Der Bundesbeauftragte
für den Datenschutz

BfD-Info 1

Bundesdatenschutzgesetz
- Text und Erläuterung -

Impressum

Herausgeber:
Der Bundesbeauftragte für den Datenschutz
Postfach 20 01 12, 53131 Bonn
Hausanschrift: Friedrich-Ebert-Str. 1, 53173 Bonn
Tel: (0228) 81995-0, Telefax: (0228) 81995-550
E-Mail: poststelle@bfd.bund.de
Internet: http://www.datenschutz.bund.de

Druck:
Druckhaus Dresden GmbH
Bärensteiner Str. 30, 01277 Dresden

Auflage: 9. Auflage, Januar 2003

Inhaltsverzeichnis

Vorwort

Am 23. Mai 2001 ist das Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze in Kraft getreten, das umfangreiche Neuerungen im Datenschutzrecht gebracht hat. Damit wurden nicht nur die europäische Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 in deutsches Recht umgesetzt, sondern darüber hinaus auch wichtige Anstöße zur Fortentwicklung des Datenschutzes gegeben.

Angesichts der rasanten Entwicklung der Informationstechnik mit weltweiter Vernetzung und Datenübermittlung und immer neuer Formen der elektronischen Kommunikation wachsen auch die Anforderungen an einen effizienten Datenschutz, um dem einzelnen Bürger einen Freiraum in einer globalisierten und vernetzten Welt zu erhalten. Wer die Sammlung, Auswertung und Weitergabe von Daten zu seiner Person durch die verschiedensten Stellen in Staat und Wirtschaft nicht mehr nachverfolgen kann, verliert die Kontrolle darüber und damit auch einen Teil seiner Selbständigkeit und Mündigkeit.

Aus diesem Grunde gilt es, die datenschutzrechtlichen Bestimmungen ständig fortzuentwickeln und neuen Gegebenheiten anzupassen. So enthält das neue Bundesdatenschutzgesetz neben vielen anderen Änderungen und Verbesserungen erstmals den Grundsatz von Datenvermeidung und Datensparsamkeit sowie Vorschriften zur Datenübermittlung ins Ausland, zum Einsatz von Chipkarten und zur Videoüberwachung.

Neben Rechtsvorschriften und datenschutzrechtlicher Kontrolle wird es für einen wirkungsvollen Datenschutz aber immer wichtiger, dass jeder Bürger auch selbst seine persönlichen Daten schützt. Dazu gehören der verantwortungsvolle und zurückhaltende Umgang mit diesen Daten und die Kenntnis und Wahrnehmung der Rechte, die ihm das Bundesdatenschutzgesetz einräumt. Hilfreich soll insoweit auch ein Datenschutzaudit sein.

Hierzu soll diese „BfD-INFO 1“ beitragen. Sie enthält neben dem Gesetzestext und weiteren wichtigen Materialien eine kurze Einführung, die helfen soll, sich die nicht immer einfache Materie zu erschließen. Zugleich eignet sie sich als Basisinformation auch für diejenigen, die beruflich mit personenbezogenen Daten umgehen.

Bonn, März 2002

Dr. Joachim Jacob
Der Bundesbeauftragte für den Datenschutz

1 Der Bundesbeauftragte für den Datenschutz

1.1 Zur Person

Der Bundesbeauftragte für den Datenschutz, Dr. Joachim Jacob, stellt sich vor

Dr. Joachim Jacob wurde 1939 in Bamberg geboren. Er ist verheiratet und hat drei Kinder. Seit 1. Juli 1993 ist er Bundesbeauftragter für den Datenschutz. Im Mai 1998 wurde er erneut für fünf Jahre vom Deutschen Bundestag in sein Amt gewählt.

Seit 1966 war er in verschiedenen Bereichen des Bundesministeriums des Innern tätig, u.a. als persönlicher Referent eines Staatssekretärs, danach als Vizepräsident des Statistischen Bundesamtes und Direktor bei der Bundesakademie für öffentliche Verwaltung. Von 1989 bis zu seiner Wahl als Bundesdatenschutzbeauftragter war er Vertreter des damaligen Bundesbeauftragten. Während der Deutschen EG-Präsidentschaft (2. Halbjahr 1994) hatte er den Vorsitz in der Ratsgruppe „Wirtschaftsfragen (Datenschutz)“. Von 1995 bis September 2001 war er Mitglied im Datenschutzkontrollorgan von Interpol (Supervisory Board for the Internal Control of Interpol’s Archives). Seit 1998 ist er deutscher Vertreter in der Gemeinsamen Kontrollinstanz

und im Beschwerdeausschuss von Europol.

1.2 Zur Institution

Gesetzesbestimmungen: §§ 22 bis 26 Bundesdatenschutzgesetz (BDSG)

Der Deutsche Bundestag hat mit dem Bundesbeauftragten für den Datenschutz eine Institution geschaffen, die ihn unparteiisch und fachkundig über alle Entwicklungen auf dem Gebiet des Datenschutzes unterrichtet und ihm Hinweise gibt, wann und wo er durch Gesetze oder andere Maßnahmen in die Entwicklung eingreifen sollte.
Hauptaufgaben des Bundesbeauftragten für den Datenschutz sind:

- Beratung des Bundestages, der Bundesregierung, aller öffentlichen Stellen des Bundes sowie sonstiger Stellen (vgl. § 26)*,

- Durchführung von Kontrollen (vgl. §§ 24, 25),

- Bearbeitung von Eingaben (vgl. § 21),

- Europäische und internationale Zusammenarbeit in Datenschutzfragen.

Beratung

Der Bundesbeauftragte berät

- den Bundestag und die Bundesregierung durch Erstellen von Tätigkeitsberichten, Erstattung von Gutachten und im Rahmen

von Gesetzgebungsverfahren,

- die Ministerien (auch bei der Vorbereitung von Gesetzen und Vorschriften über den Datenschutz),

- die Behörden und öffentlichen Stellen des Bundes (einschließlich ihrer Personalvertretungen) bei allen Fragen, die mit der praktischen Umsetzung des Datenschutzes verbunden sind.

Eingaben

Der Bundesbeauftragte berät auch im Rahmen seiner Zuständigkeiten die Bürgerinnen und Bürger. Hier wird er bei der Überprüfung von über 4.500 schriftlichen und mündlichen Eingaben und Anfragen im Jahr kontrollierend und auch beratend als Anwalt der Bürgerinnen und Bürger tätig (vgl. S...).

_____

* in Klammern gesetzte Paragraphen sind stets solche des BDSG

Kontrollen

Sehr wichtig ist auch die Kontrolle, ob die rechtlichen Bestimmungen zum Datenschutz umgesetzt und eingehalten werden, damit der Datenschutz nicht nur auf dem bekannt „geduldigen“ Papier steht. Der Bundesbeauftragte kontrolliert alle öffentlichen Stellen des Bundes, also Bundesministerien, Dienststellen des Zolls, des Bundesgrenzschutzes, der Bundeswehr, die Wasser- und Schifffahrtsdirektionen wie auch bestimmte Träger der sozialen Sicherung, z.B. Arbeitsämter, Betriebskrankenkassen oder

Ersatzkassen. Außerdem hat der Bundesbeauftragte die Datenschutzaufsicht über die Telekommunikations- und Postdienstunternehmen inne. Jedes Jahr werden etwa 30 Behörden und Unternehmen in einer mehrtägigen Kontrolle umfassend oder in bestimmten Ausschnitten daraufhin überprüft, ob der Datenschutz eingehalten wird. Dabei geht es bei den Rechtsgrundlagen um das Bundesdatenschutzgesetz oder die bereichsspezifischen Rechtsvorschriften, aber z.B. auch um die Gestaltung von Fragebögen, die Sicherheit in Computernetzen oder die datenschutzgerechte Aktenvernichtung. Kontrolliert wird ebenfalls, ob z.B. Auskunftswünsche von Betroffenen richtig erfüllt worden sind und ob bei Datenübermittlungen an andere Stellen nicht zu großzügig verfahren wird. Die Kontrollergebnisse werden in einem schriftlichen Kontrollbericht niedergelegt.

Tätigkeitsberichte

Wer mehr über die Tätigkeit des Bundesbeauftragten für den Datenschutz wissen möchte, kann dies in seinen Tätigkeitsberichten nachlesen. Der Tätigkeitsbericht, in dem der Bundesbeauftragte für den Datenschutz den Bundestag und die Öffentlichkeit alle zwei Jahre über die wesentlichen Entwicklungen im Datenschutz und die Schwerpunkte seiner Aufgabenwahrnehmung unterrichtet, kann kostenlos beim Bundesbeauftragten angefordert werden.
Der Tätigkeitsbericht bietet dem Bundesbeauftragten auch die Möglichkeit, Kritik und Vorschläge gegenüber dem Parlament und der Öffentlichkeit zu äußern. Hierfür stehen ihm die Mittel der Information, der Empfehlung und

Kritik zur Verfügung. Weisungsrechte besitzt er nicht. Der Bundesbeauftragte hat auch die Möglichkeit, einen festgestellten Datenschutzverstoß bei den Strafverfolgungsbehörden anzuzeigen und Strafantrag zu stellen. Er wirkt aber in aller erster Linie mit der Autorität seiner Argumente, gegründet auf seine herausgehobene Stellung. Die Tätigkeitsberichte finden im Deutschen Bundestag große Beachtung. Sie werden in den zuständigen Ausschüssen beraten. In vielen Fällen hat der Bundestag Anregungen aufgegriffen, etwa

- durch die Aufforderung an die Bundesregierung, den Bundesbeauftragten bei allen datenschutzrelevanten Vorhaben, insbesondere bei Gesetzgebungsvorhaben, frühzeitig zu beteiligen,

- durch die Aufforderung an die Bundesregierung, zu bestimmten Fragen Gesetzentwürfe vorzubereiten, oder

- durch die Aufforderungen an die Bundesregierung, die Verwaltungspraxis in bestimmten Punkten datenschutzfreundlicher zu gestalten oder über bestimmte Problembereiche gesondert Bericht zu erstatten.

Die Rechtsstellung des Bundesbeauftragten für den Datenschutz

Der Bundesbeauftragte für den Datenschutz wird vom Bundestag gewählt. Seine Amtszeit beträgt fünf Jahre. Eine einmalige Wiederwahl ist zulässig.

Hervorzuheben ist, dass der Bundesbeauftragte für den Datenschutz in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen ist. Dies bedeutet z.B., dass weder einzelne Minister noch die Bundesregierung ihm fachaufsichtliche Weisungen in Bezug auf seine Amtstätigkeit geben können. Er untersteht lediglich der Rechtsaufsicht der Bundesregierung und nur hinsichtlich dienstrechtlicher Fragen der Dienstaufsicht des Bundesministeriums des Innern.

Der Bundesbeauftragte für den Datenschutz hat umfassende Untersuchungsbefugnisse. Alle öffentlichen Stellen des Bundes sind verpflichtet, ihn und seine Mitarbeiter bei der Erfüllung ihrer Aufgaben zu unterstützen. Insbesondere müssen sie

- seine Fragen beantworten,
- ihm Einsicht in alle Unterlagen und Akten gewähren, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, und
- ihm jederzeit Zutritt zu allen Diensträumen gestatten.

Der Bundesbeauftragte für den Datenschutz hat auch Zugang zu Unterlagen, die einer besonderen Geheimhaltung unterliegen (vgl. dazu § 24 Abs. 2). Er hat das Recht, jederzeit auch ohne konkreten Anlass, Kontrollen durchzuführen, wobei es keine Rolle spielt, wie die personenbezogenen Daten verarbeitet worden sind, ob automatisiert oder in Akten.

Der Bundesbeauftragte hat ein Zeugnisverweigerungsrecht, darf also auch vor Gericht schweigen und seine Unterlagen jedem

Dritten vorenthalten. Der Bürger kann sich ihm somit anvertrauen, ohne befürchten zu müssen, dass davon etwas nach außen dringt.

Stellt der Bundesbeauftragte Datenschutzverstöße fest, so beanstandet er sie förmlich. Darauf kann er aber verzichten, wenn die Mängel unerheblich sind oder zwischenzeitlich beseitigt wurden. Im Falle einer Beanstandung muss sich das zuständige Ministerium oder die sonstige höchste vorgesetzte Stelle um die Angelegenheit kümmern. Sie wird dann auch prüfen müssen, ob Anlass besteht, über den Einzelfall hinaus korrigierende Maßnahmen zu treffen.

Der Bundesbeauftragte für den Datenschutz nimmt seine Aufgaben derzeit mit knapp 70 Mitarbeiterinnen und Mitarbeitern wahr. Die Organisation seiner seit 1978 bestehenden Dienststelle kann der nachfolgenden Übersicht entnommen werden (Stand: Januar 2002).

Ia Grundsatzangelegenheiten, nicht öffentlicher Bereich

Ib Europäische und internationale Angelegenheiten

II Rechtswesen, Finanzen, Arbeitsverwaltung, Verteidigung, Zivildienst, Auswärtiger Dienst

III Sozialwesen (Renten-, Kranken-, Unfall- und Pflegeversicherung), Personalwesen

IV Wirtschaft und Verkehr, Gesundheit, Forschung, Statistik, Archivwesen, Postdienstunternehmen, Umweltangelegenheiten

V Polizei, Nachrichtendienste

VI Technologischer Datenschutz, Informationstechnik beim Bundesbeauftragten für den Datenschutz

VII Allgemeine Innere Verwaltung, Strafrecht, Behandlung der Unterlagen des ehemaligen Ministeriums für Staatssicherheit der DDR

VIII Telekommunikations-, Tele- und Mediendienste

2 Sicherung des Persönlichkeitsrechts durch das Bundesdatenschutzgesetz

2.1 Das Ziel des Datenschutzes

Gesetzesbestimmungen: § 1 Abs. 1 Bundesdatenschutzgesetz, Art. 1 und 2 Grundgesetz

Ziel des Datenschutzes ist es, den Menschen vor der Gefährdung durch die nachteiligen Folgen einer Datenverarbeitung zu schützen.
Das Gesetz umschreibt seine Zweckbestimmung in § 1 Abs. 1 BDSG wie folgt:

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

Den gleichen Zweck verfolgen

Datenschutzvorschriften in anderen Gesetzen.

Das Persönlichkeitsrecht wird abgeleitet aus den Grundrechten der Verfassung.

„Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist die Verpflichtung aller staatlichen Gewalt.“ (Artikel 1 Abs. 1 Grundgesetz)

„Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“ (Artikel 2 Abs. 1 Grundgesetz)

Diese Verfassungsartikel sind auch die Grundlage des Datenschutzes.

Das Bundesverfassungsgericht hat dazu im sog. Volkszählungsurteil vom 15. Dezember 1983*) folgendes festgestellt:

Das Recht auf informationelle Selbstbestimmung

„Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".

Zur Begründung führt das Gericht aus:

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle

Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."

Das Recht auf informationelle Selbstbestimmung soll es dem Einzelnen ermöglichen, sich seine Privatsphäre zu erhalten, und verhindern, dass er deshalb in zunehmende Abhängigkeit von Stellen in Staat und Wirtschaft gerät, weil diese immer mehr von ihm wissen.

Allerdings braucht der moderne Rechts- und Sozialstaat auch in großem Umfang personenbezogene Daten, um seine vielfältigen Aufgaben fachlich richtig und gerecht erfüllen zu können.
Die Sozialämter, die Schulen, die Steuerbehörden und die Polizei könnten ihre Aufgaben nicht ordentlich erfüllen, wenn sie allein auf die freiwillige Mitwirkung der Menschen angewiesen wären. Das Recht auf informationelle Selbstbestimmung kann deshalb nicht schrankenlos sein. Das hat auch das Bundesverfassungsgericht festgestellt, zugleich aber eindeutige Grenzen für Einschränkungen dieses Rechts bestimmt:

Einschränkungen des Rechts auf informationelle Selbstbestimmung sind nur aufgrund eines Gesetzes zulässig.

Das Gesetz muss

- im überwiegenden Allgemeininteresse erforderlich sein,

- die Voraussetzungen für die Einschränkung des Grundrechts und deren Umfang für den Bürger erkennbar regeln, also dem Gebot der Normenklarheit entsprechen und

- den Grundsatz der Verhältnismäßigkeit beachten.

Wenn Gesetze in das Recht auf informationelle Selbstbestimmung des Einzelnen eingreifen, dann muss der Gesetzgeber folgende Punkte beachten:

- Nur das erforderliche Minimum an Daten darf verlangt werden.

- Die Daten dürfen grundsätzlich nur für den Zweck verwendet werden, für den sie erhoben oder erfasst wurden.

- Der Gesetzgeber muss durch ergänzende Vorkehrungen dafür sorgen, dass auch bei der Organisation und beim Verfahren des Umgangs mit personenbezogenen Daten auf die Rechte des Einzelnen Rücksicht genommen wird (z.B. durch Mitwirkungs- und Kontrollrechte).

Das Recht auf den Schutz personenbezogener Daten wurde auch in Art. 8 der Charta der Grundrechte der Europäischen Union aufgenommen. Die Charta ist jedoch noch nicht rechtsverbindlicher Bestandteil der Europäischen Verträge. Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.

Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr**) gibt in Art. 1 Abs. 1 den Mitgliedsstaaten vor, nach den Bestimmungen der Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

Die Novellierung des BDSG vom 18. Mai 2001, in Kraft getreten am 23. Mai 2001, dient unter anderem der Umsetzung der Richtlinie in deutsches Recht. Wesentliche Bestimmungen des überarbeiteten BDSG werden im folgenden vorgestellt.

_____

***)** Ein Auszug aus dem Volkszählungsurteil ist als Anhang 3 abgedruckt
****)** Als Anhang 2 abgedruckt

2.2 Rahmenbedingungen für einen wirksamen Datenschutz

Das Bundesdatenschutzgesetz stellt allgemeine datenschutzrechtliche Grundregeln auf. Diese Grundregeln passen allerdings nicht überall. Und sie sind nicht überall ausreichend. Man braucht nur etwa an die Gesundheits- und Sozialbehörden, die Meldeämter, die Polizei und den Verfassungsschutz zu denken. Darum gibt es zahlreiche datenschutzrechtliche Spezialregelungen in anderen Gesetzen.
Es sind dies z.B.:

- Sozialgesetzbuch,
- Straßenverkehrsgesetz,
- Melderechtsrahmengesetz,
- Bundeszentralregistergesetz,

- Ausländerzentralregistergesetz,
- Bundesverfassungsschutzgesetz,
- Bundesgrenzschutzgesetz,
- Telekommunikationsgesetz,
- Postgesetz,
- Informations- und Kommunikationsdienste-Gesetz und andere mehr.

Diese sog. „**bereichsspezifischen Regelungen**“ gehen dem Bundesdatenschutzgesetz vor.
In einer vernetzten Welt mit rasanten Entwicklungen im Bereich der Informationstechnologie, in der überall Daten gesammelt werden, kann aber auch der Schutz des informationellen Selbstbestimmungsrechtes nicht über das Recht allein gewährleistet werden. Es reicht daher nicht aus, nur einen rechtlichen Rahmen zu schaffen.

Vielmehr funktioniert auch und besonders der Datenschutz in einer vernetzten Welt nur durch das Zusammenspiel verschiedenster Maßnahmen. Maßnahmen der rechtsausfüllenden Selbstregulierung durch die Wirtschaft, Selbstschutzvorkehrungen des Einzelnen, vor allem aber der Einsatz datenvermeidender und datensparsamer Technik müssen ineinander greifen.

Dieses Zusammenwirken ein wenig durchschaubarer zu machen, ist das Ziel dieser Broschüre:

Ausgangspunkt ist das neue Bundesdatenschutzgesetz. Auch wenn gesetzliche Regelungen allein nicht genügen, sind sie unabdingbare Voraussetzung für alle anderen Maßnahmen zum Schutz des informationellen Selbstbestimmungsrechtes. Das

Bundesdatenschutzgesetz trägt zur Sicherung des Datenschutzes bei, indem es Regeln für den Umgang mit personenbezogenen Daten aufstellt. Dabei geht das Bundesdatenschutzgesetz davon aus, dass jegliche Verarbeitung von personenbezogenen Daten einer ausdrücklichen Erlaubnis bedarf, sei es über ein Gesetz oder über eine ausdrücklich erteilte Einwilligung des Einzelnen. Es enthält Schutzregelungen für das informationelle Selbstbestimmungsrecht bezüglich der Datenverarbeitung, die die Datenverarbeiter zu beachten haben. Diese begründen spiegelbildlich auch die Rechte der von der Datenverarbeitung betroffenen Bürgerinnen und Bürger. Das Gesetz verpflichtet die Datenverarbeiter also von vorneherein, die rechtlichen „Spielregeln“ der Datenverarbeitung zu beachten, den Bürger in bestimmten Fällen zu informieren und zu benachrichtigen. Es weist aber auch den betroffenen Bürgern eine Reihe von Rechten ausdrücklich zu.

Das Gesetz setzt bereits bei der Vorbeugung an. Vorrangiges Ziel des Datenschutzes ist es, eine Gefährdung des Persönlichkeitsrechts des Einzelnen von vorneherein zu verhindern, durch das Aufstellen von Regeln und die Nutzbarmachung der Technik. „Datenschutzfreundliche Technik“ soll eingesetzt werden, um möglichst ohne personenbezogene Daten, oder – wo das nicht möglich ist – mit so wenig wie möglich personenbezogenen Daten auszukommen. Riesige Datenmengen sollen erst gar nicht entstehen. Die technisch-organisatorischen Maßnahmen, die nach § 9 Bundesdatenschutzgesetz und seiner dazu ergangenen Anlage zu treffen sind, sollen dann die Datenverarbeitung über Organisation und Einsatz von Technik sichern.

Erforderlich ist auch eine Datenschutzaufsicht, die sich nicht nur als begleitende und ggf. sanktionierende Kontrollinstanz versteht, sondern einen Schwerpunkt in der vorbeugenden Beratung von Datenverarbeitern, aber auch von Bürgerinnen und Bürgern sieht. Behörden und Unternehmen, Bürgerinnen und Bürger sollten daher keine Scheu haben, dort Rat zu suchen.

In einer Informationsgesellschaft mit einer immer größer werdenden Flut unterschiedlichster Formen der Datenverarbeitung und Informationsgewinnung können aber auch Kontrollbehörden nicht überall sein. Alle Rechte und technischen Möglichkeiten sind nur begrenzt von Nutzen, wenn Bürgerinnen und Bürger sie nicht kennen, von ihnen keinen Gebrauch machen und sich auch selbst und eigenverantwortlich nicht gegen einen möglichen Missbrauch ihrer Daten schützen.

Dabei können und sollten sie die Hilfe der Datenschutzaufsichtsbehörden in Anspruch nehmen. Auch die Verantwortung der datenverarbeitenden Stellen muss hier greifen. Sie sind aufgerufen, im Rahmen der Gesetze eigene selbstverpflichtende Regelungen innerhalb ihrer Branchen oder auch im internationalen Rahmen zu entwickeln.
Eine besonders wichtige Rolle haben auch die Datenschutzbeauftragten inne, die sich als Institution in der Privatwirtschaft bewährt haben und die jetzt auch für alle öffentlichen Stellen im Geltungsbereich des Bundesdatenschutzgesetzes vorgeschrieben sind. Ihre Aufgabe ist es, auf die Sicherung des Datenschutzes hinzuwirken. Sie sind wichtige Ansprechpartner für Bürgerinnen und Bürger

ebenso wie für die Beschäftigten ihrer Organisationen.

Das neue Bundesdatenschutzgesetz ermöglicht im Zusammenwirken von Wirtschaft und Datenschutzaufsicht vielfältige neue Perspektiven für selbstregulierte Schutzmaßnahmen im Datenschutz.

Wenn es dann doch zu einem Verstoß gegen Datenschutzrecht und einem Schaden gekommen ist, bleibt dies nicht ohne Folgen. Der Gesetzgeber hat hier im neuen Bundesdatenschutzgesetz Straf- und erweiterte Bußgeldvorschriften vorgesehen. Es gibt auch erstmals einen einheitlichen eigenständigen Schadensersatzanspruch. Er ist anzuwenden sowohl für die öffentlichen Stellen als auch für die Privatwirtschaft.

