2) Unbeschadet des Absatzes 1 Satz 1 kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; die Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben. Bei den Post- und Telekommunikationsunternehmen ist der Bundesbeauftragte für den Datenschutz zuständig. Sofern die Übermittlung durch öffentliche Stellen erfolgen soll, nehmen diese die Prüfung nach Satz 1 vor.

(3) Die Länder teilen dem Bund die nach Absatz 2 Satz 1 ergangenen Entscheidungen mit.

**§ 4d Meldepflicht**

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz 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 vier Arbeitnehmer 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) Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). 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) Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an den Bundesbeauftragten für den Datenschutz zu wenden.

**§ 4e Inhalt der Meldepflicht**

Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

§ 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.

**§ 4f Beauftragter für den Datenschutz**

(1) Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Die Sätze 1 und 2 gelten nicht für nicht-öffentliche Stellen, die höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigen. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung erheben, verarbeiten oder nutzen, haben sie unabhängig von der Anzahl der Arbeitnehmer einen Beauftragten für den Datenschutz zu bestellen.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Mit dieser Aufgabe kann auch eine Person außerhalb der verantwortlichen Stelle betraut werden. Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum
Beauftragten für den Datenschutz bestellen.

(3) Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuchs, bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(5) Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.

**§ 4g Aufgaben des Beauftragten für den Datenschutz**

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Im Fall des § 4d Abs. 2 macht der Beauftragte für den Datenschutz die Angaben nach § 4e Satz 1 Nr.. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar. Im Fall des § 4d Abs. 3 gilt Satz 2 entsprechend für die verantwortliche Stelle.

(3) Auf die in § 6 Abs. 2 Satz 4 genannten Behörden findet Absatz 2 Satz 2 keine Anwendung. Absatz 1 Satz 2 findet mit der Maßgabe Anwendung, dass der behördliche Beauftragte für den Datenschutz das Benehmen mit dem Behördenleiter herstellt; bei Unstimmigkeiten zwischen dem behördlichen Beauftragten für den Datenschutz und dem Behördenleiter entscheidet die oberste Bundesbehörde.

**§ 5 Datengeheimnis**

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

**§ 6 Unabdingbare Rechte des Betroffenen**

(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten. Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

**§ 6a Automatisierte Einzelentscheidung**

(1) Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.

(2) Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder

2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet und dem Betroffenen von der verantwortlichen Stelle die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitgeteilt wird. Als geeignete Maßnahme gilt insbesondere die Möglichkeit des Betroffenen, seinen Standpunkt geltend zu machen. Die verantwortliche Stelle ist verpflichtet, ihre Entscheidung erneut zu prüfen.

(3) Das Recht des Betroffenen auf Auskunft nach den §§ 19 und 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

**§ 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) 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. 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.

**§ 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien**

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,
2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
3. darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und
4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

**§ 7 Schadensersatz**

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. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

**§ 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen**

(1) Fügt eine verantwortliche öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist ihr Träger dem Betroffenen unabhängig von einem Verschulden zum Schadensersatz verpflichtet.

(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt auf einen Betrag von 130 000 Euro begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 130 000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer automatisierten Verarbeitung mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) Hat bei der Entstehung des Schadens ein Verschulden des Betroffenen mitgewirkt, gilt § 254 des Bürgerlichen Gesetzbuchs.

(6) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

**§ 9 Technische und organisatorische Maßnahmen**

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

**§ 9a Datenschutzaudit**

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

**§ 10 Einrichtung automatisierter Abrufverfahren**

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,
2. Dritte, an die übermittelt wird,
3. Art der zu übermittelnden Daten,
4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Ein-

richtung von Abrufverfahren, bei denen die in § 6 Abs. 2 und in § 19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn das für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesministerium zugestimmt hat.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf allgemein zugänglicher Daten. Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann.

**§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag**

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1 Nr.. 2, 10 und 11, Abs. 2 Nr.. 1 bis 3 und Abs. 3 sowie § 44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,
   b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,
   die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

**§ 27 Anwendungsbereich**

(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch

1. nicht-öffentliche Stellen,

2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
   b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.