Aber, es gilt: „*Vorbeugen ist besser, also seien Sie ihr eigener Datenschutzbeauftragter!*“

2.3 Der Anwendungsbereich des Bundesdatenschutzgesetzes

Gesetzesbestimmungen: §§ 1 Abs. 2, 2, 12, 27, 34 Abs. 2 BDSG

Das Bundesdatenschutzgesetz gilt uneingeschränkt für öffentliche Stellen des Bundes und für nicht öffentliche Stellen (Private). Nur sehr eingeschränkt gilt es für die öffentlichen Stellen der Länder.

Aber welche Stellen sind damit genau gemeint?

Öffentliche Stellen des Bundes sind

- Behörden des Bundes,
- Organe der Rechtspflege des Bundes,
- andere öffentlich-rechtlich organisierte Einrichtungen im Bundesbereich (z.B. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts unter Bundesaufsicht),
- bestimmte Vereinigungen öffentlicher Stellen des Bundes und bestimmte von diesen beherrschte Unternehmen, Gesellschaften oder Einrichtungen, auch in privater Rechtsform.

Öffentliche Stellen der Länder sind

- Behörden der Länder,
- Organe der Rechtspflege der Länder,
- andere öffentlich-rechtlich organisierte Einrichtungen im Landes- und Kommunalbereich,
- bestimmte Vereinigungen, Gesellschaften, Unternehmen und Einrichtungen öffentlicher Stellen eines Landes, auch in privater Rechtsform.

Das BDSG gilt aber nur, soweit

- der Datenschutz nicht im gleichen Umfang durch ein Landesdatenschutzgesetz geregelt ist (dann gilt nur dieses) und
- diese Stellen Bundesrecht ausführen oder als

Organe der Rechtspflege (ausgenommen Verwaltungsangelegenheiten) tätig werden.

Die Länder haben jeweils ein Landesdatenschutzgesetz; nähere Informationen geben die Landesdatenschutzbeauftragten (Anschriften siehe Anhang 4).

Nicht öffentliche Stellen sind

- natürliche Personen,
- juristische Personen des Privatrechts,
- Personenvereinigungen des Privatrechts;

aber nicht, soweit sie hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen (also als „beliehene Unternehmer“ tätig werden).

Nicht öffentliche Stellen unterliegen dem BDSG aber nur, soweit

- sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder
- Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben.

Ausgenommen ist die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten.

Das BDSG ist auch schon bei der Erhebung personenbezogener Daten zu beachten. Dies ist besonders wichtig, damit der Umgang mit den personenbezogenen Daten von Anfang an in die

richtigen Bahnen gelenkt wird.

Ebenso wichtig ist, dass das BDSG im öffentlichen Bereich auch für Daten in Akten und anderen Unterlagen gilt. Über die bereits genannten Einschränkungen im nicht öffentlichen Bereich hinaus gilt das BDSG dort auch für solche personenbezogenen Daten, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

Ferner gilt das Auskunftsrecht gegenüber Kreditauskunfteien und anderen geschäftsmäßigen Datenverarbeitern auch außerhalb einer automatisierten Verarbeitung oder einer Verarbeitung in nicht automatisierten Dateien, also auch für Daten in Akten.

2.4 Grundsätzlich ist verboten, was nicht ausdrücklich erlaubt ist!

Gesetzesbestimmungen: §§ 4, 4a BDSG

Verarbeitung und Nutzung sind verboten, ...

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gilt als allgemeiner Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt. Das bedeutet, die Erhebung, Verarbeitung und Nutzung von Daten sind verboten, es sei denn,

es sei denn, ...

- sie sind durch das BDSG oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet oder

eine Rechtsvorschrift oder der Betroffene erlauben sie.

- der Betroffene hat dazu seine Einwilligung erklärt.

Wenn eine Rechtsvorschrift den Umgang mit personenbezogenen Daten ausdrücklich erlaubt oder sogar anordnet, kommt es auf die

Einwilligung des Betroffenen nicht an.

Soll eine Einwilligung Grundlage für eine Erhebung, Verarbeitung oder Nutzung sein, ist zu beachten:

- Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

- Der Betroffene ist vorher über die Tragweite seiner Einwilligung aufzuklären (z.B. über den Zweck der Erhebung, Verarbeitung oder Nutzung); soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen ist er auch darüber zu informieren, was geschieht, wenn er nicht einwilligt (z.B. dass Ansprüche verloren gehen können).

Die Einwilligung muss auf der freien Entscheidung des Betroffenen beruhen; d.h. sie muss frei von Zwang sein. In diesem Zusammenhang ist auch zu berücksichtigen, ob sich der Betroffene in einer besonderen Situation (z.B. Arbeitsverhältnis) befindet, oder ob auf Grund einer faktischen Situation (beispielsweise Monopolstellung desjenigen, der die Einwilligung einholen will) ein Zwang besteht.

Bei der Verarbeitung besonderer Arten personenbezogener Daten gem. § 3 Abs. 9 BDSG (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

2.5 Der Zweckbindungsgrundsatz

Gesetzesbestimmungen: §§ 14, 28, 29 BDSG

Öffentliche Stellen

Die Speicherung, Veränderung und Nutzung personenbezogener Daten durch öffentliche Stellen ist zulässig, wenn

Zweckentfremdung ist grundsätzlich verboten, ...

- dies zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und

- sie für die Zwecke erfolgt, für die die Daten erhoben worden sind (falls keine Erhebung voranging: für die sie gespeichert worden sind). Hiermit wird der Zweckbindungsgrundsatz angesprochen. Das heißt, dass personenbezogene Daten grundsätzlich nur zu den Zwecken verarbeitet werden dürfen, für die sie erhoben beziehungsweise gespeichert worden sind. Von diesem Grundsatz sieht das Gesetz aber eine Reihe zum Teil weitreichender Ausnahmen vor.

Welche Ausnahmen von der Zweckbindung gibt es?

aber eine Verwendung für einige andere Zwecke erlaubt das Gesetz

Die Verarbeitung personenbezogener Daten für einen anderen Zweck ist dann zulässig, wenn

- eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
- der Betroffene eingewilligt hat,
- es offensichtlich im Interesse des Betroffenen liegt,
- Angaben des Betroffenen überprüft werden müssen, weil begründete Zweifel an ihrer

Richtigkeit bestehen,
- die Daten allgemein zugänglich sind oder veröffentlicht werden dürften (aber nicht, wenn das entgegenstehende schutzwürdige Interesse des Betroffenen offensichtlich überwiegt),

oder wenn sie

- zur Gefahrenabwehr, oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
- zur Verfolgung von Straftaten oder Ordnungswidrigkeiten,
- zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte eines anderen oder
- zur Durchführung wissenschaftlicher Forschung (nach näher bestimmten Voraussetzungen)

erforderlich ist.

Für die zweckändernde Verarbeitung oder Nutzung besonderer Arten personenbezogener Daten gilt eine Sonderregelung. Unter anderem ist danach eine Zweckänderung zulässig, wenn die Daten für den geänderten Zweck erhoben werden dürften (vgl. § 13 Abs. 2 Nr. 1 - 6 oder 9). Sonderregelungen gelten auch für eine zweckändernde Verarbeitung von besonderen personenbezogenen Daten zur Durchführung wissenschaftlicher Forschung beziehungsweise für die Zwecke des § 13 Abs. 2 Nr. 7 – Gesundheitsvorsorge, medizinische Diagnostik und Weiteres (vgl. § 14 Abs. 5 und 6).

Auf der anderen Seite stellt das Gesetz klar, dass bestimmte Verwendungen von Daten nicht als Zweckänderung anzusehen sind, so die Verwendung für

Hier liegt keine Zweckentfremdung vor.

- die Rechnungsprüfung,
- die Wahrnehmung von Aufsichts- und Kontrollbefugnissen,
- Organisationsuntersuchungen sowie
- Ausbildungs- und Prüfungszwecke der speichernden Stelle, aber nur, soweit nicht überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen (z.B. bei sehr persönlichen Angaben).

Eine strikte Zweckbindung besteht für Daten, die ausschließlich gespeichert werden zu Zwecken

Und hier gilt die Zweckbindung strikt.

- der Datenschutzkontrolle,
- der Datensicherung,
- der Sicherung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage oder
- der wissenschaftlichen Forschung (§ 40).

Nicht öffentliche Stellen

Für die nicht öffentlichen Stellen gilt der Zweckbindungsgrundsatz ebenfalls. Bereits bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen (vgl. § 28 Abs. 1 Satz 2). Dies gilt auch für die geschäftsmäßige Datenverarbeitung (vgl. § 29 Abs. 1 Satz 2). Einen Ausnahmekatalog zu dem Grundsatz der Zweckbindung gibt es auch für den nicht öffentlichen Bereich:

Danach kommt eine Verwendung für andere Zwecke in Betracht

- zur Wahrung berechtigter Interessen der verantwortlichen Stelle,
- wenn die Daten allgemein zugänglich sind oder veröffentlicht werden dürften,
- zu wissenschaftlichen Zwecken,

- für Zwecke der Werbung, der Markt- oder Meinungsforschung bei listenmäßiger Übermittlung (siehe hierzu unter dem Kapitel „Besonderheiten bei der Datenverarbeitung durch nicht öffentliche Stellen").

Erforderlich ist stets eine Abwägung nach Maßgabe des Gesetzes zwischen den entgegenstehenden schutzwürdigen Interessen des Betroffenen und dem Interesse an der Zweckänderung.

2.6 Die Datenerhebung

Gesetzesbestimmungen: §§ 4, 13, 28, 29 BDSG

Die Erhebung von Daten ist sowohl bei öffentlichen Stellen als auch bei den nicht öffentlichen Stellen von den Zulässigkeitsregelungen für die Datenverarbeitung umfasst.

Maßstab ist die Aufgabe bzw. der Vertrag und dessen Zweck

Die Datenerhebung darf nur in dem erforderlichen Umfang erfolgen. Bei den öffentlichen Stellen heißt dies, dass sie für die Erfüllung der gesetzlichen Aufgaben notwendig sein muss. Im nicht öffentlichen Bereich wird der größte Teil der personenbezogenen Daten von den Stellen als Mittel für die Erfüllung eigener Geschäftszwecke verwendet. Dies ist z.B. der Fall bei den Kundendaten einer Firma, den Daten über das eigene Personal, über die Lieferanten und andere Geschäftspartner.

- Bei einem Vertragsverhältnis (oder vertragsähnlichen Vertrauensverhältnis) mit dem Betroffenen (etwa zwischen Bank und Bankkunden, Arzt und Patienten, Versicherung und Versicherten; entsprechend

eingeschränkt auch schon vor Vertragsabschluss und nach dessen Ende) ist Maßstab für die Datenerhebung der Vertrag und dessen Zweck.

- Die Datenerhebung kann auch erforderlich sein zur Wahrung berechtigter Interessen der verantwortlichen Stelle. Hier darf kein Grund zu der Annahme bestehen, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung das Interesse der verantwortlichen Stelle an der Datenerhebung überwiegen.

- Auch wenn Daten allgemein zugänglich sind oder veröffentlicht werden dürften, können sie für eigene Geschäftszwecke erhoben werden, es sei denn, schutzwürdige Interessen des Betroffenen würden gegenüber den berechtigten Interessen der verantwortlichen Stelle offensichtlich überwiegen.

- Besondere Arten personenbezogener Daten (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) dürfen – ohne wirksame Einwilligung des Betroffenen – nur in vom Gesetz abschließend aufgeführten Ausnahmefällen erhoben werden.

Zum Beispiel gilt dies:

- zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten,

- bei Daten, die der Betroffene offenkundig öffentlich gemacht hat,

- für wissenschaftliche Forschungszwecke nach Güterabwägung

und in weiteren im Einzelnen aufgeführten Ausnahmetatbeständen (vgl. §§ 13 Abs. 2 Nr. 1 - 9, 28 Abs. 6 Nr. 1 – 4, sowie Absatz 7 - 9, 29 Abs. 5).
Bei der Datenverarbeitung der öffentlichen Stellen wird häufig die Ausnahme greifen, die das Erheben besonderer Arten personenbezogener Daten erlaubt, soweit eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert.

Keine heimliche Datenerhebung

- Die Daten sind grundsätzlich beim Betroffenen zu erheben. Es ist ihm mitzuteilen, zu welchem Zweck dies geschieht. Nur in Ausnahmefällen dürfen die Daten bei anderen und ohne Kenntnis des Betroffenen erhoben werden.

Offen und direkt beim Betroffenen

- Ist der Betroffene gegenüber einer öffentlichen Stelle zur Auskunft verpflichtet (z.B. bei amtlichen Statistiken), so muss ihm gesagt werden, nach welchen Rechtsvorschriften das der Fall ist. Er ist auch aufzuklären, wenn er ohne die von ihm verlangten Auskünfte seine Ansprüche nicht durchsetzen kann oder ihm sonstige Rechtsvorteile entgehen.

- Andernfalls muss dem Betroffenen gesagt werden, dass die Auskunft freiwillig ist

Ausnahmen:

Ausnahmen von der Datenerhebung beim Betroffenen

Ohne Mitwirkung des Betroffenen (z.B. durch Anfragen bei Behörden oder anderen Stellen) dürfen Daten nur erhoben werden, wenn

- eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt (z.B. Einholung eines Strafregisterauszugs nach dem Bundeszentralregistergesetz) oder

- die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht und keine Beeinträchtigung überwiegender schutzwürdiger Interessen des Betroffenen zu erwarten ist,

- die Erhebung beim Betroffenen einen unverhältnismäßig hohen Aufwand zur Folge hätte (z.B., weil er sehr schwer zu finden ist) und auch hier keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Ob die befragte Stelle die erbetenen Daten übermitteln darf, muss diese aber besonders prüfen.

Wenn die personenbezogenen Daten beim Betroffenen erhoben werden, so muss er, wenn er nicht bereits auf andere Weise Kenntnis hat, informiert werden. Er hat Anspruch darauf zu erfahren,

- welche die verantwortliche Stelle ist, die die Daten erhoben hat,

- welche die Zweckbestimmung für die erhobenen Daten ist,

- und gegebenenfalls auch, welche die Kategorien von Empfängern der Daten sind, sofern er nach den Umständen des Einzelfalls

nicht mit einer Übermittlung an diese rechnen muss.

Nur so ist gewährleistet, dass der Betroffene im Weiteren seine Datenschutzrechte wahrnehmen kann.

2.7 Die Übermittlung von Daten

Gesetzesbestimmungen: §§ 4b, 4c, 15, 16, 28 - 30, 39 BDSG

Übermittlung nach Erforderlichkeit...

Für öffentliche Stellen kennt das Gesetz unterschiedliche Regelungen, je nachdem, ob an

- eine andere öffentliche Stelle oder
- eine nicht öffentliche Stelle

übermittelt wird.

Besondere Regelungen sowohl für die öffentlichen als auch für die nicht öffentlichen Stellen gelten für die Datenübermittlungen an eine Stelle im Ausland.

Das Übermitteln an eine öffentliche Stelle ist zulässig, wenn

- es für die Aufgabenerfüllung der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, erforderlich ist und

- der Verwendungszweck beim Dritten, an den die Daten übermittelt werden, gleich ist oder eine zulässige Zweckänderung vorliegt.

Werden Daten zur Erfüllung der eigenen

Aufgaben an eine nicht öffentliche Stelle übermittelt, so gelten dieselben Regelungen wie bei einer Übermittlung an eine öffentliche Stelle (siehe vorstehend).

oder nach Interessenabwägung.

Die Übermittlung an eine nicht öffentliche Stelle ist außerdem zulässig, wenn der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt hat und der Betroffene keine schutzwürdigen Interessen am Ausschluss der Übermittlung hat. Der Betroffene muss in diesen Fällen informiert werden. Dies gilt nicht, wenn er von der Übermittlung schon auf anderem Wege weiß oder die öffentliche Sicherheit einer Unterrichtung im Wege steht.

Besondere Vorschriften gelten wiederum für die Übermittlung besonderer Arten personenbezogener Daten (vgl. § 3 Abs. 9).
Wie bereits dargelegt, gilt der Zweckbindungsgrundsatz auch bei der Übermittlung im nicht öffentlichen Bereich. Zu weiteren Besonderheiten im nicht öffentlichen Bereich siehe das Kapitel „Besonderheiten bei der Datenverarbeitung durch nicht öffentliche Stellen“ (Seite ....).

Wann ist die Übermittlung ins Ausland zulässig?

Gesetzesbestimmungen: §§ 4b, 4c BDSG

Für die Übermittlung in sog. „Drittländer“ außerhalb der EU gilt: zulässig nur, wenn

Für die Datenübermittlung ins Ausland gelten besondere Regelungen für die öffentlichen wie die nicht öffentlichen Stellen.

Der Datenverkehr innerhalb der Mitgliedstaaten

der Europäischen Union – also innerhalb des Europäischen Binnenmarktes – und mit den anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum im Anwendungsbereich des Gemeinschaftsrechts ist genauso zu behandeln wie der inländische (vgl. § 4b Abs. 1).

-kein schutzwürdiges Ausschlussinteresse des Betroffenen besteht

-ein angemessenes Datenschutzniveau besteht.

Die Datenübermittlung in ein Land außerhalb der Europäischen Union, sog. „Drittland“, ist zulässig, wenn der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat, insbesondere in dem Drittland ein angemessenes Datenschutzniveau gewährleistet ist.
Das gleiche gilt innerhalb der Europäischen Union außerhalb des Anwendungsbereiches des Gemeinschaftsrechts; d.h., in den Bereichen der nicht dem Binnenmarkt zuzurechnenden zweiten und dritten Säule. Damit sind die gemeinsame Außen- und Sicherheitspolitik sowie die Zusammenarbeit auf den Gebieten Justiz und Inneres gemeint.

Wie ist das angemessene Datenschutzniveau festzustellen?

Ob in einem Land ein angemessenes Datenschutzniveau besteht, kann festgestellt werden

Kriterien für das angemessene Schutzniveau sind: „Art der Daten, Zweckbestimmung...“

- durch die verantwortliche Stelle selbst, die Daten übermitteln will nach den Kriterien „Art der Daten, Zweckbestimmung, Dauer der geplanten Verarbeitung, Herkunft und Bestimmungsland, für den Empfänger geltende Rechtsnormen, Standesregeln und Sicherheitsmaßnahmen“ (vgl. § 4b Abs. 3),

- durch die EU-Kommission nach Art. 25 Abs. 6

der EU-Richtlinie (so bisher geschehen für die Schweiz und Ungarn).

- Ein Sonderweg wurde für den Datenverkehr mit den USA geschaffen. Es handelt sich um die sogenannten „Safe Harbor Principles“, kurz „safe harbor“ („sicherer Hafen“). Die nach nationalem Recht zulässige Datenübermittlung ist danach als Datenübermittlung in die USA zulässig, sofern sich der dortige Datenempfänger freiwillig den Regelungen von „safe harbor“ unterworfen hat.

Ausnahmen:

Darüber hinaus kommt eine Übermittlung an einen Drittstaat auch im Rahmen weitreichender Ausnahmeregelungen in Betracht (vgl. § 4c Abs. 1).

Bedeutsam ist auch die Genehmigung der Übermittlung durch die zuständige Datenschutzaufsichtsbehörde (vgl. § 4c Abs. 2).

2.8 Die vorherige Kontrolle risikoreicher Datenverarbeitung (sog. Vorabkontrolle)

Gesetzesbestimmungen: §§ 4d Abs. 5 und 6, 4g und 4e BDSG

Für automatisierte Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, sieht das BDSG eine Prüfung vor Beginn der Verarbeitung (Vorabkontrolle) vor (vgl. § 4d Abs. 5).

Beispiele für die Vorabkontrolle

Beispielhaft – nicht abschließend – nennt das Gesetz zwei Fallgestaltungen, in denen die

Vorabkontrolle notwendig ist:

- bei der Verarbeitung von personenbezogenen Daten besonderer Art (§ 3 Abs. 9),
- bei Verfahren, die dazu dienen, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.

Ausnahme:

Die Vorabkontrolle ist nicht durchzuführen in folgenden Fällen:

- gesetzliche Verpflichtung zur Durchführung der Datenverarbeitung,
- Einwilligung des Betroffenen,
- Erhebung, Verarbeitung oder Nutzung im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses.

Zuständig für die Durchführung der Vorabkontrolle ist der Datenschutzbeauftragte. Dem Datenschutzbeauftragten sind von der verantwortlichen Stelle für die Datenverarbeitung vor der Durchführung der Vorabkontrolle bestimmte Informationen zur Verfügung zu stellen (vgl. § 4g Abs. 2 Satz 1 i.V.m. § 4e Satz 1).

2.9 Die technischen und organisatorischen Maßnahmen

Gesetzesbestimmungen: §§ 9, 10 BDSG

Ein sehr wichtiger, oft arbeits- und kostenintensiver Bereich des Datenschutzes sind die technischen und organisatorischen

Maßnahmen für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten, die getroffen werden müssen, damit diese vor Missbrauch, Fehlern und Unglücksfällen möglichst sicher sind. Welche Maßnahmen notwendig sind, hängt nicht nur von der Art der Daten ab, sondern ebenso von der Aufgabe, den organisatorischen Bedingungen, den räumlichen Verhältnissen, der personellen Situation und anderen Rahmenbedingungen. Das Gesetz verzichtet deshalb darauf, bestimmte einzelne Maßnahmen zwingend vorzuschreiben, sondern verlangt nur allgemein,

> *„die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften dieses Gesetzes ... zu gewährleisten.“*

Welche Wirkung diese Maßnahmen im Bereich der automatisierten Verarbeitung haben müssen, legt das Gesetz in Form einer Anlage zu § 9[*)] katalogmäßig fest. Die Maßnahmen müssen beispielsweise geeignet sein,

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren,

- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können,

- zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich im Rahmen ihrer Zugriffsberechtigung zugreifen können und personenbezogene Daten bei der Verarbeitung, Nutzung und nach der

Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,

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

Die technisch-organisatorische Umsetzung verlangt ein abgestimmtes Konzept

Bei den technischen und organisatorischen Maßnahmen ist von entscheidender Bedeutung, dass sie als ein zusammenwirkendes Schutzsystem verstanden werden. Viele Maßnahmen des Datenschutzes wirken zugleich im Sinne einer Sicherung eines ordentlichen Betriebsablaufs. Deshalb ist es wichtig, das Datenschutzkonzept jeweils in engem Zusammenhang mit sonstigen Sicherheitskonzepten zu entwickeln und anzuwenden.

Während das Gesetz allgemein in Bezug auf technische Fragen eher zurückhaltend ist, stellt es für die Einrichtung eines **automatisierten Verfahrens zum Abruf personenbezogener Daten** durch Dritte genaue Anforderungen auf, weil es darin eine besonders einschneidende Maßnahme sieht.

Damit die Zulässigkeit des Abrufverfahrens kontrolliert werden kann, müssen die beteiligten Stellen folgendes schriftlich festlegen:

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

Die Einrichtung des automatisierten Abrufverfahrens ist nur zulässig, wenn es unter

Berücksichtigung der schutzwürdigen Interessen der Betroffenen einerseits und der Aufgaben oder Geschäftszwecke der beteiligten Stellen andererseits angemessen ist.

---

*) Der volle Text der Anlage ist am Ende des Gesetzes abgedruckt.

2.10 Der Beauftragte für den Datenschutz – neu verpflichtend vorgeschrieben im öffentlichen Bereich, eine bewährte Institution im Bereich der Privatwirtschaft

Gesetzesbestimmungen: §§ 4f, 4g BDSG

Mit den §§ 4f, 4g BDSG werden einheitliche Bestimmungen für die Institution eines Beauftragten für den Datenschutz im öffentlichen wie im nicht öffentlichen Bereich geschaffen.

Die behördlichen und betrieblichen Beauftragten für den Datenschutz sind wichtige Ansprechpartner in Fragen des Datenschutzes für die Bürgerinnen und Bürger sowie die Beschäftigten in den Behörden und Unternehmen.
Alle Behörden im Anwendungsbereich des Bundesdatenschutzgesetzes müssen einen behördlichen Beauftragten für den Datenschutz bestellen. Je nach Struktur der Stelle genügt auch die Bestellung eines Beauftragten für mehrere Bereiche. Bei den nicht öffentlichen Stellen hängt die Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz von der Größe der Stelle und der Zahl der mit der Verarbeitung personenbezogener Daten beschäftigten Arbeitnehmer ab. Die freiwillige Bestellung eines Datenschutzbeauftragten mit der Folge, dass ggf.

eine sonst erforderliche Meldepflicht bei der Aufsichtsbehörde entfällt, ist immer möglich. Bei der geschäftsmäßigen Datenverarbeitung zum Zweck der Übermittlung oder anonymisierten Übermittlung muss immer ein Datenschutzbeauftragter bestellt werden. Dies gilt auch stets, wenn wegen besonders risikoreicher Datenverarbeitung eine Vorabkontrolle durchgeführt werden muss (siehe Seite ..... Vorabkontrolle). Der Beauftragte für den Datenschutz hat nach dem Gesetz eine herausgehobene Stellung, die sich darin zeigt, dass er dem Leiter der öffentlichen oder nicht öffentlichen Stelle unmittelbar zu unterstellen ist. Um seine Unabhängigkeit in der Wahrnehmung seiner fachlichen Aufgaben zu gewährleisten, bestimmt das Gesetz, dass er in der Ausübung seiner Fachkunde weisungsfrei ist. Damit kann ihm niemand, auch nicht der Leiter der Stelle, vorschreiben, wie er datenschutzrechtliche Fragen bewertet. Der Leiter der Stelle kann sich aber über das Votum des Datenschutzbeauftragten hinwegsetzen. Denn letztlich trägt er die Verantwortung für die datenverarbeitende Stelle.

Um der hohen Bedeutung des Datenschutzbeauftragten für einen wirkungsvollen Datenschutz Rechnung zu tragen, darf nach dem Gesetz für diese Aufgabe nur bestellt werden, wer die erforderliche „Fachkunde und Zuverlässigkeit“ besitzt. Der fachkundige Datenschutzbeauftragte muss also sowohl die technische als auch die rechtliche Seite seiner Aufgaben kennen und gute Kenntnisse in allen Bereichen haben, die für die Organisation, in der er arbeitet, von Bedeutung sind. Nur so hat er die notwendigen Voraussetzungen, dem Datenschutz in seiner Organisation Geltung zu verleihen.

Besonders bedeutsam für alle, die sich mit einer datenschutzrechtlichen Beschwerde oder Frage an ihn wenden, ist die gesetzliche Verschwiegenheitspflicht des Datenschutzbeauftragten. Über die Identität des Betroffenen (Beschwerdeführers) oder Umstände, die Rückschlüsse hierüber erlauben, darf er keine Auskünfte geben. Eine Ausnahme gilt nur, wenn die betroffene Person ihn von seiner Verschwiegenheitsverpflichtung befreit.

Die Aufgaben des Datenschutzbeauftragten sind vielfältig. Insbesondere muss er:

Aufgabenkatalog

- auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz hinwirken,
- die ordnungsgemäße Programmanwendung überwachen,
- die bei der Verarbeitung personenbezogener Daten eingesetzten Mitarbeiterinnen und Mitarbeiter mit den Anforderungen des Datenschutzes vertraut machen,
- zum Schutz des informationellen Selbstbestimmungsrechtes die für besonders risikoreiche Datenverarbeitungen erforderliche Vorabkontrolle durchführen,
- die öffentlich zugänglichen Angaben des Verfahrensverzeichnisses (vgl. § 4e Satz 1, Nr. 1 - 8) in geeigneter Weise auf Antrag jedermann verfügbar machen. Einer besonderen Berechtigung oder Begründung bedarf es für denjenigen, der von diesem Recht Gebrauch machen möchte, nicht.

Die öffentlichen und nicht öffentlichen Stellen müssen dem Datenschutzbeauftragten eine Übersicht über die in § 4e Satz 1 BDSG genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung stellen. Sie sind auch im übrigen verpflichtet, ihn insgesamt bei der Erfüllung seiner Aufgaben zu unterstützen.

Zum Schutz des Datenschutzbeauftragten, auch mit dem Ziel der Absicherung seiner Unabhängigkeit, bestimmt das Gesetz, dass er nicht wegen der Erfüllung seiner Aufgaben benachteiligt werden darf. Seine Bestellung kann nur unter erschwerten Bedingungen widerrufen werden.

2.11 Das Datenschutzaudit

Gesetzesbestimmung: § 9a BDSG

Datenschutzrechtliches Gütesiegel für technische Produkte sowie Datenschutzkonzepte

Mit dem sogenannten "Datenschutzaudit" können sowohl Anbieter von Datenverarbeitungssystemen und –programmen als auch datenverarbeitende Stellen ihre Datenschutzkonzepte sowie ihre technischen Einrichtungen mit einem datenschutzrechtlichen Gütesiegel versehen lassen.

Hier wird der hohen Bedeutung der Förderung des Datenschutzes durch den Einsatz von Technik und von datenschutzgerechten Gesamtkonzepten Rechnung getragen, in dem diese auch ökonomisch als Wettbewerbsvorteil über das Gütesiegel belohnt werden. Die Prüfung soll durch unabhängige und zugelassene Gutachter erfolgen.

Veröffentlichung des Ergebnisses

Das Ergebnis der Prüfung kann veröffentlicht werden. Alle weiteren Anforderungen an das Verfahren sind einer noch ausstehenden besonderen gesetzlichen Regelung vorbehalten.

2.12 Was hat sich geändert?

Wesentliche Änderungen durch das neue Recht sind:

- Der Anwendungsbereich des BDSG für nicht öffentliche Stellen wurde dahingehend erweitert, dass jegliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus automatisierter Verarbeitung oder in oder aus nicht automatisierten Dateien erfasst wird; ausgenommen sind lediglich Erhebung, Verarbeitung oder Nutzung für ausschließlich persönliche oder familiäre Tätigkeiten.
- Bereits bei der Datenerhebung ebenso wie für alle weiteren Phasen der Datenverarbeitung gilt der Zweckbindungsgrundsatz; Ausnahmen sind gesetzlich geregelt.
- Die Datenerhebung auch im nicht öffentlichen Bereich wird unter den gesetzlichen Erlaubnisvorbehalt gestellt (gesetzliche Grundlage oder Einwilligung) anstelle der früheren Regelung der „Datenerhebung nach Treu und Glauben“.
- Der Grundsatz, Daten nur im erforderlichen Umfang zu verarbeiten und Datenvermeidung durch den Einsatz technischer Verfahren zu betreiben, ist jetzt gesetzlich festgeschrieben.
- Es wurden Regelungen geschaffen zur Übermittlung personenbezogener Daten in das Ausland – auch für den nicht öffentlichen Bereich.

- Es wurde eine einheitlichen Rechtsgrundlage für den Beauftragten für den Datenschutz eingeführt, der damit auch für den öffentlichen Bereich vorgeschrieben wird.
- Für automatisierte Verfahren, die das Persönlichkeitsrecht besonders gefährden, ist eine vorherige Kontrolle durch den Beauftragten für den Datenschutz geboten (sog. Vorabkontrolle).
- Es wurde ein datenschutzrechtliches Gütesiegel für technische Systeme sowie Datenschutzkonzepte (Datenschutzaudit) geschaffen.

3 Besonderheiten bei der Datenverarbeitung durch nicht öffentliche Stellen, Privatwirtschaft, Vereine etc.

3.1 Die Datenverarbeitung für eigene Zwecke

Gesetzesbestimmung: § 28 BDSG

Listenmäßige Übermittlung ist möglich...

Eine Besonderheit gilt bei der Datenverarbeitung für eigene Zwecke durch nicht öffentliche Stellen für die sogenannte listenmäßige oder sonst zusammengefasste Übermittlung von Daten für Zwecke der Werbung, der Markt- oder Meinungsforschung.
Danach gestattet der Gesetzgeber die Übermittlung eines bestimmten Kataloges von Daten. Dieser Katalog besteht aus

- einer nicht näher bestimmten Angabe:

Zugehörigkeit des Betroffenen zu einer bestimmten Personengruppe (sogenanntes freies Merkmal),
- Berufs-, Branchen- oder Geschäftsbezeichnungen,
- Namen,
- Titel,
- Akademische Grade,
- Anschrift,
- Geburtsjahr.

Übermittlungsfähig wären danach z.B. im Rahmen einer listenmäßigen Übermittlung die katalogmäßig genannten Daten zusätzlich zu der Angabe, dass es sich bei der Person, deren Daten übermittelt werden, um einen Wanderer handelt. Wenn dann außerdem noch übermittelt würde, welche Automarke der Wanderer fährt, wäre aber der zulässige Umfang bei der listenmäßigen Übermittlung bereits überschritten.

aber, es dürfen keine sensiblen Angaben enthalten sein

Eine listenmäßige Übermittlung ist nicht zulässig,
- wenn es um die folgenden sensiblen Angaben geht:
  - strafbare Handlungen,
  - Ordnungswidrigkeiten,
  - arbeitsrechtliche Verhältnisse
- und, wenn diese Angaben im Zusammenhang mit einem Vertragsverhältnis (oder vertragsähnlichem Vertrauensverhältnis) gespeichert worden sind.

Für andere sensitive Daten wie die gesundheitlichen Verhältnisse oder die politischen Meinungen und religiösen Überzeugungen gelten die besonderen Regelungen für die Übermittlung besonderer Arten personenbezogener Daten (vgl. § 28 Abs. 6).

Achtung:
Widerspruchsrecht!

Zum Ausgleich der erleichterten Vorschriften für die Datenverarbeitung im Bereich Werbung-, Markt- und Meinungsforschung hat der Betroffene hier zusätzliche Rechte.
Er kann diesen Übermittlungen widersprechen und, wenn schon Daten übermittelt worden sind, bei dem Dritten, dem diese übermittelt wurden, die Sperrung verlangen. Bereits bei der Ansprache für die Zwecke der Werbung-, Markt- oder Meinungsforschung muss der Betroffene über sein Widerspruchsrecht und die verantwortliche Stelle für die Datenverarbeitung informiert werden. Wenn die werbende Stelle personenbezogene Daten des Betroffenen nutzt, die bei einer Stelle gespeichert sind, die ihr nicht bekannt ist, muss sie sicherstellen, dass der Betroffene auch hier Kenntnis über die Herkunft der Daten erhalten kann. Häufig ist dies der Fall bei der Einschaltung von Adressmittlern. Dies sind Direktwerbeunternehmen, die für ein werbendes Unternehmen – auch unter Einsatz von Fremdadressen – tätig werden. Auch sog. Lettershops, die für ein Unternehmen Werbeschreiben versenden, ohne eigene Datenbestände für diese Zwecke zu führen, sind hier gemeint. Durch das Recht auf Kenntnis über die Herkunft der Daten ist gesichert, dass der Betroffene auch erfährt, an wen er seinen Widerspruch adressieren muss.

Der Dritte, an den die Daten übermittelt worden sind, darf diese nur unter den auch für die übermittelnde Stelle geltenden Voraussetzungen für andere Zwecke verarbeiten oder nutzen.
Wer keine Werbung per Post erhalten möchte, kann sich in die sogenannte „Robinson-Liste“ eintragen lassen. Für den Bereich Fax, E-Mail und SMS gibt es ebenfalls Robinson-Listen, auch

wenn eine unangeforderte Werbung außerhalb einer bestehenden Geschäftsbeziehung per Fax, E-Mail und SMS ohnehin als grundsätzlich unzulässig, weil kostenverursachend und belästigend, anzusehen ist.

- Wer **keine Werbung per Post** wünscht, fordert ein Antragsformular unter folgender Anschrift an:

  Deutscher Direkt-Marketing-Verband
  - Robinson-Liste -
  Postfach 14 01
  71243 Ditzingen
  Telefon: 07156 / 95 10 10 .

- Wer **keine Werbung per Fax** wünscht, ruft per Fax ein Antragsformular ab beim

  Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V. (BITKOM)
  unter der Telefax-Nummer: 01805/00 07 61.

- Wer **keine Werbung per E-Mail** wünscht, kann seine E-Mail-Adresse eintragen

  in die vom Interessenverband Deutsches Internet e.V. und der Gesellschaft zum Schutz privater Daten in elektronischen Informations- und Kommunikationsdiensten e.V. geführten Deutschen Mailschutzliste

  http://www.robinsonliste.de .

- Wer **keine Werbung per SMS** wünscht, trägt seine Telefonnummer online in die vom

  Interessenverband Deutsches Internet e.V.

(I.D.I)
geführte SMS-Schutzliste ein

http://www.sms-robinson.de .

Der Vollständigkeit halber sei darauf hingewiesen, dass die Nutzung dieser Listen durch die Werbewirtschaft freiwillig ist. Ein Eintrag dort garantiert nicht, dass man überhaupt keine Werbung mehr erhält.

Ferner gibt die Deutsche Telekom die Daten, die auf Wunsch des Kunden in das Telefonverzeichnis und ggf. in ein elektronisches Verzeichnis (z.B. CD-ROM) aufgenommen werden sollen, an die

Deutsche Telekom Medien GmbH
Postfach 16 02 11
60065 Frankfurt a. M.
Tel. : 069/2682-0

weiter. Auch zu einem späteren Zeitpunkt kann der Kunde gegenüber der Telekom einer Eintragung widersprechen; bei der Neuauflage des Telefonverzeichnisses darf dann seine Anschrift nicht mehr ausgedruckt sein (Näheres zur Telekommunikation siehe BfD-Info 5).

3.2 Die geschäftsmäßige Datenverarbeitung zum Zweck der Übermittlung

Gesetzesbestimmungen: §§ 29, 30 BDSG

Auch die geschäftsmäßige Datenverarbeitung unterliegt den allgemeinen Zulässigkeitsvoraussetzungen. Geschäftsmäßige

Datenverarbeitung liegt vor, wenn im Rahmen einer auf Dauer angelegten Tätigkeit die Datenverarbeitung als solche den Geschäftszweck bildet. Das Gesetz selbst nennt als Beispiele die geschäftsmäßige Datenverarbeitung zum Zweck der Übermittlung, wenn dies der Werbung, der Tätigkeit von Auskunfteien, dem Adresshandel oder der Markt- und Meinungsforschung dient.
Auf der Grundlage des § 29 BDSG ist es zulässig, personenbezogene Daten zum Zweck der Übermittlung zu erheben, zu speichern oder zu verändern, wenn entweder

- eine Abwägung mit den schutzwürdigen Interessen des Betroffenen ergibt, dass kein Grund zu der Annahme besteht, dass dieser ein Ausschlussinteresse an der Verarbeitung hat, oder
- die Daten aus allgemein zugänglichen Quellen entnommen werden können bzw. veröffentlicht werden dürften. Auch hier ist eine Güterabwägung mit den schutzwürdigen Interessen des Betroffenen an einem Ausschluss der Verarbeitung vorzunehmen. Die Verarbeitung ist danach nicht zulässig, wenn die schutzwürdigen Ausschlussinteressen des Betroffenen offensichtlich überwiegen.

Wie bereits dargelegt (vgl. Seite ##), gilt der Grundsatz der Zweckbindung der Daten auch bei der geschäftsmäßigen Datenverarbeitung schon bei der Erhebung sowie für die weitere Verarbeitung.

Bei einer zulässigen Übermittlung listenmäßig zusammengefasster Daten gilt auch hier das Widerspruchsrecht des Betroffenen einschließlich der diesbezüglichen Informationspflicht über das

Widerspruchsrecht bei der Ansprache zu Zwecken der Werbung, Markt- oder Meinungsforschung. Der Betroffene hat auch hier einen Anspruch auf Sperrung seiner Daten.

Kein Eintrag in Adress- und vergleichbare Verzeichnisse gegen den Willen des Betroffenen

Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Telefon-, Branchen- oder vergleichbare Verzeichnisse muss unterbleiben, wenn der entsprechende entgegenstehende Wille des Betroffenen aus dem zugrundeliegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist.

Für Markt- und Meinungsforschungsinstitute und andere Stellen, die geschäftsmäßig Daten speichern, um sie in anonymisierter Form zu übermitteln, besteht eine Verpflichtung, Namen und Adressen gesondert zu speichern. Eine Befugnis, Daten in personenbezogener Form ohne Einwilligung des Betroffenen weiterzugeben, haben sie nicht.

3.3 Was hat sich geändert?

Wesentliche Änderungen im neuen Recht sind:

- Strikte Geltung des Zweckbindungsgrundsatzes auch bei den nicht öffentlichen Stellen und zwar sowohl bei
  - der Datenverarbeitung für eigene Zwecke,
  - als auch bei der geschäftsmäßigen Datenverarbeitung,
- Einbeziehung der Datenerhebung unter Beachtung des Zweckbindungsgrundsatzes,

- Stärkung der Rechte der von der Datenverarbeitung betroffenen Bürgerinnen und Bürger

    - durch die unter Nr. 2.5 erwähnten Neuerungen
    - sowie im Bereich der Datenverarbeitung für Zwecke der Werbung-, Markt- und Meinungsforschung durch eine Unterrichtungspflicht gegenüber den Betroffenen über ihr Widerspruchsrecht und die für die Datenverarbeitung verantwortlichen Stellen,

- Schaffung besonderer Regelungen für die Erhebung, Verarbeitung und Nutzung sensitiver Daten

- und Erweiterung der Rechte der betroffenen Bürgerinnen und Bürger bei der Aufnahme in Adressverzeichnisse, Telefonbücher und vergleichbare Verzeichnisse. Jeder muss den entgegenstehenden dokumentierten Willen der Betroffenen respektieren.

4 Rechte der Bürgerinnen und Bürger

Welche Rechte die Bürgerinnen und Bürger im Zusammenhang mit der Erhebung, Verarbeitung und Nutzung ihrer Daten haben, regelt das BDSG unter der Überschrift „Rechte des Betroffenen“ (zur Definition des Begriffes „Betroffener“ siehe unter § 3 Abs. 1, bzw. in Kapitel 6).
Aber auch an anderer Stelle trifft das BDSG

Regelungen für bestimmte Bereiche, z.B. für die Videoüberwachung, bei denen sich aus den Pflichten für die datenverarbeitenden Stellen spiegelbildlich die Rechte der Bürgerinnen und Bürger ergeben.

4.1 Das Recht auf Auskunft

Gesetzesbestimmungen: §§ 19, 19a, 33, 34 BDSG

Jeder – unabhängig von Alter, Wohnsitz und Nationalität – hat das Recht auf Auskunft über die zu seiner Person gespeicherten Daten.

Welche Auskunft können Sie verlangen?

- Über die zu Ihrer Person gespeicherten Daten, einschließlich der Angabe, woher sie stammen und an wen sie weitergegeben werden.
  Das BDSG spricht hier von Empfängern oder Kategorien von Empfängern. Der Begriff des Empfängers umfasst nicht nur Dritte außerhalb der verantwortlichen Stelle, sondern auch natürliche Personen oder Stellen, die im Geltungsbereich des BDSG für einen anderen im Auftrag Daten verarbeiten sowie auch verschiedene Organisationseinheiten innerhalb einer Stelle. Auch die Information über die Kategorien der Empfänger kann für den Einzelnen von erheblicher Bedeutung sein, z.B. macht es einen Unterschied, ob es sich bei den Empfängern um natürliche Personen handelt, oder um bestimmte Branchen oder Unternehmen wie z.B. Auskunfteien oder andere geschäftsmäßige Datenverarbeiter

etc.,

- über den Zweck der Speicherung (d.h. die betreffende Verwaltungsaufgabe oder den speziellen Geschäftszweck).

Wie erhalten Sie Auskunft?

Gehen Sie gezielt vor!

- Es empfiehlt sich, die Auskunft schriftlich anzufordern. Zur Legitimation genügt es in der Regel, die Kopie eines Personaldokuments beizulegen. Einschreiben ist nicht erforderlich.

- Bei persönlicher Vorsprache wird eine sofortige Erledigung oft nicht möglich sein.

- Wenn Sie anrufen, kann man Sie meist nicht sicher identifizieren. Deshalb gilt der Grundsatz: Keine telefonische Datenauskunft.

- Schreiben Sie möglichst genau, worüber Sie Auskunft wünschen (also z.B. *„meine Daten im Zusammenhang mit Wohngeld" oder „im Zusammenhang mit unserem Mietvertrag"*, aber nicht *„alles, was die Stadtverwaltung über mich hat"*).

Wenden Sie sich an die verantwortliche Stelle. Wer als verantwortliche Stelle infrage kommt, erfahren Sie im nachfolgenden Kapitel „Das Einsichtsrecht in das Verfahrensverzeichnis“. Außerdem können Ihnen die Datenschutzkontrollinstitutionen weiterhelfen (Anhänge 4 und 5).

Was kostet eine Auskunft?

Grundsätzlich brauchen Sie für die Auskunft nichts zu bezahlen. Es gibt hierzu aber

Ausnahmen:

- Schriftliche Auskünfte von Kreditauskunfteien und ähnlichen Einrichtungen, die Sie gegenüber Dritten wirtschaftlich nutzen können (etwa um Ihre Bonität nachzuweisen). Das geforderte Entgelt darf nicht höher sein als die entstandenen direkt zurechenbaren Kosten. Aber auch bei derartigen Auskünften brauchen Sie dafür nichts zu bezahlen, wenn besondere Umstände dafür sprechen, dass Daten unrichtig oder unzulässig gespeichert sind oder sich dies aus der Auskunft ergibt.

- Bei einer mündlichen Auskunft oder einer Auskunft auf einem Blatt ohne Namensangabe entstehen Ihnen keine Kosten. Auf die Möglichkeit, durch persönliche Kenntnisnahme die Auskunft unentgeltlich zu erhalten, muss die speichernde Stelle Sie ausdrücklich hinweisen.

Was ist an Besonderheiten zu beachten?

Bei öffentlichen Stellen

Für eine Auskunft aus Akten müssen Sie mithelfen.

- Über personenbezogene Daten in Akten erhalten Sie nur Auskunft, wenn

  - Sie Angaben machen, die das Auffinden der Daten ermöglichen, und

  - der Arbeitsaufwand nicht außer Verhältnis zu Ihrem Informationsinteresse steht. Legen Sie deshalb dar, warum Ihnen die Auskunft wichtig ist.

- Eine Auskunft darüber, ob Daten an einen Nachrichtendienst (Bundesamt für

Verfassungsschutz, Militärischer Abschirmdienst und Bundesnachrichtendienst) übermittelt wurden, ist nur mit dessen Zustimmung zugelassen.

Bei nicht öffentlichen Stellen

- Von Kreditauskunfteien und anderen Stellen, die geschäftsmäßig Daten zum Zweck der Übermittlung speichern, können Sie Auskunft auch über Daten verlangen, die weder in einer automatisierten Verarbeitung noch in einer nicht-automatisierten Datei gespeichert sind (z.B. ungeordnete Akten oder Hefter).

- Diese Stellen müssen Ihnen auch sagen, woher sie Ihre Daten haben und an wen sie die Daten weitergeben, es sei denn, die Stelle könnte geltend machen, dass ihr Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber Ihrem Auskunftsinteresse überwiegt.

In welchen Fällen hat man keinen Anspruch auf Auskunft?

Öffentliche Stellen verweigern die Auskunft, soweit

Nicht immer gibt es eine Auskunft

- sonst die Gefahr besteht, dass sie ihre Aufgabe nicht ordnungsgemäß erfüllen können, z.B. wenn laufende polizeiliche Ermittlungen gefährdet würden,

- es notwendig ist zum Schutz der öffentlichen Sicherheit oder Ordnung (kommt nur selten vor) oder

- die Daten oder die Tatsache, dass die Stelle

sie speichert, geheim gehalten werden müssen (aus gesetzlichen Gründen oder im Geheimhaltungsinteresse eines Dritten, z.B. Adoptionsgeheimnis; im übrigen sehr selten), und deswegen das Interesse des Betroffenen an der Auskunft zurücktreten muss. Die Auskunft darf aber nie pauschal abgelehnt werden, sondern nur nach sorgfältiger Abwägung im Einzelfall.

Nicht öffentliche Stellen dürfen eine Auskunft nur in Fällen ablehnen, in denen auch keine Benachrichtigungspflicht besteht (Einzelheiten in § 34 Abs. 4 i.V.m. § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 - 7).

Was tun, wenn die Auskunft verweigert wird?

Sie haben grundsätzlich Anspruch auf eine vollständige Auskunft, d.h. alle Angaben, für die nach dem Gesetz grundsätzlich eine Auskunftsverpflichtung besteht, müssen Ihnen mitgeteilt werden.

Soweit die auskunftspflichtige Stelle von einer der oben beschriebenen gesetzlichen Möglichkeiten Gebrauch macht und nur teilweise Auskunft erteilt, muss sie auf die Unvollständigkeit der Auskunft ausdrücklich hinweisen, damit Sie die Möglichkeit haben, eine Überprüfung zu verlangen.

Im allgemeinen ist die auskunftserteilende Stelle auch verpflichtet zu begründen, aufgrund welcher gesetzlichen Bestimmung und aufgrund welcher Tatsachen sie eine Auskunft über bestimmte Punkte ablehnt. Eine solche Begründung ist nur entbehrlich, wenn sonst der mit der Auskunftsverweigerung verfolgte Zweck (z.B.

laufende polizeiliche Ermittlungen nicht zu behindern) gefährdet würde.

Hier bekommen Sie Hilfe

Haben Sie Zweifel, ob Ihnen korrekt Auskunft erteilt worden ist, können Sie sich an die zuständige Datenschutzkontrollinstitution wenden. Fügen Sie Ihren Schriftwechsel in Kopie bei. Ihr Vorgang wird dann umfassend überprüft, und Sie erhalten in jedem Fall Bescheid, ob Ihre Rechte beachtet wurden (siehe auch Nr. 4.8). Sie haben außerdem die Möglichkeit einer gerichtlichen Klage.

4.2 Das Einsichtsrecht in das Verfahrensverzeichnis

Gesetzliche Bestimmungen: §§ 4g Abs. 2, 4d sowie 4e, 38 Abs. 2 BDSG

Die Behörden und öffentlichen Stellen des Bundes führen ebenso wie die verantwortlichen Stellen im nicht öffentlichen Bereich eine Übersicht über ihre automatisierten Verarbeitungen, in denen personenbezogene Daten gespeichert werden. Diese kann von jedermann eingesehen werden.

Es ist Aufgabe des behördlichen und betrieblichen Datenschutzbeauftragten, auf Antrag die Angaben in dem Verfahrensverzeichnis den Antragstellern in geeigneter Weise verfügbar zu machen. Wenn eine Stelle im nicht öffentlichen Bereich keinen Datenschutzbeauftragten hat und auch nach dem Gesetz nicht meldepflichtig ist, muss das Einsichtsrecht von der Stelle selbst gewährleistet werden. Der Inhalt des Verzeichnisses kann Ihnen Anhaltspunkte geben, bezogen auf welche

Daten Sie Ihr Auskunftsrecht ausüben möchten. Bis auf die allgemeine Beschreibung, die es ermöglicht, die Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu beurteilen, sind alle Angaben öffentlich.

Es handelt sich hier um folgende Angaben:

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.

Die öffentlichen Stellen des Bundes müssen darüber hinaus die Rechtsgrundlage der Verarbeitung angeben.

Hinweis: Dem Verzeichnis kann also nicht entnommen werden, ob überhaupt und, wenn ja, welche Daten gerade über Sie oder eine andere Person wo gespeichert sind.

Ausnahmen:

Nicht öffentlich einsehbar sind die Verzeichnisse folgender Behörden

- Verfassungsschutzbehörden,
- Bundesnachrichtendienst,
- Militärischer Abschirmdienst,
- andere Behörden des Bundesministers der Verteidigung, soweit die Sicherheit des Bundes berührt wird,
- Staatsanwaltschaft und Polizei,
- öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern.

4.3 Die Rechte auf Benachrichtigung, Berichtigung, Sperrung oder Löschung

Die Benachrichtigung

Gesetzesbestimmungen: §§ 19 a, 33 BDSG

Ein anderes wichtiges Mittel, damit Sie wissen (können), wer welche Daten über Sie verarbeitet, ist die Benachrichtigung.

Wann werden Sie benachrichtigt?

Jede verantwortliche Stelle ist verpflichtet, alle Betroffenen individuell zu benachrichtigen, über die sie Daten **ohne deren Kenntnis** erhoben hat und deren Daten sie speichern oder verarbeiten möchte.

Der Zeitpunkt der Benachrichtigung ist unterschiedlich. Bei öffentlichen Stellen muss die Unterrichtung, sofern eine Übermittlung vorgesehen ist, spätestens bei der ersten Übermittlung erfolgen. Im nicht öffentlichen Bereich (Privatwirtschaft) benachrichtigen die

Stellen, die geschäftsmäßig personenbezogene Daten verarbeiten, ebenfalls erst bei der erstmaligen Übermittlung. Die nicht öffentlichen Stellen, die personenbezogene Daten für eigene Zwecke verarbeiten, müssen bereits zum Zeitpunkt der ersten Speicherung benachrichtigen.

Die Benachrichtigung muss umfassen:

- Angabe der verantwortlichen Stelle (öffentliche Stelle bzw. Firma, Anschrift),
- die Tatsache, dass erstmals Daten über die Person, die benachrichtigt wird, gespeichert oder übermittelt werden, und
- die Art der Daten,
- die Zweckbestimmung der Erhebung bei Verarbeitung oder Nutzung
- sowie die Empfänger oder Kategorien von Empfängern, soweit der Betroffene nicht mit der Übermittlung an diese rechnen muss.

Ausnahmen!

In bestimmten im Gesetz genannten Fällen erfolgt keine Benachrichtigung, etwa weil eine überwiegende Geheimhaltungspflicht besteht, die Unterrichtung einen unverhältnismäßigen Aufwand erfordert oder der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat (vgl. hierzu im Einzelnen §§ 19a Abs. 2, 33 Abs. 2).

Das Recht auf Berichtigung

Gesetzesbestimmungen: §§ 20, 35 BDSG

Wann sind personenbezogene Daten zu berichtigen?

Jede Stelle ist verpflichtet, **unrichtige Daten zu berichtigen**. Es liegt aber auch am Betroffenen

selbst, darauf hinzuweisen, wenn Daten unrichtig oder überholt sind.

In nicht dateimäßig strukturierten Akten werden unrichtige Daten nicht durch richtige ausgetauscht, es wird aber ein Berichtigungsvermerk beigefügt. Ebenso ist zu vermerken, wenn der Betroffene die Richtigkeit bestreitet.

Wann sind personenbezogene Daten zu löschen?

Daten, die man nicht haben dürfte oder nicht mehr braucht, sind zu löschen

Von öffentlichen Stellen, wenn

- ihre Speicherung unzulässig ist, etwa weil schon die Erhebung unzulässig war, oder
- die Kenntnis der Daten für die Aufgabenerfüllung nicht mehr erforderlich ist.

Von nicht öffentlichen Stellen, wenn

- die Speicherung unzulässig ist, etwa weil schon die Erhebung unzulässig war, oder
- 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, oder
- für eigene Zwecke verarbeitete Daten für die Erfüllung des Speicherungszwecks nicht mehr erforderlich sind, oder
- geschäftsmäßig zum Zweck der Übermittlung verarbeitete Daten aufgrund einer am Ende des vierten Kalenderjahres nach der ersten Speicherung vorzunehmenden Prüfung nicht mehr erforderlich sind (z.B. bei Auskunfteien

und Adressverlagen).

Eine Löschung ist nur für personenbezogene Daten vorgesehen, die entweder aus automatisierter Datenverarbeitung stammen oder aus einer manuellen Datei, jedoch nicht für einzelne Daten, die in nicht dateimäßig strukturierten Akten festgehalten sind. Sind allerdings komplette Akten unzulässig angelegt, so sind sie ebenfalls zu vernichten. Ebenso ist im allgemeinen mit nicht mehr erforderlichen Akten zu verfahren.

Wann sind personenbezogene Daten zu sperren?

Personenbezogene Daten sind immer dann zu sperren, wenn einer fälligen Löschung besondere Gründe entgegenstehen, etwa

- gesetzlich, satzungsmäßig oder vertraglich festgelegte Aufbewahrungsfristen,
- schutzwürdige Interessen des Betroffenen, etwa weil ihm Beweismittel verloren gingen, oder
- ein unverhältnismäßig hoher Aufwand wegen der besonderen Art der Speicherung.

Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu sperren, wenn der Betroffene ihre Richtigkeit bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

Öffentliche Stellen haben personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, zu sperren, wenn sie im Einzelfall

feststellen, dass sonst schutzwürdige Interessen des Betroffenen beeinträchtigt würden, und sie die Daten nicht mehr zur Aufgabenerfüllung benötigen.

Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn dies

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

4.4 Das Widerspruchsrecht

Gesetzesbestimmungen § 20 Abs. 5, 35 Abs. 5 BDSG

Wann greift das Widerspruchsrecht?

Das Widerspruchsrecht nach § 20 Abs. 5 und § 35 Abs. 5 BDSG richtet sich gegen rechtmäßige Datenverarbeitungen.

Es handelt sich hier um Ausnahmetatbestände

Der Widerspruch ist begründet,

- sofern besondere Umstände in der Person des Betroffenen vorliegen,
- und das schutzwürdige Interesse des Betroffenen das Interesse der verantwortlichen Stelle an der Erhebung, Verarbeitung oder Nutzung der entsprechenden personenbezogenen Daten überwiegt.

Achtung

Es gibt kein Widerspruchsrecht, wenn eine Rechtsvorschrift eine Verpflichtung zur Erhebung, Verarbeitung oder Nutzung vorschreibt.

4.5 Die Rechte bei automatisierten Einzelentscheidungen

Gesetzesbestimmung: § 6a BDSG

Welches sind die Rechte bei automatisierten Einzelentscheidungen?

Die Maschine darf nicht über den Menschen entscheiden!
Diesen Grundsatz setzt das BDSG in der Regelung zur automatisierten Einzelentscheidung in § 6a BDSG um.

Danach dürfen Entscheidungen,

- die für den Betroffenen eine rechtliche Folge nach sich ziehen
- oder ihn erheblich beeinträchtigen,

nicht ausschließlich auf automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Was ist hier gemeint? Gemeint sind automatisierte Entscheidungsverfahren, die beispielsweise die berufliche Leistungsfähigkeit, die Kreditwürdigkeit, die Zuverlässigkeit oder eine sonstige Verhaltensweise betreffen können.

Ein Beispiel ist das sog. „Scoring-Verfahren“, das u. a. von Kreditauskunfteien verwandt wird. Scoring-Verfahren, auch Punktwertverfahren genannt, stellen eine auf mathematisch-statistischen Verfahren gründende Auswertungsmethode dar, die eine Mehrzahl von

Menschen oder Merkmalen in eine Reihenfolge nach einem oder mehreren Kriterien bringt. Der ermittelte Score-Wert wird dann als Risikoprognose an Vertragspartner weitergegeben. Solche Verfahren können durchaus zulässig sein. Maßgeblich ist, dass eine für den Betroffenen negative Entscheidung nicht allein auf einen Score-Wert gestützt wird.

Das Verbot der automatisierten Entscheidung gilt nicht,

- wenn die Entscheidung im Rahmen eines Vertragsverhältnisses oder sonstigen Rechtsverhältnisses ergeht und dem Anliegen des Betroffenen stattgegeben wird,
- wenn die berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet sind
- und der Betroffene von der verantwortlichen Stelle über die Tatsache des Vorliegens einer automatisierten Entscheidung (nach § 6a Abs. 1) informiert wird.

Als eine geeignete Maßnahme zur Sicherung der Interessen des Betroffenen gilt insbesondere, wenn ihm die Möglichkeit eingeräumt wird, seinen Standpunkt geltend zu machen und die verantwortliche Stelle daraufhin ihre Entscheidung erneut überprüft. Die erneute Überprüfung darf dann nicht in ausschließlich automatisierter Form erfolgen.

Besonderes Auskunftsrecht bei automatisierten Entscheidungen

Als weitere Besonderheit bei automatisierten Einzelentscheidungen bezieht sich das Auskunftsrecht des Betroffenen auch auf den logischen Aufbau des Verfahrens (vgl. § 6a Abs. 3).
Dem Betroffenen müssen nicht alle Einzelheiten der verwandten Software mitgeteilt werden. Er

hat aber einen Anspruch über die tragenden Funktionsprinzipien der Programme informiert zu werden. Wenn Standardsoftware verwandt wird, genügt auch deren genaue Bezeichnung.

4.6 Die Rechte beim Einsatz von Videoüberwachung

Gesetzesbestimmung: § 6b BDSG

§ 6b bestimmt die Voraussetzungen, unter denen die „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen“ (Videoüberwachung) zulässig ist. Unter "öffentlich zugänglichem Raum" ist der Raum zu verstehen, in dem sich jedermann berechtigt aufhalten kann, ohne in irgendwelche Rechtsbeziehungen zum Inhaber des Hausrechts dieses Raumes treten zu müssen. Im Einzelfall bedarf es der Auslegung, was darunter zu fassen ist. Beispiele für öffentlich zugängliche Räume sind Kaufhäuser, Bürgersteige oder auch Einkaufspassagen. Nicht erfasst ist die Beobachtung im Arbeitnehmerbereich innerhalb von Unternehmen oder Behörden.

Wann ist die Videoüberwachung zulässig?

Erlaubt ist die Überwachung

- zur Aufgabenerfüllung öffentlicher Stellen,
- zur Wahrnehmung des Hausrechts oder

zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke, soweit sie erforderlich ist. Das bedeutet, dass immer zu prüfen ist, ob es für den angestrebten Zweck wirklich einer Videoüberwachung bedarf, welche Alternativen es hierzu möglicherweise gibt, und ob nicht in das Persönlichkeitsrecht weniger einschneidende Maßnahmen infrage kommen.

Voraussetzungen

1. Erforderlichkeits-prüfung

2. Güterabwägung

Ist danach die Videoüberwachung erforderlich, sind weiterhin die mit der Videoüberwachung verfolgten Zwecke gegen die schutzwürdigen Interessen der von der Überwachung Betroffenen abzuwägen. Ergeben sich hier Anhaltspunkte, dass schutzwürdige Interessen der Betroffenen überwiegen, ist die Videoüberwachung ebenfalls unzulässig.

Keine heimliche Beobachtung!

Eine heimliche Beobachtung ist unzulässig. Die Videoüberwachung muss durch geeignete Maßnahmen kenntlich gemacht werden. Da bei einer Videoüberwachung öffentlich zugänglicher Räume damit gerechnet werden muss, dass Menschen verschiedener Nationalitäten erfasst werden, sollten die Hinweisschilder mehrsprachig sein. Die hier zu stellenden Anforderungen müssen nach der Lage im Einzelfall beurteilt werden.

Wenn nicht nur eine Beobachtung erfolgen soll, sondern auch eine Verarbeitung oder Nutzung (Speicherung der Filme/Auswertung), sind weitere Zulässigkeitsschranken zu beachten.

So hat eine erneute Prüfung der Erforderlichkeit für die weitere Verarbeitung oder Nutzung zu erfolgen. Kontrollfrage: Genügt nicht die einfache Beobachtung?

Auch eine neue Abwägung mit den schutzwürdigen Interessen des Betroffenen ist durchzuführen.

Benachrichtigung

Wenn die durch Videoüberwachung erhobenen Daten einer bestimmten Person zugeordnet werden, muss diese Person über die Verarbeitung oder Nutzung entsprechend §§ 19a

und 33 BDSG benachrichtigt werden. So ist gewährleistet, dass diese von der Überwachung und der anschließenden Auswertung Kenntnis erhält und selbst für die Wahrung ihrer Rechte eintreten kann.

Unverzügliche Löschung

Daten, die nicht mehr für den angestrebten Zweck der Überwachung benötigt werden, müssen unverzüglich gelöscht werden. Dasselbe gilt, wenn schutzwürdige Interessen des Betroffenen der weiteren Speicherung entgegenstehen.

4.7 Die Rechte beim Einsatz von Chipkarten

Gesetzesbestimmung: § 6c BDSG

§ 6c BDSG stellt Regeln für den Einsatz „mobiler personenbezogener Speicher- und Verarbeitungsmedien“ auf. Unter diese Begriffsbestimmung fallen auch die Chipkarten. Erfasst sind nur Karten mit einem Prozessorchip, z.B. die Karten der deutschen Kreditwirtschaft.

Die Stelle, die z.B. Chipkarten ausgibt oder sonst in der in § 6c BDSG genannten Art einsetzt, muss den Betroffenen informieren:

1. über ihre Identität und Anschrift ,
2. über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten in allgemein verständlicher Form,
3. darüber, wie der Betroffene seine Rechte auf Auskunft, Berichtigung, Löschung und Sperrung, sowie das Widerspruchsrecht (§§ 19, 20, 34, 35) ausüben kann, und

4. welche Maßnahmen bei Verlust oder Zerstörung der Karte zu treffen sind.

Die Unterrichtungspflicht besteht nicht, wenn der Betroffene bereits auf andere Weise Kenntnis erlangt hat.

Damit das Auskunftsrecht in der Praxis auch wahrgenommen werden kann, müssen in angemessenem Umfang Geräte oder Einrichtungen zur Wahrnehmung des Auskunftsrechts (z.B. Lesegeräte) zur Verfügung gestellt werden.

Auch hier muss die Auskunft unentgeltlich erfolgen.

Weiterhin bestimmt das Gesetz, dass für den Betroffenen eindeutig erkennbar sein muss, wenn ein Kommunikationsvorgang – beispielsweise Lesevorgang bei kontaktlosen Chipkarten – auf dem Speichermedium eine Datenverarbeitung auslöst. Er wird so davor geschützt, dass andere ohne seine Kenntnisnahme Daten lesen, eingeben oder sonst verarbeiten.

4.8 Das Recht auf Anrufung des Bundesbeauftragten für den Datenschutz und anderer Kontrollinstitutionen

Gesetzesbestimmungen: §§ 21, 38 BDSG

Wer annimmt, bei der Erhebung, Verarbeitung oder Nutzung seiner persönlichen Daten durch öffentliche Stellen des Bundes oder ein Telekommunikations- oder Postdienstunternehmen in seinen Rechten

verletzt worden zu sein, kann sich an den Bundesbeauftragten für den Datenschutz wenden. Als unabhängige Beschwerdeinstanz mit umfassenden Kontrollbefugnissen (siehe weiteres in Kapitel 1) geht der Bundesbeauftragte allen Eingaben nach und unterrichtet den Betroffenen vom Ergebnis.

Alle Eingaben werden vertraulich behandelt. Auf Wunsch des Betroffenen bleibt sein Name auch gegenüber der öffentlichen Stelle ungenannt, über die er sich beschwert.

Entsprechend können Sie den jeweiligen Landesbeauftragten für den Datenschutz anrufen, wenn Sie Ihre Rechte durch eine öffentliche Stelle eines Landes verletzt sehen.

Wer meint, durch den Umgang mit seinen Daten seitens einer nicht öffentlichen Stelle in seinen Rechten verletzt zu sein, kann sich an die Aufsichtsbehörde des jeweiligen Landes wenden. Die örtliche Zuständigkeit richtet sich nach dem Sitz der nicht öffentlichen Stelle.

Anschriften und Telefonnummern der Datenschutzkontrollinstitutionen finden Sie in den Anhängen 4 und 5.

4.9 Das Recht auf Schadensersatz

Gesetzesbestimmungen: §§ 7, 8 BDSG

Wenn eine verantwortliche Stelle einem Betroffenen durch eine unzulässige oder unrichtige Datenverarbeitung einen Schaden zufügt, ist sie zum Ersatz des Schadens verpflichtet (vgl. § 7). Diese

Schadensersatzverpflichtung gilt sowohl für öffentliche als auch für nicht öffentliche Stellen.

Schmerzensgeld!

Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen auch der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen (Schmerzensgeld).
Der Schmerzensgeldanspruch bei der verschuldensabhängigen Haftung ergibt sich aus dem Bürgerlichen Gesetzbuch.

Kein Schadensersatz bei Beachtung der gebotenen Sorgfalt

Die verantwortliche Stelle kann sich von der Haftung befreien, wenn sie den Nachweis erbringt, dass sie den Schaden nicht zu vertreten hat. Sie muss beweisen, dass sie die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

Gefährdungshaftung im öffentlichen Bereich

Öffentliche Stellen haften auch unabhängig von einem Verschulden bis zu einem Höchstbetrag von 250.000 DM (Gefährdungshaftung).
Auch bei der verschuldensunabhängigen Haftung gibt es bei schweren Persönlichkeitsverletzungen einen Schmerzensgeldanspruch (vgl. § 8 Abs. 2).

4.10 Was hat sich geändert?

Wesentliche Änderungen im neuen Recht sind:

- Verbesserungen bei Auskunfts-, Benachrichtigungs- und Widerspruchsrecht,
- Aufnahme einer einschränkenden Bestimmung zur automatisierten Einzelentscheidung - Grundsatz: „*Die Maschine soll nicht über den Menschen entscheiden!"* - ,
- Gesetzliche Vorgaben zu den

Zulässigkeitsvoraussetzungen der Videoüberwachung öffentlich zugänglicher Räume, auch durch Stellen der Privatwirtschaft,

- Aufnahme einer Regelung zu „mobilen personenbezogenen Speicher- und Verarbeitungsmedien" (Chipkarten), die Informationspflichten gegenüber den Bürgerinnen und Bürgern begründet und damit zu mehr Transparenz und Rechtssicherheit führen soll,
- Einführung einer allgemeinen Regelkontrolle der Datenschutzaufsichtsbehörden, die danach auch ohne besonderen Anlass (z.B. eine Beschwerde) tätig werden können,
- Schaffung eines eigenständigen Schadensersatzanspruches, der sowohl für die öffentlichen als auch für die nicht öffentlichen Stellen gilt.

5 Seien Sie Ihr eigener Datenschutzbeauftragter!

Privatsphäre und Herrschaft über die eigenen persönlichen Daten müssen gewahrt werden, auch und gerade in einer vernetzten Welt, in der der Einzelne von vielen Datensammlern ins Visier genommen wird. Zum Schutz Ihrer Privatsphäre können Sie mithelfen, denn Datenschutzaufsichtsbehörden können nicht überall sein. Datenschutzrecht stößt ebenso in einem globalen Datenaustausch an Grenzen, auch wenn mit der EU-Datenschutzrichtlinie und ihrer Umsetzung ein europäischer Rechtsrahmen geschaffen wurde.
Datenschutz durch Technik bietet vielfältige Möglichkeiten des Selbstschutzes für den

Einzelnen. Sorgen Sie für die Sicherheit und Vertraulichkeit Ihrer Daten im Internet, indem Sie die Möglichkeiten zur Verschlüsselung, zur sicheren Übertragung von Daten nutzen. Wenn Sie nicht möchten, dass Sie beim Surfen im Internet überall Spuren hinterlassen, machen Sie von den Verfahren zur Anonymisierung und Pseudonymisierung Gebrauch. Fordern Sie als Verbraucher den Einsatz von technischen Systemen ein, die möglichst ohne Ihre persönlichen Daten auskommen. Es ist Ihr Recht! Hier können nicht die technischen Möglichkeiten im Einzelnen dargestellt werden. Sie unterliegen auch einem ständigen Wandel. Sie können sich aber jeweils aktuell bei den für Sie zuständigen Aufsichtsbehörden informieren.
Selbstschutz ist aber nicht nur in der virtuellen Welt gefragt. Datensammler beschreiten unterschiedliche Wege, um Ihre persönlichen Daten zu bekommen. Das kann das Gewinnrätsel sein, um Ihre Adresse und persönlichen Interessen zu erfahren. Das kann auch die Haushaltsumfrage oder die Kundenkarte sein, die Aufschluss über Ihr Konsumverhalten geben. Sie bestimmen, wie viel Sie von Sich preisgeben wollen. Bevor Sie aber Ihre Einwilligung geben, wägen Sie gut ab. Privatsphäre ist ein zu wertvolles Gut, um es meistbietend zu verkaufen.

6 Begriffe und ihre Bedeutung

Gesetzesbestimmung: § 3 BDSG

Personenbezogene Daten...

sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder

bestimmbaren natürlichen Person (Betroffener), wie z.B. Alter, Anschrift, Vermögen, Äußerungen, Überzeugungen.

Automatisierte Verarbeitung... ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

Nicht automatisierte Datei... ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

Erheben... ist das Beschaffen von Daten über den Betroffenen.

Verarbeiten... ist das ☞Speichern, ☞Verändern, ☞Übermitteln, ☞Sperren und ☞Löschen von personenbezogenen Daten.

Nutzen... ist das Verwenden von Daten, soweit nicht ☞Verarbeiten vorliegt (z.B. Abruf auf Bildschirm).

Speichern... ist das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren ☞Verarbeitung oder ☞Nutzung.

Verändern... ist das inhaltliche Umgestalten personenbezogener gespeicherter Daten.

Übermitteln... ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten

einsieht oder abruft.

Sperren... ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere ☞Verarbeitung oder ☞Nutzung einzuschränken.

Löschen... ist das Unkenntlichmachen gespeicherter personenbezogener Daten.

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.

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

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.

Empfänger... ist jede Person oder Stelle, die Daten erhält.

Dritter... ist jede Person oder Stelle außerhalb der verantwortlichen Stelle;
<u>Dritte sind nicht</u>

- der Betroffene sowie
- diejenigen 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.

Besondere Arten personenbezogener Daten...

sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

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.

Anhang 1

Bundesdatenschutzgesetz (BDSG)

vom 20. Dezember 1990 (BGBl. I S. 2954) in der Fassung der Neubekanntmachung vom 14. Januar 2003 (BGBl. I S. 66)

Bundesdatenschutzgesetz (BDSG)*)

Inhaltsübersicht

*) Dieses Gesetz dient der Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31).

Erster Abschnitt

Allgemeine und gemeinsame Bestimmungen

§ 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 Sondervermögen 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 Daten-

schutz 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 Einrichtung 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.

Zweiter Abschnitt

Datenverarbeitung der öffentlichen Stellen

Erster Unterabschnitt

Rechtsgrundlagen der Datenverarbeitung

§ 12

Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die §§ 12 bis 16, 19 bis 20 auch für die öffentlichen Stellen der Länder, soweit sie

1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder
2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) Für Landesbeauftragte für den Datenschutz gilt § 23 Abs. 4 entsprechend.

(4) Werden personenbezogene Daten für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse erhoben, verarbeitet oder genutzt, gelten anstelle der §§ 13 bis 16, 19 bis 20 der § 28 Abs. 1 und 3 Nr. 1 sowie die §§ 33 bis 35, auch soweit personenbezogene Daten weder automatisiert verarbeitet noch in nicht automatisierten Dateien verarbeitet oder genutzt oder dafür erhoben werden.

§ 13

Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.

(1a) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(2) Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,
2. der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat,
3. 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,
4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,
6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,
7. 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,
8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder
9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

§ 14

Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. 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 Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,

8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es 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.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) 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.

(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, die eine Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder
2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche 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.

Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) zu den in § 13 Abs. 2 Nr. 7 genannten Zwecken richtet sich nach den für die in § 13 Abs. 2 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

§ 15

Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten, an den die Daten übermittelt werden, liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 10 Abs. 4 bleibt unberührt.

(3) Der Dritte, an den die Daten übermittelt werden, darf diese für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 14 Abs. 2 zulässig.

(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, dass bei diesen ausreichende Datenschutzmaßnahmen getroffen werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 16

Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder
2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das Übermitteln von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 14 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

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

(3) In den Fällen der Übermittlung nach Absatz 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 Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§ 17

(weggefallen)

§ 18

Durchführung des Datenschutzes in der Bundesverwaltung

(1) Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Das Gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange diesen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. Für ihre automatisierten Verarbeitungen haben sie die Angaben nach § 4e sowie die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. Bei allgemeinen Verwaltungszwecken dienenden automatisierten Verarbeitungen, bei welchen das Auskunftsrecht des Betroffenen nicht nach § 19 Abs. 3 oder 4 eingeschränkt wird, kann hiervon abgesehen werden. Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden, können die Festlegungen zusammengefasst werden.

Zweiter Unterabschnitt

Rechte des Betroffenen

§ 19

Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

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

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist unentgeltlich.

§ 19a

Benachrichtigung

(1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

(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 Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder
3. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 2 oder 3 abgesehen wird.

(3) § 19 Abs. 2 bis 4 gilt entsprechend.

§ 20

Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht

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

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

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

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

1. 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, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, 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 weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, sind zu sperren, wenn die Behörde im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

(7) 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.

(8) 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 wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(9) § 2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.

§ 21

Anrufung des Bundesbeauftragten für den Datenschutz

Jedermann kann sich an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

Dritter Unterabschnitt

Bundesbeauftragter für den Datenschutz

§ 22

Wahl des Bundesbeauftragten für den Datenschutz

(1) Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Der Bundesbeauftragte muss bei seiner Wahl das 35. Lebensjahr vollendet haben. Der Gewählte ist vom Bundespräsidenten zu ernennen.

(2) Der Bundesbeauftragte leistet vor dem Bundesminister des Innern folgenden Eid:

„Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe.“

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

(4) Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Rechtsaufsicht der Bundesregierung.

(5) Der Bundesbeauftragte wird beim Bundesministerium des Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesministeriums des Innern. Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu

stellen; sie ist im Einzelplan des Bundesministeriums des Innern in einem eigenen Kapitel auszuweisen. Die Stellen sind im Einvernehmen mit dem Bundesbeauftragten zu besetzen. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden.

(6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.

§ 23

Rechtsstellung des Bundesbeauftragten für den Datenschutz

(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz beginnt mit der Aushändigung der Ernennungsurkunde. Es endet

1. mit Ablauf der Amtszeit,
2. mit der Entlassung.

Der Bundespräsident entlässt den Bundesbeauftragten, wenn dieser es verlangt oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Fall der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiterzuführen.

(2) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(3) Der Bundesbeauftragte hat dem Bundesministerium des Innern Mitteilung über Geschenke zu machen, die er in Bezug auf sein Amt erhält. Das Bundesministerium des Innern entscheidet über die Verwendung der Geschenke.

(4) Der Bundesbeauftragte ist berechtigt, über Personen, die ihm in seiner Eigenschaft als Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeiter des Bundesbeauftragten mit der Maßgabe, dass über die Ausübung dieses Rechts der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.

(5) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesministeriums des Innern weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten. Für den Bundesbeauftragten und seine Mitarbeiter gelten die §§ 93, 97, 105 Abs. 1, § 111 Abs. 5 in Verbindung mit § 105 Abs. 1 sowie § 116 Abs. 1 der Abgabenordnung nicht. Satz 5 findet keine Anwendung, soweit die Finanzbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben des Auskunftspflichtigen oder der für ihn tätigen Personen handelt. Stellt der Bundesbeauftragte einen Datenschutzverstoß fest, ist er befugt, diesen anzuzeigen und den Betroffenen hierüber zu informieren.

(6) Die Genehmigung, als Zeuge auszusagen, soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. § 28 des Bundesverfassungsgerichtsgesetzes bleibt unberührt.

(7) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, im Fall des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Bundesbeamten der Besoldungsgruppe B 9 zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im Übrigen sind die §§ 13 bis 20 des Bundesministergesetzes in der Fassung der Bekanntmachung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Gesetz zur Kürzung des Amtsgehalts der Mitglieder der Bundesregierung und der Parlamentarischen Staatssekretäre vom 22. Dezember 1982 (BGBl. I S. 2007), mit der Maßgabe anzuwenden, dass an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich unmittelbar vor seiner Wahl zum Bundesbeauftragten als Beamter oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 9 zu durchlaufenden Amt befunden hat.*)

---

*) Gemäß Artikel 3 Nr. 2 des Versorgungsänderungsgesetzes 2001 vom 20. Dezember 2001 (BGBl. I S. 3926) ist am 1. Januar 2003 § 23 Abs. 7 wie folgt geändert worden:

a) Satz 3 wird wie folgt gefasst:
„Im Übrigen sind die §§ 13 bis 20 und 21a Abs. 5 des Bundesministergesetzes mit den Maßgaben anzuwenden, dass an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren und an die Stelle der Besoldungsgruppe B 11 in § 21a Abs. 5 des Bundesministergesetzes die Besoldungsgruppe B 9 tritt."

b) In Satz 4 wird die Angabe „§§ 15 bis 17" durch die Angabe „§§ 15 bis 17 und 21a Abs. 5" ersetzt.

(8) Absatz 5 Satz 5 bis 7 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 24

Kontrolle durch den Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.

(2) Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf

1. von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs und
2. personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt. Personenbezogene Daten, die der Kontrolle durch die Kommission nach § 15 des Artikel 10-Gesetzes unterliegen, unterliegen nicht der Kontrolle durch den Bundesbeauftragten, es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. Der Kontrolle durch den Bundesbeauftragten unterliegen auch nicht personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Bundesbeauftragten widerspricht.

(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,
2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in § 6 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. § 25 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 25

Beanstandungen durch den Bundesbeauftragten für den Datenschutz

(1) Stellt der Bundesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,
2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,
3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht, gegenüber deren Vorständen,
4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 4 unterrichtet der Bundesbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.

(2) Der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an den Bundesbeauftragten zu.

§ 26

Weitere Aufgaben des Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. Er unterrichtet den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in § 25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. § 38 Abs. 1 Satz 3 und 4 gilt entsprechend.

Dritter Abschnitt

Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Erster Unterabschnitt

Rechtsgrundlagen der Datenverarbeitung

§ 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 nicht-öffentlichen 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 dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. 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 § 4a Abs. 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.

§ 32

(weggefallen)

Zweiter Unterabschnitt

Rechte des Betroffenen

§ 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 dürfen 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.

Dritter Unterabschnitt

Aufsichtsbehörde

§§ 36 und 37

(weggefallen)

§ 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.

Vierter Abschnitt

Sondervorschriften

§ 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.

§ 40

Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(3) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 41

Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

(2) Führt die journalistisch-redaktionelle Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen berufsmäßig journalistisch mitwirken oder mitgewirkt haben, geschlossen werden kann,
2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann,
3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe der Deutschen Welle durch Ausforschung des Informationsbestandes beeinträchtigt würde.

Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) Im Übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5, 7, 9 und 38a. Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

§ 42

Datenschutzbeauftragter der Deutschen Welle

(1) Die Deutsche Welle bestellt einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz tritt. Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. Im Übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.

(3) Jedermann kann sich entsprechend § 21 Satz 1 an den Beauftragten für den Datenschutz wenden.

(4) Der Beauftragte für den Datenschutz erstattet den Organen der Deutschen Welle alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. Er erstattet darüber hinaus besondere Berichte auf Beschluss eines Organes der Deutschen Welle. Die Tätigkeitsberichte übermittelt der Beauftragte auch an den Bundesbeauftragten für den Datenschutz.

(5) Weitere Regelungen entsprechend den §§ 23 bis 26 trifft die Deutsche Welle für ihren Bereich. Die §§ 4f und 4g bleiben unberührt.

Fünfter Abschnitt

Schlussvorschriften

§ 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.

Sechster Abschnitt

Übergangsvorschriften

§ 45

Laufende Verwendungen

Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, sind binnen drei Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen. Soweit Vorschriften dieses Gesetzes in Rechtsvorschriften außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr zur Anwendung gelangen, sind Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, binnen fünf Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.

§ 46

Weitergeltung von Begriffsbestimmungen

(1) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Datei verwendet, ist Datei

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder
2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(2) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Akte verwendet, ist Akte jede amtlichen oder

dienstlichen Zwecken dienende Unterlage, die nicht dem Dateibegriff des Absatzes 1 unterfällt; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(3) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Empfänger verwendet, ist Empfänger jede Person oder Stelle außerhalb der verantwortlichen Stelle. Empfänger 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.

Anlage
(zu § 9 Satz 1)

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

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

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

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

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

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

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

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

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

Anhang 2

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Dies ist ein inoffizieller Text. Der rechtsverbindliche Text ist im Amtsblatt der Europäischen Gemeinschaften abgedruckt (Nr. L 281 vom 23. November 1995 S. 31).

Inhalt

Artikel 30

KAPITEL VII - GEMEINSCHAFTLICHE DURCHFÜHRUNGSMASSNAHMEN

Artikel 31 - Ausschussverfahren

Artikel 32

Artikel 33

Artikel 34

Erwägungsgründe

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION -

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 100 a,

auf Vorschlag der Kommission , nach Stellungnahme des Wirtschafts- und Sozialausschusses, gemäß dem Verfahren des Artikels 189 b des Vertrags, in Erwägung nachstehender Gründe:

(1) Die Ziele der Gemeinschaft, wie sie in dem durch den Vertrag über die Europäische Union geänderten Vertrag festgelegt sind, bestehen darin, einen immer engeren Zusammenschluss der europäischen Völker zu schaffen, engere Beziehungen zwischen den in der Gemeinschaft zusammengeschlossenen Staaten herzustellen, durch gemeinsames Handeln den wirtschaftlichen und sozialen Fortschritt zu sichern, indem die Europa trennenden Schranken beseitigt werden, die ständige Besserung der Lebensbedingungen ihrer Völker zu fördern, Frieden und Freiheit zu wahren und zu festigen und für die Demokratie einzutreten und sich dabei auf die in den Verfassungen und Gesetzen der Mitgliedstaaten sowie in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten anerkannten Grundrechte zu stützen.

(2) Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen.

(3) Für die Errichtung und das Funktionieren des Binnenmarktes, der gemäß Artikel 7 a des Vertrags den freien Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleisten soll, ist es nicht nur erforderlich, dass personenbezogene Daten von einem Mitgliedstaat in einen anderen Mitgliedstaat übermittelt werden können, sondern auch, dass die Grundrechte der Personen gewahrt werden.

(4) Immer häufiger werden personenbezogene Daten in der Gemeinschaft in den verschiedenen Bereichen wirtschaftlicher und sozialer Tätigkeiten verarbeitet. Die Fortschritte der Informationstechnik erleichtern die Verarbeitung und den Austausch dieser Daten beträchtlich.

(5) Die wirtschaftliche und soziale Integration, die sich aus der Errichtung und dem Funktionieren des Binnenmarktes im Sinne von Artikel 7 a des Vertrags ergibt, wird notwendigerweise zu einer spürbaren Zunahme der grenzüberschreitenden Ströme personenbezogener Daten zwischen allen am wirtschaftlichen und sozialen Leben der Mitgliedstaaten Beteiligten im öffentlichen wie im privaten Bereich führen. Der Austausch personenbezogener Daten zwischen in verschiedenen Mitgliedstaaten niedergelassenen Unternehmen wird zunehmen. Die Verwaltungen der Mitgliedstaaten sind aufgrund des Gemeinschaftsrechts gehalten, zusammenzuarbeiten und untereinander personenbezogene Daten auszutauschen, um im Rahmen des Raums ohne Grenzen, wie er durch den Binnenmarkt hergestellt wird, ihren Auftrag erfüllen oder Aufgaben anstelle der Behörden eines anderen Mitgliedstaats durchführen zu können.

(6) Die verstärkte wissenschaftliche und technische Zusammenarbeit sowie die koordinierte Einführung neuer Telekommunikationsnetze in der Gemeinschaft erfordern und erleichtern den grenzüberschreitenden Verkehr personenbezogener Daten.

(7) Das unterschiedliche Niveau des Schutzes der Rechte und Freiheiten von Personen, insbesondere der Privatsphäre, bei der Verarbeitung personenbezogener Daten in den Mitgliedstaaten kann die Übermittlung dieser Daten aus dem Gebiet eines Mitgliedstaats in das Gebiet eines anderen Mitgliedstaats verhindern. Dieses unterschiedliche Schutzniveau kann somit ein Hemmnis für die Ausübung einer Reihe von Wirtschaftstätigkeiten auf Gemeinschaftsebene darstellen, den Wettbewerb verfälschen und die Erfüllung des Auftrags der im Anwendungsbereich des Gemeinschaftsrechts tätigen Behörden verhindern. Dieses unterschiedliche Schutzniveau ergibt sich aus der Verschiedenartigkeit der einzelstaatlichen Rechts- und Verwaltungsvorschriften.

(8) Zur Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten ist ein gleichwertiges Schutzniveau hinsichtlich der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten unerlässlich. Insbesondere unter Berücksichtigung der großen Unterschiede, die gegenwärtig zwischen den einschlägigen einzelstaatlichen Rechtsvorschriften bestehen, und der Notwendigkeit, die Rechtsvorschriften der Mitgliedstaaten zu koordinieren, damit der grenzüberschreitende Fluss personenbezogener Daten kohärent und in Übereinstimmung mit dem Ziel des Binnenmarktes im Sinne des Artikels 7 a des Vertrags geregelt wird, lässt sich dieses für den Binnenmarkt grundlegende Ziel nicht allein durch das Vorgehen der Mitgliedstaaten verwirklichen. Deshalb ist eine Maßnahme der Gemeinschaft zur Angleichung der Rechtsvorschriften erforderlich.

(9) Die Mitgliedstaaten dürfen aufgrund des gleichwertigen Schutzes, der sich aus der Angleichung der einzelstaatlichen Rechtsvorschriften ergibt, den freien Verkehr personenbezogener Daten zwischen ihnen nicht mehr aus Gründen behindern, die den Schutz der Rechte und Freiheiten natürlicher Personen und insbesondere das Recht auf die Privatsphäre betreffen. Die Mitgliedstaaten besitzen einen Spielraum, der im Rahmen der Durchführung der Richtlinie von den Wirtschafts- und Sozialpartnern genutzt werden kann. Sie können somit in ihrem einzelstaatlichen Recht allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung festlegen. Hierbei streben sie eine Verbesserung des gegenwärtig durch ihre Rechtsvorschriften gewährten Schutzes an. Innerhalb dieses Spielraums können unter Beachtung des Gemeinschaftsrechts Unterschiede bei der Durchführung der Richtlinie auftreten, was Auswirkungen für den Datenverkehr sowohl innerhalb eines Mitgliedstaats als auch in der Gemeinschaft haben kann.

(10) Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte und -freiheiten, insbesondere des auch in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten Rechts auf die Privatsphäre. Die Angleichung dieser Rechtsvorschriften darf deshalb nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen, sondern muss im Gegenteil darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen.

(11) Die in dieser Richtlinie enthaltenen Grundsätze zum Schutz der Rechte und Freiheiten der Personen, insbesondere der Achtung der Privatsphäre, konkretisieren und erweitern die in dem Übereinkommen des Europarats vom 28. Januar 1981 zum Schutze der Personen bei der automatischen Verarbeitung personenbezogener Daten enthaltenen Grundsätze.

(12) Die Schutzprinzipien müssen für alle Verarbeitungen personenbezogener Daten gelten, sobald die Tätigkeiten des für die Verarbeitung Verantwortlichen in den Anwendungsbereich des Gemeinschaftsrechts fallen. Auszunehmen ist die Datenverarbeitung, die von einer natürlichen Person in Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten - wie zum Beispiel Schriftverkehr oder Führung von Anschriftenverzeichnissen - vorgenommen wird.

(13) Die in den Titeln V und VI des Vertrags über die Europäische Union genannten Tätigkeiten, die die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates oder die Tätigkeiten des Staates im Bereich des Strafrechts betreffen, fallen unbeschadet der Verpflichtungen der Mitgliedstaaten gemäß Artikel 56 Absatz 2 sowie gemäß den Artikeln 57 und 100 a des Vertrags zur Gründung der Europäischen Gemeinschaft nicht in den Anwendungsbereich des Gemeinschaftsrechts. Die Verarbeitung personenbezogener Daten, die zum Schutz des wirtschaftlichen Wohls des Staates erforderlich ist, fällt nicht unter diese Richtlinie, wenn sie mit Fragen der Sicherheit des Staates zusammenhängt.

(14) In Anbetracht der Bedeutung der gegenwärtigen Entwicklung im Zusammenhang mit der Informationsgesellschaft bezüglich Techniken der Erfassung, Übermittlung, Veränderung, Speicherung, Aufbewahrung oder Weitergabe von personenbezogenen Ton- und Bilddaten muss diese Richtlinie auch auf die Verarbeitung dieser Daten Anwendung finden.

(15) Die Verarbeitung solcher Daten wird von dieser Richtlinie nur erfasst, wenn sie automatisiert erfolgt oder wenn die Daten, auf die sich die Verarbeitung bezieht, in Dateien enthalten oder für solche bestimmt sind, die nach bestimmten personenbezogenen Kriterien strukturiert sind, um einen leichten Zugriff auf die Daten zu ermöglichen.

(16) Die Verarbeitung von Ton- und Bilddaten, wie bei der Videoüberwachung, fällt nicht unter diese Richtlinie, wenn sie für Zwecke der öffentlichen Sicherheit, der Landesverteidigung, der Sicherheit des Staates oder der Tätigkeiten des Staates im Bereich des Strafrechts oder anderen Tätigkeiten erfolgt, die nicht unter das Gemeinschaftsrecht fallen.

(17) Bezüglich der Verarbeitung von Ton- und Bilddaten für journalistische, literarische oder künstlerische Zwecke, insbesondere im audiovisuellen Bereich, finden die Grundsätze dieser Richtlinie gemäß Artikel 9 eingeschränkt Anwendung.

(18) Um zu vermeiden, dass einer Person der gemäß dieser Richtlinie gewährleistete Schutz vorenthalten wird, müssen auf jede in der Gemeinschaft erfolgte Verarbeitung personenbezogener Daten die Rechtsvorschriften eines Mitgliedstaats angewandt werden. Es ist angebracht, auf die Verarbeitung, die von einer Person, die dem in dem Mitgliedstaat niedergelassenen für die Verarbeitung Verantwortlichen unterstellt ist, vorgenommen werden, die Rechtsvorschriften dieses Staates anzuwenden.

(19) Eine Niederlassung im Hoheitsgebiet eines Mitgliedstaats setzt die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus. Die Rechtsform einer solchen Niederlassung, die eine Agentur oder eine Zweigstelle sein kann, ist in dieser Hinsicht nicht maßgeblich. Wenn der Verantwortliche im Hoheitsgebiet mehrerer Mitgliedstaaten niedergelassen ist, insbesondere mit einer Filiale, muss er vor allem zur Vermeidung von Umgehungen sicherstellen, dass jede dieser Niederlassungen die Verpflichtungen einhält, die im jeweiligen einzelstaatlichen Recht vorgesehen sind, das auf ihre jeweiligen Tätigkeiten anwendbar ist.

(20) Die Niederlassung des für die Verarbeitung Verantwortlichen in einem Drittland darf dem Schutz der Personen gemäß dieser Richtlinie nicht entgegenstehen. In diesem Fall sind die Verarbeitungen dem Recht des Mitgliedstaats zu unterwerfen, in dem sich die für die betreffenden Verarbeitungen verwendeten Mittel befinden, und Vorkehrungen zu treffen, um sicherzustellen, dass die in dieser Richtlinie vorgesehenen Richte und Pflichten tatsächlich eingehalten werden.

(21) Diese Richtlinie berührt nicht die im Strafrecht geltenden Territorialitätsregeln.

(22) Die Mitgliedstaaten können in ihren Rechtsvorschriften oder bei der Durchführung der Vorschriften zur Umsetzung dieser Richtlinie die allgemeinen Bedingungen präzisieren, unter denen die Verarbeitungen rechtmäßig sind. Insbesondere nach Artikel 5 in Verbindung mit den Artikeln 7 und 8 können die Mitgliedstaaten neben den allgemeinen Regeln besondere Bedingungen für die Datenverarbeitung in spezifischen Bereichen und für die verschiedenen Datenkategorien gemäß Artikel 8 vorsehen.

(23) Die Mitgliedstaaten können den Schutz von Personen sowohl durch ein allgemeines Gesetz zum Schutz von Personen bei der Verarbeitung personenbezogener Daten als auch durch gesetzliche Regelungen für bestimmte Bereiche, wie zum Beispiel die statistischen Ämter, sicherstellen.

(24) Diese Richtlinie berührt nicht die Rechtsvorschriften zum Schutz juristischer Personen bei der Verarbeitung von Daten, die sich auf sie beziehen.

(25) Die Schutzprinzipien finden zum einen ihren Niederschlag in den Pflichten, die den Personen, Behörden, Unternehmen, Geschäftsstellen oder anderen für die Verarbeitung verantwortlichen Stellen obliegen; diese Pflichten betreffen insbesondere die Datenqualität, die technische Sicherheit, die Meldung bei der Kontrollstelle und die Voraussetzungen, unter denen eine Verarbeitung vorgenommen werden kann. Zum anderen kommen sie zum Ausdruck in den Rechten der Personen, deren Daten Gegenstand von Verarbeitungen sind, über diese informiert zu werden, Zugang zu den Daten zu erhalten, ihre Berichtigung verlangen bzw. unter gewissen Voraussetzungen Widerspruch gegen die Verarbeitung einlegen zu können.

(26) Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten

alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. Die Verhaltensregeln im Sinne des Artikels 27 können ein nützliches Instrument sein, mit dem angegeben wird, wie sich die Daten in einer Form anonymisieren und aufbewahren lassen, die die Identifizierung der betroffenen Person unmöglich macht.

(27) Datenschutz muss sowohl für automatisierte als auch für nicht-automatisierte Verarbeitungen gelten. In der Tat darf der Schutz nicht von den verwendeten Techniken abhängen, da andernfalls ernsthafte Risiken der Umgehung entstehen würden. Bei manuellen Verarbeitungen erfasst diese Richtlinie lediglich Dateien, nicht jedoch unstrukturierte Akten. Insbesondere muss der Inhalt einer Datei nach bestimmten personenbezogenen Kriterien strukturiert sein, die einen leichten Zugriff auf die Daten ermöglichen. Nach der Definition in Artikel 2 Buchstabe c können die Mitgliedstaaten die Kriterien zur Bestimmung der Elemente einer strukturierten Sammlung personenbezogener Daten sowie die verschiedenen Kriterien zur Regelung des Zugriffs zu einer solchen Sammlung festlegen. Akten und Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien strukturiert sind, fallen unter keinen Umständen in den Anwendungsbereich dieser Richtlinie.

(28) Die Verarbeitung personenbezogener Daten muss gegenüber den betroffenen Personen nach Treu und Glauben erfolgen. Sie hat den angestrebten Zweck zu entsprechen, dafür erheblich zu sein und nicht darüber hinauszugehen. Die Zwecke müssen eindeutig und rechtmäßig sein und bei der Datenerhebung festgelegt werden. Die Zweckbestimmungen der Weiterverarbeitung nach der Erhebung dürfen nicht mit den ursprünglich festgelegten Zwecken unvereinbar sein.

(29) Die Weiterverarbeitung personenbezogener Daten für historische, statistische oder wissenschaftliche Zwecke ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, wenn der Mitgliedstaat geeignete Garantien vorsieht. Diese Garantien müssen insbesondere ausschließen, dass die Daten für Maßnahmen oder Entscheidungen gegenüber einzelnen Betroffenen verwendet werden.

(30) Die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn sie auf der Einwilligung der betroffenen Person beruht oder notwendig ist im Hinblick auf den Abschluss oder die Erfüllung eines für die betroffene Person bindenden Vertrags, zur Erfüllung einer gesetzlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse, in Ausübung hoheitlicher Gewalt oder wenn sie im Interesse einer anderen Person erforderlich ist, vorausgesetzt, dass die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen. Um den Ausgleich der in Frage stehenden Interessen unter Gewährleistung eines effektiven Wettbewerbs sicherzustellen, können die Mitgliedstaaten insbesondere die Bedingungen näher bestimmen, unter denen personenbezogene Daten bei rechtmäßigen Tätigkeiten im Rahmen laufender Geschäfte von Unternehmen und anderen Einrichtungen an Dritte weitergegeben werden können. Ebenso können sie die Bedingungen festlegen, unter denen personenbezogene Daten an Dritte zum Zweck der kommerziellen Werbung oder der Werbung von Wohltätigkeitsverbänden oder anderen Vereinigungen oder Stiftungen, z.B. mit politischer Ausrichtung, weitergegeben werden können, und zwar unter Berücksichtigung der Bestimmungen dieser Richtlinie, nach denen betroffene Personen ohne Angabe von Gründen und ohne Kosten Widerspruch gegen die Verarbeitung von Daten, die sie betreffen, erheben können.

(31) Die Verarbeitung personenbezogener Daten ist ebenfalls als rechtmäßig anzusehen, wenn sie erfolgt, um ein für das Leben der betroffenen Person wesentliches Interesse zu schützen.

(32) Es ist nach einzelstaatlichem Recht festzulegen, ob es sich bei dem für die Verarbeitung Verantwortlichen, der mit der Wahrnehmung einer Aufgabe betraut wurde, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, um eine Behörde oder um eine andere unter das öffentliche Recht oder das Privatrecht fallende Person, wie beispielsweise eine Berufsvereinigung, handeln soll.

(33) Daten, die aufgrund ihrer Art geeignet sind, die Grundfreiheiten oder die Privatsphäre zu beeinträchtigen, dürfen nicht ohne ausdrückliche Einwilligung der betroffenen Person verarbeitet werden. Ausnahmen von diesem Verbot müssen ausdrücklich vorgesehen werden bei spezifischen Notwendigkeiten, insbesondere wenn die Verarbeitung dieser Daten für gewisse auf das Gesundheitswesen bezogene Zwecke von Personen vorgenommen wird, die nach dem einzelstaatlichen Recht dem Berufsgeheimnis unterliegen, oder wenn die Verarbeitung für berechtigte Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, deren Ziel es ist, die Ausübung von Grundfreiheiten zu ermöglichen.

(34) Die Mitgliedstaaten können, wenn dies durch ein wichtiges öffentliches Interesse gerechtfertigt ist, Ausnahmen vom Verbot der Verarbeitung sensibler Datenkategorien vorsehen in Bereichen wie dem öffentlichen Gesundheitswesen und der sozialen Sicherheit - insbesondere hinsichtlich der Sicherung von Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen -, der wissenschaftlichen Forschung und der öffentlichen Statistik. Die Mitgliedstaaten müssen jedoch geeignete besondere Garantien zum Schutz der Grundrechte und der Privatsphäre von Personen vorsehen.

(35) Die Verarbeitung personenbezogener Daten durch staatliche Stellen für verfassungsrechtlich oder im Völkerrecht niedergelegte Zwecke von staatlich anerkannten Religionsgesellschaften erfolgt ebenfalls im Hinblick auf ein wichtiges öffentliches Interesse.

(36) Wenn es in bestimmten Mitgliedstaaten zum Funktionieren des demokratischen Systems gehört, dass die politischen Parteien im Zusammenhang mit Wahlen Daten über die politische Einstellung von Personen sammeln, kann die Verarbeitung derartiger Daten aus Gründen eines wichtigen öffentlichen Interesses zugelassen werden, sofern angemessene Garantien vorgesehen werden.

(37) Für die Verarbeitung personenbezogener Daten zu journalistischen, literarischen oder künstlerischen Zwecken, insbesondere im audiovisuellen Bereich, sind Ausnahmen von bestimmten Vorschriften dieser Richtlinie vorzusehen, soweit sie erforderlich sind, um die Grundrechte der Person mit der Freiheit der Meinungsäußerung und insbesondere der Freiheit, Informationen zu erhalten oder weiterzugeben, die insbesondere in Artikel 10 der Europäischen Konvention zum Schutze der Menschenrechte und der Grundfreiheiten garantiert ist, in Einklang zu bringen. Es obliegt deshalb den Mitgliedstaaten, unter Abwägung der Grundrechte Ausnahmen und Einschränkungen festzulegen, die bei den allgemeinen Maßnahmen zur Rechtmäßigkeit der Verarbeitung von Daten, bei den Maßnahmen zur Übermittlung der Daten in Drittländer sowie hinsichtlich der Zuständigkeiten der Kontrollstellen erforderlich sind, ohne dass jedoch Ausnahmen bei den Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung vorzusehen sind. Ferner sollte mindestens die in diesem Bereich zuständige Kontrollstelle bestimmte nachträgliche Zuständigkeiten erhal-

ten, beispielsweise zur regelmäßigen Veröffentlichung eines Berichts oder zur Befassung der Justizbehörden.

(38) Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden.

(39) Bestimmte Verarbeitungen betreffen Daten, die der Verantwortliche nicht unmittelbar bei der betroffenen Person erhoben hat. Des weiteren können Daten rechtmäßig an Dritte weitergegeben werden, auch wenn die Weitergabe bei der Erhebung der Daten bei der betroffenen Person nicht vorgesehen war. In diesen Fällen muss die betroffene Person zum Zeitpunkt der Speicherung der Daten oder spätestens bei der erstmaligen Weitergabe der Daten an Dritte unterrichtet werden.

(40) Diese Verpflichtung erübrigt sich jedoch, wenn die betroffene Person bereits unterrichtet ist. Sie besteht auch nicht, wenn die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist oder wenn die Unterrichtung der betroffenen Person unmöglich ist oder unverhältnismäßigen Aufwand erfordert, was bei Verarbeitungen für historische, statistische oder wissenschaftliche Zwecke der Fall sein kann. Diesbezüglich können die Zahl der betroffenen Personen, das Alter der Daten und etwaige Ausgleichsmaßnahmen in Betracht gezogen werden.

(41) Jede Person muss ein Auskunftsrecht hinsichtlich der sie betreffenden Daten, die Gegenstand einer Verarbeitung sind, haben, damit sie sich insbesondere von der Richtigkeit dieser Daten und der Zulässigkeit ihrer Verarbeitung überzeugen kann. Aus denselben Gründen muss jede Person außerdem das Recht auf Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten, zumindest im Fall automatisierter Entscheidungen im Sinne des Artikels 15 Absatz 1, besitzen. Dieses Recht darf weder das Geschäftsgeheimnis noch das Recht an geistigem Eigentum, insbesondere das Urheberrecht zum Schutz von Software, berühren. Dies darf allerdings nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.

(42) Die Mitgliedstaaten können die Auskunfts- und Informationsrechte im Interesse der betroffenen Person oder zum Schutz der Rechte und Freiheiten Dritter einschränken. Zum Beispiel können sie vorsehen, dass Auskunft über medizinische Daten nur über ärztliches Personal erhalten werden kann.

(43) Die Mitgliedstaaten können Beschränkungen des Auskunfts- und Informationsrechts sowie bestimmter Pflichten des für die Verarbeitung Verantwortlichen vorsehen, soweit dies beispielsweise für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, für zwingende wirtschaftliche oder finanzielle Interessen eines Mitgliedstaats oder der Union oder für die Ermittlung und Verfolgung von Straftaten oder von Verstößen gegen Standesregeln bei reglementierten Berufen erforderlich ist. Als Ausnahmen und Beschränkungen sind Kontroll-, Überwachungs- und Ordnungsfunktionen zu nennen, die in den drei letztgenannten Bereichen in bezug auf öffentliche Sicherheit, wirtschaftliches oder finanzielles Interesse und Strafverfolgung erforderlich sind. Die Erwähnung der Aufgaben in diesen drei Bereichen lässt die Zulässigkeit von Ausnahmen und Einschränkungen aus Gründen der Sicherheit des Staates und der Landesverteidigung unberührt.

(44) Die Mitgliedstaaten können aufgrund gemeinschaftlicher Vorschriften gehalten sein, von den das Auskunftsrecht, die Information der Personen und die Qualität der Daten

betreffenden Bestimmungen dieser Richtlinie abzuweichen, um bestimmte der oben genannten Zweckbestimmungen zu schützen.

(45) Auch wenn die Daten Gegenstand einer rechtmäßigen Verarbeitung aufgrund eines öffentlichen Interesses, der Ausübung hoheitlicher Gewalt oder der Interessen eines einzelnen sein können, sollte doch jede betroffene Person das Recht besitzen, aus überwiegenden, schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen Widerspruch dagegen einzulegen, dass die sie betreffenden Daten verarbeitet werden. Die Mitgliedstaaten können allerdings innerstaatliche Bestimmungen vorsehen, die dem entgegenstehen.

(46) Für den Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung personenbezogener Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, und zwar sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung, um insbesondere deren Sicherheit zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern. Die Mitgliedstaaten haben dafür Sorge zu tragen, dass der für die Verarbeitung Verantwortliche diese Maßnahmen einhält. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(47) Wird eine Nachricht, die personenbezogene Daten enthält, über Telekommunikationsdienste oder durch elektronische Post übermittelt, deren einziger Zweck darin besteht, Nachrichten dieser Art zu übermitteln, so gilt in der Regel die Person, von der die Nachricht stammt, und nicht die Person, die den Übermittlungsdienst anbietet, als Verantwortlicher für die Verarbeitung der in der Nachricht enthaltenen personenbezogenen Daten. Jedoch gelten die Personen, die diese Dienste anbieten, in der Regel als Verantwortliche für die Verarbeitung der personenbezogenen Daten, die zusätzlich für den Betrieb des Dienstes erforderlich sind.

(48) Die Meldeverfahren dienen der Offenlegung der Zweckbestimmungen der Verarbeitungen sowie ihrer wichtigsten Merkmale mit dem Zweck der Überprüfung ihrer Vereinbarkeit mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.

(49) Um unangemessene Verwaltungsformalitäten zu vermeiden, können die Mitgliedstaaten bei Verarbeitungen, bei denen eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen nicht zu erwarten ist, von der Meldepflicht absehen oder sie vereinfachen, vorausgesetzt, dass diese Verarbeitungen den Bestimmungen entsprechen, mit denen der Mitgliedstaat die Grenzen solcher Verarbeitungen festgelegt hat. Eine Befreiung oder eine Vereinfachung kann ebenso vorgesehen werden, wenn ein vom für die Verarbeitung Verantwortlichen benannten Datenschutzbeauftragter sicherstellt, dass eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen durch die Verarbeitung nicht zu erwarten ist. Ein solcher Beauftragter, ob Angestellter des für die Verarbeitung Verantwortlichen oder externer Beauftragter, muss seine Aufgaben in vollständiger Unabhängigkeit ausüben können.

(50) Die Befreiung oder Vereinfachung kann vorgesehen werden für Verarbeitungen, deren einziger Zweck das Führen eines Registers ist, das gemäß einzelstaatlichem Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht.

(51) Die Vereinfachung oder Befreiung von der Meldepflicht entbindet jedoch den für die Verarbeitung Verantwortlichen von keiner der anderen sich aus dieser Richtlinie ergebenden Verpflichtungen.

(52) In diesem Zusammenhang ist die nachträgliche Kontrolle durch die zuständigen Stellen im allgemeinen als ausreichende Maßnahme anzusehen.

(53) Bestimmte Verarbeitungen können jedoch aufgrund ihrer Art, ihrer Tragweite oder ihrer Zweckbestimmung - wie beispielsweise derjenigen, betroffene Personen von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrags auszuschließen - oder aufgrund der besonderen Verwendung einer neuen Technologie besondere Risiken im Hinblick auf die Rechte und Freiheiten der betroffenen Personen aufweisen. Es obliegt den Mitgliedstaaten, derartige Risiken in ihren Rechtsvorschriften aufzuführen, wenn sie dies wünschen.

(54) Bei allen in der Gesellschaft durchgeführten Verarbeitungen sollte die Zahl der Verarbeitungen mit solchen besonderen Risiken sehr beschränkt sein. Die Mitgliedstaaten müssen für diese Verarbeitungen vorsehen, dass vor ihrer Durchführung eine Vorabprüfung durch die Kontrollstelle oder in Zusammenarbeit mit ihr durch den Datenschutzbeauftragten vorgenommen wird. Als Ergebnis dieser Vorabprüfung kann die Kontrollstelle gemäß einzelstaatlichem Recht eine Stellungnahme abgeben oder die Verarbeitung genehmigen. Diese Prüfung kann auch bei der Ausarbeitung einer gesetzgeberischen Maßnahme des nationalen Parlaments oder einer auf eine solche gesetzgeberische Maßnahme gestützten Maßnahme erfolgen, die die Art der Verarbeitung und geeignete Garantien festlegt.

(55) Für den Fall der Missachtung der Rechte der betroffenen Personen durch den für die Verarbeitung Verantwortlichen ist im nationalen Recht eine gerichtliche Überprüfungsmöglichkeit vorzusehen. Mögliche Schäden, die den Personen aufgrund einer unzulässigen Verarbeitung entstehen, sind von dem für die Verarbeitung Verantwortlichen zu ersetzen, der von seiner Haftung befreit werden kann, wenn er nachweist, dass der Schaden ihm nicht angelastet werden kann, insbesondere weil ein Fehlverhalten der betroffenen Person oder ein Fall höherer Gewalt vorliegt. Unabhängig davon, ob es sich um eine Person des Privatrechts oder des öffentlichen Rechts handelt, müssen Sanktionen jede Person treffen, die die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht einhält.

(56) Grenzüberschreitender Verkehr von personenbezogenen Daten ist für die Entwicklung des internationalen Handels notwendig. Der in der Gemeinschaft durch diese Richtlinie gewährte Schutz von Personen steht der Übermittlung personenbezogener Daten in Drittländer, die ein angemessenes Schutzniveau aufweisen, nicht entgegen. Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, ist unter Berücksichtigung aller Umstände im Hinblick auf eine Übermittlungen oder eine Kategorie von Übermittlung zu beurteilen.

(57) Bietet hingegen ein Drittland kein angemessenes Schutzniveau, so ist die Übermittlung personenbezogener Daten in dieses Land zu untersagen.

(58) Ausnahmen von diesem Verbot sind unter bestimmten Voraussetzungen vorzusehen, wenn die betroffene Person ihre Einwilligung erteilt hat oder die Übermittlung im Rahmen eines Vertrags oder Gerichtsverfahrens oder zur Wahrung eines wichtigen öffentlichen Interesses erforderlich ist, wie zum Beispiel bei internationalem Datenaustausch zwischen Steuer- oder Zollverwaltungen oder zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind. Ebenso kann eine Übermittlung aus einem gesetzlich vorgesehenen Register erfolgen, das der öffentlichen Einsichtnahme oder der Einsichtnahme

durch Personen mit berechtigtem Interesse dient. In diesem Fall sollte eine solche Übermittlung nicht die Gesamtheit oder ganze Kategorien der im Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, so sollte die Übermittlung nur auf Antrag dieser Person oder nur dann erfolgen, wenn diese Person die Adressaten der Übermittlung sind.

(59) Besondere Maßnahmen können getroffen werden, um das unzureichende Schutzniveau in einem Drittland auszugleichen, wenn der für die Verarbeitung Verantwortliche geeignete Sicherheiten nachweist. Außerdem sind Verfahren für die Verhandlungen zwischen der Gemeinschaft und den betreffenden Drittländern vorzusehen.

(60) Übermittlungen in Drittstaaten dürfen auf jeden Fall nur unter voller Einhaltung der Rechtsvorschriften erfolgen, die die Mitgliedstaaten gemäß dieser Richtlinie, insbesondere gemäß Artikel 8, erlassen haben.

(61) Die Mitgliedstaaten und die Kommission müssen in ihren jeweiligen Zuständigkeitsbereichen die betroffenen Wirtschaftskreise ermutigen, Verhaltensregeln auszuarbeiten, um unter Berücksichtigung der Besonderheiten der Verarbeitung in bestimmten Bereichen die Durchführung dieser Richtlinie im Einklang mit den hierfür vorgesehenen einzelstaatlichen Bestimmungen zu fördern.

(62) Die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten ist ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogenen Daten.

(63) Diese Stellen sind mit den notwendigen Mitteln für die Erfüllung dieser Aufgabe auszustatten, d. h. Untersuchungs- und Einwirkungsbefugnissen, insbesondere bei Beschwerden, sowie Klagerecht. Die Kontrollstellen haben zur Transparenz der Verarbeitungen in dem Mitgliedstaat beizutragen, dem sie unterstehen.

(64) Die Behörden der verschiedenen Mitgliedstaaten werden einander bei der Wahrnehmung ihrer Aufgaben unterstützen müssen, um sicherzustellen, dass die Schutzregeln in der ganzen Europäischen Union beachtet werden.

(65) Auf Gemeinschaftsebene ist eine Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten einzusetzen, die ihre Aufgaben in völliger Unabhängigkeit wahrzunehmen hat. Unter Berücksichtigung dieses besonderen Charakters hat sie die Kommission zu beraten und insbesondere zur einheitlichen Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften beizutragen.

(66) Für die Übermittlung von Daten an Drittländer ist es zur Anwendung dieser Richtlinie erforderlich, der Kommission Durchführungsbefugnisse zu übertragen und ein Verfahren gemäß den Bestimmungen des Beschlusses 87/373/EWG des Rates festzulegen.

(67) Am 20. Dezember 1994 wurde zwischen dem Europäischen Parlament, dem Rat und der Kommission ein Modus vivendi betreffend die Maßnahmen zur Durchführung der nach dem Verfahren des Artikels 189 b des EG-Vertrags erlassenen Rechtsakte vereinbart.

(68) Die in dieser Richtlinie enthaltenen Grundsätze des Schutzes der Rechte und Freiheiten der Personen und insbesondere der Achtung der Privatsphäre bei der Verarbeitung

personenbezogener Daten können - besonders für bestimmte Bereiche - durch spezifische Regeln ergänzt oder präzisiert werden, die mit diesen Grundsätzen in Einklang stehen.

(69) Den Mitgliedstaaten sollte eine Frist von längstens drei Jahren ab Inkrafttreten ihrer Vorschriften zur Umsetzung dieser Richtlinie eingeräumt werden, damit sie die neuen einzelstaatlichen Vorschriften fortschreitend auf alle bereits laufenden Verarbeitungen anwenden können. Um eine kosteneffiziente Durchführung dieser Vorschriften zu erleichtern, wird den Mitgliedstaaten eine weitere Frist von zwölf Jahren nach Annahme dieser Richtlinie eingeräumt, um die Anpassung bestehender manueller Dateien an bestimmte Vorschriften dieser Richtlinie sicherzustellen. Werden in solchen Dateien enthaltene Daten während dieser erweiterten Umsetzungsfrist manuell verarbeitet, so sollten die Dateien zum Zeitpunkt der Verarbeitung mit diesen Vorschriften in Einklang gebracht werden.

(70) Die betroffene Person braucht nicht erneut ihre Einwilligung zu geben, damit der Verantwortliche nach Inkrafttreten der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie eine Verarbeitung sensibler Daten fortführen kann, die für die Erfüllung eines in freier Willenserklärung geschlossenen Vertrags erforderlich ist, und vor Inkrafttreten der genannten Vorschriften mitgeteilt wurde.

(71) Diese Richtlinie steht den gesetzlichen Regelungen eines Mitgliedstaats im Bereich der geschäftsmäßigen Werbung gegenüber in seinem Hoheitsgebiet ansässigen Verbrauchern nicht entgegen, sofern sich diese gesetzlichen Regelungen nicht auf den Schutz der Person bei der Verarbeitung personenbezogener Daten beziehen.

(72) Diese Richtlinie erlaubt bei der Umsetzung der mit ihr festgelegten Grundsätze die Berücksichtigung des Grundsatzes des öffentlichen Zugangs zu amtlichen Dokumenten -

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I - ALLGEMEINE BESTIMMUNGEN

Artikel 1 - Gegenstand der Richtlinie

(1) Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.

(2) Die Mitgliedstaaten beschränken oder untersagen nicht den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gemäß Absatz 1 gewährleisteten Schutzes.

Artikel 2 - Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

a) "personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

b) "Verarbeitung personenbezogener Daten" ("Verarbeitung") jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten;

c) "Datei mit personenbezogenen Daten" ("Datei") jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, gleichgültig ob diese Sammlung zentral, dezentralisiert oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt geführt wird;

d) "für die Verarbeitung Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden;

e) "Auftragsverarbeiter" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;

f) "Dritter" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten;

g) "Empfänger" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die Daten erhält, gleichgültig, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines einzelnen Untersuchungsauftrags möglicherweise Daten erhalten, gelten jedoch nicht als Empfänger;

h) "Einwilligung der betroffenen Person" jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.

Artikel 3 - Anwendungsbereich

(1) Diese Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht-automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.

(2) Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,

- die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des

Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;

- die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.

Artikel 4 - Anwendbares einzelstaatliches Recht

(1) Jeder Mitgliedstaat wendet die Vorschriften, die er zur Umsetzung dieser Richtlinie erlässt, auf alle Verarbeitungen personenbezogener Daten an,

a) die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt. Wenn der Verantwortliche eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten besitzt, ergreift er die notwendigen Maßnahmen, damit jede dieser Niederlassungen die im jeweils anwendbaren einzelstaatlichen Recht festgelegten Verpflichtungen einhält;

b) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht in seinem Hoheitsgebiet, aber an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet;

c) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht im Gebiet der Gemeinschaft niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden.

(2) In dem in Absatz 1 Buchstabe c genannten Fall hat der für die Verarbeitung Verantwortliche einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter zu benennen, unbeschadet der Möglichkeit eines Vorgehens gegen den für die Verarbeitung Verantwortlichen selbst.

KAPITEL II - ALLGEMEINE BEDINGUNGEN FÜR DIE RECHTMÄSSIGKEIT DER VERARBEITUNG PERSONENBEZOGENER DATEN

Artikel 5

Die Mitgliedstaaten bestimmen nach Maßgabe dieses Kapitels die Voraussetzungen näher, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

ABSCHNITT I - GRUNDSÄTZE IN BEZUG AUF DIE QUALITÄT DER DATEN

Artikel 6

(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten

a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;

b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen;

c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;

d) sachlich richtig und, wenn nötig, auf den neusten Stand gebracht sind; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden;

e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiter verarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Die Mitgliedstaaten sehen geeignete Garantien für personenbezogene Daten vor, die über die vorgenannte Dauer hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden.

(2) Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen.

ABSCHNITT II - GRUNDSÄTZE IN BEZUG AUF DIE ZULÄSSIGKEIT DER VERARBEITUNG VON DATEN

Artikel 7

Die Mitgliedstaaten sehen vor, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist:

a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;

b) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen;

c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;

e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde;

f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte

und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen.

ABSCHNITT III - BESONDERE KATEGORIEN DER VERARBEITUNG

Artikel 8 - Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Mitgliedstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben.

(2) Absatz 1 findet in folgenden Fällen keine Anwendung:

a) Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, nach den Rechtsvorschriften des Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden;

oder

b) die Verarbeitung ist erforderlich, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, zulässig ist;

oder

c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich, sofern die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben;

oder

d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, die keinen Erwerbszweck verfolgt, im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden;

oder

e) die Verarbeitung bezieht sich auf Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich.

(3) Absatz 1 gilt nicht, wenn die Verarbeitung der Daten 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 erfolgt, das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Be-

rufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen.

(4) Die Mitgliedstaaten können vorbehaltlich angemessener Garantien aus Gründen eines wichtigen öffentlichen Interesses entweder im Wege einer nationalen Rechtsvorschrift oder im Wege einer Entscheidung der Kontrollstelle andere als die in Absatz 2 genannten Ausnahmen vorsehen.

(5) Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, darf nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen, wobei ein Mitgliedstaat jedoch Ausnahmen aufgrund innerstaatlicher Rechtsvorschriften, die geeignete besondere Garantien vorsehen, festlegen kann. Ein vollständiges Register der strafrechtlichen Verurteilungen darf allerdings nur unter behördlicher Aufsicht geführt werden. Die Mitgliedstaaten können vorsehen, dass Daten, die administrative Strafen oder zivilrechtliche Urteile betreffen, ebenfalls unter behördlicher Aufsicht verarbeitet werden müssen.

(6) Die in den Absätzen 4 und 5 vorgesehenen Abweichungen von Absatz 1 sind der Kommission mitzuteilen.

(7) Die Mitgliedstaaten bestimmen, unter welchen Bedingungen eine nationale Kennziffer oder andere Kennzeichen allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen.

Artikel 9 - Verarbeitung personenbezogener Daten und Meinungsfreiheit

Die Mitgliedstaaten sehen für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen und Ausnahmen von diesem Kapitel sowie von den Kapiteln IV und VI nur insofern vor, als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen.

ABSCHNITT IV - INFORMATION DER BETROFFENEN PERSON

Artikel 10 - Information bei der Erhebung personenbezogener Daten bei der betroffenen Person

Die Mitgliedstaaten sehen vor, dass die Person, bei der die sie betreffenden Daten erhoben werden, vom für die Verarbeitung Verantwortlichen oder seinem Vertreter zumindest die nachstehenden Informationen erhält, sofern diese ihr noch nicht vorliegen:

a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls eines Vertreters,

b) Zweckbestimmungen der Verarbeitung, für die die Daten bestimmt sind,

c) weitere Informationen, beispielsweise betreffend

- die Empfänger oder Kategorien der Empfänger der Daten,

- die Frage, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist, sowie mögliche Folgen einer unterlassenen Beantwortung,

- das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten, sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

Artikel 11 - Informationen für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden

(1) Für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden, sehen die Mitgliedstaaten vor, dass die betroffene Person bei Beginn der Speicherung der Daten bzw. im Fall einer beabsichtigten Weitergabe der Daten an Dritte spätestens bei der ersten Übermittlung vom für die Verarbeitung Verantwortlichen oder seinem Vertreter zumindest die nachstehenden Informationen erhält, sofern diese ihr noch nicht vorliegen:

a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls eines Vertreters,

b) Zweckbestimmungen der Verarbeitung,

c) weitere Informationen, beispielsweise betreffend

- die Datenkategorien, die verarbeitet werden,

- die Empfänger oder Kategorien der Empfänger der Daten,

- das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten, sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

(2) Absatz 1 findet - insbesondere bei Verarbeitungen für Zwecke der Statistik oder der historischen oder wissenschaftlichen Forschung - keine Anwendung, wenn die Information der betroffenen Person unmöglich ist, unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist. In diesen Fällen sehen die Mitgliedstaaten geeignete Garantien vor.

ABSCHNITT V - AUSKUNFTSRECHT DER BETROFFENEN PERSON

Artikel 12 - Auskunftsrecht

Die Mitgliedstaaten garantieren jeder betroffenen Person das Recht, vom für die Verarbeitung Verantwortlichen folgendes zu erhalten:

a) frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten

- die Bestätigung, dass es Verarbeitungen sie betreffender Daten gibt oder nicht gibt, sowie zumindest Informationen über die Zweckbestimmungen dieser Verarbeitungen, die Kategorien der Daten, die Gegenstand der Verarbeitung sind, und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt werden;

- eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie die verfügbaren Informationen über die Herkunft der Daten;

- Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten, zumindest im Fall automatisierter Entscheidungen im Sinne von Artikel 15 Absatz 1;

b) je nach Fall die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen dieser Richtlinie entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind;

c) die Gewähr, dass jede Berichtigung, Löschung oder Sperrung, die entsprechend Buchstabe b durchgeführt wurde, den Dritten, denen die Daten übermittelt wurden, mitgeteilt wird, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist.

ABSCHNITT VI - AUSNAHMEN UND EINSCHRÄNKUNGEN

Artikel 13 - Ausnahmen und Einschränkungen

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1, Artikel 10, Artikel 11 Absatz 1, Artikel 12 und Artikel 21 beschränken, sofern eine solche Beschränkung notwendig ist für

a) die Sicherheit des Staates;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen;

e) ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten;

f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c, d und e genannten Zwecke verbunden sind;

g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

(2) Vorbehaltlich angemessener rechtlicher Garantien, mit denen insbesondere ausgeschlossen wird, dass die Daten für Maßnahmen oder Entscheidungen gegenüber bestimmten Personen verwendet werden, können die Mitgliedstaaten in Fällen, in denen offensichtlich keine Gefahr eines Eingriffs in die Privatsphäre der betroffenen Person besteht, die in Artikel 12 vorgesehenen Rechte gesetzlich einschränken, wenn die Daten ausschließlich für Zwecke der wissenschaftlichen Forschung verarbeitet werden oder personenbezogen nicht länger als erforderlich lediglich zur Erstellung von Statistiken aufbewahrt werden.

ABSCHNITT VII - WIDERSPRUCHSRECHT DER BETROFFENEN PERSON

Artikel 14 - Widerspruchsrecht der betroffenen Person

Die Mitgliedstaaten erkennen das Recht der betroffenen Person an,

a) zumindest in den Fällen von Artikel 7 Buchstaben e und f jederzeit aus überwiegenden, schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen dagegen Widerspruch einlegen zu können, dass sie betreffende Daten verarbeitet werden; dies gilt nicht bei einer im einzelstaatlichen Recht vorgesehenen entgegenstehenden Bestimmung. Im Fall eines berechtigten Widerspruchs kann sich die vom für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung nicht mehr auf diese Daten beziehen;

b) auf Antrag kostenfrei gegen eine vom für die Verarbeitung Verantwortlichen beabsichtigte Verarbeitung sie betreffender Daten für Zwecke der Direktwerbung Widerspruch einzulegen oder vor der ersten Weitergabe personenbezogener Daten an Dritte oder vor deren erstmaliger Nutzung im Auftrag Dritter zu Zwecken der Direktwerbung informiert zu werden und ausdrücklich auf das Recht hingewiesen zu werden, kostenfrei gegen eine solche Weitergabe oder Nutzung Widerspruch einlegen zu können. Die Mitgliedstaaten ergreifen die erforderlichen Maßnahmen, um sicherzustellen, dass die betroffenen Personen vom Bestehen des unter Buchstabe b Unterabsatz 1 vorgesehenen Rechts Kenntnis haben.

Artikel 15 - Automatisierte Einzelentscheidungen

(1) Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens.

(2) Die Mitgliedstaaten sehen unbeschadet der sonstigen Bestimmungen dieser Richtlinie vor, dass eine Person einer Entscheidung nach Absatz 1 unterworfen werden kann, sofern diese

a) im Rahmen des Abschlusses oder der Erfüllung eines Vertrags ergeht und dem Ersuchen der betroffenen Person auf Abschluss oder Erfüllung des Vertrags stattgegeben wurde oder die Wahrung ihrer berechtigten Interessen durch geeignete Maßnahmen - beispielsweise die Möglichkeit, ihren Standpunkt geltend zu machen - garantiert wird

oder

b) durch ein Gesetz zugelassen ist, das Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festlegt.

ABSCHNITT VIII - VERTRAULICHKEIT UND SICHERHEIT DER VERARBEITUNG

Artikel 16 - Vertraulichkeit der Verarbeitung

Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, sowie der Auftragsverarbeiter selbst dürfen personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten, es sei denn, es bestehen gesetzliche Verpflichtungen.

Artikel 17 - Sicherheit der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang - insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden - und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(2) Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche im Fall einer Verarbeitung in seinem Auftrag einen Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen.

(3) Die Durchführung einer Verarbeitung im Auftrag erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere folgendes vorgesehen ist:

- der Auftragsverarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen;

- die in Absatz 1 genannten Verpflichtungen gelten auch für den Auftragsverarbeiter, und zwar nach Maßgabe der Rechtsvorschriften des Mitgliedstaats, in dem er seinen Sitz hat.

(4) Zum Zwecke der Beweissicherung sind die datenschutzrelevanten Elemente des Vertrags oder Rechtsakts und die Anforderungen in bezug auf Maßnahmen nach Absatz 1 schriftlich oder in einer anderen Form zu dokumentieren.

ABSCHNITT IX - MELDUNG

Artikel 18 - Pflicht zur Meldung bei der Kontrollstelle

(1) Die Mitgliedstaaten sehen eine Meldung durch den für die Verarbeitung Verantwortlichen oder gegebenenfalls seinen Vertreter bei der in Artikel 28 genannten Kontrollstelle vor, bevor eine vollständig oder teilweise automatisierte Verarbeitung oder eine Mehrzahl von Verarbeitungen zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen durchgeführt wird.

(2) Die Mitgliedstaaten können eine Vereinfachung der Meldung oder eine Ausnahme von der Meldepflicht nur in den folgenden Fällen und unter folgenden Bedingungen vorsehen:

- sie legen für Verarbeitungskategorien, bei denen unter Berücksichtigung der zu verarbeitenden Daten eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen unwahrscheinlich ist, die Zweckbestimmungen der Verarbeitung, die Daten oder Kategorien der verarbeiteten Daten, die Kategorie(n) der betroffenen Personen, die Empfänger oder Kategorien der Empfänger, denen die Daten weitergegeben werden, und die Dauer der Aufbewahrung fest, und/oder

- der für die Verarbeitung Verantwortliche bestellt entsprechend dem einzelstaatlichen Recht, dem er unterliegt, einen Datenschutzbeauftragten, dem insbesondere folgendes obliegt:

- die unabhängige Überwachung der Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Bestimmungen,

- die Führung eines Verzeichnisses mit den in Artikel 21 Absatz 2 vorgesehenen Informationen über die durch den für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung, um auf diese Weise sicherzustellen, dass die Rechte und Freiheiten der betroffenen Personen durch die Verarbeitung nicht beeinträchtigt werden.

(3) Die Mitgliedstaaten können vorsehen, dass Absatz 1 keine Anwendung auf Verarbeitungen findet, deren einziger Zweck das Führen eines Registers ist, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht.

(4) Die Mitgliedstaaten können die in Artikel 8 Absatz 2 Buchstabe d) genannten Verarbeitungen von der Meldepflicht ausnehmen oder die Meldung vereinfachen.

(5) Die Mitgliedstaaten können die Meldepflicht für nicht automatisierte Verarbeitungen von personenbezogenen Daten generell oder in Einzelfällen vorsehen oder sie einer vereinfachten Meldung unterwerfen.

Artikel 19 - Inhalt der Meldung

(1) Die Mitgliedstaaten legen fest, welche Angaben die Meldung zu enthalten hat. Hierzu gehört zumindest folgendes:

a) Name und Anschrift des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters;

b) die Zweckbestimmung(en) der Verarbeitung;

c) eine Beschreibung der Kategorie(n) der betroffenen Personen und der diesbezüglichen Daten oder Datenkategorien;

d) die Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können;

e) eine geplante Datenübermittlung in Drittländer;

f) eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach Artikel 17 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

(2) Die Mitgliedstaaten legen die Verfahren fest, nach denen Änderungen der in Absatz 1 genannten Angaben der Kontrollstelle zu melden sind.

Artikel 20 - Vorabkontrolle

(1) Die Mitgliedstaaten legen fest, welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können, und tragen dafür Sorge, dass diese Verarbeitungen vor ihrem Beginn geprüft werden.

(2) Solche Vorabprüfungen nimmt die Kontrollstelle nach Empfang der Meldung des für die Verarbeitung Verantwortlichen vor, oder sie erfolgen durch den Datenschutzbeauftragten, der im Zweifelsfall die Kontrollstelle konsultieren muss.

(3) Die Mitgliedstaaten können eine solche Prüfung auch im Zuge der Ausarbeitung einer Maßnahme ihres Parlaments oder einer auf eine solche gesetzgeberische Maßnahme gestützten Maßnahme durchführen, die die Art der Verarbeitung festlegt und geeignete Garantien vorsieht.

Artikel 21 - Öffentlichkeit der Verarbeitungen

(1) Die Mitgliedstaaten erlassen Maßnahmen, mit denen die Öffentlichkeit der Verarbeitungen sichergestellt wird.

(2) Die Mitgliedstaaten sehen vor, dass die Kontrollstelle ein Register der gemäß Artikel 18 gemeldeten Verarbeitungen führt. Das Register enthält mindestens die Angaben nach Artikel 19 Absatz 1 Buchstaben a bis e. Das Register kann von jedermann eingesehen werden.

(3) Die Mitgliedstaaten sehen vor, dass für Verarbeitungen, die von der Meldung ausgenommen sind, der für die Verarbeitung Verantwortliche oder eine andere von den Mitgliedstaaten benannte Stelle zumindest die in Artikel 19 Absatz 1 Buchstaben a) bis e) vorgesehenen Angaben auf Antrag jedermann in geeigneter Weise verfügbar macht. Die Mitgliedstaaten können vorsehen, dass diese Bestimmungen keine Anwendung auf Verarbeitungen findet, deren einziger Zweck das Führen von Registern ist, die gemäß den Rechts- und Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt sind und die entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen stehen.

KAPITEL III - RECHTSBEHELFE, HAFTUNG UND SANKTIONEN

Artikel 22 - Rechtsbehelfe

Unbeschadet des verwaltungsrechtlichen Beschwerdeverfahrens, das vor Beschreiten des Rechtsweges insbesondere bei der in Artikel 28 genannten Kontrollstelle eingeleitet werden kann, sehen die Mitgliedstaaten vor, dass jede Person bei der Verletzung der Rechte, die ihr durch die für die betreffende Verarbeitung geltenden einzelstaatlichen Rechtsvorschriften garantiert sind, bei Gericht einen Rechtsbehelf einlegen kann.

Artikel 23 - Haftung

(1) Die Mitgliedstaaten sehen vor, dass jede Person, der wegen einer rechtswidrigen Verarbeitung oder jeder anderen mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht zu vereinbarenden Handlung ein Schaden entsteht, das Recht hat, von dem für die Verarbeitung Verantwortlichen Schadenersatz zu verlangen.

(2) Der für die Verarbeitung Verantwortliche kann teilweise oder vollständig von seiner Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann.

Artikel 24 - Sanktionen

Die Mitgliedstaaten ergreifen geeignete Maßnahmen, um die volle Anwendung der Bestimmungen dieser Richtlinie sicherzustellen, und legen insbesondere die Sanktionen fest, die bei Verstößen gegen die zur Umsetzung dieser Richtlinie erlassenen Vorschriften anzuwenden sind.

KAPITEL IV - ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER

Artikel 25 - Grundsätze

(1) Die Mitgliedstaaten sehen vor, dass die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt.

(3) Die Mitgliedstaaten und die Kommission unterrichten einander über die Fälle, in denen ihres Erachtens ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

(4) Stellt die Kommission nach dem Verfahren des Artikels 31 Absatz 2 fest, dass ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels aufweist, so treffen die Mitgliedstaaten die erforderlichen Maßnahmen, damit keine gleichartige Datenübermittlung in das Drittland erfolgt.

(5) Zum geeigneten Zeitpunkt leitet die Kommission Verhandlungen ein, um Abhilfe für die gemäß Absatz 4 festgestellte Lage zu schaffen.

(6) Die Kommission kann nach dem Verfahren des Artikels 31 Absatz 2 feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen, die es insbesondere infolge der Verhandlungen gemäß Absatz 5 eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet. Die Mitgliedstaaten treffen die aufgrund der Feststellung der Kommission gebotenen Maßnahmen.

Artikel 26 - Ausnahmen

(1) Abweichend von Artikel 25 sehen die Mitgliedstaaten vorbehaltlich entgegenstehender Regelungen für bestimmte Fälle im innerstaatlichen Recht vor, dass eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, vorgenommen werden kann, sofern

a) die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat oder

b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist oder

c) die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll, oder

d) die Übermittlung entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist oder

e) die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist oder

f) die Übermittlung aus einem Register erfolgt, das gemäß den Rechts- oder Verwaltungsvorschriften 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 für die Einsichtnahme im Einzelfall
gegeben sind.

(2) Unbeschadet des Absatzes 1 kann ein Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland genehmigen, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet; diese Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben.

(3) Der Mitgliedstaat unterrichtet die Kommission und die anderen Mitgliedstaaten über die von ihm nach Absatz 2 erteilten Genehmigungen. Legt ein anderer Mitgliedstaat oder die Kommission einen in bezug auf den Schutz der Privatsphäre, der Grundrechte und der Personen hinreichend begründeten Widerspruch ein, so erlässt die Kommission die geeigneten Maßnahmen nach dem Verfahren des Artikels 31 Absatz 2. Die Mitgliedstaaten treffen die aufgrund des Beschlusses der Kommission gebotenen Maßnahmen.

(4) Befindet die Kommission nach dem Verfahren des Artikels 31 Absatz 2, dass bestimmte Standardvertragsklauseln ausreichende Garantien gemäß Absatz 2 bieten, so treffen die Mitgliedstaaten die aufgrund der Feststellung der Kommission gebotenen Maßnahmen.

KAPITEL V - VERHALTENSREGELN

Artikel 27

(1) Die Mitgliedstaaten und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung der einzelstaatlichen Vorschriften beitragen sollen, die die Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassen.

(2) Die Mitgliedstaaten sehen vor, dass die Berufsverbände und andere Vereinigungen, die andere Kategorien von für die Verarbeitung Verantwortlichen vertreten, ihre Entwürfe für einzelstaatliche Verhaltensregeln oder ihre Vorschläge zur Änderung oder Verlängerung bestehender einzelstaatlicher Verhaltensregeln der zuständigen einzelstaatlichen Stelle unterbreiten können. Die Mitgliedstaaten sehen vor, dass sich diese Stelle insbesondere davon überzeugt, dass die ihr unterbreiteten Entwürfe mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in Einklang stehen. Die Stelle holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihr dies angebracht erscheint.

(3) Die Entwürfe für gemeinschaftliche Verhaltensregeln sowie Änderungen oder Verlängerungen bestehender gemeinschaftlicher Verhaltensregeln können der in Artikel 29 genannten Gruppe unterbreitet werden. Die Gruppe nimmt insbesondere dazu Stellung, ob die ihr unterbreiteten Entwürfe mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in Einklang stehen. Sie holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihr dies angebracht erscheint. Die Kommission kann dafür Sorge tragen, dass die Verhaltensregeln, zu denen die Gruppe eine positive Stellungnahme abgegeben hat, in geeigneter Weise veröffentlicht werden.

KAPITEL VI - KONTROLLSTELLE UND GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

Artikel 28 - Kontrollstelle

(1) Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen. Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.

(2) Die Mitgliedstaaten sehen vor, dass die Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten angehört werden.

(3) Jede Kontrollstelle verfügt insbesondere über:

- Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen;

- wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20 vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermah-

nung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;

- das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie. Gegen beschwerende Entscheidungen der Kontrollstelle steht der Rechtsweg offen.

(4) Jede Person oder ein sie vertretender Verband kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde. Jede Kontrollstelle kann insbesondere von jeder Person mit dem Antrag befasst werden, die Rechtmäßigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gemäß Artikel 13 Anwendung finden. Die Person ist unter allen Umständen darüber zu unterrichten, dass eine Überprüfung stattgefunden hat.

(5) Jede Kontrollstelle legt regelmäßig einen Bericht über ihre Tätigkeit vor. Dieser Bericht wird veröffentlicht.

(6) Jede Kontrollstelle ist im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr gemäß Absatz 3 übertragenen Befugnisse zuständig, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anwendbar ist. Jede Kontrollstelle kann von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden. Die Kontrollstellen sorgen für die zur Erfüllung ihrer Kontrollaufgaben notwendige gegenseitige Zusammenarbeit, insbesondere durch den Austausch sachdienlicher Informationen.

(7) Die Mitgliedstaaten sehen vor, dass die Mitglieder und Bediensteten der Kontrollstellen hinsichtlich der vertraulichen Informationen, zu denen sie Zugang haben, dem Berufsgeheimnis, auch nach Ausscheiden aus dem Dienst, unterliegen.

Artikel 29 - Datenschutzgruppe

(1) Es wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten eingesetzt (nachstehend „Gruppe" genannt). Die Gruppe ist unabhängig und hat beratende Funktion.

(2) Die Gruppe besteht aus je einem Vertreter der von den einzelnen Mitgliedstaaten bestimmten Kontrollstellen und einem Vertreter der Stelle bzw. der Stellen, die für die Institutionen und Organe der Gemeinschaft eingerichtet sind, sowie einem Vertreter der Kommission. Jedes Mitglied der Gruppe wird von der Institution, der Stelle oder den Stellen, die es vertritt, benannt. Hat ein Mitgliedstaat mehrere Kontrollstellen bestimmt, so ernennen diese einen gemeinsamen Vertreter. Gleiches gilt für die Stellen, die für die Institutionen und die Organe der Gemeinschaft eingerichtet sind.

(3) Die Gruppe beschließt mit der einfachen Mehrheit der Vertreter der Kontrollstellen.

(4) Die Gruppe wählt ihren Vorsitzenden. Die Dauer der Amtszeit des Vorsitzenden beträgt zwei Jahre. Wiederwahl ist möglich.

(5) Die Sekretariatsgeschäfte der Gruppe werden von der Kommission wahrgenommen.

(6) Die Gruppe gibt sich eine Geschäftsordnung.

(7) Die Gruppe prüft die Fragen, die der Vorsitzende von sich aus oder auf Antrag eines Vertreters der Kontrollstellen oder auf Antrag der Kommission auf die Tagesordnung gesetzt hat.

Artikel 30

(1) Die Gruppe hat die Aufgabe,

a) alle Fragen im Zusammenhang mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen;

b) zum Schutzniveau in der Gemeinschaft und in Drittländern gegenüber der Kommission Stellung zu nehmen;

c) die Kommission bei jeder Vorlage zur Änderung dieser Richtlinie, zu allen Entwürfen zusätzlicher oder spezifischer Maßnahmen zur Wahrung der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zu allen anderen Entwürfen von Gemeinschaftsmaßnahmen zu beraten, die sich auf diese Rechte und Freiheiten auswirken;

d) Stellungnahmen zu den auf Gemeinschaftsebene erarbeiteten Verhaltensregeln abzugeben.

(2) Stellt die Gruppe fest, dass sich im Bereich des Schutzes von Personen bei der Verarbeitung personenbezogener Daten zwischen den Rechtsvorschriften oder der Praxis der Mitgliedstaaten Unterschiede ergeben, die die Gleichwertigkeit des Schutzes in der Gemeinschaft beeinträchtigen könnten, so teilt sie dies der Kommission mit.

(3) Die Gruppe kann von sich aus Empfehlungen zu allen Fragen abgeben, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen.

(4) Die Stellungnahmen und Empfehlungen der Gruppe werden der Kommission und dem in Artikel 31 genannten Ausschuss übermittelt.

(5) Die Kommission teilt der Gruppe mit, welche Konsequenzen sie aus den Stellungnahmen und Empfehlungen gezogen hat. Sie erstellt hierzu einen Bericht, der auch dem Europäischen Parlament und dem Rat übermittelt wird. Dieser Bericht wird veröffentlicht.

(6) Die Gruppe erstellt jährlich einen Bericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und in Drittländern, den sie der Kommission, dem Europäischen Parlament und dem Rat übermittelt. Dieser Bericht wird veröffentlicht.

KAPITEL VII - GEMEINSCHAFTLICHE DURCHFÜHRUNGSMASSNAHMEN

Artikel 31 - Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt, der sich aus Vertretern der Mitgliedstaaten zusammensetzt und in dem der Vertreter der Kommission den Vorsitz führt.

(2) Der Vertreter der Kommission unterbreitet dem Ausschuss einen Entwurf der zu treffenden Maßnahmen. Der Ausschuss gibt seine Stellungnahme zu diesem Entwurf innerhalb einer Frist ab, die der Vorsitzende unter Berücksichtigung der Dringlichkeit der betreffenden Frage festsetzen kann. Die Stellungnahme wird mit der Mehrheit abgegeben, die in Artikel 148 Absatz 2 des Vertrags vorgesehen ist. Bei der Abstimmung im Ausschuss werden die Stimmen der Vertreter der Mitgliedstaaten gemäß dem vorgenannten Artikel gewogen. Der Vorsitzende nimmt an der Abstimmung nicht teil. Die Kommission erlässt Maßnahmen, die unmittelbar gelten. Stimmen sie jedoch mit der Stellungnahme des Ausschusses nicht überein, werden sie von der Kommission unverzüglich dem Rat mitgeteilt. In diesem Fall gilt folgendes:

- Die Kommission verschiebt die Durchführung der von ihr beschlossenen Maßnahmen um drei Monate vom Zeitpunkt der Mitteilung an;

- der Rat kann innerhalb des im ersten Gedankenstrich genannten Zeitraums mit qualifizierter Mehrheit einen anderslautenden Beschluss fassen.

SCHLUSSBESTIMMUNGEN

Artikel 32

(1) Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie binnen drei Jahren nach ihrer Annahme nachzukommen. Wenn die Mitgliedstaaten derartige Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Die Mitgliedstaaten tragen dafür Sorge, dass Verarbeitungen, die zum Zeitpunkt des Inkrafttretens der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie bereits begonnen wurden, binnen drei Jahren nach diesem Zeitpunkt mit diesen Bestimmungen in Einklang gebracht werden. Abweichend von Unterabsatz 1 können die Mitgliedstaaten vorsehen, dass die Verarbeitungen von Daten, die zum Zeitpunkt des Inkrafttretens der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie bereits in manuellen Dateien enthalten sind, binnen zwölf Jahren nach Annahme dieser Richtlinie mit den Artikeln 6, 7 und 8 in Einklang zu bringen sind. Die Mitgliedstaaten gestatten jedoch, dass die betroffene Person auf Antrag und insbesondere bei Ausübung des Zugangsrechts die Berichtigung, Löschung oder Sperrung von Daten erreichen kann, die unvollständig, unzutreffend oder auf eine Art und Weise aufbewahrt sind, die mit den vom für die Verarbeitung Verantwortlichen verfolgten rechtmäßigen Zwecken unvereinbar ist.

(3) Abweichend von Absatz 2 können die Mitgliedstaaten vorbehaltlich geeigneter Garantien vorsehen, dass Daten, die ausschließlich zum Zwecke der historischen Forschung aufbewahrt werden, nicht mit den Artikeln 6, 7 und 8 in Einklang gebracht werden müssen.

(4) Die Mitgliedstaaten teilen der Kommission den Wortlaut der innerstaatlichen Vorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 33

Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig, und zwar erstmals drei Jahre nach dem in Artikel 32 Absatz 1 genannten Zeitpunkt, einen Bericht über die Durchführung dieser Richtlinie vor und fügt ihm gegebenenfalls geeignete Änderungsvorschläge bei. Dieser Bericht wird veröffentlicht. Die Kommission prüft insbesondere die Anwendung dieser Richtlinie auf die Verarbeitung personenbezogener Bild- und Tondaten und unterbreitet geeignete Vorschläge, die sich unter Berücksichtigung der Entwicklung der Informationstechnologie und der Arbeiten über die Informationsgesellschaft als notwendig erweisen könnten.

Artikel 34

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Anhang 3

Auszug aus dem Urteil des Ersten Senats des Bundesverfassungsgerichts vom 15. Dezember 1983 - 1 BvR 209/83 u.a. - sog. Volkszählungsurteil

Leitsätze 1 bis 3 der Entscheidung:

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

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

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

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

Auszug aus Abschnitt C. II. des Volkszählungsurteils:

Prüfungsmaßstab ist in erster Linie das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht.

1. a) Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient - neben speziellen Freiheitsverbürgungen - das in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht, das gerade auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen der menschlichen Persönlichkeit Bedeutung gewinnen kann (vgl. BVerfGE 54, 148 [153]). Die bisherigen Konkretisierungen durch die Rechtsprechung umschreiben den Inhalt des Persönlichkeitsrechts nicht abschließend. Es umfaßt - wie bereits in der Entscheidung BVerfGE 54, 148 [155] unter Fortführung früherer Entscheidung (BVerfGE 27, 1 [6] - Mikrozen-

sus; 27, 344 [350 f.] - Scheidungsakten; 32, 373 [379] - Arztkartei; 35, 202 [220] - Lebach; 44, 353 [372 f.] - Suchtkrankenberatungsstelle) angedeutet worden ist - auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (vgl. ferner BVerfGE 56, 37 [41 ff.] - Selbstbezichtigung; 63, 131 [142 f.] - Gegendarstellung).

Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten [vgl. § 2 Abs. 1 BDSG]) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus - vor allem beim Aufbau integrierter Informationssysteme - mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsichts- und Einflußnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.

Individuelle Selbstbestimmung setzt aber - auch unter den Bedingungen moderner Informationsverarbeitungstechnologien - voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.

Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

b) Dieses Recht auf „informationelle Selbstbestimmung“ ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über „seine“ Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum - Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden (BVerfGE 4, 7 [15]; 8, 274 [329]; 27, 1 [7]; 27, 344 [351 f.]; 33, 303 [334]; 50, 290 [353]; 56, 37 [49]). Grundsätzlich muß daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen.

Diese Beschränkungen bedürfen nach Art. 2 Abs. 1 GG - wie in § 6 Abs. 1 des Bundesstatistikgesetzes auch zutreffend anerkannt worden ist - einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klarer und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfGE 45, 400 [420] m.w.N.). Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Dieser mit Verfassungsrang ausgestattete Grundsatz folgt bereits aus dem Wesen der Grundrechte selbst, die als Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat von der öffentlichen Gewalt jeweils nur soweit beschränkt werden dürfen, als es zum Schutz öffentlicher Interessen unerläßlich ist (BVerfGE 19, 342 [348]; st.Rspr.). Angesichts der bereits dargelegten Gefährdungen durch die Nutzung der automatischen Datenverarbeitung hat der Gesetzgeber mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken (vgl. BVerfGE 53, 30 [65]; 63, 131 [143]).

2. Die Verfassungsbeschwerden geben keinen Anlaß zur erschöpfenden Erörterung des Rechts auf informationelle Selbstbestimmung. Zu entscheiden ist nur über die Tragweite dieses Rechts für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt. Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses“ Datum mehr.

Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungs- und Verwendungsmöglichkeiten bestehen, läßt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten. Dabei ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymisierter Form erhoben und verarbeitet werden (dazu unter a), und solchen, die für statistische Zwecke bestimmt sind (dazu unter b).

a) Schon bislang ist anerkannt, daß die zwangsweise Erhebung personenbezogener Daten nicht unbeschränkt statthaft ist, namentlich dann, wenn solche Daten für den Verwaltungsvollzug (etwa bei der Besteuerung oder der Gewährung von Sozialleistungen)

verwendet werden sollen. Insoweit hat der Gesetzgeber bereits verschiedenartige Maßnahmen zum Schutz der Betroffenen vorgesehen, die in die verfassungsrechtlich gebotene Richtung weisen (vgl. beispielsweise die Regelungen in den Datenschutzgesetzen des Bundes und der Länder; §§ 30, 31 der Abgabenordnung - AO -; § 35 des Ersten Buches des Sozialgesetzbuches - SGB I - in Verbindung mit §§ 67 bis 86 SGB X). Wieweit das Recht auf informationelle Selbstbestimmung und im Zusammenhang damit der Grundsatz der Verhältnismäßigkeit sowie die Pflicht zu verfahrensrechtlichen Vorkehrungen den Gesetzgeber zu diesen Regelungen von Verfassungs wegen zwingen, hängt von Art, Umfang und denkbaren Verwendungen der erhobenen Daten sowie der Gefahr ihres Mißbrauchs ab (vgl. BVerfGE 49, 89 [142]; 53, 30 [61]). Ein überwiegendes Allgemeininteresse wird regelmäßig überhaupt nur an Daten mit Sozialbezug bestehen unter Ausschluß unzumutbarer intimer Angaben und von Selbstbezichtigungen. Nach dem bisherigen Erkenntnis- und Erfahrungsstand erscheinen vor allem folgende Maßnahmen bedeutsam:

Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen.

Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein - amtshilfefester - Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote erforderlich. Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungs-, Auskunfts- und Löschungspflichten wesentlich.

Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung.

Anhang 4

Anschriften der Datenschutzbeauftragten des Bundes und der Länder

Bund	Der Bundesbeauf-trag für den Datenschutz	Dr. Joachim Jacob Postfach 20 01 12 53131 Bonn Friedrich-Ebert-Str. 1 53173 Bonn	Tel.: 02 28 / 8 19 95-0 Fax: 02 28 / 8 19 95-5 50 E-Mail: poststelle@bfd.bund.de Internet: http://www.bfd.bund.de
Baden-Württemberg	Der Landesbeauf-tragte für den Daten-schutz Baden-Württemberg	Peter Zimmermann Postfach 10 29 32 70025 Stuttgart Marienstr. 12 70178 Stuttgart	Tel.: 07 11 / 61 55 41-0 Fax: 07 11 / 61 55 41-15 E-Mail: poststelle@lfd.bwl.de Internet: http://www.baden-wuerttemberg.datenschutz.de
Bayern	Der Bayerische Landesbeauftragte für den Datenschutz	Reinhard Vetter Postfach 22 12 19 80502 München Wagmüllerstr. 18 80538 München	Tel.: 0 89 / 21 26 72-0 Fax: 0 89 / 21 26 72-50 E-Mail: poststelle@datenschutz-bayern.de Internet: http://www.datenschutz-bayern.de
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit	Prof. Dr. Hansjürgen Garstka Pallasstr. 25/26 10781 Berlin	Tel.: 0 30 / 75 60 78 09 Fax: 0 30 / 2 15 50 50 E-Mail: mailbox@datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de
Brandenburg	Der Landesbeauf-tragte für den Daten-schutz und für das Recht auf Akteneinsicht	Dr. Alexander Dix Stahnsdorfer Damm 77 14532 Kleinmachnow	Tel.: 03 32 03 / 3 56-0 Fax: 03 32 03 / 3 56-49 E-Mail: poststelle@lda.brandenburg.de Internet: http://www.lda.brandenburg.de
Bremen	Landesbeauftragter für den Datenschutz	Sven Holst Postfach 10 03 80 27503 Bremerhaven Arndtstr. 1 27570 Bremerhaven	Tel.: 04 71 / 92 46 10 Fax: 04 71 / 9 24 61 31 E-Mail: office@datenschutz.bremen.de Internet: http://www.datenschutz.bremen.de
Hamburg	Der Hamburgische Datenschutz-beauftragte	Dr. Hans-Hermann Schrader Baumwall 7 20459 Hamburg	Tel.: 0 40 / 4 28 41-20 44 Fax: 0 40 / 4 28 41 23 72 E-mail: mailbox@datenschutz.hamburg.de Internet: www.hamburg.datenschutz.de
Hessen	Der Hessische Da-tenschutz-beauftragte	Prof. Dr. Friedrich von Zezschwitz Postfach 31 63 65021 Wiesbaden Uhlandstr. 4 65189 Wiesbaden	Tel.: 06 11 / 14 08-0 Fax: 06 11 / 14 08-9 00 E-Mail: poststelle@datenschutz.hessen.de Internet: http://www.datenschutz.hessen.de
Mecklen-burg-Vorpommern	Landesbeauftragter für den Datenschutz	Dr. Werner Kessel Schloß Schwerin 19053 Schwerin	Tel.: 03 85 / 5 94 94-0 Fax: 03 85 / 5 94 94-58 E-Mail: datenschutz@mvnet.de Internet: http://www.lfd.m-v.de
Niedersach-sen	Der Landesbeauf-tragte für den Daten-schutz Niedersach-sen	Burckhard Nedden Postfach 2 21 30002 Hannover Brühlstr. 9 30169 Hannover	Tel.: 05 11 / 1 20-45 00 Fax: 05 11 / 1 20 45 99 E-Mail: poststelle@lfd.niedersachsen.de Internet: http://www.lfd.niedersachsen.de

Anhang 4

Nordrhein-Westfalen	Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen	Bettina Sokol Postfach 20 04 44 40102 Düsseldorf Reichsstr. 43 40217 Düsseldorf	Tel.: 02 11 / 38 42 40 Fax: 02 11 / 3 84 24 10 E-Mail: datenschutz@lfd.nrw.de Internet: http://www.lfd.nrw.de
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz	Prof. Dr. Walter Rudolf Postfach 30 40 55020 Mainz Deutschhausplatz 12 55116 Mainz	Tel.: 0 61 31 / 2 08 24 49 Fax: 0 61 31 / 2 08 24 97 E-Mail: poststelle@datenschutz.rlp.de Internet: http://www.datenschutz.rlp.de
Saarland	Der Landesbeauftragte für Datenschutz	Karl Albert Postfach 10 26 31 66026 Saarbrücken Fritz-Dobisch-Str. 12 66111 Saarbrücken	Tel.: 06 81 / 9 47 81-0 Fax: 06 81 / 9 47 81 29 E-Mail: lfd-saar@t-online.de Internet: http://www.lfd.saarland.de
Sachsen	Der Sächsische Datenschutzbeauftragte	Dr. Thomas Giesen Postfach 12 09 05 01008 Dresden Bernhard-von-Lindenau-Platz 1 01067 Dresden	Tel.: 03 51 / 49 35-4 01 Fax: 03 51 / 49 35-4 90 E-Mail: ---------- Internet: ----------
Sachsen-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt	Klaus-Rainer Kalk Postfach 19 47 39009 Magdeburg Berliner Chaussee 9 39114 Magdeburg	Tel.: 03 91 / 8 18 03-0 Fax: 03 91 / 8 18 03 33 E-Mail: ---------- Internet: http://www.datenschutz.sachsen-anhalt.de
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Dr. Helmut Bäumler Postfach 71 16 24171 Kiel Holstenstraße 98 24103 Kiel	Tel.: 04 31 / 9 88 12 00 Fax: 04 31 / 9 88 12 23 E-Mail: mail@datenschutzzentrum.de Internet: http://www.datenschutzzentrum.de
Thüringen	Die Thüringer Landesbeauftragte für den Datenschutz	Silvia Liebaug Postfach 10 19 51 99019 Erfurt Johann-Sebastian-Bach-Straße 1 99096 Erfurt	Tel.: 03 61 / 3 77 19 00 Fax: 03 61 / 3 77 19 04 E-Mail: poststelle@datenschutz.thueringen.de Internet: http://www.datenschutz.thueringen.de

Anhang 5

Anschriften der Aufsichtsbehörden für den nicht öffentlichen Bereich

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
Baden-Württemberg	Innenministerium Baden-Württemberg Postfach 10 24 43 70020 Stuttgart Dorotheenstr. 6 70173 Stuttgart Tel.: 07 11 / 2 31-4 Fax: 07 11 / 2 31-32 99	Innenministerium Baden-Württemberg Postfach 10 24 43 70020 Stuttgart Dorotheenstr. 6 70173 Stuttgart Tel.: 07 11 / 2 31-4 Fax: 07 11 / 2 31-32 99
Bayern	Bayerisches Staatsministerium des Innern Odeonsplatz 3 80539 München Tel.: 0 89 / 21 92-01 Fax: 0 89 / 21 92-1 22 66	Regierung von Mittelfranken Postfach 6 06 91511 Ansbach Promenade 27 (Schloß) 91522 Ansbach Tel.: 09 81 / 53-3 01 Fax: 09 81 / 53-2 06
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit Pallasstr. 25/26 10781 Berlin Tel.: 0 30 / 75 60 78 09 Fax: 0 30 / 2 15 50 50 E-Mail: mailbox@datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de	Berliner Beauftragter für Datenschutz und Informationsfreiheit Pallasstr. 25/26 10781 Berlin Tel.: 0 30 / 75 60 78 09 Fax: 0 30 / 2 15 50 50 E-Mail: mailbox@datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de
Brandenburg	Ministerium des Innern Henning-von-Tresckow-Str. 9 - 13 14467 Potsdam Tel.: 03 31 / 8 66 23 60 Fax: 03 31 / 8 66 23 02 E-Mail: Lfd-bbg@t-online.de Internet: http://www.mi.brandenburg.de	Ministerium des Innern Henning-von-Tresckow-Str. 9-13 14467 Potsdam Tel.: 03 31 / 8 66 23 60 Fax: 03 31 / 8 66 23 02 E-Mail: Lfd-bbg@t-online.de Internet: http://www.mi.brandenburg.de
Bremen	Der Landesbeauftragte für den Daten-schutz Postfach 10 03 80 27503 Bremerhaven Arndtstr. 1 27570 Bremerhaven Tel.: 04 71 / 92 46 10 Fax: 04 71 / 9 24 61 31 E-Mail: office@datenschutz.bremen.de Internet: http://www.datenschutz.bremen.de	Der Landesbeauftragte für den Daten-schutz Postfach 10 03 80 27503 Bremerhaven Arndtstr. 1 27570 Bremerhaven Tel.: 04 71 / 92 46 10 Fax: 04 71 / 9 24 61 31 E-Mail: office@datenschutz.bremen.de Internet: http://www.datenschutz.bremen.de

Anhang 5

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
Hamburg	Der Hamburgische Datenschutzbeauftragte Baumwall 7 20459 Hamburg Tel.: 0 40 / 4 28 41-20 45 Fax: 0 40 / 4 28 41-23 72 E-Mail: mailbox@datenschutz.hamburg.de Internet: http://www.hamburg.datenschutz.de	Der Hamburgische Datenschutzbeauftragte Baumwall 7 20459 Hamburg Tel.: 0 40 / 4 28 41-20 44 Fax: 0 40 / 4 28 41-23 72 E-Mail: mailbox@datenschutz.hamburg.de Internet: http://www.hamburg.datenschutz.de
Hessen	Hessisches Ministerium des Innern und für Sport Friedrich-Ebert-Allee 12 65185 Wiesbaden Tel.: 06 11 / 3 53-0 Fax: 06 11 / 3 53-13 43 Internet: http://www.hmdi.hessen.de	Regierungspräsidium Gießen Landgraf-Philipp-Platz 3-7 35390 Gießen Tel.: 06 41 / 3 03-1 Fax: 06 41 / 3 03-25 09 Internet: http://www.rp-giessen.de Regierungspräsidium Darmstadt Wilhelminenstraße 1-3 64283 Darmstadt Tel.: 0 61 51 / 12-0 Fax: 0 61 51 / 12 68 34 E-Mail: datenschutz@rpda.hessen.de Internet: http://www.rpda.de Regierungspräsidium Kassel Steinweg 6 34117 Kassel Tel.: 05 61 / 1 06-0 Fax: 05 61 / 1 06 10 12 Internet: http://www.rp-kassel.de
Mecklenburg-Vorpommern	Innenministerium des Landes Mecklenburg-Vorpommern Arsenal am Pfaffenteich 3 19048 Schwerin Tel.: 03 85 / 5 88 22 50 Fax: 03 85 / 5 88 29 78	Innenministerium des Landes Mecklenburg-Vorpommern Arsenal am Pfaffenteich 3 19048 Schwerin Tel.: 03 85 / 5 88 22 50 Fax: 03 85 / 5 88 29 78

Anhang 5

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
Niedersachsen	Niedersächsisches Innenministerium Lavesallee 6 30169 Hannover Tel.: 05 11 / 1 20-0 Fax: 05 11 / 1 20-65 50	Der Landesbeauftragte für den Datenschutz Niedersachsen Postfach 2 21 30002 Hannover Brühlstraße 9 30169 Hannover Tel.: 05 11 / 1 20 45 00 Fax: 05 11 / 1 20 45 99 E-Mail: poststelle@lfd.niedersachsen.de Internet: http://www.lfd.niedersachsen.de
Nordrhein-Westfalen	Innenministerium des Landes Nordrhein-Westfalen Haroldstr. 5 40190 Düsseldorf Tel.: 02 11 / 8 71 01 Fax: 02 11 / 8 71 33 55	Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen Bettina Sokol Postfach 20 04 44 40102 Düsseldorf Reichsstraße 43 40217 Düsseldorf Tel.: 02 11 / 38 42 40 Fax: 02 11 /3 84 24 10 E-Mail: datenschutz@lfd.nrw.de Internet: http://www.lfd.nrw.de
Rheinland-Pfalz	Ministerium des Innern und für Sport Schillerplatz 3-5 55116 Mainz Tel.: 0 61 31 / 16 32 59 Fax: 0 61 31 / 16 33 69	Aufsichts- und Dienstleistungsdirektion (ADD) Trier Willy-Brandt-Platz 3 54290 Trier Tel.: 06 51 / 94 94-0 Fax: 06 51 / 94 94-1 70 E-Mail: poststelle@add.rlp.de Internet: http://www.add.rlp.de
Saarland	Ministerium des Innern und für Sport - Abt. B - Mainzer Str. 136 66121 Saarbrücken Tel.: 06 81 / 9 62-0 Fax: 06 81 / 9 62-16 05	Ministerium des Innern und für Sport - Abt. B - Mainzer Str. 136 66121 Saarbrücken Tel.: 06 81 / 9 62-0 Fax: 06 81 / 9 62-16 05
Sachsen	Sächsisches Staatsministerium	Regierungspräsidium Chemnitz

Anhang 5

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
	des Innern Referat 26 - Datenschutz Wilhelm-Buck-Straße 2 01097 Dresden Tel.: 03 51 / 5 64-32 60 Fax: 03 51 / 5 64-31 99 E-Mail: datenschutz@smi.sachsen.de	Altchemnitzer Str. 41 09120 Chemnitz Tel.: 03 71 / 5 32-11 49 Fax: 03 71 / 5 32-11 59 E-Mail: post@rpc.sachsen.de Regierungspräsidium Dresden Postfach 10 06 53 01076 Dresden Stauffenbergallee 2 01099 Dresden Tel.: 03 51 / 8 25-14 20 Fax: 03 51 / 8 25-99 99 Regierungspräsidium Leipzig Braustr. 2 04107 Leipzig Tel.: 03 41 / 9 77-14 70 Fax: 03 41 / 9 77-11 99
Sachsen-Anhalt	Ministerium des Innern des Landes Sachsen-Anhalt Halberstädter Str. 2 39112 Magdeburg Tel.: 03 91 / 5 67 54 04 Fax: 03 91 / 5 67 52 90	Regierungspräsidium Halle Willy-Lohmann-Str. 7 06114 Halle (Saale) Tel.: 03 45 / 51 40 Fax: 03 45 / 5 14 14 44
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Postfach 71 16 24171 Kiel Holstenstraße 98 24103 Kiel Tel.: 04 31 / 9 88 12 00 Fax: 04 31 / 9 88 12 23 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Postfach 71 16 24171 Kiel Holstenstraße 98 24103 Kiel Tel.: 04 31 / 9 88 12 00 Fax: 04 31 / 9 88 12 23 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de
Thüringen	Thüringer Innenministerium Steigerstr. 24 99096 Erfurt Tel.: 03 61 / 3 79 00 Fax: 03 61 / 3 79 31 11 E-Mail: poststelle@tim.thueringen.de	Thüringer Landesverwaltungsamt Weimarplatz 4 99423 Weimar Tel.: 03 61 / 37 73 72 58 Fax: 03 61 / 37 73 73 46 E-Mail: poststelle@tlva.thueringen.de