(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

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

(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.

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) 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

4. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

In den Fällen des Satzes 1 Nr. 3 ist anzunehmen, dass dieses Interesse besteht, wenn im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses gespeicherte Daten übermittelt werden sollen, die sich

1. auf strafbare Handlungen,

2. auf Ordnungswidrigkeiten sowie

3. bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse

beziehen.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten nach Absatz 3 übermittelt werden, der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren.

(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nichtöffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.

(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) 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. 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. 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 Strafgesetzbuchs 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) Für einen anderen Zweck dürren 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. 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) 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. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4aAbs. 3 zulässig. Absatz 3 Nr. 2 gilt entsprechend.

**§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung**

(1) Das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien, dem Adresshandel oder der Markt und Meinungsforschung dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt.

§ 28 Abs. 1 Satz 2 ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. a) der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder
   b) es sich um listenmäßig oder sonst zusammengefasste Daten nach § 28 Abs. 3 Nr. 3 handelt, die für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen, und

2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Abs. 3 Satz 2 gilt entsprechend. Bei der Übermittlung nach Nummer 1 Buchstabe a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Telefon-, Branchen oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

**§ 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form**

(1) Werden personenbezogene Daten geschäftsmäßig erhoben und gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zwecks der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Die Veränderung personenbezogener Daten ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Veränderung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, soweit nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Veränderung offensichtlich überwiegt.

(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.

(4) § 29 gilt nicht.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

**§ 31 Besondere Zweckbindung**

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

**§ 33 Benachrichtigung des Betroffenen**

(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. 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. 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) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

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

2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürren oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen,

4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,

5. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

6. 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,

7. 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 gefährden 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 Personen 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.

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) Der Betroffene kann Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

Er soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene über Herkunft und Empfänger nur Auskunft verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. In diesem Fall ist Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind.

(2) Der Betroffene kann von Stellen, die geschäftsmäßig personenbezogene Daten zum Zweck der Auskunftserteilung speichern, Auskunft über seine personenbezogenen Daten verlangen, auch wenn sie weder in einer automatisierten

Verarbeitung noch in einer nicht automatisierten Datei gespeichert sind. Auskunft über Herkunft und Empfänger kann der Betroffene nur verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt.

(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) Die Auskunft ist unentgeltlich. 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. Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. 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) 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. 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 Zwecks 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 Fall 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 Zweck 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.

**§ 38 Aufsichtsbehörde**

(1) Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5. Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten und nutzen; § 14 Abs. 2 Nr. 1 bis 3, 6 und 7 gilt entsprechend. Insbesondere darf die Aufsichtsbehörde zum Zweck der Aufsicht Daten an andere Aufsichtsbehörden übermitteln. Sie leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe). Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie befugt, die Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten. Sie veröffentlicht regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht. § 21 Satz 1 und § 23 Abs. 5 Satz 4 bis 7 gelten entsprechend.

(2) Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1. Das Register kann von jedem eingesehen werden. Das Einsichtsrecht erstreckt sich nicht auf die Angaben nach § 4e Satz 1 Nr. 9 sowie auf die Angabe der zugriffsberechtigten Personen.

(3) Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

(4) Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. § 24 Abs. 6 gilt entsprechend. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.

(5) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln, kann die Aufsichtsbehörde anordnen, dass im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. Bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie den Einsatz einzelner Verfahren untersagen, wenn die Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.

(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnittes unterliegenden Gewerbebetriebe bleibt unberührt.

§ 38a Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen

(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.

(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

§ 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der verantwortlichen Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht-öffentliche Stelle muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

**§ 43 Bußgeldvorschriften**

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder

11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder

6. entgegen § 30 Abs. 1 Satz 2 die in § 30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 2 Satz 3 die in § 40 Abs. 2 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfundzwanzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu zweihundertfünfzigtausend Euro geahndet werden.

**§ 44 Strafvorschriften**

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde.